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
DOI: https://doi.org/10.5169/seals-46287

ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI

par Jean-René JOLY

INTRODUCTION

Cet article passe en revue les propriétés diophantiennes classiques des corps finis. Ces propriétés peuvent se grouper en quatre catégories:

(1) Le théorème de Chevalley, et ses variantes ou améliorations: théorèmes de Chevalley-Warning, Warning, Ax, Katz, Terjanian, ... Indiquons (ou rappelons) que le théorème de Chevalley (pour *un* polynôme à n variables $F(X_1, ..., X_n)$ sur un corps fini k) est l'énoncé suivant: si F est sans terme constant, et si $\deg(F) < n$, alors l'équation $F(X_1, ..., X_n) = 0$ admet sur k une solution autre que la solution « triviale » $(0, 0, ..., 0)$. Ces divers théorèmes sont étudiés aux chapitres 3 et 7.

(2) Les résultats de Hasse, Weil, Lang-Weil, Nisnevich, ..., concernant l'« hypothèse de Riemann » en caractéristique p. Le théorème de Lang-Weil, par exemple, peut s'énoncer grosso modo de la façon suivante: si V est une variété absolument irréductible de dimension r définie sur un corps fini k à q éléments, le nombre de points de V rationnels sur k est voisin de q^r, avec un « terme d'erreur » de l'ordre de grandeur de $q^{r-(1/2)}$. Les propriétés de ce type sont étudiées au chapitre 8.

(3) Les résultats relatifs aux fonctions zêta des variétés algébriques sut un corps fini, et notamment le théorème de rationalité de Dwork: si V esf une variété algébrique définie sur un corps fini k; si, pour tout entier positi- m, N_m désigne le nombre de points de V rationnels sur k_m (l'unique extenr sion de degré m de k); et si t désigne une variable, alors il existe une fraction rationnelle en t, à coefficients rationnels, soit $Z(V; t)$ (c'est la « fonction zêta » de V), telle qu'on ait $\sum_{m \geqq 1} N_m t^m/m = \log Z(V; t)$; la connaissance de la famille *finie* des coefficients de $Z(V; t)$ est alors équivalente à celle de la suite *infinie* $(N_m)_{m \geqq 1}$. Les propriétés des fonctions zêta sont exposées au chapitre 9.

(4) Enfin, les résultats spécifiques relatifs aux équations diagonales, c'est-à-dire aux équations de la forme $a_1 X_1^{d1} + \ldots + a_n X_n^{dn} = b$. L'étude de ces équations (sur un corps fini, spécialement sur un corps de restes modulo p) est traditionnelle, et remonte à Gauss et Jacobi. Les équations diagonales se prêtent à un calcul exact du nombre de leurs solutions, et ont été utilisées de ce fait (notamment par Davenport-Hasse et Weil) pour vérifier sur des cas particuliers, et avant leur démonstration par Dwork et Weil, la rationalité des fonctions zêta et l'hypothèse de Riemann; elles ont permis plus généralement d'étayer les « conjectures de Weil » relatives à la forme exacte des fonctions zêta. Les équations diagonales sont étudiées aux chapitres 4 et 6.

Naturellement, ces diverses catégories de résultats ne sont pas indépendantes: en particulier, les contenus des chapitres 8 et 9 sont étroitement liés, et ce découpage en deux chapitres n'a été pratiqué que pour la commodité de l'exposition. Indiquons d'autre part que les chapitres 1, 2 et 5, non mentionnés ci-dessus, sont consacrés respectivement à un rappel des propriétés générales des corps finis, à l'étude des polynômes sur un corps fini, et à l'étude des sommes de Gauss et de Jacobi attachées à un corps fini. Voir d'ailleurs la table des matières.

* * *

Les chapitres 1 à 6 de cet article sont tout à fait élémentaires, et ne supposent connus que les rudiments de la théorie des groupes finis et de la théorie des corps: ce qui est largement couvert par les chapitres II, IV, V et VII du Van der Waerden, par exemple; le chapitre 7 utilise (mais avec tous les rappels nécessaires) quelques propriétés très simples des corps cyclotomiques. Les chapitres 8 et 9 sont plus techniques, et supposent connu un minimum de géométrie algébrique: toutefois, le langage employé étant le langage classique des variétés affines ou projectives, l'intuition devrait pouvoir suppléer le plus souvent à d'éventuelles lacunes en ce domaine. Ainsi, la quasi totalité des neuf chapitres est en principe accessible à tout lecteur (et notamment à tout débutant en théorie des nombres) ayant un niveau équivalent au deuxième cycle des universités françaises. Cet article a d'ailleurs pour origine lointaine un cours de première année de troisième cycle: « propriétés diophantiennes des corps finis », Grenoble, novembre/décembre 1969.

* * *

Les notations employées sont celles de Bourbaki, ou, plus simplement, celles de l'« Algebra » de Lang; rappelons seulement que **Z**, **Q**, **R**, **C**, $\mathbf{F}_p$ désignent respectivement l'anneau des entiers rationnels, le corps des nombres rationnels, celui des nombres réels, celui des nombres complexes, celui des restes modulo p; et que, si a et b sont deux entiers non nuls, (a, b) représente leur p.g.c.d.

La bibliographie (en fin d'article) comporte deux parties: la première est la liste des ouvrages généraux auxquels il est fait référence dans le texte (par numéro entre crochets); la seconde est la liste des articles cités, qui sont classés (et auxquels il est fait référence) par nom(s) d'auteur(s) et année de publication. La première liste mentionne plusieurs monographies relatives aux « vraies » équations diophantiennes (sur les corps locaux et globaux): [**4**], [**14**], [**18**], ainsi que [**3**] (chap. 1, 2 et 4), [**7**] (chap. 7) et [**13**] (chap. 1 et 2): pour l'application à ces équations des résultats examinés dans le présent article, voir [**4**], 1re partie (notamment pp. 204-205), [**13**], chap. 2 (notamment p. 29), et aussi [**3**], chap. 1, sect. 5 et 6.

TABLE DES MATIÈRES

CHAPITRE PREMIER

CORPS FINIS (RAPPELS)

Ce chapitre résume les propriétés générales des corps finis. Rappelons que d'après le *théorème de Wedderburn*, tout corps fini est commutatif (pour une démonstration, voir par exemple [**1**], pp. 35-37, ou [**19**], p. 1).

§ 1. *Classification des corps finis.*

1.1. Soit k un corps fini. Sa caractéristique est certainement différente de 0; c'est un nombre premier p, et le sous-corps premier de k s'identifie à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Notons f le degré de l'extension $k/\mathbf{F}_p$; k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, au produit direct de f exemplaires de $\mathbf{F}_p$; en particulier:

PROPOSITION 1. — *Si q désigne le nombre d'éléments de k, on a $q = p^f$.*

Considérons alors k^*, groupe multiplicatif de k; il est d'ordre $q - 1$; on a donc, pour tout élément a de k^*, $a^{q-1} = 1$, et a fortiori $a^q = a$; comme cette égalité reste vraie pour $a = 0$, elle est vérifiée par tout élément de k; en conséquence:

PROPOSITION 2. — *Si Ω désigne une clôture algébrique de k (donc aussi de $\mathbf{F}_p$), k est égal à l'ensemble des racines dans Ω du polynôme $X^q - X$. En particulier, k est le corps de décomposition dans Ω du polynôme $X^q - X$, et tout corps fini ayant même nombre d'éléments q (donc même caractéristique p) que k est nécessairement isomorphe à k.*

Pour $k = \mathbf{F}_p$, l'identité $a^q = a$ s'écrit $a^p = a$, et constitue le *petit théorème de Fermat* sur les restes modulo p. Pour k quelconque, la proposition 2 permet d'écrire

$$X^{q-1} - 1 = \prod_{a \in k^*} (X - a); \quad X^q - X = \prod_{a \in k} (X - a);$$

la première de ces deux égalités montre que les fonctions symétriques élémentaires des éléments de k^* *autres que le produit* sont toutes nulles, et que le produit de tous les éléments de k^* est égal à -1; pour $k = \mathbf{F}_p$, cette dernière propriété constitue le *théorème de Wilson* sur les restes modulo p.

1.2. Soient maintenant p un nombre premier, f un entier $\geqslant 1$, et posons $q = p^f$. Désignons par Ω une clôture algébrique de $\mathbf{F}_p$, et notons k l'ensemble des racines dans Ω du polynôme $X^q - X$. Ce polynôme ayant toutes ses racines simples (son dérivé vaut -1), on voit que card $(k) = q$; de plus, q étant une puissance de la caractéristique, on a, quels que soient a et b dans k, $(a+b)^q = a^q + b^q = a + b$; on a évidemment aussi $(ab)^q = a^q b^q = ab$, et k est un sous-corps de Ω; en particulier:

PROPOSITION 3. — *Quels que soient p premier et $f \geqslant 1$, il existe un corps fini possédant exactement $q = p^f$ éléments.*

Ce corps est unique à isomorphisme près (prop. 2); on le note généralement $\mathbf{F}_q$.

1.3. Mêmes données que dans la section précédente. Soient f_1 et f_2 deux entiers $\geqslant 1$, et posons, pour $i = 1, 2$,

$$q_i = q^{f_i}; \qquad k_i = \mathbf{F}_{q_i} \subset \Omega;$$

on a alors évidemment $[k_i : \mathbf{F}_q] = f_i$. Si $k_1 \subset k_2$, la multiplicativité du degré montre que f_1 divise f_2. Inversement, supposons que f_1 divise f_2; on peut écrire $f_2 = mf_1$, donc $q_2 = {q_1}^m$; si $a \in k_1$, on a alors $a^{q_1} = a$ (prop. 2), donc $a^{{q_1}^m} = a^{q_2} = a$, et par conséquent $a \in k_2$ (prop. 2); ainsi, $k_1 \subset k_2$. Au total (et en conservant ces notations):

PROPOSITION 4. — *L'inclusion $k_1 \subset k_2$ équivaut à la relation f_1 divise f_2, donc à la relation q_2 est une puissance de q_1.*

COROLLAIRE 1. — *Soient respectivement f' et f'' le p.g.c.d. et le p.p.c.m. de f_1 et f_2. Posons $q' = q^{f'}$, $q'' = q^{f''}$, $k' = \mathbf{F}_{q'}$, $k'' = \mathbf{F}_{q''}$. Alors l'intersection et le composé de k_1 et k_2 sont respectivement k' et k''.*

§ 2. *Groupe additif et groupe multiplicatif d'un corps fini.*

Soit k un corps fini à $q = p^f$ éléments.

2.1. L'extension $k/\mathbf{F}_p$ étant de degré f, k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, et a fortiori en tant que groupe additif, au produit direct de f exemplaires de $\mathbf{F}_p$; en conséquence:

PROPOSITION 5. — *Le groupe additif k^+ de k est un groupe de type $(p, ..., p)$ (f fois).*

2.2. Passons au groupe multiplicatif k^*; il est commutatif, d'ordre $q-1$; si N désigne le p.p.c.m. des ordres des éléments de k^*, on vérifie sans peine qu'il existe dans k^* un élément g d'ordre exactement égal à N (c'est là une propriété générale des groupes commutatifs d'ordre fini). Tout élément de k^* est évidemment racine du polynôme $X^N - 1$; ce polynôme, de degré N, possède donc au moins $q-1$ racines, d'où $N \geqslant q-1$; or, par construction même, N divise $q-1$; ainsi, $N = q-1$; mais alors g est d'ordre $q-1$, c'est un générateur de k^*, et on peut énoncer:

PROPOSITION 6. — *Le groupe multiplicatif k^* de k est un groupe cyclique d'ordre $q-1$.*

Pour une autre démonstration de ce résultat, utilisant les propriétés de l'indicatrice d'Euler, voir [**17**], pp. 12-13.

2.3. Soit d un entier $\geqslant 1$; on se propose d'étudier le groupe des puissances d-ièmes et le groupe des racines d-ièmes de l'unité dans k^*, c'est-à-dire l'image et le noyau de l'homomorphisme $u_d: k^* \to k^*$, défini par $u_d(x) = x^d$ $(x \in k^*)$. Posons $\delta = (q-1, d)$, $u_\delta(x) = x^\delta$ $(x \in k^*)$ et notons g un générateur de k^* (prop. 6). L'identité de Bezout $a(q-1) + bd = \delta$ montre que u_d et u_δ ont même noyau (noter que $x^{q-1} = 1$ pour tout $x \in k^*$); k^* étant fini, il en résulte que l'image de u_d et celle de u_δ ont même ordre; mais la première est évidemment contenue dans la seconde: u_d et u_δ ont donc aussi même image. Maintenant, comme δ divise $q-1$, il est clair que l'image de u_δ est le sous-groupe de k^* engendré par g^δ, et que le noyau de u_δ est le sous-groupe de k^* engendré par $g^{(q-1)/\delta}$ (pour le voir, identifier par exemple k^* à $\mathbf{Z}/(q-1)\,\mathbf{Z}$, g s'identifiant à la classe de 1 (mod $q-1$)). En résumé:

PROPOSITION 7. — *Soient k un corps fini à q éléments, g un générateur de k^*, d un entier $\geqslant 1$, et posons $\delta = (q-1, d)$. Alors:*

(i) *Dans k^*, les puissances d-ièmes et les puissances δ-ièmes forment un même sous-groupe, cyclique, engendré par g^δ, et d'ordre égal à $(q-1)/\delta$.*

(ii) *De même, les racines d-ièmes et les racines δ-ièmes de l'unité forment un même sous-groupe, cyclique, engendré par $g^{(q-1)/\delta}$, et d'ordre égal à δ.*

COROLLAIRE 1. — *Le groupe quotient k^*/k^{*d} est cyclique, d'ordre égal à δ.*

COROLLAIRE 2. — *Pour qu'un élément a de k^* soit une puissance d-ième, il faut et il suffit que $a^{(q-1)/\delta} = 1$.*

Pour $k = \mathbf{F}_p$, p impair, et $d = \delta = 2$, le corollaire 2 coïncide avec le *critère d'Euler* sur les restes et non-restes quadratiques modulo p.

§ 3. *Extensions algébriques d'un corps fini.*

Soit toujours k un corps fini à q éléments.

3.1. Soit K une extension algébrique de k, de degré fini m; il est clair que $\mathrm{card}\,(K) = q^m$, et donc que $K = \mathbf{F}_{q^m}$. Soit alors i un entier $\geqslant 0$; comme q^i est une puissance de la caractéristique de K, l'application σ_i: $K \to K$, définie par $\sigma_i(x) = x^{q^i}$ $(x \in K)$, est un automorphisme de K, et même, puisque $k = \mathbf{F}_q$, un k-automorphisme de K (prop. 2); si j est un autre entier $\geqslant 0$, on a évidemment $\sigma_{i+j} = \sigma_i \circ \sigma_j$; enfin, si (par exemple) $i \leqslant j$, l'ensemble des $x \in K$ tels que $\sigma_i(x) = \sigma_j(x)$, donc tels que $x^{q^{j-i}} = x$, est évidemment égal à $K \cap \mathbf{F}_{q^{j-i}}$, et ne peut par conséquent être égal à $K = \mathbf{F}_{q^m}$ que si $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^{j-i}}$, donc (prop. 4) si $i \equiv j \pmod m$; en particulier, les m k-automorphismes σ_i avec $0 \leqslant i < m$ sont distincts, et on peut affirmer:

PROPOSITION 8. — *L'extension K/k est galoisienne; son groupe de Galois est cyclique, d'ordre m, engendré par l'automorphisme* (dit de Frobenius) $x \mapsto x^q$.

Le fait que K/k est galoisienne peut se voir plus directement: en effet, k étant évidemment parfait, K/k est séparable, et il suffit de prouver que K/k est normale, ce qui résulte du fait que K est le corps de décomposition, dans une clôture algébrique de k, du polynôme $X^{q^m} - X$ (prop. 2).

3.2. Mêmes données que ci-dessus. Soit $Tr : K \to k$, l'application *trace*. La proposition 8 montre que, pour tout élément x de K, on a

$$Tr(x) = x + x^q + \ldots + x^{q^{m-1}}. \tag{3.2.1}$$

En outre:

PROPOSITION 9. — *L'application $Tr : K \to k$, est surjective. Si $x \in K$, les deux assertions suivantes sont équivalentes:*

(a) $Tr(x) = 0$;

(b) *il existe $y \in K$ tel que $x = y^q - y$.*

Démonstration. — Considérons K comme espace vectoriel sur k; Tr est alors une forme linéaire, et cette forme linéaire n'est pas nulle (si elle l'était, (3.2.1) impliquerait que le polynôme $X + X^q + \ldots + X^{q^{m-1}}$, de

degré q^{m-1}, admet pour racines les q^m éléments de K: absurde): elle est donc surjective, ce qui prouve la première assertion, et ce qui montre en outre que le noyau de Tr est un hyperplan de K; comme $Tr(y^q - y) = 0$ pour tout élément y de K, il reste, pour établir l'équivalence de (a) et (b), à prouver que l'ensemble des éléments de la forme $y^q - y$ ($y \in K$) est également un hyperplan de K; et il suffit pour cela de remarquer que l'application $y \mapsto y^q - y$ de K dans K est k-linéaire et de rang $m - 1$, puisque son noyau (formé des $y \in K$ tels que $y^q = y$, donc égal à k: prop. 2, ou prop. 8) est de dimension 1.

3.3. Mêmes données et notations que ci-dessus. Soit maintenant $N: K \to k$, l'application *norme*. La proposition 8 montre que, pour tout élément x de K, on a

$$N(x) = x.x^q \dots x^{q^{m-1}} = x^{(q^m-1)/(q-1)}. \tag{3.3.1}$$

En outre:

PROPOSITION 10. — *L'application $N: K^* \to k^*$, est surjective. Si $x \in K^*$, les deux assertions suivantes sont équivalentes:*

(a) $N(x) = 1$;

(b) *il existe $y \in K^*$ tel que $x = y^{q-1}$.*

Démonstration. — N est un homomorphisme du groupe K^* dans le groupe k^*, et il résulte de (3.3.1) et de la proposition 7 (avec $d=(q^m-1)/(q-1)$) que le noyau de N est d'ordre $(q^m-1)/(q-1)$; comme l'ordre de K^* est égal à $q^m - 1$, l'image de N est nécessairement d'ordre $q - 1 = \text{card}(k^*)$, d'où la surjectivité de N. Le noyau de N contenant évidemment tous les éléments de K^* de la forme y^{q-1} ($y \in K^*$), qui en constituent un sous-groupe, il reste donc, pour établir l'équivalence de (a) et (b), à montrer que ce sous-groupe est précisément d'ordre $(q^m-1)/(q-1)$; mais il suffit pour cela de remarquer que l'application $y \mapsto y^{q-1}$ de K^* dans K^* est un homomorphisme dont le noyau (formé des $y \in K^*$ tels que $y^{q-1} = 1$, donc égal à k^*) est d'ordre $q - 1$, et dont l'image est alors effectivement d'ordre $(q^m-1)/(q-1)$, puisque K^* est lui-même d'ordre $q^m - 1$.

Notes sur le chapitre premier

Théorème de Wedderburn: pour la démonstration originale, voir Wedderburn (1905); l'idée d'utiliser (comme dans [**1**] ou [**19**]) les propriétés des polynômes cyclotomiques pour simplifier cette démonstration est due à Witt (1931).

§ **1**: la classification des corps (commutatifs) finis (« champs de Galois ») remonte essentiellement à Galois (1830).

§ **2**: le fait que le groupe multiplicatif du corps $\mathbf{F}_p$ est cyclique est dû à Euler (1760); sa démonstration utilisait les propriétés de l'« indicatrice d'Euler ». Ce résultat est un ingrédient essentiel de la théorie des restes quadratiques (Euler, Legendre, Gauss), cubiques (Jacobi, Eisenstein), biquadratiques (Gauss, Jacobi), et plus généralement des restes de puissances quelconques (Kummer, etc.); à ce sujet, voir par exemple Dickson, *History of the Theory of Numbers.*

§ **3**: les propositions 9 et 10 sont des cas particuliers du *théorème* 90 de Hilbert relatif aux extensions cycliques (voir [**10**], pp. 213-215).

CHAPITRE 2

POLYNÔMES ET IDÉAUX DE POLYNÔMES

On sait que si K est un corps *infini*, et si F est un polynôme à une ou plusieurs variables, à coefficients dans K, et *identiquement nul* sur K, alors F est *nul*: tous ses coefficients sont nuls. Ceci n'est plus vrai pour un corps fini: ainsi, sur $k = \mathbf{F}_q$, le polynôme $X^q - X$, non nul, est pourtant identiquement nul (chap. 1, sect. 1.1 et 1.2); c'est à cette particularité des corps finis qu'est consacré le présent chapitre.

Dans tout le cours de ce chapitre (ainsi que dans les chapitres suivants), k désignera un corps fini à $q = p^f$ éléments, n un entier $\geqslant 1$, $X = (X_1, ..., X_n)$ une famille de n variables, et $k[X] = k[X_1, ..., X_n]$ l'anneau des polynômes en $X_1, ..., X_n$ à coefficients dans k; d'autre part, les éléments $\mathbf{a} = (a_1, ..., a_n)$ de k^n seront appelés *points* (ou *points rationnels sur* k, si cette précision est nécessaire); si $F \in k[X]$, si $\mathbf{a}$ est un point de k^n, et si $F(\mathbf{a}) = 0$, on dira que $\mathbf{a}$ est un *zéro* de F.

§ 1. *Polynômes réduits et polynômes identiquement nuls.*

1.1. Soit F un élément de $k[X]$.

DÉFINITION 1. — *Si le degré de F par rapport à chacune des n variables X_i est inférieur ou égal à $q-1$, on dit que F est un polynôme* réduit.

Les polynômes réduits forment évidemment un sous-espace vectoriel R de $k[X]$ (le corps des scalaires étant k); une base naturelle de ce sous-espace est l'ensemble des monômes $X_1^{d_1} \dots X_n^{d_n}$ tels que $0 \leqslant d_i \leqslant q-1$ pour $i = 1, \dots, n$; R est donc de dimension q^n sur k.

1.2. Soit encore F un élément de $k[X]$.

DÉFINITION 2. — *On appelle* fonction polynomiale associée à F *l'application* $\mathbf{x} \mapsto F(\mathbf{x})$ *de k^n dans k. Si cette fonction polynomiale est nulle (donc si $F(\mathbf{x}) = 0$ en tout point $\mathbf{x}$ de k^n), on dit que le polynôme F est* identiquement nul.

Les polynômes identiquement nuls forment un idéal I de $k[X]$; notons d'autre part Γ l'idéal de $k[X]$ engendré par les éléments $X_i^q - X_i$ $(i=1, \dots, n)$; comme chacun de ces polynômes est identiquement nul (chap. 1, § 1), il est clair que $\Gamma \subset I$: on va voir qu'en fait, il y a égalité.

1.3. THÉORÈME 1. — (i) *Dans $k[X]$, les idéaux I et Γ sont égaux.* (ii) *En tant qu'espace vectoriel sur k, $k[X]$ est somme directe de R (voir sect. 1.1) et de Γ :*

$$k[X] = R \oplus \Gamma . \tag{1.3.1}$$

Démonstration. — On aura besoin de deux lemmes.

LEMME 1. — *Si un polynôme F de $k[X]$ est à la fois réduit et identiquement nul, alors il est nul ; autrement dit :*

$$R \cap I = (0) . \tag{1.3.2}$$

Ce lemme se démontre par récurrence sur n. Tout d'abord, la propriété est vraie pour $n = 1$: si en effet F, polynôme à une variable, est réduit et identiquement nul, il est de degré $\leqslant q-1$ (déf. 1) et il possède d'autre part au moins q racines: les q éléments de k (déf. 2); et ceci n'est possible que si $F = 0$. Ensuite, si la propriété est vraie pour $n-1$ variables (avec $n \geqslant 2$), elle est encore vraie pour n variables: soit en effet F un polynôme *réduit* à n variables; en l'ordonnant suivant les puissances décroissantes de X_1, on peut le mettre sous la forme

$$F_1(X_2, \dots, X_n) X_1^{q-1} + \dots + F_{q-1}(X_2, \dots, X_n) X_1 + F_q(X_2, \dots, X_n),$$

les F_j ($1 \leqslant j \leqslant q$) étant q polynômes *réduits, à* $n-1$ *variables* $X_2, ..., X_n$. Supposons maintenant F *identiquement nul*: alors, quel que soit le point $(x_2, ..., x_n)$ de k^{n-1}, le polynôme $f_1 X_1^{q-1} + ... + f_{q-1} X_1 + f_q$ (où, par définition, $f_j = F_j(x_2, ..., x_n)$ pour $j = 1, ..., q$) est lui-même identiquement nul; mais c'est un polynôme réduit, à une seule variable X_1: la première partie de la démonstration prouve donc qu'il est nul, c'est-à-dire que $f_1 = ... = f_q = 0$, ou encore que $F_1(x_2, ..., x_n) = ... = F_q(x_2, ..., x_n) = 0$; or ceci a lieu, rappelons-le, quel que soit $(x_2, ..., x_n)$ dans k^{n-1}: ainsi, les q polynômes F_j sont identiquement nuls, et l'hypothèse de récurrence permet d'affirmer qu'ils sont nuls; mais alors, F est lui-même nul, C.Q.F.D.

LEMME 2. — *Pour tout polynôme* F *de* $k[X]$, *il existe un polynôme réduit* F^* *tel que* $F \equiv F^* \pmod{\Gamma}$; *autrement dit :*

$$k[X] = R + \Gamma . \tag{1.3.3}$$

Prouvons ce lemme: par linéarité, on peut se ramener au cas où F est un monôme $X_1^{d_1} ... X_n^{d_n}$; Γ étant un idéal, on peut même se limiter au cas où ce monôme ne contient qu'une seule variable, par exemple, au cas où $F = X_1^{d_1}$; mais alors, pour $d_1 \leqslant q-1$, il n'y a rien à démontrer (faire $F^* = 0$); et pour $d_1 \geqslant q$, il suffit de raisonner par récurrence sur d_1, en remarquant qu'on a la congruence $X_1^{d_1} \equiv X_1^{d_1-(q-1)} \pmod{\Gamma}$.

Démontrons maintenant le théorème 1 lui-même. Comme $\Gamma \subset I$, il résulte du lemme 1 que

$$R \cap \Gamma = (0) . \tag{1.3.4}$$

Les égalités (1.3.3) et (1.3.4) montrent alors que $k[X] = R \oplus \Gamma$: (ii) se trouve ainsi établi. Reste à prouver (i), et il suffit évidemment de montrer que $I \subset \Gamma$; mais si $F \in I$, on peut écrire (lemme 2)

$$F = F^* + G \quad (F^* \in R,\ G \in \Gamma) ; \tag{1.3.5}$$

comme $\Gamma \subset I$, $F^* = F - G$, différence de deux éléments de I, est un élément de I, donc un polynôme identiquement nul; le lemme 1 montre alors que F^* est nul, et (1.3.5) donne $F = G \in \Gamma$, ce qui prouve bien l'inclusion $I \subset \Gamma$. Le théorème est ainsi démontré.

1.4. D'après le théorème 1, tout polynôme $F \in k[X]$ s'écrit d'une façon et d'une seule $F = F^* + G$, avec F^* réduit et G identiquement nul.

DÉFINITION 3. — *On dit que* F^* *est le* polynôme réduit associé à F.

La démonstration du lemme 2 donne une méthode effective pour calculer F^* à partir de F, et permet en outre d'énoncer:

THÉORÈME 2. — *Si F est un élément de $k[X]$, et si F^* est le polynôme réduit associé à F, on a l'inégalité* $\deg(F^*) \leqslant \deg(F)$.

§ 2. *Fonctions polynomiales.*

2.1. Soit A l'ensemble de toutes les applications de k^n dans k, et soit φ l'application qui, à tout polynôme $F \in k[X]$, fait correspondre sa fonction polynomiale associée. Il est clair que A est muni naturellement d'une structure de k-algèbre (ainsi d'ailleurs que $k[X]$) et que $\varphi: k[X] \to A$, est un homomorphisme de k-algèbres.

THÉORÈME 3. — (i) *L'homomorphisme φ est surjectif et a pour noyau l'idéal Γ ; φ donne donc lieu à un isomorphisme d'algèbres*

$$k[X]/\Gamma \xrightarrow{\sim} A\,. \tag{2.1.1}$$

(ii) *Soit φ_R la restriction à $R \subset k[X]$ de l'homomorphisme φ; φ_R est un isomorphisme de l'espace vectoriel R sur l'espace vectoriel A. Si F est un élément de $k[X]$, on a $\varphi_R{}^{-1}(\varphi(F)) = F^*$.*

Démonstration. — (ii) est une conséquence immédiate de (i) et de l'égalité (1.3.1) (th. 1, (ii)). Prouvons (i): le noyau de φ est par définition égal à I; mais $I = \Gamma$ (th. 1, (i)); le noyau de φ est donc bien Γ. Reste à établir la surjectivité de φ, c'est-à-dire le lemme suivant:

LEMME 3. — *Pour toute application $f: k^n \to k$, il existe dans $k[X]$ un polynôme F tel que $F(\mathbf{x}) = f(\mathbf{x})$ en tout point $\mathbf{x}$ de k^n.*

Prouvons ce lemme; pour tout point $\mathbf{a} = (a_1, \ldots, a_n)$ de k^n, notons $f_{\mathbf{a}}$ l'application de k^n dans k définie par

$$f_{\mathbf{a}}(\mathbf{x}) = \begin{cases} 1 & \text{si} \quad \mathbf{x} = \mathbf{a}\,; \\ 0 & \text{si} \quad \mathbf{x} \neq \mathbf{a}\,. \end{cases} \tag{2.1.2}$$

La famille $(f_{\mathbf{a}})_{\mathbf{a} \in k^n}$ est évidemment une base sur k de l'espace vectoriel A; par linéarité, on peut donc se limiter au cas où f est de la forme $f_{\mathbf{a}}$; mais il suffit alors de prendre pour F le polynôme

$$F_{\mathbf{a}} = \left(1 - (X_1 - a_1)^{q-1}\right) \ldots \left(1 - (X_n - a_n)^{q-1}\right) \tag{2.1.3}$$

(voir chap. 1, sect. 1.1). Ceci démontre le lemme 3, et achève de prouver le théorème 3.

2.2. Concrètement, le théorème 3 signifie ceci: toute application $f: k^n \to k$, est une fonction polynomiale, et on peut supposer que le polynôme F tel que $F(\mathbf{x}) = f(\mathbf{x})$ en tout point $\mathbf{x}$ de k^n est *réduit*; F est alors entièrement déterminé par f. Si on remarque que le polynôme $F_{\mathbf{a}}$ défini par (2.1.3) est réduit, on voit qu'on peut même écrire explicitement

$$F(X) = \sum_{\mathbf{a} \in k^n} f(\mathbf{a}) F_{\mathbf{a}}(X) . \tag{2.2.4}$$

2.3. On a remarqué (sect. 1.1) que la dimension de l'espace vectoriel R est égale à q^n; comme $k[X] = R \oplus \Gamma$, l'espace quotient $k[X]/\Gamma$ est aussi de dimension q^n. Par ailleurs, l'espace vectoriel A, qui admet pour base sur k la famille $(f_{\mathbf{a}})_{\mathbf{a} \in k^n}$ (sect. 2.1), est également de dimension q^n. L'homomorphisme injectif (2.1.1) est donc en fait bijectif, ce qui donne une deuxième démonstration de la surjectivité de φ. Exercice pour le lecteur: donner une troisième démonstration de la surjectivité de φ en utilisant la théorie des polynômes d'interpolation.

2.4. Le théorème 3 permet d'évaluer la « probabilité » pour qu'une équation $F = 0$ ($F \in k[X]$) admette au moins une solution dans k^n. Tout d'abord, on ne modifie pas l'ensemble des solutions de l'équation en remplaçant F par F^*; on peut donc supposer F réduit, et on s'aperçoit ainsi qu'il existe essentiellement $\mathrm{card}(R) = q^{q^n}$ équations distinctes. D'autre part, les polynômes réduits F tels que l'équation $F = 0$ *n'ait aucune solution* correspondent bijectivement par φ_R aux applications de k^n dans k^*; il y en a donc exactement $(q-1)^{q^n}$, et il existe ainsi $q^{q^n} - (q-1)^{q^n}$ polynômes réduits F tels que l'équation $F = 0$ *ait au moins une solution*. En définitive, la « probabilité » cherchée est donc égale à $1 - (1-q^{-1})^{q^n}$.

§ 3. *Idéaux de polynômes.*

3.1. Soit $F_1, \ldots, F_s$ une famille de s éléments de $k[X]$, et soit J l'idéal de $k[X]$ engendré par les F_j ($j = 1, \ldots, s$); considérons le système d'équations

$$F_1 = 0, \ldots, F_s = 0 , \tag{3.1.1}$$

et soit V l'ensemble des solutions de (3.1.1) dans k^n, c'est-à-dire l'ensemble des zéros de J rationnels sur k. Soit enfin $I(V)$ l'ensemble des polynômes $G \in k[X]$ qui s'annulent en tout point de V; $I(V)$ est évidemment un idéal de $k[X]$; $I(V)$ contient J, et aussi Γ; $I(V)$ contient donc $J + \Gamma$; en fait:

THÉORÈME 4. — *On a l'égalité*

$$I(V) = J + \Gamma . \tag{3.1.2}$$

Démonstration. — Considérons le polynôme

$$F = 1 - (1 - F_1^{q-1}) \dots (1 - F_s^{q-1}) ; \tag{3.1.3}$$

F appartient à l'idéal J: en effet, considéré comme polynôme par rapport à $F_1, \dots, F_s$, le second membre de (3.1.3) ne contient pas de terme constant; d'autre part, F prend constamment la valeur 0 sur V, et la valeur 1 en dehors de V (voir chap. 1, sect. 1.1). Soit alors H un élément de $I(V)$, donc un polynôme nul sur V; il est clair que le polynôme $G = H - HF$ est identiquement nul, et appartient donc à Γ; il est clair également, puisque J est un idéal contenant F, que HF appartient à J; on voit ainsi que $H = HF + G$ appartient à $J + \Gamma$, donc que $I(V) \subset J + \Gamma$, C.Q.F.D.

3.2. Le *théorème de la base finie* de Hilbert (voir **[10]**, p. 144) montre que tout idéal de $k[X]$ peut être engendré par un nombre fini de polynômes: le théorème 4 est donc en fait applicable à n'importe quel idéal J de $k[X]$ (dans le même ordre d'idées, on peut d'ailleurs remarquer que dans la démonstration du théorème 4, on a implicitement remplacé l'idéal J engendré par $F_1, \dots, F_s$, par l'idéal principal (F), contenu dans J, et dont l'ensemble des zéros dans k^n est le même que celui de J).

Notons d'autre part que le *théorème des zéros* de Hilbert (**[10]**, p. 256, **[12]**, p. 32, ou **[15]**, p. 4) implique que, dans l'anneau $k[X]$, l'idéal $J + \Gamma = I(V)$ est égal à sa racine, c'est-à-dire à l'intersection des idéaux premiers qui le contiennent; comme $\dim(V) = 0$ (V est un ensemble fini de points rationnels sur k), ces idéaux premiers sont d'ailleurs tous maximaux, ce sont exactement les idéaux de la forme $\mathfrak{M}_{\mathbf{a}} = (X_1 - a_1, \dots, X_n - a_n)$, $\mathbf{a} = (a_1, \dots, a_n)$ parcourant l'ensemble V.

Notes sur le chapitre 2

§ **1** et **2**: les résultats contenus dans ces deux paragraphes sont essentiellement dus à Chevalley (1935); ils donneront notamment (chap. 3, sect. 1.1) une démonstration immédiate du « théorème de Chevalley-Warning ».

§ **3**: le théorème 3 est dû à Terjanian (1966).

CHAPITRE 3

THÉORÈMES DE CHEVALLEY ET WARNING

Ce chapitre est centré sur la propriété suivante: si un polynôme sans terme constant sur un corps fini k a un nombre de variables strictement supérieur à son degré, alors il admet sur k un zéro *non trivial* (c'est-à-dire autre que le point (0, ..., 0)); ce résultat, conjecturé par Artin vers 1934, a été démontré par Chevalley en 1935, puis précisé par Warning la même année (pour plus amples détails, voir les Notes en fin de chapitre).

On conserve ici les conventions adoptées au début du chapitre 2.

§ 1. *Le théorème de Chevalley-Warning.*

1.1. Il s'agit du résultat suivant:

THÉORÈME 1. — *Soit $F_1, ..., F_s$ une famille de s polynômes appartenant à $k[X]$, de degrés respectifs $d_1, ..., d_s$, et soit V l'ensemble des solutions dans k^n du système d'équations*

$$F_1 = 0, ..., F_s = 0; \tag{1.1.1}$$

soient enfin $N = \mathrm{card}(V)$ le nombre de solutions de (1.1.1) dans k^n, et $d = d_1 + ... + d_s$ la somme des degrés des polynômes F_j. Alors, si $n > d$, le nombre N est divisible par p (la caractéristique de k).

Démonstration. — Introduisons les deux polynômes suivants:

$$\bar{F} = (1 - F_1^{q-1}) \dots (1 - F_s^{q-1}); \tag{1.1.2}$$

$$F_V = \sum_{a \in V} (1 - (X_1 - a_1)^{q-1}) \dots (1 - (X_n - a_n)^{q-1}); \tag{1.1.3}$$

(avec les notations du chap. 2, sect. 2.1, on a donc $F_V = \sum_{a \in V} F_a$). On voit immédiatement que $\bar{F}$ et F_V prennent la valeur 1 en tout point de V, et la valeur 0 partout ailleurs; le polynôme $G = \bar{F} - F_V$ est donc identiquement nul; comme F_V est manifestement réduit, et que $\bar{F} = F_V + G$, F_V n'est autre que le polynôme réduit associé à $\bar{F}$ (chap. 2, sect. 1.4), ce qui implique (chap. 2, th. 2) $\deg(F_V) \leqslant \deg(\bar{F})$, donc, en utilisant l'hypothèse $n > d$, $\deg(F_V) \leqslant d(q-1) < n(q-1)$. Mais F_V comporte a priori un monôme

en $X_1^{q-1} \ldots X_n^{q-1}$, de degré $n(q-1)$; le coefficient de ce monôme, égal à $(-1)^n N$, doit donc être nul dans le corps k, de caractéristique p: en d'autres termes, N doit être divisible par p, C.Q.F.D.

On verra (§ 4) que l'hypothèse $n > d$ ne peut pas être affaiblie: on peut en effet, quels que soient k et n, construire un polynôme de degré n, à n variables et à coefficients dans k, et pour lequel on ait $N = 1$.

COROLLAIRE 1 (théorème de Chevalley). — *Mêmes données et hypothèses (notamment $n > d$) que dans le théorème* 1. *Si de plus chacun des polynômes F_j $(j=1, \ldots, s)$ est sans terme constant, alors le système* (1.1.1) *admet dans k^n une solution autre que la solution triviale* $(0, \ldots, 0)$.

Démonstration. — L'absence de termes constants implique que $(0, \ldots, 0)$ est solution du système (1.1.1): d'où $N \geqslant 1$; mais N est divisible par p (th. 1); on a donc $N \geqslant p$, et le nombre $N - 1$ de solutions non triviales est donc $\geqslant p - 1 \geqslant 2 - 1 = 1$, C.Q.F.D.

Le théorème 1 et son corollaire 1 s'appliquent en particulier au cas $s = 1$ d'un seul polynôme de degré d, à n variables et tel que $n > d$. Ainsi, toute forme quadratique à trois variables ou plus sur un corps fini k admet un zéro non trivial sur k; en langage géométrique, toute conique, quadrique, ... projective, définie sur un corps fini k, admet au moins un point rationnel sur k. On aura l'occasion de revenir fréquemment sur ce genre de propriété. Notons par ailleurs qu'un polynôme satisfaisant à $n > d$ peut être tel que $N = 0$; ainsi, si $p \neq 2$, le polynôme $(X_1 + \ldots + X_n)^{q-1} + 1$, de degré $q - 1$, ne peut prendre que les valeurs 1 et $2 \neq 0$ (chap. 1, sect. 1.1): donc, si grand que soit n, et en particulier si $n > d = q - 1$, ce polynôme donne lieu à $N = 0$. Pour un autre exemple, voir le chapitre 4 (sect. 2.3).

1.2. Le théorème de Chevalley fournit une démonstration du théorème de Wedderburn autre que celles mentionnées au chapitre 1. Soient en effet K un corps commutatif et r un nombre réel positif; on dit que K *possède la propriété* (C_r) si tout polynôme homogène, de degré d, à n variables, à coefficients dans K, et tel que $n > d^r$, admet dans K^n un zéro non trivial (voir par exemple [7], p. 6); avec cette terminologie, le théorème 1 (ou son corollaire 1) implique:

COROLLAIRE 2. — *Tout corps fini (commutatif) possède la propriété* (C_1).

Convenons d'autre part, toujours pour un corps commutatif K, de désigner par (B_0) la propriété suivante: tout corps gauche de centre K et de degré fini sur K est égal à K. On a alors le résultat suivant:

PROPOSITION 1. — *Si un corps commutatif K possède la propriété* (C_1), *alors il possède la propriété* (B_0).

Démonstration. — Soit en effet L un corps gauche de centre K et de degré fini n sur K. On sait que n est un carré (soit $n=d^2$) et que si $e_1, ..., e_n$ est une base de L sur K (en tant qu'espace vectoriel), la norme réduite $Nrd_{L/K}(x)$ d'un élément quelconque $x = x_1e_1 + ... + x_ne_n$ de L est un polynôme homogène et de degré d, à coefficients dans K, par rapport aux composantes $x_1, ..., x_n$ de x, qui sont dans K (voir par exemple Bourbaki, Algèbre, chap. VIII, § 12; dans le cas bien connu du corps **H** des quaternions ordinaires sur **R**, rapporté à la base canonique 1, i, j, k, on a $n = 4 = 2^2$ et $Nrd_{\mathbf{H}/\mathbf{R}}(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$); cette norme réduite ne s'annule que pour $x = 0$, donc pour $x_1 = ... = x_n = 0$; comme K est supposé posséder la propriété (C_1), on a nécessairement $n = d^2 \leqslant d$, donc $d = 1$, $n = 1$ et $L = K$, C.Q.F.D.

Redémontrons alors le théorème de Wedderburn; soit L un corps fini, non supposé commutatif, et soit k son centre; k est un corps fini *commutatif*, et il possède la propriété (C_1) (cor. 2), donc la propriété (B_0) (prop. 1); mais comme L est évidemment de degré fini sur k, on a alors $L = k$ (par définition de (B_0)), et par conséquent L est commutatif, C.Q.F.D.

§ 2. *Seconde démonstration du théorème de Chevalley-Warning.*

2.1. Cette seconde démonstration, indépendante de la théorie des polynômes réduits, repose sur le théorème suivant (dont on aura également besoin au § 3):

THÉORÈME 2. — *Soit* $F \in k[X]$ *un polynôme à n variables, et de degré d. Alors, si* $d < n(q-1)$, *on a*

$$\sum_{x \in k^n} F(x) = 0 . \tag{2.1.1}$$

Démonstration. — Par linéarité, on peut se ramener au cas où F est un monôme $X_1^{u_1} ... X_n^{u_n}$, avec $d = u_1 + ... + u_n < n(q-1)$; on a alors

$$\sum_{\mathbf{x} \in k^n} F(\mathbf{x}) = \prod_{i=1}^{n} \Big(\sum_{x_i \in k} x_i^{u_i} \Big) ; \tag{2.1.2}$$

l'inégalité relative à d montre que pour un i au moins, $u_i < q - 1$, et il suffit évidemment de prouver que, dans (2.1.2), le i-ème facteur du membre de droite est alors nul, ce qui résulte du lemme suivant:

LEMME 1. — *Soit u un entier $\geqslant 0$, et posons $S_u = \sum_{x \in k} x^u$; alors*

(i) *si u est non nul et divisible par $q-1$, $S_u = -1$;*

(ii) *sinon, $S_u = 0$.*

En particulier, si $u < q-1$, $S_u = 0$.

Prouvons ce lemme; comme $x^q = x$ pour tout $x \in k$, on ne restreint pas la généralité de la démonstration en supposant $0 \leqslant u \leqslant q-1$; on est ainsi amené à distinguer trois cas:

(1) $u = 0$: S_u est alors somme de q termes égaux à 1; comme q est divisible par la caractéristique p de k, on a bien $S_u = 0$;

(2) $u = q-1$: alors $x^u = 0$ pour $x = 0$, et $x^u = 1$ sinon; S_u est donc somme de $q-1$ termes égaux à 1, et on conclut comme en (1);

(3) $0 < u < q-1$: la proposition 7 (chap. 1) avec $d = u$ montre qu'il existe dans k^* un élément a tel que $a^u \neq 1$; comme $x \mapsto ax$ est une bijection de k sur k, on peut écrire $S_u = \sum_{x \in k} (ax)^u = a^u S_u$; mais ceci donne $(a^u - 1) S_u = 0$, donc, en simplifiant par $a^u - 1 \neq 0$, $S_u = 0$, C.Q.F.D.

On aurait également pu régler les cas (2) et (3) de la façon suivante: soit g un générateur de k^*; les éléments x de k sont alors 0, et les g^i avec $0 \leqslant i \leqslant q-2$; S_u est donc égal à la somme de la progression géométrique $1 + g^u + g^{2u} + \ldots + g^{(q-2)u}$; d'où $S_u = (1-g^{(q-1)u})/(1-g^u)$, ce qui vaut bien 0, puisque $g^{q-1} = 0$. Remarquons par ailleurs que la nullité des $q-2$ quantités S_u $(0<u<q-1)$ équivaut, compte tenu des *formules de Newton*, à la nullité des $q-2$ fonctions symétriques élémentaires des éléments de k^* autres que le produit (voir chap. 1, sect. 1.1).

2.2. Utilisons maintenant le théorème 2 pour redémontrer le théorème de Chevalley-Warning. Considérons le polynôme $\bar{F}$ défini par (1.1.2) (sect. 1.1); il est de degré $d(q-1) < n(q-1)$, puisqu'on a supposé $n > d$; le théorème 2 permet donc d'écrire

$$\sum_{\mathbf{x} \in k^n} \bar{F}(\mathbf{x}) = 0 ; \tag{2.2.1}$$

mais $\bar{F}(\mathbf{x})$ vaut 1 si $\mathbf{x} \in V$, et 0 si $\mathbf{x} \notin V$; d'où une seconde égalité:

$$\sum_{\mathbf{x} \in k^n} \bar{F}(\mathbf{x}) = N.1 ; \tag{2.2.2}$$

(2.2.1) et (2.2.2) donnent alors $N.1 = 0$, soit, puisque k est de caractéristique p, $N \equiv 0 \pmod{p}$, C.Q.F.D.

§ 3. *Le « second » théorème de Warning.*

3.1. Il s'agit du résultat suivant, établi par Warning, en même temps que le théorème 1, dans son article déjà cité (Warning (1935)):

THÉORÈME 3. — *Mêmes données et hypothèses (en particulier $n > d$) que dans le théorème* 1. *Alors, si $N > 0$ (donc si le système (*1.1.1*) admet au moins une solution), on a en fait $N \geqslant q^{n-d}$.*

Démonstration. — Plaçons-nous dans l'espace affine k^n, et soit toujours V l'ensemble des solutions de (1.1.1); pour abréger, convenons (dans cette section seulement) de dire *variété* au lieu de *sous-variété affine de k^n*; *alors :*

LEMME 1. — *Si W_1 et W_2 sont deux variétés parallèles de dimension $d = d_1 + \ldots + d_s$ (voir th.* 1*), on a la congruence*

$$\text{(3.1.1)} \qquad \operatorname{card}(W_1 \cap V) \equiv \operatorname{card}(W_2 \cap V) \pmod{p}.$$

Prouvons ce lemme. On peut se limiter au cas où $W_1 \neq W_2$, puis, quitte à effectuer un changement de coordonnées dans k^n (ce qui ne modifie pas les d_j), supposer que W_1 et W_2 sont définies respectivement par les systèmes d'équations $X_1 = 0, X_2 = 0, \ldots, X_{n-d} = 0$, et $X_1 = 1, X_2 = 0, \ldots, X_{n-d} = 0$. Introduisons le polynôme (à une seule variable T)

$$R(T) = T^{q-1} - 1 = \prod_{a \in k^*} (T - a),$$

puis le polynôme (à n variables $X_1, \ldots, X_n$, mais ne dépendant en fait que de $X_1, \ldots, X_{n-d}$)

$$G(X) = (-1)^{n-d} R(X_2) \ldots R(X_{n-d}) \prod_{a \neq 0,1} (X_1 - a);$$

G est un polynôme de degré total $(n-d)(q-1) - 1$; de plus, il vaut évidemment -1 sur W_1, 1 sur W_2 et 0 ailleurs; $\bar{F}$ désignant toujours le polynôme défini par (1.1.2) (sect. 1.1), $H = G\bar{F}$ est donc un polynôme à n variables, de degré total $(n-d)(q-1) - 1 + d(q-1) = n(q-1) - 1 < n(q-1)$, et ce polynôme vaut -1 sur $W_1 \cap V$, 1 sur $W_2 \cap V$, et 0 partout ailleurs; d'où:

$$\text{(3.1.2)} \qquad \sum_{\mathbf{x} \in k^n} H(\mathbf{x}) = \big(\operatorname{card}(W_2 \cap V) - \operatorname{card}(W_1 \cap V)\big) \cdot 1;$$

mais le théorème 2 est applicable à H: le second membre de (3.1.2) est donc égal à 0, dans le corps k de caractéristique p, ce qui équivaut à (3.1.1), et prouve le lemme 1.

Passons à la démonstration du théorème 3, et distinguons deux cas:

(1) *Il existe au moins une variété W de dimension d telle que* card $(W \cap V) \not\equiv 0 \pmod{p}$: le lemme 1 montre alors que pour toute variété W' parallèle à W et de même dimension d, on a également card $(W' \cap V) \not\equiv 0 \pmod{p}$; comme il existe exactement q^{n-d} telles variétés W' (W comprise), qu'elles forment une partition de k^n, et que chacune d'elles contient évidemment au moins un point de V, l'inégalité $N \geqslant q^{n-d}$ se trouve immédiatement établie dans ce premier cas.

(2) *Pour toute variété W de dimension d, on a* card $(W \cap V) \equiv 0 \pmod{p}$; puisque V contient (par hypothèse) au moins un point, on peut cependant affirmer ceci: il existe un entier m $(1 \leqslant m \leqslant d)$ possédant la propriété suivante:

> *pour toute variété M de dimension m, on a* card $(M \cap V) \equiv 0 \pmod{p}$, *mais il existe une variété L de dimension $m-1$ telle que* card $(L \cap V) \not\equiv 0 \pmod{p}$.

Fixons une telle variété L, et désignons par a le reste de division de card $(L \cap V)$ par p; on a donc $1 \leqslant a \leqslant p-1$. Considérons maintenant les variétés M de dimension m passant par L; il y en a exactement

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

(nombre de points rationnels sur k dans l'espace projectif de dimension $n-m$); chacune de ces variétés M contient au moins a points de V (ceux qui sont dans $L \cap V$), et comme par ailleurs card $(M \cap V) \equiv 0 \pmod{p}$, chaque différence ensembliste $M - L$ contient au moins $p - a \geqslant 1$ points de V; mais les différences $M - L$ forment une partition de $k^n - L$; ainsi,

$$N = \text{card}\,(V) > q^{n-m} + \ldots + q + 1 > q^{n-d},$$

ce qui règle le second cas et achève de prouver le théorème 3.

3.2. On verra au paragraphe suivant (sect. 4.3) que, sous les hypothèses du théorème 3, l'inégalité $N \geqslant q^{n-d}$ est la meilleure possible.

§ 4. *Polynômes normiques et théorème de Terjanian.*

4.1. Le théorème 1 utilise de façon essentielle l'hypothèse $n > d$. Si $n \leqslant d$, il tombe en défaut, comme on peut le voir sur l'exemple suivant (dans cet exemple et dans tout le reste de ce chapitre, on se limite au cas d'un seul polynôme: $s = 1$):

soit n un entier $\geqslant 1$, et soit K l'unique extension de degré n de k, c'est-à-dire le corps $\mathbf{F}_{q^n}$; soit $\omega_1, \ldots, \omega_n$ une base de K sur k, et posons

$$P(X) = \prod_{j=0}^{n-1} (\omega_1{}^{q^j} X_1 + \ldots + \omega_n{}^{q^j} X_n) ; \tag{4.1.1}$$

les $\omega_i{}^{q^j}$ $(0 \leqslant j \leqslant n-1)$ étant les conjugués de ω_i dans l'extension galoisienne K/k (chap. 1, prop. 8), P est à coefficients dans k; de plus, P est un polynôme de degré n, à n variables (on a donc $n = d$, n étant d'ailleurs quelconque); enfin, P n'admet dans k^n que le zéro trivial $\mathbf{x} = (0, \ldots, 0)$: en effet, si $\mathbf{x} = (x_1, \ldots, x_n)$ est un point de k^n, et si on pose $\xi = \omega_1 x_1 + \ldots + \omega_n x_n$, il est évident (voir chap. 1, sect. 3.3) que $P(\mathbf{x})$ est égal à la norme de ξ dans l'extension K/k; l'égalité $P(\mathbf{x}) = 0$ ne peut donc avoir lieu que si $\xi = 0$, c'est-à-dire si $x_1 = \ldots = x_n = 0$. Ainsi, si N désigne le nombre de solutions dans k^n de l'équation $P = 0$, on a $N = 1$, et $N \not\equiv 0 \pmod{p}$, comme annoncé.

(Notons au passage que le théorème 3 reste vrai si $n \leqslant d$, mais qu'il perd alors tout intérêt, puisqu'il se réduit à l'énoncé suivant: si $N > 0$, on a $N \geqslant 1/q^{d-n}$).

4.2. L'exemple donné dans la section 4.1 justifie la définition ci-dessous:

DÉFINITION 1. — *On appelle* polynôme normique *de degré n sur k tout polynôme F de degré n à n variables, à coefficients dans k, et ayant pour seul zéro dans k^n le point* $(0, \ldots, 0)$ *(un polynôme normique est donc sans terme constant).*

Les polynômes normiques possèdent la propriété suivante, mise en évidence par Terjanian:

THÉORÈME 4. — *Soit $F \in k[X]$ un polynôme normique de degré n, et soit $G \in k[X]$ un polynôme (quelconque) de degré strictement inférieur à n. Alors l'équation*

$$F(X) = G(X) \tag{4.2.1}$$

admet au moins une solution dans k^n.

Démonstration. — Introduisons nq variables notées X_{ij} $(1 \leqslant i \leqslant n,$ $1 \leqslant j \leqslant q)$, et, pour tout i, soit $S_i \in k[X_{i1}, \ldots, X_{iq}]$ un polynôme normique de degré q (de tels S_i existent effectivement: utiliser l'exemple donné dans la section 4.1, avec $n = q$). Introduisons une variable supplémentaire Y, et considérons le polynôme R à $n(R) = nq + 1$ variables défini par

$$R = F(S_1, ..., S_n) - G(S_1, ..., S_n)\, Y^{q-1}.$$

Son degré $d(R)$ est $\leqslant nq$, d'où $n(R) > d(R)$; de plus, R n'a pas de terme constant, puisque F et les S_i n'en ont pas, et que $G(S_1, ..., S_n)$ se trouve multiplié par Y^{q-1}. Le théorème de Chevalley montre alors que R admet dans k^{nq+1} un zéro non trivial $(x_{11}, ..., x_{nq}, y)$; si on pose $s_i = S_i(x_{i1}, ..., x_{iq})$, on a

$$F(s_1, ..., s_n) - G(s_1, ..., s_n)\, y^{q-1} = 0. \tag{4.2.2}$$

Mais y n'est certainement pas nul: sinon, on aurait $F(s_1, ..., s_n) = 0$, donc (F étant normique) $s_1 = ... = s_n = 0$, donc (les S_i étant eux-mêmes normiques) $x_{11} = ... = x_{nq} = 0$, et en définitive $(x_{11}, ..., x_{nq}, y) = (0, ..., 0, 0)$ dans k^{nq+1}, ce qui est exclu par hypothèse. Or, cette propriété $(y \neq 0)$ implique $y^{q-1} = 1$; il résulte alors de (4.2.2) que $(s_1, ..., s_n)$ est une solution de (4.2.1) dans k^n, et le théorème 4 est démontré.

COROLLAIRE 1. — *Soit $F \in k[X]$ un polynôme normique. Alors, quel que soit $a \in k$, l'équation $F(X) = a$ admet au moins une solution dans k^n. Autrement dit, la fonction polynomiale associée à un polynôme normique est surjective.*

Si on applique ce corollaire 1 au polynôme P défini par (4.1.1) (sect. 4.1), on retrouve le fait, démontré différemment au chapitre 1, que la norme relative à l'extension K/k est surjective.

4.3. Terminons ce paragraphe en montrant que l'inégalité $N \geqslant q^{n-d}$ du théorème 3 est la meilleure possible; de façon précise: *quels que soient n, et $d < n$, il existe un polynôme $F \in k[X]$, de degré d, et tel que l'équation $F = 0$ admette exactement q^{n-d} solutions dans k^n.* En effet, soit P un polynôme normique de degré d (donc à d variables) sur k (l'existence d'un tel P est assurée par l'exemple de la section 4.1, avec d au lieu de n); posons alors $F(X_1, ..., X_n) = P(X_1, ..., X_d)$ (les variables $X_{d+1}, ..., X_n$ ne figurent donc pas dans F); pour que $F(\mathbf{x}) = 0$ ($\mathbf{x} \in k^n$), il est évidemment nécessaire et suffisant que les d premières composantes de $\mathbf{x}$ soient nulles; mais les points $\mathbf{x}$ de k^n possédant cette propriété sont exactement en nombre q^{n-d}, et l'assertion ci-dessus se trouve démontrée. Remarquons qu'un raisonnement analogue permet d'ailleurs plus généralement de prouver le résultat suivant:

THÉORÈME 5. — *Soit $F \in k[X]$ un polynôme à n variables, et soit N le nombre de zéros de F dans k^n. Si m variables seulement figurent explicitement dans F, alors N est divisible par q^{n-m}.*

Notes sur le chapitre 3

§ **1**: le théorème de Chevalley-Warning a une histoire intéressante. En 1933, Tsen avait prouvé que le corps $K = C(T)$ des fractions rationnelles à une variable T sur un corps algébriquement clos C possède la propriété (B_0) (autrement dit, a un groupe de Brauer nul: Tsen (1933)); Artin nota que la démonstration de Tsen consistait: (1) à prouver que K possède la propriété (C_1); puis (2) à déduire directement la propriété (B_0) de la propriété (C_1), sans utiliser la définition particulière de K; comme les corps finis possèdent la propriété (B_0) (théorème de Wedderburn !) et que par ailleurs ils « ne sont pas trop loin » de leur clôture algébrique (chap. 1, § 1), Artin fut amené à conjecturer que les corps finis possèdent la propriété (C_1); ce qui fut aussitôt démontré en caractéristique 2 par Völsch, puis en caractéristique quelconque par Chevalley, sous une forme d'ailleurs plus forte que celle prévue par Artin (Chevalley (1935)); c'est Warning qui, examinant la démonstration de Chevalley, s'aperçut que, pour les corps finis, la « bonne » propriété n'était pas la propriété (C_1), mais la divisibilité de N par p (Warning (1935)): d'où finalement le nom de « théorème de Chevalley-Warning » attribué au théorème 1. Ce théorème a d'ailleurs été amélioré par Ax (1964), qui a prouvé ceci (mêmes notations que dans le th. 1): si b est le plus grand entier strictement inférieur à n/d, N est divisible par q^b (donc par p^{fb}). Ce résultat d'Ax a lui-même été perfectionné récemment par Katz (1971); à ce sujet, voir le chapitre 7.

Indiquons que l'étude de la propriété (C_1) (et plus généralement de la propriété (C_r)) a été reprise systématiquement dans les années cinquante par Lang (1952) et Nagata (1957) et a connu depuis lors des développements importants; à ce sujet, voir [7], ainsi que Terjanian (1972). Signalons par ailleurs qu'il existe des corps possédant la propriété (B_0), « très proches » de leur clôture algébrique (de façon précise, quasi-finis), et ne possédant pourtant pas la propriété (C_1), ni même la propriété (C_r), si grand que soit r: voir Ax (1965, a, b; 1968).

§ **2**: le calcul modulo p de N par la formule (2.2.2) est parfois baptisé « méthode de Kronecker » ou « méthode de Lebesgue » (voir Lebesgue (1837, I), th. 1); pour des généralisations de cette formule, voir Dwork (1960, a; 1966, b); voir également les chapitres 7 et 9.

§ **3** et **4**: comme indiqué dans le texte, les théorèmes 3 et 4 sont dus respectivement à Warning (1935) et Terjanian (1966). Pour des résultats analogues au théorème 5 (mais moins triviaux !), voir Carlitz (1953, b; 1954, b), et Redei (1946).

CHAPITRE 4

ÉQUATIONS DIAGONALES (I)

Une équation *diagonale* est une équation de la forme $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$; si $d_1 = \ldots = d_n$, l'équation est (abusivement) dite *homogène*; ce chapitre est consacré à l'existence de solutions d'équations diagonales homogènes (§ 1) puis quelconques (§ 3) sur un corps fini k; le paragraphe 2 résout le « problème de Waring » pour k, ce qui revient, pour un exposant d fixé, à déterminer les entiers n et les éléments b de k tels que l'équation $X_1^d + \ldots + X_n^d = b$ admette une solution sur k; enfin, le paragraphe 4 donne quelques indications sur les équations *multilinéaires* (pour une définition, voir sect. 4.1), avec une application aux équations diagonales homogènes de degré 2.

Les méthodes utilisées dans ce chapitre sont très élémentaires: les résultats obtenus sont en conséquence assez pauvres (et aussi assez disparates); pour des résultats plus précis sur les équations diagonales (et notamment pour l'évaluation exacte ou approchée du nombre de solutions), se reporter au chapitre 6; voir également les Notes en fin de chapitre. On conserve ici les conventions en vigueur dans les chapitres 2 et 3; en particulier, k désigne toujours un corps fini à $q = p^f$ éléments.

§ 1. *Equations diagonales homogènes.*

1.1. Si $F \in k[X]$ est une forme (c'est-à-dire un polynôme homogène) de degré $d \geqslant 1$, il est clair que $F(0, \ldots, 0) = 0$; s'il existe un point $\mathbf{x}$ de k^n autre que $(0, \ldots, 0)$ tel que $F(\mathbf{x}) = 0$, on dit que F est *isotrope* sur k, ou que F *représente (proprement)* 0 *sur* k. Si d'autre part a est un élément non nul de k, et s'il existe un point $\mathbf{x}$ de k^n tel que $F(\mathbf{x}) = a$, on dit que F représente a sur k; par homogénéité, F représente alors tout élément de la forme ab^d ($b \in k^*$); F représente donc en fait toute la classe de a (mod k^{*d}) dans le groupe multiplicatif k^*.

THÉORÈME 1. — *Soit* $F = a_1 X_1^d + \ldots + a_n X_n^d \in k[X]$ *une forme diagonale de degré* $d \geqslant 1$, *à* n *variables. Si* F *n'est pas isotrope, elle représente au moins* n *classes de* k^* (mod k^{*d}).

Démonstration. — On procède par récurrence sur n. Si $n = 1$, F représente a_1 (qui n'est pas nul, puisque F est non isotrope): F représente donc une classe, celle de a_1. Supposons alors le théorème démontré pour $n - 1$ variables ($n \geqslant 2$) et prouvons-le pour n variables. Posons $G = a_1 X_1^d + \ldots + a_{n-1} X_{n-1}^d$; en tant que forme à $n - 1$ variables, G est non isotrope, et représente donc, par hypothèse de récurrence, au moins $n - 1$ classes (mod k^{*d}); soit C la réunion de ces classes. Comme toute classe représentée par G est a fortiori représentée par F, il suffit de prouver qu'il existe dans k^* un élément b n'appartenant pas à C, et cependant représenté par F. On distinguera deux cas:

(1) $a_n \notin C$: on peut alors prendre $b = a_n$.

(2) $a_n \in C$: il est clair dans ce cas que $-a_n \notin C$ (si G représentait $-a_n$, F serait isotrope). Soit alors m l'entier ainsi défini:

la forme $a_n(X_1^d + \ldots + X_m^d)$ ne représente que des éléments de C, mais la forme $a_n(X_1^d + \ldots + X_{m+1}^d)$ représente au moins un élément de k^* n'appartenant pas à C.

Un tel m existe effectivement; car si, pour tout $r \geqslant 1$, on pose $H_r = a_n(X_1^d + \ldots + X_r^d)$, on voit que H_1 représente uniquement $a_n k^{*d} \subset C$, mais que, pour r assez grand (par exemple, pour $r \geqslant p - 1$), H_r représente $-a_n \notin C$ (parce que $-1 = 1^d + \ldots + 1^d$ ($p - 1$ fois): k est de caractéristique p). Par définition de m, on peut trouver b appartenant à k^* mais non à C, et $y_1, \ldots, y_m, y_{m+1}$ appartenant à k, tels que

$$a_n(y_1^d + \ldots + y_m^d + y_{m+1}^d) = b\,, \tag{1.1.1}$$

mais que

$$a_n(y_1^d + \ldots + y_m^d) \in C\,.$$

Par définition de C, il existe alors $x_1, \ldots, x_{n-1}$ dans k tels que

$$a_1 x_1^d + \ldots + a_{n-1} x_n^d{}_{-1} = a_n(y_1^d + \ldots + y_m^d)\,.$$

Posons $x_n = y_{m+1}$ et ajoutons $a_n x_n^d$ aux deux membres de cette égalité; compte tenu de (1.1.1), on obtient

$$a_1 x_1^d + \ldots + a_n x_n^d = b\,,$$

et F représente bien $b \notin C$.
Ceci règle le deuxième cas et achève de prouver le théorème 1.

1.2. Le nombre total de classes de k^* (mod k^{*d}) est égal à $\delta = (q-1, d)$ (chap. 1, prop. 7, cor. 1); le théorème 1 admet donc les deux conséquences suivantes:

COROLLAIRE 1. — *Si* $F = a_1X_1^d + \ldots + a_nX_n^d$ *est non isotrope, et si* $n = \delta$, *alors* F *représente tout élément de* k.

COROLLAIRE 2. — *Si* $F = a_1X_1^d + \ldots + a_nX_n^d$ *est une forme diagonale de degré* d *à* n *variables et si* $n > \delta$, *alors* F *est certainement isotrope.*

1.3. La section 2.3 du chapitre 1 montre que, dans ce qui précède, on aurait pu remplacer partout d par δ, ou, ce qui revient au même, supposer que d divise $q-1$, et remplacer δ par d. Le corollaire 1 apparaît alors comme un cas particulier du théorème 4 du chapitre 3, et le corollaire 2, comme un cas particulier du théorème de Chevalley (chap. 3, th. 1, cor. 1). Quant au théorème 1, il admet l'interprétation « probabiliste » suivante: si $b \in k^*$, si $n \leqslant \delta$, et si le premier membre de l'équation $a_1X_1^d + \ldots + a_nX_n^d = b$ est une forme non isotrope, la « probabilité » pour que l'équation admette une solution dans k^n est au moins égale à n/δ.

Pour d'autres résultats sur les équations diagonales homogènes, voir les sections 2.3, 3.4, 4.3, et les Notes en fin de chapitre.

§ 2. *Sommes de puissances d-ièmes.*

2.1. Soient toujours k un corps fini à $q = p^f$ éléments, et d un entier $\geqslant 1$; notons k_d le sous-ensemble de k formé des sommes $x_1^d + \ldots + x_n^d$, avec $n \geqslant 1$ quelconque et $x_1, \ldots, x_n \in k$; k_d est évidemment un *sous-corps* de k: en effet, il est stable pour l'addition et la multiplication; il contient 0, 1, et aussi $-1 = 1^d + \ldots + 1^d$ ($p-1$ fois); enfin, si $x \in k_d$ et si $x \neq 0$, alors $x^{-1} \in k_d$, puisqu'on peut écrire $x^{-1} = x^{d-1}(x^{-1})^d$, que $(x^{-1})^d \in k_d$, et que k_d est stable pour la multiplication.

2.2. Le théorème ci-dessous détermine explicitement k_d:

THÉORÈME 2. — *Etant donné* $k = \mathbf{F}_q$ *et* d, *posons toujours* $\delta = (q-1, d)$, *et notons d'autre part* q_1 *la plus petite puissance* p^g *de* p *telle que* (1) g *divise* f; (2) *le quotient* $(p^f-1)/(p^g-1)$ *divise* d. *Alors:*

(i) k_d *est égal à l'unique sous-corps de* k *contenant* q_1 *éléments (ce qu'on peut écrire* $k_d = \mathbf{F}_{q_1}$).

(ii) *Tout élément de* k_d *est somme d'au plus* δ *puissances d-ièmes.*

Démonstration. — (i) k^* est un groupe cyclique d'ordre $q-1$, et ses sous-groupes correspondent bijectivement aux diviseurs positifs de $q-1$; par ailleurs, k étant un corps à p^f éléments, ses sous-corps correspondent bijectivement aux diviseurs positifs de f (chap. 1, prop. 4). Comme g divise f si et seulement si p^g-1 divise p^f-1 (petit exercice d'arithmétique), on peut énoncer:

LEMME 1. — *Pour qu'un sous-groupe H de k^* soit le groupe multiplicatif d'un sous-corps de k, il faut et il suffit que l'ordre de H soit de la forme p^g-1, g étant un diviseur de f.*

Mais le groupe k^{*d} est d'ordre $(q-1)/\delta$ (chap. 1, prop. 7); d'autre part, k_d est évidemment le plus petit sous-corps l de k tel que $k^{*d} \subset l^*$; si alors on pose $k_d = \mathbf{F}_{q_1}$, $q_1 = p^{f_1}$, le lemme 1 montre que f_1 est le plus petit diviseur positif g de f tel que $(q-1)/\delta$ divise p^g-1, c'est-à-dire (puisque $\delta = (q-1, d)$ et que $q = p^f$) tel que $(p^f-1)/(p^g-1)$ divise d, C.Q.F.D.

(ii) Pour tout $n \geqslant 1$, notons S_n l'ensemble des éléments de k^* qui sont de la forme ${x_1}^d + \ldots + {x_n}^d$ (les $x_i \in k$, certains x_i pouvant être nuls); il est clair que

$$(2.2.1) \qquad k^{*d} = S_1 \subset S_2 \subset \ldots \subset S_n \subset S_{n+1} \subset \ldots \subset {k_d}^*,$$

et que, dans k^*, chaque S_n est réunion d'un certain nombre de classes (mod k^{*d}); comme le nombre total de ces classes est égal à δ, la suite (2.2.1) comporte au maximum $\delta - 1$ inclusions strictes. D'autre part, il est évident que si, pour une valeur n_0 de l'indice, on a $S_{n_0} = S_{n_0+1}$, alors, pour tout $n \geqslant n_0$, on a également $S_n = S_{n+1}$; dans la suite (2.2.1), les inclusions strictes occupent donc nécessairement les premières places. Il résulte de ces deux remarques qu'à partir du rang δ, toutes les inclusions de la suite (2.2.1) sont en fait des égalités, et que ${k_d}^* = S_\delta$, C.Q.F.D.

2.3. Tirons les conséquences de ce théorème. Tout d'abord, pour d fixé, on a « le plus souvent » $k_d = k$; en effet, il résulte de la définition de q_1 que si $k_d \neq k$, alors $p^{f/2} < d$, ou encore $q < d^2$; en particulier:

COROLLAIRE 1. — *Pour d fixé, il n'existe qu'un nombre fini de corps k tels que $k_d \neq k$.*

Supposons maintenant k fixé. Si $f = 1$, donc si $k = \mathbf{F}_p$, on a évidemment $k_d = k$ quel que soit d. En revanche, si $f \geqslant 2$, on peut toujours trouver d tel que $k_d \neq k$, par exemple $d = p^{f-1} + \ldots + p + 1$: le théorème 2, (i) donne alors $f_1 = 1$ et $q_1 = p$, donc $k_d = \mathbf{F}_p$ (ce qui est évident direc-

tement, puisque, pour tout $x \in k$, x^d est dans ce cas la norme de x dans l'extension $k/\mathbf{F}_p$: chap. 1, sect. 3.3). Ainsi:

COROLLAIRE 2. — *Soit* $k = \mathbf{F}_q$, $q = p^f$. *Si* $f \geqslant 2$, *il existe au moins un exposant* d *tel que* $k_d \neq k$.

(Il en existe même une infinité: car si d est tel que $k_d \neq k$, la même propriété est vraie pour tout multiple de d; mais ceci n'a pas grande signification, car d intervient en réalité par l'intermédiaire de $\delta = (q-1, d)$, qui ne peut prendre qu'un nombre fini de valeurs).

Supposons toujours k fixé, avec $f \geqslant 2$, et soit d un entier tel que $k_d \neq k$; avec les notations du théorème 2, on a $k_d = \mathbf{F}_{q1}$; si $b \in k^*$, on aura donc $b \in k_d$ si et seulement si $b^{q1-1} = 1$; les parties (i) et (ii) du théorème donnent alors:

COROLLAIRE 3. — *Si* $b^{q1-1} = 1$, *et si* $n \geqslant \delta$, *l'équation diagonale* $X_1^d + \ldots + X_n^d = b$ *admet une solution dans* k^n.

(ii) *Si au contraire* $b^{q1-1} \neq 1$, *alors, si grand que soit* n, *l'équation* $X_1^d + \ldots + X_n^d = b$ *n'admet aucune solution dans* k^n.

Exemple: $k = \mathbf{F}_4$, $d = 3$; on a $k_d = \mathbf{F}_2 \neq k$; si $b \in \mathbf{F}_4$, $b \neq 0, 1$, l'équation $X_1^3 + \ldots + X_n^3 = b$ n'a pas de solution sur $\mathbf{F}_4$, si grand que soit le nombre d'inconnues, n.

§ 3. *Equations diagonales quelconques.*

3.1. Passons maintenant aux équations diagonales quelconques, donc de la forme $F = b$, avec

$$F = a_1 X_1^{d1} + \ldots + a_n X_n^{dn},$$

les $d_i \geqslant 1$, les $a_i \in k$ (on les supposera tous différents de zéro, ce qui ne diminue pas la généralité) et $b \in k$ (et éventuellement nul). Désignons par N le nombre de solutions de l'équation $F = b$ dans k^n, et par $\overline{N}$ le reste de division de N par p (ou encore, l'élément $N.1$ de $k = \mathbf{F}_q$). Enfin, pour simplifier les calculs, posons $\delta_i = (q-1, d_i)$ $(i=1, \ldots, n)$, puis

$$\Phi = a_1 X_1^{\delta 1} + \ldots + a_n X_n^{\delta n},$$

$a_0 = -b$, et $G = a_0 + \Phi$. Il est clair alors que le nombre de solutions dans k^n de l'équation $G = 0$ est égal au nombre de solutions dans k^n de $F = b$, donc à N (voir chap. 1, sect. 2.3; bien entendu, les *ensembles* de

solutions de ces deux équations sont en général distincts). En outre, dans le polynôme G, chaque exposant divise $q-1$.

3.2. On peut alors évaluer N par la « méthode de Lebesgue » (chap. 3, § 2 et Notes). On a en effet (loc. cit.)

$$(3.2.1) \qquad \overline{N} = \sum_{\mathbf{x}\in k^n} (1 - G(\mathbf{x})^{q-1}) = -\sum_{\mathbf{x}\in k^n} G(\mathbf{x})^{q-1}.$$

Ecrivons $G(\mathbf{x}) = a_0 + a_1 x_1^{\delta_1} + \ldots + a_n x_n^{\delta_n}$, et développons $G(\mathbf{x})^{q-1}$; il vient

$$(3.2.2) \qquad N = -\sum_{\mathbf{x}\in k^n} \sum_{\mathbf{j}} \binom{q-1}{\mathbf{j}} a_0^{j_0} a_1^{j_1} \ldots a_n^{j_n} x_1^{\delta_1 j_1} \ldots x_n^{\delta_n j_n},$$

la seconde sommation portant sur l'ensemble des vecteurs entiers $\mathbf{j} = (j_0, \ldots, j_n)$ tels que (1) $j_i \geqslant 0$ pour $i = 0, \ldots, n$; (2) $j_0 + \ldots + j_n = q-1$, et le symbole $\binom{q-1}{\mathbf{j}}$ désignant le « coefficient multinomial » $(q-1)!/j_0! \ldots j_n!$ Mais (chap. 3, sect. 2.1) on a $\sum_{x\in k} x^u = -1$ si $u > 0$ et si $q-1$ divise u, et $\sum_{x\in k} x^u = 0$ sinon; ceci permet de simplifier la formule (3.2.2) et d'énoncer:

LEMME 2. — *Soit J l'ensemble des vecteurs entiers $\mathbf{j} = (j_0, \ldots, j_n)$ tels que*

(1) $j_0 \geqslant 0$, $j_i > 0$ *pour* $i = 1, \ldots, n$;

(2) $j_0 + j_1 + \ldots + j_n = q-1$;

(3) $(q-1)/\delta_i$ *divise* j_i *pour* $i = 1, \ldots, n$;

alors $\overline{N}$ est donné par la formule

$$(3.2.3) \qquad \overline{N} = (-1)^{n+1} \sum_{\mathbf{j}\in J} \binom{q-1}{\mathbf{j}} a_0^{j_0} a_1^{j_1} \ldots a_n^{j_n}.$$

3.3. Première conséquence de ce lemme:

THÉORÈME 3. — *Si les entiers δ_i satisfont à la condition*

$$(H1) \qquad 1/\delta_1 + \ldots + 1/\delta_n > 1,$$

le nombre N de solutions de $F = b$ dans k^n est divisible par p.

Démonstration. — Si la condition (H1) est vérifiée, l'ensemble J défini dans le lemme 2 est vide, et on a bien $\overline{N} = 0$.

Ce théorème montre notamment que si les exposants de F satisfont à la condition

(*H2*) $\quad 1/d_1 + \ldots + 1/d_n > 1,$

le nombre N est divisible par p. Si $d_1 = \ldots = d_n = d$ (cas homogène), (H2) se réduit à l'inégalité $n > d$, et on retombe sur un cas particulier du théorème de Chevalley-Warning (chap. 3, th. 1). En revanche, dans le cas non homogène, la condition (H2) peut être réalisée en même temps que l'inégalité $n \leqslant d$:

Exemple: des équations diagonales telles que

$$X_1^2 + X_2^3 + X_3^5 + 1 = 0\,; \qquad X_1^2 + X_2^3 + X_3^6 + X_4^6 = 0\,,$$

ont, sur un corps fini quelconque k, un nombre de solutions divisible par la caractéristique p de k (ce nombre est d'ailleurs non nul, donc $\geqslant p$, car la première équation a pour solution $(1, -1, 0)$, la seconde, $(1, -1, 0, 0)$); or, pour la première équation, $n = 3 \leqslant d = 5$; pour la seconde, $n = 4 \leqslant d = 6$.

3.4. Autre conséquence du lemme 2:

THÉORÈME 4. — *Supposons réalisées les deux conditions suivantes :*

(H3) $\quad 1/\delta_1 + \ldots + 1/\delta_n = 1;$

(H4) *Chaque* $\delta_i\ (1 \leqslant i \leqslant n)$ *divise* $p - 1$.

Alors, quel que soit $b \in k$, *l'équation* $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$ *admet au moins une solution dans* k^n.

Démonstration. — Avec les notations des sections 3.1 et 3.2, il suffit de prouver que, dans le lemme 2, $\overline{N} \neq 0$. Mais la condition (H3) entraîne que J est réduit au seul élément $\mathbf{h} = (0, h_1, \ldots, h_n)$, avec $h_i = (q-1)/\delta_i$ pour $i = 1, \ldots, n$; le lemme donne donc

$$\overline{N} = (-1)^{n+1} \binom{q-1}{\mathbf{h}} a_1^{h_1} \ldots a_n^{h_n}\,;$$

comme les a_i ont été supposés non nuls, il reste à prouver que, sous l'hypothèse (H4), le coefficient $\binom{q-1}{\mathbf{h}}$ n'est pas divisible par p, ou encore, v_p désignant la valuation p-adique, que

$$v_p((q-1)!) = v_p(h_1!) + \ldots + v_p(h_n!)\,;$$

mais ceci résulte facilement de l'estimation bien connue

$$v_p(m!) = [m/p] + [m/p^2] + \ldots$$

valable pour tout entier $m \geqslant 1$ (la notation [...] signifie: partie entière de ...; cette estimation se déduit immédiatement de l'écriture de m en base p).

Dans le cas homogène, le théorème 4 peut s'énoncer:

THÉORÈME 5. — *Soit* $F = a_1 X_1^d + \ldots + a_n X_n^d$ *une forme diagonale homogène de degré d à n variables ; posons* $\delta = (q-1, d)$ *; alors, si* $n = \delta$, *et si* δ *divise* $p - 1$, *la forme F représente tout élément non nul de k.*

Ce résultat étend le théorème 2 à des formes F non isotropes; signalons que le théorème 5 reste vrai si on remplace l'hypothèse (H4) par l'hypothèse plus faible: $\delta \leqslant p - 1$ (voir Schwarz (1950)); en revanche, si $\delta \geqslant p$, le théorème 5 peut tomber en défaut: ainsi, dans l'exemple donné à la fin du paragraphe 2, la forme $X_1^3 + X_2^3 + X_3^3$ sur $k = \mathbf{F}_4$ (avec $n = d = \delta = q - 1 = 3$) représente seulement les éléments de $\mathbf{F}_2$; et de fait, $\delta = 3 \geqslant p = 2$.

Notons enfin que si $q = p$, les conditions: δ_i divise $p - 1$, δ divise $p - 1$, sont automatiquement vérifiées: sur un corps fini *premier*, les théorèmes 4 et 5 sont donc valables sans restriction.

§ 4. *Equations multilinéaires.*

4.1. Soit toujours k un corps fini à $q = p^f$ éléments, soient r et d deux entiers $\geqslant 1$, et soit $n = rd$. On se propose dans cette section de calculer le nombre $N(F, b)$ de solutions dans k^n de l'équation $F = b$ $(b \in k)$, le polynôme F étant de la forme

$$(4.1.1) \qquad F = a_1 X_1 \ldots X_d + a_2 X_{d+1} \ldots X_{2d} + \ldots + a_r X_{n-d+1} \ldots X_n$$

(un tel polynôme est parfois dit abusivement *multilinéaire*). Il est clair qu'on peut supposer tous les a_j non nuls (chap. 3, th. 5) et qu'on peut même (quitte éventuellement à multiplier les deux membres de l'équation par b^{-1}, et à faire une « homothétie » sur certaines variables) supposer $a_1 = \ldots = a_r = 1$, et $b = 0$ ou 1. On est ainsi ramené à calculer les nombres de solutions dans k^n des deux équations $F_{r,d} = 0$ et $F_{r,d} = 1$, avec

$$(4.1.2) \qquad F_{r,d} = X_1 \ldots X_d + X_{d+1} \ldots X_{2d} + \ldots + X_{n-d+1} \ldots X_n ,$$

nombres qu'on notera respectivement $N(r, d)$ et $N_1(r, d)$.

4.2. THÉORÈME 6. — *Les nombres* $N(r, d)$ *et* $N_1(r, d)$ *sont donnés par*

$$(4.2.1) \qquad N(r, d) = q^{n-1} + (q-1)\, q^{r-1} A(q, d)^r ,$$

$$(4.2.2) \qquad N_1(r, d) = q^{n-1} - q^{r-1} A(q, d)^r ,$$

avec par définition $A(q, d) = q^{d-1} - (q-1)^{d-1}$.

Démonstration. — On établit les deux formules *simultanément* par récurrence sur l'entier r. Si $r = 1$, et donc $n = d$, on voit directement que $N(1, d) = q^n - (q-1)^n$, et que $N_1(1, d) = (q-1)^{n-1}$, ce qui coïncide bien avec les valeurs données dans ce cas par (4.2.1) et (4.2.2). Supposons alors ces formules prouvées jusqu'à un entier $r - 1 \geqslant 1$, et démontrons-les pour l'entier r. En classant les solutions de l'équation $F_{r,d} = 0$ selon la valeur prise par le monôme $X_{n-d+1} \ldots X_n$, on obtient

$$\begin{aligned} N(r, d) &= \sum_{c \in k} N(F_{r-1,d}, c)\, N(F_{1,d}, -c) \\ &= N(r-1, d)\, N(1, d) + (q-1)\, N_1(r-1, d)\, N_1(1, d) \end{aligned}$$

(voir sect. 4.1). L'hypothèse de récurrence donne la valeur des quatre termes $N(r-1, d)$, $N(1, d)$, $N_1(r-1, d)$ et $N_1(1, d)$, et on vérifie, après calcul, que la valeur ainsi obtenue pour $N(r, d)$ coïncide bien avec celle fournie par (4.2.1). Raisonnement analogue pour (4.2.2). (On peut aussi déduire directement (4.2.2) de (4.2.1) en remarquant que, puisque toutes les équations $F_{r,d} = b$ ($b \in k^*$) ont même nombre de solutions, $N_1(r, d)$, on a évidemment $q^n = N(r, d) + (q-1)\, N_1(r, d)$).

Corollaire 1. — *Si, dans l'équation* $F = b$ *(voir* (4.1.1)*), les coefficients* a_j *sont tous différents de* 0 *(et si en outre, quand* $r = 1$, b *est également différent de* 0*), alors* $N(F, b)$ *est un polynôme en* q, *à coefficients entiers rationnels, de terme dominant* q^{n-1}. *En particulier, si on considère* q *comme « infiniment grand », on peut écrire*

$$N(F, b) = q^{n-1} + O(q^{n-2}).$$

On reviendra longuement sur ce genre de résultat aux chapitres 6, 7, 8 et 9.

4.3. Le théorème 6 permet en particulier de déterminer le nombre N de solutions dans k^n d'une équation diagonale homogène de degré 2,

$$a_1 X_1^2 + \ldots + a_n X_n^2 = b, \tag{4.3.1}$$

($a_1, \ldots, a_n, b \in k$); on peut naturellement supposer tous les coefficients a_i différents de 0; on peut également supposer $p \neq 2$ (en caractéristique 2, on a $N = q^{n-1}$); comme la détermination de N sera effectuée ultérieurement (chap. 6, sect. 1.3) par un autre procédé, on se bornera ici à indiquer la démarche du calcul, en laissant au lecteur le soin d'en expliciter les détails.

(1) Pour $n = 1$, on a évidemment $N = 1$ si $b = 0$; sinon, on a $N = 2$ ou 0 selon que $a_1 b \in k^{*2}$ ou que $a_1 b \notin k^{*2}$.

(2) Pour $n = 2$, on vérifie sans peine, soit par le calcul, soit par un raisonnement géométrique, que N est donné par les formules ci-dessous:

$$\text{pour } b = 0, N = \begin{cases} 2q - 1, \text{ si } -a_1 a_2 \in k^{*2}, \\ 1, \text{ si } -a_1 a_2 \notin k^{*2}; \end{cases}$$

$$\text{pour } b \neq 0, N = \begin{cases} q - 1, \text{ si } -a_1 a_2 \in k^{*2}, \\ q + 1, \text{ si } -a_1 a_2 \notin k^{*2}. \end{cases}$$

Supposons maintenant $n \geqslant 3$. Comme toute forme quadratique à trois variables ou plus sur k est isotrope (théorème de Chevalley: chap. 3, th. 1, cor. 1), la théorie générale de la réduction des formes quadratiques (voir [**17**], chap. IV, notamment pp. 60-62) montre qu'on peut (par une transformation linéaire inversible à coefficients dans k, ce qui n'affecte pas la valeur de N) mettre le premier membre de (4.3.1) sous l'une des deux formes suivantes:

$$(4.3.2) \qquad Y_1 Y_2 + \ldots + Y_{2r-1} Y_{2r} + a Y_n^2,$$

avec $n = 2r + 1$ et $a = (-1)^r a_1 \ldots a_n$, *si n est impair*;

$$(4.3.3) \qquad Y_1 Y_2 + \ldots + Y_{2r-1} Y_{2r} + Y_{n-1}^2 + a Y_n^2,$$

avec $n = 2r + 2$ et $a = (-1)^2 a_1 \ldots a_n$, *si n est pair.*
(La valeur de a s'obtient en écrivant l'invariance du discriminant).

(3) Calculons alors N quand n est *impair*, $n = 2r + 1$. En classant (comme dans la démonstration du théorème 6) les solutions de $F = b$ (F étant mis sous la forme (4.3.2)) suivant la valeur prise par le monôme aY_n^2, on obtient, avec les notations de la section 4.1,

$$(4.3.4) \qquad N = \sum_{c \in k,\, c \neq b} N_1(r, 2)\, N(aY_n^2, c) + N(r, 2)\, N(aY_n^2, b).$$

$N(r, 2)$ et $N_1(r, 2)$ sont donnés par le théorème 6, $N(aY_n^2, c)$ et $N(aY_n^2, b)$ sont donnés par (1); si on remarque que k^* contient $(q-1)/2$ carrés et autant de non-carrés, on arrive finalement à ceci:

$$\text{pour } b = 0, N = q^{n-1};$$

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

(4) Le calcul de N quand n est *pair* se fait de la même manière: on réécrit la formule (4.3.4) en y remplaçant aY_n^2 par Y_{n-1}^2, $+ aY_n^2$, on utilise le théorème 6 et les formules de (2), et on obtient finalement ceci:

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

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

Notes sur le chapitre 4

§ **1**: la méthode de démonstration du théorème 1 est empruntée à Demyanov (1956). Cette méthode s'applique également aux équations diagonales homogènes sur un corps p-adique; à ce sujet, voir également Schwarz (1956), Davenport-Lewis (1963), et surtout [7], pp. 101-138, et [**13**], pp. 17-22 et 40-52.

§ **2**: le théorème 3, (ii) et son corollaire 1 sont dus à Tornheim (1938); voir aussi Schwarz (1948, a). Pour l'application du théorème 3, (i) au problème de Waring dans un anneau d'entiers algébriques, voir Bateman-Stemmler (1962) pour un exposant d premier, et Joly (1968) pour un exposant d quelconque.

§ **3**: les théorèmes 4 et 5 sont dus à Morlaye (1971); voir également Schwarz (1948, b; 1950) et Carlitz (1956, b).

§ **4**: pour une autre démonstration du théorème 7, voir Porter (1966, e).

Les équations diagonales sur un corps fini ont suscité une vaste littérature; mentionnons seulement ici (en dehors des articles déjà cités, et de ceux qui le seront au chapitre 6) Cohen (1956), Chowla-Mann-Straus (1959), Gray (1960), Chowla (1961), Tietäväinen (1968), et Lewis (1960).

CHAPITRE 5

SOMMES DE GAUSS ET DE JACOBI

Le premier paragraphe de ce chapitre donne la description du groupe des caractères additifs et du groupe des caractères multiplicatifs d'un corps fini, et montre comment ces caractères peuvent servir au calcul du nombre de solutions d'une équation (prop. 3 et 5). Le reste du chapitre est consacré à une étude élémentaire des sommes de Gauss et de Jacobi; ces sommes sont des entiers algébriques, construits à l'aide de caractères, et dont l'utilisation, combinée avec les propositions 3 et 5, permettra notamment (1) de calculer le nombre de solutions d'une équation diagonale quelconque (chap. 6); (2) de calculer dans certains cas la fonction zêta de l'ensemble algébrique défini par une telle équation (chap. 9); (3) de démontrer le théorème d'Ax, c'est-à-dire la relation de divisibilité $q^b \mid N$ annoncée au chapitre 3 (chap. 7). Pour d'autres utilisations classiques des sommes de Gauss et de Jacobi (étude des corps cyclotomiques, démonstration élémentaire des lois de réciprocité, etc.), voir **[8]**, § 20, **[11]**, chap. IV, ou **[3]**, chap. 5; voir également les Notes en fin de chapitre.

On conserve ici encore les conventions et notations des chapitres précédents; en particulier, k désigne toujours un corps fini à $q = p^f$ éléments.

§ 1. *Caractères additifs et caractères multiplicatifs d'un corps fini.*

1.1. Rappelons que si G est un groupe fini commutatif, on appelle *caractère* de G tout homomorphisme $\chi: G \to \mathbf{C}^*$, de G dans le groupe multiplicatif du corps des nombres complexes; les caractères de G forment de manière naturelle un groupe multiplicatif, dit *dual* de G, et noté $\widehat{G}$ (ou $X(G)$); l'élément neutre de G est le caractère ε défini par $\varepsilon(x) = 1$ pour tout $x \in G$: on l'appelle *caractère trivial* (ou *principal*); si $x \in G$, si $\chi \in \widehat{G}$, et si m désigne l'ordre de G, on a $\chi(x)^m = \chi(x^m) = \chi(e) = 1$ (e désignant l'élément neutre de G); les valeurs d'un caractère χ de G sont donc des racines m-ièmes de l'unité; en particulier, si χ^{-1} est l'inverse de χ dans G, et si $x \in G$, alors $\chi^{-1}(x) = \overline{\chi(x)}$ (complexe conjugué de $\chi(x)$): c'est pour-

quoi le caractère χ^{-1} est généralement noté $\bar{\chi}$, et appelé *caractère conjugué* de χ.

On aura besoin par la suite des deux résultats suivants (pour des démonstrations, d'ailleurs immédiates, voir [**17**], pp. 103-107):

(i) *Les groupes G et $\widehat{G}$ sont isomorphes (non canoniquement) ; en particulier, $\widehat{G}$ a même ordre que G.*

(ii) (Relations d'orthogonalité). — *Si χ est un caractère de G, on a*

$$\sum_{x \in G} \chi(x) = \begin{cases} \mathrm{card}(G), & si\ \chi = \varepsilon ; \\ 0, & si\ \chi \neq \varepsilon . \end{cases} \tag{1.1.1}$$

De même, si x est un élément de G, on a

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} \mathrm{card}(G), & si\ x = e ; \\ 0, & si\ x \neq e . \end{cases} \tag{1.1.2}$$

On va appliquer ce qui précède au groupe additif k^+ de k (sect. 1.2), puis au groupe multiplicatif k^* (sect. 1.3); $\widehat{k^+}$ sera dit *dual additif* de k, et $\widehat{k^*}$, *dual multiplicatif;* les éléments de $\widehat{k^+}$ et de $\widehat{k^*}$ seront qualifiés respectivement de *caractères additifs* et de *caractères multiplicatifs* de k.

1.2. Commençons par l'étude des caractères additifs; on peut en construire de la manière suivante: soit Tr l'application trace relative à l'extension $k/\mathbf{F}_p$, et soit ζ une racine primitive p-ième de l'unité dans $\mathbf{C}$ (par exemple $e^{2\pi i/p}$); pour tout élément x de k, posons

$$\beta(x) = \zeta^{Tr(x)} \tag{1.2.1}$$

(ce qui a un sens, puisque $Tr(x) \in \mathbf{F}_p$ est un entier rationnel modulo p); alors β est évidemment un caractère additif de k, et ce caractère n'est pas trivial (parce que la trace est surjective: chap. 1, prop. 9). Plus généralement, si $y \in k$, et si on pose $\beta_y(x) = \beta(xy)$ $(x, y \in k)$, β_y est un caractère additif de k, et ce caractère n'est trivial que si $y = 0$.

Il se trouve que le procédé ci-dessus fournit *tous* les caractères additifs de k; de façon précise:

PROPOSITION 1. — *Soit β un caractère additif non trivial de k (par exemple celui défini par (1.2.1)) et, pour tout x et tout y dans k, posons*

(1.2.2) $$\beta_y(x) = \beta(xy).$$

Alors l'application $y \mapsto \beta_y$ *est un isomorphisme du groupe additif* k^+ *sur son dual* $\widehat{k^+}$.

Démonstration. — Cette application est évidemment un homomorphisme de groupes; compte tenu de la propriété (i) (sect. 1.1), il suffit de prouver que cet homomorphisme est injectif; mais par hypothèse, β est non trivial; il existe donc $a \in k$ tel que $\beta(a) \neq 1$; soit alors $y \in k$, $y \neq 0$; si on pose $x = ay^{-1}$, on a évidemment $\beta_y(x) = \beta(a) \neq 1$, donc $\beta_y \neq \varepsilon$, C.Q.F.D.

PROPOSITION 2. — *Soient* β *un caractère additif non trivial de* k *et* a *un élément quelconque de* k. *Alors*

(1.2.3) $$\sum_{y \in k} \beta(ay) = \begin{cases} q, & si\ a = 0; \\ 0, & si\ a \neq 0. \end{cases}$$

Démonstration. — (1.2.3) résulte, soit de (1.1.1) appliqué au caractère fixe β_a et à l'élément y parcourant k^+, soit de (1.1.2) appliqué à l'élément fixe a et au caractère β_y parcourant $\widehat{k^+}$.

1.3. La proposition 2 donne un moyen de compter les solutions d'une équation polynomiale:

PROPOSITION 3. — *Soit* F *un polynôme à* n *variables et à coefficients dans* k. *Si* β *désigne un caractère additif non trivial de* k, *le nombre* N *de solutions dans* k^n *de l'équation* $F = 0$ *est donné par*

(1.3.1) $$N = q^{-1} \sum_{y,\, \mathbf{x}} \beta\big(yF(x_1, \ldots, x_n)\big),$$

la sommation étant étendue à tous les points $(y, x_1, \ldots, x_n)$ *de* k^{n+1}.

Démonstration. — Soit $V \subset k^n$ l'ensemble des solutions de $F = 0$. Si $\mathbf{x} \in V$, donc si $F(\mathbf{x}) = 0$, (1.2.3), appliqué à $a = F(\mathbf{x})$, donne

$$\sum_{y \in k} \beta\big(yF(\mathbf{x})\big) = q,$$

et par conséquent

(1.3.2) $$\sum_{\mathbf{x} \in V} \sum_{y \in k} \beta\big(yF(\mathbf{x})\big) = qN.$$

Si au contraire $\mathbf{x} \notin V$, donc si $F(\mathbf{x}) \neq 0$, (1.2.3) donne

$$\sum_{y \in k} \beta(yF(\mathbf{x})) = 0 ;$$

donc

$$\sum_{\mathbf{x} \in V} \sum_{y \in k} \beta(yF(\mathbf{x})) = 0 . \tag{1.3.3}$$

Il suffit alors d'additionner (1.3.2) et (1.3.3) et de multiplier les deux membres par q^{-1} pour obtenir la formule (1.3.1). Cette formule sera utilisée systématiquement aux chapitres 6, 7 et 9.

1.4. Passons à l'étude des caractères multiplicatifs de k. Notons d'abord que si $\chi : k^* \to \mathbf{C}^*$, est un tel caractère, sa valeur en 0 n'est pas définie; pour des raisons de commodité, on conviendra *toujours* de prolonger χ en une application $k \to \mathbf{C}^*$, en posant

$$\chi(0) = \begin{cases} 1 , \text{ si } \chi = \varepsilon ; \\ 0 , \text{ si } \chi \neq \varepsilon . \end{cases} \tag{1.4.1}$$

Avec cette convention, on a $\chi(xy) = \chi(x)\chi(y)$ quels que soient $x, y \in k$.

D'autre part, on peut construire un caractère multiplicatif d'ordre $q - 1$ (donc un générateur de $\widehat{k^*}$: voir (i), sect. 1.1) de la façon suivante: soit ω une racine primitive $(q-1)$-ième de l'unité dans $\mathbf{C}$ (par exemple $e^{2\pi i/(q-1)}$), et soit g un générateur du groupe cyclique k^*; pour tout $x \in k^*$, il existe $i \in \mathbf{Z}$ tel que $x = g^i$; désignons par $\mathrm{ind}(x)$ la classe de i modulo $q - 1$ et posons

$$\theta(x) = \omega^{ind(x)} ; \tag{1.4.2}$$

alors θ est bien un caractère multiplicatif d'ordre $q - 1$ de k (c'est un isomorphisme de k^* sur le groupe des racines $(q-1)$-ièmes de l'unité dans $\mathbf{C}$).

Enfin, on a évidemment le résultat suivant:

PROPOSITION 4. — *Soit θ un caractère multiplicatif d'ordre $q - 1$ de k (par exemple celui défini par (1.4.2)). Alors l'application $h \mapsto \theta^h$ définit de manière naturelle un isomorphisme du groupe cyclique $\mathbf{Z}/(q-1)\mathbf{Z}$ sur le groupe $\widehat{k^*}$, dual de k^*.*

1.5. Soit maintenant χ un caractère multiplicatif quelconque de k, et soit δ l'ordre de χ (en tant qu'élément de $\widehat{k^*}$). Si $x \in k^*$, on a $\chi(x^\delta) =$

$\chi^\delta(x) = 1$, et χ est trivial sur $k^{*\delta}$; χ définit donc un caractère (qu'on notera encore χ) du groupe quotient $k^*/k^{*\delta}$; mais δ divise évidemment $q-1$, et ce quotient est d'ordre δ (chap. 1, prop. 7, cor. 1); ainsi, le sous-groupe (cyclique, d'ordre δ) de $\widehat{k^*}$ engendré par χ s'identifie au dual du groupe (cyclique, d'ordre δ) $k^*/k^{*\delta}$, et le noyau de χ est exactement $k^{*\delta}$.

Cela étant:

PROPOSITION 5. — *Soit d un entier $\geqslant 1$, et posons $\delta = (q-1, d)$. Soit d'autre part χ un caractère multiplicatif d'ordre δ de k (par exemple $\theta^{(q-1)/\delta}$, θ étant défini par (1.4.2)), et soit a un élément non nul de k. Alors:*

(i) *Pour que a soit une puissance d-ième dans k, il faut et il suffit que $\chi(a) = 1$.*

(ii) *Le nombre $m(a)$ de solutions dans k de l'équation à une variable $X^d = a$ est donné par*

$$m(a) = \sum_{j=0}^{\delta-1} \chi^j(a). \tag{1.5.1}$$

(iii) *Avec la convention (1.4.1), l'égalité (1.5.1) reste vraie pour $a = 0$.*

Démonstration. — La proposition 7 du chapitre 1 permet de supposer que $d = \delta$. (i) résulte alors du fait que le noyau de χ est $k^{*\delta}$. Prouvons (ii), et notons $\bar{a}$ la classe de a (mod $k^{*\delta}$); les relations d'orthogonalité (1.1.2), appliquées à $G = k^*/k^{*\delta}$, à $x = \bar{a}$, et aux caractères χ^j $(0 \leqslant j \leqslant \delta - 1)$ qui forment le dual de G (voir ci-dessus) donnent

$$\sum_{j=0}^{\delta-1} \chi^j(a) = \begin{cases} \delta, & \text{si } a \in k^{*\delta}; \\ 0, & \text{si } a \notin k^{*\delta}. \end{cases}$$

D'autre part, $m(a)$ vaut δ si $a \in k^{*\delta}$ (k^* contient δ racines δ-ièmes de l'unité) et 0 sinon; (ii) se trouve ainsi établi. Enfin (iii) est évident: car $m(0) = 1$, $\chi^0(0) = \varepsilon(0) = 1$, et $\chi^j(0) = 0$ pour $1 \leqslant j \leqslant \delta - 1$, puisque, pour ces valeurs de j, $\chi^j \neq \varepsilon$.

La formule (1.5.1) sera utilisée au chapitre 6. La partie (i) de la proposition 5 est essentiellement équivalente à l'extension du critère d'Euler donnée au chapitre 1 (prop. 7, cor. 2). Si d'ailleurs on suppose p (donc q) impair, et $d = 2$ (donc $\delta = 2$), le caractère χ de la proposition 5 est entièrement déterminé (il est égal à $\theta^{(q-1)/2}$); ce caractère vaut 1 sur les carrés de k^*, et -1 sur les non-carrés: on l'appelle *caractère de Legendre*; pour $q = p$, il coïncide évidemment avec le *symbole de Legendre*.

§ 2. *Sommes de Gauss.*

2.1. Soient χ un caractère multiplicatif et β un caractère additif de k.

DÉFINITION 1. — *On appelle* somme de Gauss *associée à χ et β la quantité*

$$\tau(\chi|\beta) = \sum_{x \in k^*} \chi(x)\beta(x). \tag{2.1.1}$$

Les valeurs prises par β et χ étant des racines p-ièmes de l'unité, et 0 ou des racines $(q-1)$-ièmes de l'unité, $\tau(\chi \mid \beta)$ est un entier du corps des racines $p(q-1)$-ièmes de l'unité.

Si le caractère β est fixé une fois pour toutes (par exemple, si $\beta(x) = \zeta^{Tr(x)}$, avec $\zeta = e^{2\pi i/p}$: sect. 1.2), on écrit $\tau(\chi)$ au lieu de $\tau(\chi \mid \beta)$, et (pour $y \in k$) $\tau_y(\chi)$ au lieu de $\tau(\chi \mid \beta_y)$ (sect. 1.2): on a donc

$$\tau_y(\chi) = \sum_{x \in k^*} \chi(x)\beta(xy). \tag{2.1.2}$$

2.2. Si l'un des caractères χ et β est trivial, la somme de Gauss associée est également « triviale » et sa valeur se calcule immédiatement à l'aide des relations d'orthogonalité (1.1.1) appliquées à χ ou à β:

(i) *si χ est trivial, mais non β, on a* $\tau(\chi \mid \beta) = -1$;

(ii) *si β est trivial, mais non χ, on a* $\tau(\chi \mid \beta) = 0$;

(iii) *enfin, si χ et β sont tous deux triviaux, on a* $\tau(\chi \mid \beta) = q - 1$.

2.3. Passons au cas non trivial. On suppose $\chi \neq \varepsilon$, on fixe une fois pour toutes un caractère additif non trivial β, et on met tous les caractères additifs non triviaux de k sous la forme β_y $(y \in k^*)$ (prop. 1); les sommes de Gauss non triviales associées à χ sont alors les $\tau_y(\chi)$ $(y \in k^*)$.

PROPOSITION 6. — *Si $\bar{\chi}$ désigne le caractère conjugué de χ (sect. 1.1), on a*

$$\tau_y(\chi) = \bar{\chi}(y)\tau(\chi). \tag{2.3.1}$$

Démonstration. — Puisque $y \neq 0$, l'application $x \mapsto xy$ est une permutation de k^*; il suffit alors d'écrire

$$\tau_y(\chi) = \sum_{x \in k^*} \chi^{-1}(y)\chi(xy)\beta(xy) = \bar{\chi}(y) \sum_{x \in k^*} \chi(xy)\beta(xy)$$

et de faire le changement de variable $z = xy$ pour obtenir (2.3.1).

PROPOSITION 7. — *On a (toujours pour $\chi \neq \varepsilon$)*

$$\tau(\chi)\tau(\bar{\chi}) = q\chi(-1). \tag{2.3.2}$$

Démonstration. — Par définition, $\tau(\chi)\tau(\bar{\chi}) = \sum_{x\in k^*}\sum_{y\in k^*}\chi(x)\bar{\chi}(y)\beta(x)\beta(y)$; mais $\chi(x)\bar{\chi}(y) = \chi(x)\chi^{-1}(y) = \chi(xy^{-1})$, et $\beta(x)\beta(y) = \beta(x+y)$. si on fait le changement de variables $(x, y) \mapsto (y, z)$ défini par $z = xy^{-1}$, on obtient donc

$$\tau(\chi)\tau(\bar{\chi}) = \sum_{y\in k^*}\sum_{z\in k^*}\chi(z)\beta\big(y(z+1)\big). \tag{2.3.3}$$

Le second membre se fractionne en deux sommes partielles correspondant respectivement à $z = -1$ et à $z \neq -1$; comme $\beta(0) = 1$, la première somme vaut $(q-1)\chi(-1)$; quant à la seconde, elle peut s'écrire

$$\sum_{z\neq -1}\chi(z)\sum_{y\in k^*}\beta\big(y(z+1)\big);$$

mais la proposition 2, appliquée à $a = z + 1$, montre que pour tout $z \neq -1$, la somme portant sur $y \in k^*$ vaut $-\beta(0) = -1$; par ailleurs, (1.1.1), appliqué au groupe k^* et au caractère χ, donne

$$\sum_{z\neq -1}\chi(z) = -\chi(-1);$$

la deuxième somme partielle vaut donc $\chi(-1)$; si alors on reporte dans (2.3.3) les valeurs des deux sommes partielles, on obtient

$$\tau(\chi)\tau(\bar{\chi}) = (q-1)\chi(-1) + \chi(-1),$$

c'est-à-dire (2.3.2).

PROPOSITION 8. — *On a (en supposant toujours $\chi \neq \varepsilon$)*

$$|\tau(\chi)|^2 = q. \tag{2.3.4}$$

Démonstration. — Par définition, $|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)}$; on peut donc écrire $|\tau(\chi)|^2 = \sum_{x\in k^*}\sum_{y\in k^*}\chi(x)\bar{\chi}(y)\beta(x)\beta(y)$; mais $\bar{\chi}(y) = \chi^{-1}(y) = \chi(y^{-1})$, et de même $\bar{\beta}(y) = \beta(-y)$; le terme général de la somme ci-dessus est alors égal à $\chi(xy^{-1})\beta(x-y)$, ou encore (en remplaçant y par $-y$, ce qui ne change pas la somme) à $\chi(-1)\chi(xy^{-1})\beta(x+y)$: la proposition 8 résulte donc de la proposition 7, et du fait que $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$.

§ 3. *Sommes de Jacobi à deux caractères.*

3.1. Soient maintenant χ et ψ deux caractères multiplicatifs du corps fini k.

DÉFINITION 2. — *On appelle* somme de Jacobi *associée à χ et ψ la quantité*

$$\pi(\chi, \psi) = \sum_{x \in k} \chi(x)\,\psi(1-x)\,. \tag{3.1.1}$$

Comme le second membre de (3.1.1) peut également s'écrire $\sum_{x+y=1} \chi(x)\,\psi(y)$ on voit que $\pi(\chi, \psi) = \pi(\psi, \chi)$. Il est clair d'autre part que $\pi(\chi, \psi)$ est un entier du corps des racines $(q-1)$-ièmes de l'unité.

3.2. Si l'un des deux caractères χ et ψ est trivial, la somme de Jacobi est également « triviale » et sa valeur se calcule immédiatement à l'aide des relations d'orthogonalité (1.1.1) et de la convention (1.4.1):

(i) *si* $\chi = \psi = \varepsilon$, *on a* $\pi(\chi, \psi) = q$;

(ii) *si* $\chi = \varepsilon$ *et* $\psi \neq \varepsilon$ *(ou l'inverse), on a* $\pi(\chi, \psi) = 0$.

3.3. Passons au cas non trivial.

PROPOSITION 9. — *Supposons χ et ψ non triviaux. Alors*

(i) *Si* $\chi\psi = \varepsilon$, *on a*

$$\pi(\chi, \psi) = -\chi(-1)\,. \tag{3.3.1}$$

(ii) *Si au contraire* $\chi\psi \neq \varepsilon$, *la somme de Jacobi* $\pi(\chi, \psi)$ *se calcule à l'aide des sommes de Gauss non triviales* $\tau(\chi)$, $\tau(\psi)$ *et* $\tau(\chi\psi)$ *par la formule*

$$\pi(\chi, \psi) = \tau(\chi)\,\tau(\psi)/\tau(\chi\psi)\,. \tag{3.3.2}$$

(Les trois sommes de Gauss figurant dans le membre de droite sont supposées calculées à l'aide d'un même caractère additif non trivial β de k).

Démonstration. — (i) Si $\chi\psi = \varepsilon$, on a $\psi = \chi^{-1}$, et on peut écrire

$$\pi(\chi, \psi) = \sum_{x \neq 0,\,1} \chi(x)\,\chi^{-1}(1-x) = \sum_{x \neq 0,\,1} \chi(x/(1-x))\,;$$

mais le quotient $y = x/(1-x)$ est une fonction homographique régulière de x, et quand x prend toute valeur possible dans k, sauf 0 et 1, y prend toute valeur possible dans k, sauf 0 et -1; ainsi, $\pi(\chi, \psi) = \sum_{y \in k^*} \chi(y)$

$-\chi(-1)$ et (3.3.1) résulte alors de (1.1.1) appliqué au caractère multiplicatif non trivial χ.

(ii) La définition des sommes de Gauss et la convention (1.4.1) permettent d'écrire

$$\tau(\chi)\tau(\psi) = \sum_{x\in k}\sum_{y\in k}\chi(x)\psi(y)\beta(x+y);$$

dans le second membre, faisons le changement de variables $(x, y) \mapsto (z, t)$ défini par $z = x + y$ et $tz = x$ (l'apparition de la valeur 0 n'est pas gênante, du fait que $\chi(0) = \psi(0) = 0$: on laisse au lecteur le soin d'examiner ce point en détail); il vient

$$\tau(\chi)\tau(\psi) = \sum_{z\in k}\sum_{t\in k}\chi(z)\chi(t)\psi(z)\psi(1-t)\beta(z),$$

ou encore

$$\tau(\chi)\tau(\psi) = \Big(\sum_{z\in k}(\chi\psi)(z)\beta(z)\Big)\Big(\sum_{t\in k}\chi(t)\psi(1-t)\Big),$$

c'est-à-dire finalement, puisque $(\chi\psi)(0) = 0$,

$$\tau(\chi)\tau(\psi) = \tau(\chi\psi)\pi(\chi, \psi),$$

C.Q.F.D.

COROLLAIRE 1. — *Si les trois caractères χ, ψ et $\chi\psi$ sont non triviaux, on a*

$$|\pi(\chi, \psi)|^2 = q. \tag{3.3.3}$$

Démonstration. — Utiliser la proposition 9, (ii), puis la proposition 8.

COROLLAIRE 2. — *Supposons toujours le caractère χ non trivial, et notons δ son ordre. On a alors*

$$\tau(\chi)^\delta = q\chi(-1)\pi(\chi, \chi)\pi(\chi, \chi^2)\ldots\pi(\chi, \chi^{\delta-2}). \tag{3.3.4}$$

Démonstration. — Pour $1 \leqslant j \leqslant \delta - 2$, la proposition 9, (ii) donne

$$\pi(\chi, \chi^j) = \tau(\chi)\tau(\chi^j)/\tau(\chi^{j+1});$$

en multipliant membre à membre ces $\delta - 2$ égalités, on obtient

$$\pi(\chi, \chi)\pi(\chi, \chi^2)\ldots\pi(\chi, \chi^{\delta-2}) = \tau(\chi)^{\delta-1}/\tau(\chi^{\delta-1});$$

mais $\chi^{\delta-1} = \chi^{-1} = \bar{\chi}$; il suffit alors de multiplier les deux membres de cette dernière égalité par $\tau(\chi)\tau(\bar{\chi}) = q\chi(-1)$ pour obtenir (3.3.4).

§ 4. *Sommes de Jacobi à n caractères.*

4.1. Soient n un entier $\geqslant 1$, et $\chi_1, ..., \chi_n$ n caractères multiplicatifs de k. Désignons par H l'ensemble des points $\mathbf{x} = (x_1, ..., x_n)$ de k^n tels que $x_1 + ... + x_n = 1$; c'est un hyperplan affine de k^n, et on a en particulier card $(H) = q^{n-1}$.

DÉFINITION 3. — *On appelle* somme de Jacobi *associée à* $\chi_1, ..., \chi_n$ *la quantité*

$$\pi(\chi_1, ..., \chi_n) = \sum_{\mathbf{x} \in H} \chi_1(x_1) ... \chi_n(x_n) . \tag{4.1.1}$$

C'est évidemment un entier du corps des racines $(q-1)$-ièmes de l'unité. Pour $n = 1$, on a $\pi(\chi_1) = 1$; pour $n = 2$, on retrouve les sommes de Jacobi à deux caractères étudiées au paragraphe précédent; dans ce qui suit, on pourra donc supposer $n \geqslant 3$.

4.2. Si un au moins des caractères χ_i est trivial, on a une somme de Jacobi « triviale » qui se calcule explicitement:

(i) *si tous les* χ_i *sont triviaux, on a* $\pi(\chi_1, ..., \chi_n) = q^{n-1}$;

(ii) *si la famille* χ_i *comporte au moins un caractère trivial et au moins un caractère non trivial, on a* $\pi(\chi_1, ..., \chi_n) = 0$.

(Prouvons cette dernière égalité, qui n'est pas absolument évidente: quitte éventuellement à renuméroter les caractères, on peut supposer $\chi_1 \neq \varepsilon, ..., \chi_m \neq \varepsilon$, mais $\chi_{m+1} = ... = \chi_n = \varepsilon$, avec $1 \leqslant m \leqslant n-1$; comme alors $\chi_{m+1}(y) = ... = \chi_n(y) = 1$ pour tout élément y de k, et que le système de $m+1$ équations linéaires

$$X_1 + ... + X_n = 1 , \quad X_1 = x_1, ..., \quad X_m = x_m ,$$

admet exactement q^{n-m-1} solutions dans k^n quels que soient les m éléments $x_1, ..., x_m$ de k, on voit que

$$\pi(\chi_1, ..., \chi_n) = q^{n-m-1} \Big(\sum_{x_1 \in k} \chi_1(x_1) \Big) ... \Big(\sum_{x_m \in k} \chi_m(x_m) \Big) ;$$

mais chacune des sommes du membre de droite est nulle (utiliser (1.1.1) et (1.4.1)); en définitive, on a donc bien $\pi(\chi_1, ..., \chi_n) = 0$, C.Q.F.D.)

4.3. Passons maintenant au cas non trivial.

PROPOSITION 10. — *Supposons* $\chi_i \neq \varepsilon$ *pour* $i = 1, ..., n$. *Alors*

(i) *Si* $\chi_1 \dots \chi_n = \varepsilon$, *on a*

$$\pi(\chi_1, ..., \chi_n) = \chi_n(-1)\pi(\chi_1, ..., \chi_{n-1}). \tag{4.3.1}$$

(ii) *Si au contraire* $\chi_1 \dots \chi_n \neq \varepsilon$, *la somme de Jacobi* $\pi(\chi_1, ..., \chi_n)$ *peut s'exprimer à l'aide de sommes de Gauss non triviales par la formule*

$$\pi(\chi_1, ..., \chi_n) = \tau(\chi_1) \dots \tau(\chi_n)/\tau(\chi_1 \dots \chi_n). \tag{4.3.2}$$

(Les $n + 1$ sommes de Gauss figurant dans le membre de droite sont supposées calculées à l'aide d'un même caractère additif non trivial β de k).

Démonstration. — (i) Ecrivons pour abréger $\pi = \pi(\chi_1, ..., \chi_n)$, et posons

$$\rho = \sum \chi_1(x_1) \dots \chi_{n-1}(x_{n-1}) \tag{4.3.3}$$

(somme étendue à l'ensemble des points $(x_1, ..., x_{n-1})$ de k^{n-1} tels que $x_1 + \dots + x_{n-1} = 0$), puis

$$\sigma = \sum \chi_1(x_1) \dots \chi_n(x_n) \tag{4.3.4}$$

(somme étendue à l'ensemble des points $(x_1, ..., x_n)$ de H tels que $x_n \neq 1$). Il est clair que $\pi = \rho + \sigma$, et il suffit donc, pour prouver l'égalité (4.3.1), d'établir les deux égalités ci-dessous:

$$\rho = 0; \quad \sigma = -\chi_n(-1)\pi(\chi_1, ..., \chi_{n-1}). \tag{4.3.5}$$

Démontrons la première. Comme $\chi_{n-1}(0) = 0$, on peut, dans (4.3.3), limiter la sommation aux points tels que $x_{n-1} \neq 0$, puis faire le changement de variables $(x_1, ..., x_{n-2}, x_{n-1}) \mapsto (y_1, ..., y_{n-2}, t)$ défini par

$$t = -x_{n-1}, \; ty_1 = -x_1, ..., \; ty_{n-2} = -x_{n-2}.$$

(4.3.3) se transforme alors en

$$\rho = \chi_{n-1}(-1)\pi(\chi_1, ..., \chi_{n-2}) \sum_{t \in k^*} (\chi_1 \dots \chi_{n-1})(t);$$

mais par hypothèse, $\chi_1 \dots \chi_{n-1} = \chi_n^{-1} \neq \varepsilon$; compte tenu de (1.1.1), la somme figurant dans le membre de droite est alors nulle, et on a bien $\rho = 0$.

Démontrons la seconde égalité (4.3.5). Faisons, dans le membre de droite de (4.3.4), le changement de variables $(x_1, ..., x_{n-1}, x_n) \mapsto (y_1, ..., y_{n-1}, t)$ défini par

$$y_1 = x_1/(1-x_n), ..., y_{n-1} = x_{n-1}/(1-x_n), t = x_n/(1-x_n) .$$

(4.3.4) se transforme en

$$\sigma = \Big(\sum_{t \neq 0, -1} \chi_n(t) \Big) \left(\sum \chi_1(y_1) \cdots \chi_{n-1}(y_{n-1}) \right),$$

la deuxième somme étant étendue aux points $(y_1, ..., y_{n-1})$ de k^{n-1} tels que $y_1 + ... + y_{n-1} = 0$; cette deuxième somme est donc égale par définition à $\pi(\chi_1, ..., \chi_{n-1})$; comme la première somme figurant dans le membre de droite vaut $-\chi_n(-1)$ (utiliser (1.1.1)), on aboutit bien à la seconde égalité (4.3.5), ce qui achève de démontrer (i).

(ii) Même méthode que pour la proposition 9, (ii) (qui correspond au cas $n = 2$); on laisse au lecteur le soin d'effectuer le détail du calcul.

COROLLAIRE 1. — *Mêmes données que dans la proposition* 10.

(i) *Si* $\chi_1 \cdots \chi_n = \varepsilon$, *on a*

$$|\pi(\chi_1, ..., \chi_n)|^2 = q^{n-2} . \tag{4.3.6}$$

(ii) *Si au contraire* $\chi_1 \cdots \chi_n \neq \varepsilon$, *on a*

$$|\pi(\chi_1, ..., \chi_n)|^2 = q^{n-1} . \tag{4.3.7}$$

(iii) *Dans les deux cas, on a pour la somme de Jacobi* $\pi(\chi_1, ..., \chi_n)$ *la majoration en module*

$$|\pi(\chi_1, ..., \chi_n)| \leqslant q^{(n-1)/2} . \tag{4.3.8}$$

Démonstration. — (4.3.7) résulte de (4.3.2) et de (2.3.4); (4.3.6) résulte *alors* de (4.3.1) et de (4.3.7); enfin, (4.3.8) est une conséquence immédiate de (4.3.6) et (4.3.7).

Appendice. — *Détermination effective des sommes de Gauss et de Jacobi.*

A.1. Commençons par les sommes de Jacobi (et limitons-nous au cas de deux caractères). Le problème est le suivant: étant donné un corps fini k, et deux caractères multiplicatifs χ et ψ de k, donnés *explicitement*, déterminer *directement* (c'est-à-dire sans remonter à la définition) et *sans ambi-*

guïté la valeur de l'entier algébrique $\pi(\chi, \psi)$. Ce problème est difficile en général, mais, pour $k = \mathbf{F}_p$ et χ, ψ d'ordre peu élevé, il peut être résolu de façon élémentaire. Voyons-le sur deux exemples:

Exemple 1. — Posons $\rho = e^{2\pi i/3}$, $A = \mathbf{Z}[\rho]$; soit p un nombre premier $\equiv 1 \pmod 3$, et soit $p = \lambda\bar{\lambda}$ sa décomposition en facteurs irréductibles dans A, λ et $\bar{\lambda}$ étant entièrement déterminés (à la conjugaison près) par la condition $\lambda \equiv \bar{\lambda} \equiv 1 \pmod 3$. Posons $k = A/\lambda A \simeq \mathbf{F}_p$, et soit $\left(\frac{\cdot}{\lambda}\right)_3$ le symbole de restes cubiques modulo λ dans A, défini pour tout $x \in A$ par

(A.1.1) $\left(\frac{x}{\lambda}\right)_3 = 0$, *si* $x \equiv 0 \pmod \lambda$; *une puissance de* ρ, *sinon*;

$$\left(\frac{x}{\lambda}\right)_3 \equiv x^{(p-1)/3} \pmod \lambda \text{ } \textit{dans les deux cas.}$$

Ce symbole s'identifie à un caractère multiplicatif d'ordre 3 de k, qu'on notera χ. On peut alors envisager la somme de Jacobi $\pi(\chi, \chi)$, qui est un élément parfaitement déterminé de A:

PROPOSITION 11. — *On a* $\pi(\chi, \chi) = -\lambda$.

Démonstration. — Posons $\pi = \pi(\chi, \chi)$. (A.1.1) et la définition de χ permettent d'écrire $\pi = \sum_{x \in k} \chi(x)\chi(1-x) \equiv \sum_{x \in k} P(x) \pmod \lambda$, avec $P(X) = X^{(p-1)/3}(1-X)^{(p-1)/3}$; comme $\deg(P) = 2(p-1)/3 < p-1$, cette somme est nulle (dans $k = A/\lambda A$; voir chap. 3, th. 2), et π est donc divisible par λ; mais par ailleurs $\pi\bar{\pi} = p$ (prop. 9, cor. 1): π est donc un facteur irréductible de p dans A. Au total, π est donc associé à λ dans A, et on a $\pi = \varepsilon\lambda$, ε étant une racine 6-ième de l'unité. Soient maintenant ζ une racine primitive p-ième de l'unité dans $\mathbf{C}$, β le caractère additif de k défini par $\beta(x) = \zeta^x$ $(x \in k)$, et τ la somme de Gauss $\tau(\chi \mid \beta)$; on a $\tau^3 = p\pi$ (prop. 9, cor. 2), donc, puisque $p \equiv 1 \pmod 3$, $\pi \equiv \tau^3 \equiv (\sum_{x \in k^*} \chi(x)\zeta^x)^3 \equiv \sum_{x \in k^*} \chi^3(x)\zeta^{3x} = \sum_{x \in k^*} \zeta^{3x} = -1 \pmod 3$ (noter que $\chi^3(x) = 1$ pour tout $x \in k^*$ et que ζ^3 est une racine primitive p-ième de l'unité).

En résumé, on a donc $\pi = \varepsilon\lambda \equiv -1$ (mo 3), avec $\lambda \equiv 1 \pmod 3$ et $\varepsilon =$ une racine 6-ième de l'unité: ceci implique $\varepsilon = -1$ (essayer les six valeurs possibles de ε), donc finalement $\pi = -\lambda$, C.Q.F.D.

Exemple 2. — Posons $i = \sqrt{-1}$, $A = \mathbf{Z}[i]$; soit p un nombre premier $\equiv 1 \pmod 4$, et soit $p = \lambda\bar{\lambda}$ sa décomposition en facteurs irréductibles dans A, λ et $\bar{\lambda}$ étant entièrement déterminés (à la conjugaison près) par la condition $\lambda \equiv \bar{\lambda} \equiv 1 \pmod{2+2i}$. Posons (comme dans l'exemple 1) $k = A/\lambda A \simeq \mathbf{F}_p$, soient $\left(\frac{\cdot}{\lambda}\right)_2$ et $\left(\frac{\cdot}{\lambda}\right)_4$ les symboles de restes quadratiques et biquadratiques modulo λ dans A (définis comme le symbole de restes cubiques dans l'exemple 1), et soient φ et ψ les caractères multiplicatifs de k correspondants.

PROPOSITION 12. — *On a* $\pi(\varphi, \psi) = -\lambda$.

Démonstration. — Posons $\pi = \pi(\varphi, \psi)$. On vérifie immédiatement, comme pour la proposition 11, que $\pi = \varepsilon\lambda$, ε étant maintenant une racine 4-ième de l'unité. On peut déterminer ε par un argument géométrique très élégant, dû à Jacobi, et dont on verra une autre application au chapitre 9 (sect. 5.2). Soit N le nombre de solutions dans k^2 de l'équation $X^4 + Y^2 = 1$; comme $p \equiv 1 \pmod 4$, k contient quatre racines 4-ièmes de l'unité (chap. 1, prop. 7, (ii)), et cette équation admet deux solutions (x, y) telles que $x = 0$, quatre solutions (x, y) telles que $y = 0$, les autres solutions (x, y) (telles que $xy \neq 0$) se groupant huit par huit de façon évidente; ainsi, $N \equiv 6 \pmod 8$. D'autre part, on verra au chapitre 6 (sect. 3.3, formule (3.3.2)) que

$$(A.1.2) \quad N = p - 1 + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}) = p - 1 + \pi + \bar{\pi};$$

posons alors $\pi = a + bi$ $(a, b \in \mathbf{Z})$; (A.1.2) donne dans ces conditions $a \equiv 3 \pmod 4$ lorsque $p \equiv 1 \pmod 8$, et $a \equiv 1 \pmod 4$ lorsque $p \equiv 5 \pmod 8$; comme $p = a^2 + b^2$, on voit d'autre part que $b \equiv 0 \pmod 4$ lorsque $p \equiv 1 \pmod 8$, et que $b \equiv 2 \pmod 4$ lorsque $p \equiv 5 \pmod 8$; ainsi, dans les deux cas, $-\pi = -a - bi \equiv 1 \pmod{2+2i}$, donc $-\varepsilon\lambda \equiv \lambda \pmod{2+2i}$, donc $\varepsilon = -1$ (essayer les quatre valeurs possibles de ε), et finalement $\pi = \varepsilon\lambda = -\lambda$, C.Q.F.D.

Pour d'autres exemples analogues, voir [**8**], pp. 465-469.

A.2. Passons aux sommes de Gauss. Le problème est maintenant de déterminer sans ambiguïté une somme $\tau(\chi \mid \beta)$, χ et β étant deux caractères d'un corps fini k, l'un multiplicatif, l'autre additif, et supposés donnés explicitement. Si δ est l'ordre de χ, il est en général possible, au moins pour les

petites valeurs de δ, de déterminer explicitement $\omega(\chi \mid \beta) = \tau(\chi \mid \beta)^\delta$ à l'aide de la formule (3.3.4) (prop. 9, cor. 2). On peut alors écrire $\tau(\chi \mid \beta) = \varepsilon\tau_0$, ε étant une racine δ-ième de l'unité, et τ_0 étant un nombre complexe entièrement défini par les deux conditions ${\tau_0}^\delta = \omega(\chi \mid \beta)$, $0 \leqslant \arg(\tau_0) < 2\pi/\delta$. Le problème est donc de déterminer explicitement ε: sauf pour $\delta = 2$, ce dernier problème n'est pas résolu complètement à l'heure actuelle; c'est ce qu'illustrent bien les deux exemples suivants:

Exemple 1. — Soient p un nombre premier impair, $k = \mathbf{F}_p$, φ le caractère de Legendre de k, et β le caractère additif de k défini par $\beta(x) = e^{2\pi ix/p}$ $(x \in k)$. Posons $\tau = \tau(\varphi \mid \beta)$; τ est un nombre complexe parfaitement défini, et la proposition 7 montre que $\tau^2 = \varphi(-1)\,p = (-1)^{(p-1)/2}\,p$, d'où

$$(A.2.1) \qquad \tau = \begin{cases} \pm p^{1/2}, \text{ si } p \equiv 1 \pmod 4, \\ \pm ip^{1/2}, \text{ si } p \equiv 3 \pmod 4. \end{cases}$$

Problème (dit « du signe de la somme de Gauss »): dans les formules (A.2.1), quel est, en fonction de p, le « bon » signe ? En fait, c'est *toujours* le signe $+$; mais, alors que le calcul de τ^2 est immédiat, la détermination du signe de τ est relativement difficile (Gauss lui-même mit, paraît-il, huit ans à trouver une solution...). A ce sujet (et notamment pour une démonstration), voir [**8**], pp. 469-478.

Exemple 2. — Reprenons les hypothèses et notations de l'exemple 1 (sect. A.1), et soit β le caractère additif de k défini par $\beta(x) = e^{2\pi ix/p}$ $(x \in k)$. Posons maintenant $\tau = \tau(\chi \mid \beta)$ (cette somme de Gauss est dite traditionnellement « somme de Kummer »); c'est un nombre complexe parfaitement défini, et la proposition 9 (cor. 2) montre que $\tau^3 = p\pi(\chi, \chi) = -\lambda p$ (sect. A.1, prop. 11). Si alors τ_0 désigne la racine cubique de $-\lambda p$ (dans $\mathbf{C}$) telle que $0 \leqslant \arg(\tau_0) < 2\pi/3$, on a

$$(A.2.2) \qquad \tau = \varepsilon\tau_0, \quad \text{avec} \quad \varepsilon = 1, \rho \text{ ou } \rho^2.$$

Problème (dit « de la somme de Kummer »): dans la formule (A.2.2), quelle est la « bonne » valeur de ε ? Ce problème, posé dans les années 1840/1850 par Kummer (entre autres) n'est toujours pas résolu (voir [**8**], pp. 478-489). Cassels a formulé récemment une conjecture conforme aux valeurs numériques de τ effectivement calculées pour $p \leqslant 5\,000$ (et $p \equiv 1 \pmod 3$), mais cette conjecture reste à démontrer (voir Cassels (1970)).

Le cas $\delta = 4$ est également examiné (mais non résolu !) dans [**8**], pp. 489-494.

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 $|\ .\ |_p$

désigne la valeur absolue p-adique dans $\mathbf{Q}$: cette dernière inégalité équivaut bien à $q^b \mid N$.

En fait, on travaillera avec les *valuations* $\mathfrak{P}$-adiques, et non avec les valeurs absolues; d'autre part, la phase (2) de la démonstration (qui est indépendante de la phase (1)) sera traitée en premier, au paragraphe 1; les phases (1) et (3) seront traitées au paragraphe 2. Quelques conséquences ou généralisations du théorème 1 (et notamment l'extension du théorème 1 au cas d'un système d'équations) sont indiquées au paragraphe 3.

§ 1. *Relations de Stickelberger.*

1.1. Soit k un corps fini à $q = p^f$ éléments. Notons ω et ζ une racine primitive $(q-1)$-ième et une racine primitive p-ième de l'unité dans le corps des nombres complexes, posons $K = \mathbf{Q}(\omega)$, $L = \mathbf{Q}(\omega, \zeta) = K(\zeta)$, et soient A l'anneau des entiers de K et B l'anneau des entiers de L. Les théorèmes généraux sur la décomposition des idéaux premiers dans les corps cyclotomiques (voir [3], chap. 3 et 5, ou [11], chap. IV) permettent d'énoncer:
(1.1.1) L'idéal $p\mathbf{Z}$ est non ramifié dans K, il se décompose dans A en produit de g idéaux premiers de degré f: $pA = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g$; g est déterminé par l'égalité $fg = [K: \mathbf{Q}]$, et chaque corps résiduel $A/\mathfrak{p}_i$ est isomorphe à k.
(1.1.2) Chaque idéal $\mathfrak{p}_i$ est totalement ramifié dans L, l'indice de ramification étant égal à $[L: K] = p - 1$; la décomposition de $\mathfrak{p}_i$ dans B est de la forme $\mathfrak{p}_i B = \mathfrak{P}_i^{p-1}$; le degré résiduel en $\mathfrak{P}_i \mid \mathfrak{p}_i$ est égal à 1, et le corps résiduel $B/\mathfrak{P}_i$ s'identifie au corps résiduel $A/\mathfrak{p}_i$, donc à k.
Il résulte de (1.1.1) et (1.2.2) que l'idéal $p\mathbf{Z}$ se décompose dans B de la façon suivante:

$$(1.1.3) \qquad p\mathbf{Z} = \mathfrak{P}_1^{p-1}\mathfrak{P}_2^{p-1} \dots \mathfrak{P}_g^{p-1}.$$

Dans ce qui suit, on suppose choisis une fois pour toutes un idéal $\mathfrak{P}_i$ et l'idéal $\mathfrak{p}_i$ correspondant; on les note simplement $\mathfrak{P}$ et $\mathfrak{p}$, et *on identifie* $B/\mathfrak{P}$ *et* $A/\mathfrak{p}$ *au corps* k.

1.2. Soit maintenant T^* le sous-groupe de L^* engendré par ω; T^* est cyclique, d'ordre $q - 1$, et la restriction à T^* de l'homomorphisme $B \to B/\mathfrak{P} = k$ est évidemment un isomorphisme de T^* sur k^*; l'isomorphisme inverse $k^* \to T^*$ est un *caractère multiplicatif* d'ordre $q - 1$ de k, qu'on notera θ.

1.3. Une dernière notation: pour tout élément non nul α de L, on notera $\mathrm{ord}(\alpha)$ l'exposant de $\mathfrak{P}$ dans la décomposition en facteurs premiers

de l'idéal fractionnaire αB de B (ord est donc tout simplement la « valuation $\mathfrak{P}$-adique normalisée » de L); les propriétés suivantes sont alors évidentes:

(1.3.1) Quels que soient α, β non nuls dans L, on a

$$\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) + \mathrm{ord}(\beta)\,;\ \mathrm{ord}(\alpha+\beta) \geqslant \inf\big(\mathrm{ord}(\alpha), \mathrm{ord}(\beta)\big)\,.$$

(1.3.2) Si $\alpha \in B$, on a $\mathrm{ord}(\alpha) \geqslant 0$.

(1.3.3) Si $\alpha \in K$, on a $\mathrm{ord}(\alpha) \equiv 0 \pmod{p-1}$.

(1.3.4) Enfin, $\mathrm{ord}(p) = p - 1$.

((1.3.4) résulte de (1.1.3); pour prouver (1.3.3), commencer par décomposer dans K l'idéal premier αA de A, puis utiliser (1.1.2)).

1.4. Soit alors j un entier rationnel, et considérons la somme de Gauss

$$\tau(\theta^{-j} \mid \beta) = \sum_{x \in k^*} \theta^{-j}(x)\,\beta(x)\,, \tag{1.4.1}$$

β étant le caractère additif de k défini par $\beta(x) = \zeta^{Tr(x)}$ ($x \in k$; Tr désigne comme toujours la trace relative à l'extension $k/\mathbf{F}_p$); le choix de ω, ζ, $\mathfrak{P}$, et d'une identification entre $B/\mathfrak{P}$ et k, détermine entièrement θ et β; la somme de Gauss introduite en (1.4.1) ne dépend donc en fait que de j: *on posera pour simplifier* $\tau(j) = \tau(\theta^{-j} \mid \beta)$; en outre, on pourra se borner à étudier $\tau(j)$ pour $0 \leqslant j < q-1$, puisque θ est d'ordre $q-1$. Cela étant, la valuation $\mathfrak{P}$-adique $\mathrm{ord}(\tau(j))$ de $\tau(j)$ est donnée par la proposition suivante, due à Stickelberger:

PROPOSITION 1. — *Soit j un entier tel que $0 \leqslant j < q-1$, et soit*

$$j = j_0 + j_1 p + \ldots + j_{f-1} p^{f-1}$$

l'écriture de j en base p, avec $0 \leqslant j_i \leqslant p-1$ pour $i = 0, \ldots, f-1$; posons $\sigma(j) = j_0 + j_1 + \ldots + j_{f-1}$ (somme des chiffres de j en base p); on a alors:

$$\mathrm{ord}(\tau(j)) = \sigma(j)\,. \tag{1.4.2}$$

Démonstration. — Pour tout entier j, posons a priori $s(j) = \mathrm{ord}(\tau(j))$; il s'agit alors de prouver que si $0 \leqslant j < q-1$, on a $s(j) = \sigma(j)$; or, la fonction s possède les propriétés (i) à (vi) ci-dessous:

(i) *Quel que soit j, $s(j) \geqslant 0$; de plus, $s(0) = 0$.*

En effet, $\tau(j)$ est un entier de L, et $\tau(0) = -1$ est une unité de L. (Pour l'égalité $\tau(0) = -1$, voir chap. 5, sect. 2.2, (i)).

(ii) *Quels que soient j et k, on a $s(j+k) \leqslant s(j) + s(k)$.* ($k$ désigne ici un entier: aucun risque de confusion avec le *corps* k).

Pour j ou $k = 0$, il n'y a rien à prouver, puisque $s(0) = 0$; pour $j + k = q - 1$, on a $s(j+k) = s(0) = 0$, et là encore, il n'y a rien à prouver, puisque $s(j)$ et $s(k)$ sont non négatifs. Supposons donc $0 < j < q - 1$, $0 < k < q - 1$, et $j + k \neq q - 1$; on a dans ce cas

$$\tau(j)\tau(k) = \pi(\theta^{-j}, \theta^{-k})\tau(j+k) \tag{1.4.3}$$

(chap. 5, prop. 9, (ii)), et l'inégalité à démontrer résulte de la première formule (1.3.1) et de (1.3.2), puisque la somme de Jacobi $\pi(\theta^{-j}, \theta^{-k})$ est dans B.

(iii) *Quels que soient j et k, on a $s(j+k) \equiv s(j) + s(k) \pmod{p-1}$.*

Pour j ou $k = 0$, il n'y a rien à prouver, puisque $s(0) = 0$; pour $j + k = q - 1$, on a $\tau(j)\tau(k) = q\theta^j(-1) = p^f\theta^j(-1)$, donc, compte tenu de (1.3.1) et (1.3.4), $s(j) + s(k) = f(p-1) \equiv 0 \pmod{p-1}$; on a d'autre part $s(j+k) = s(0) = 0$; la congruence à démontrer se trouve donc établie dans ce cas particulier (la valeur de $\tau(j)\tau(k)$ résulte de la prop. 7 du chap. 5). Supposons maintenant $0 < j < q - 1$, $0 < k < q - 1$ et $j + k \neq q - 1$; l'égalité (1.4.3) et la première formule (1.3.1) donnent

$$s(j) + s(k) = s(j+k) + \operatorname{ord}\left(\pi(\theta^{-j}, \theta^{-k})\right);$$

la congruence à démontrer résulte alors de (1.3.3), puisque la somme de Jacobi $\pi(\theta^{-j}, \theta^{-k})$ est dans K.

(iv) *Quels que soient j, et $i \geqslant 0$, on a $s(jp^i) = s(j)$.*

En effet, pour tout $x \in k$, on a $\theta^{-jp^i}(x) = \theta^{-j}(x^{p^i})$; on a également $Tr(x^{p^i}) = Tr(x)$, puisque x et x^{p^i} sont conjugués sur $\mathbf{F}_p$ (chap. 1, prop. 8); il suffit alors de faire le changement de variable $y = x^{p^i}$ dans la formule de définition de la somme de Gauss $\tau(jp^i)$ pour obtenir $\tau(j) = \tau(jp^i)$, d'où évidemment l'égalité à démontrer.

(v) *Pour la valeur particulière $j = 1$, on a $s(1) = 1$.*

Posons $\lambda = \zeta - 1$; le polynôme minimal de ζ sur K (ou sur $\mathbf{Q}$) étant $X^{p-1} + \ldots + X + 1 = (X^p - 1)/(X-1)$, le polynôme minimal de λ est évidemment $((X+1)^p - 1)/X = X^{p-1} + pX^{p-2} + \ldots + p$, donc un polynôme d'Eisenstein relativement à p ([**11**], chap. II, § 5): il en résulte que

$$\operatorname{ord}(\lambda) = 1 \tag{1.4.4}$$

(utiliser (1.3.4) et la deuxième formule (1.3.1)). Ecrivons d'autre part la définition de $\tau(1)$ en y remplaçant ζ par $1+\lambda$:

$$\tau(1) = \sum_{x \in k^*} \theta^{-1}(x)(1+\lambda)^{Tr(x)},$$

soit, en développant $(1+\lambda)^{Tr(x)}$ par la formule du binôme et en utilisant (1.4.4):

$$\tau(1) \equiv \sum_{x \in k^*} \theta^{-1}(x)\big(1+\lambda r(x)\big) \pmod{\mathfrak{P}^2}, \tag{1.4.5}$$

$r(x)$ désignant l'unique entier rationnel compris entre 0 et $p-1$ et dont l'image dans $\mathbf{F}_p$ soit égale à $Tr(x)$. Dans le second membre de (1.4.5), faisons le changement de variable $t = \theta(x)$; comme $r(x) \equiv t + t^p + \ldots + t^{p^{f-1}} \pmod{\mathfrak{P}}$ (chap. 1, (3.2.1)), la congruence (1.4.5) devient

$$\tau(1) \equiv \sum_{t \in T^*} t^{-1} + \sum_{t \in T^*} t^{-1}(t+t^p+\ldots+t^{p^{f-1}}) \pmod{\mathfrak{P}^2}; \tag{1.4.6}$$

mais T^* est le groupe des racines $(q-1)$-ièmes de l'unité dans le corps des nombres complexes; on a donc, pour tout entier rationnel u,

$$\sum_{t \in T^*} t^u = \begin{cases} q-1, \text{ si } u \equiv 0 \pmod{q-1}; \\ 0, \text{ sinon}; \end{cases}$$

comme par ailleurs $q = p^f \equiv 0 \pmod{\mathfrak{P}^2}$, la congruence (1.4.6) se réduit à

$$\tau(1) \equiv -\lambda \pmod{\mathfrak{P}^2}; \tag{1.4.7}$$

d'où évidemment, compte tenu de la deuxième formule (1.3.1), $s(1) = \operatorname{ord}(\tau(1)) = \operatorname{ord}(\lambda) = 1$ (utiliser (1.4.4)), C.Q.F.D.

(vi) *On a enfin l'égalité* $\sum_{0 \leq j < q-1} s(j) = f(p-1)(q-2)/2$.

En effet, on a déjà remarqué (voir la démonstration de (iii)) que

$$s(j) + s(q-1-j) = f(p-1); \tag{1.4.8}$$

comme $s(0) = s(q-1) = 0$, la relation (1.4.8) donne, en faisant varier j de 1 à $q-2$ et en additionnant,

$$\sum_{0 \leq j < q-1} \big(s(j)+s(q-1-j)\big) = 2 \sum_{0 \leq j < q-1} s(j) = f(p-1)(q-2),$$

ce qui implique (vi).

Ces diverses propriétés étant établies, prouvons maintenant (toujours en supposant $0 \leqslant j < q-1$) que $\sigma(j) = s(j)$; les propriétés (i), puis (v), puis (ii) et (iii), montrent d'abord que pour $0 \leqslant j \leqslant p-1$, on a $s(j) = j = j_0 = \sigma(j)$; les propriétés (ii) et (iv) donnent d'autre part

$$s(j) \leqslant s(j_0) + s(j_1) + \ldots + s(j_{f-1});$$

comme $0 \leqslant j_i \leqslant p-1$ pour $i = 0, \ldots, f-1$, ces deux remarques impliquent, pour $0 \leqslant j < q-1$,

$$s(j) \leqslant j_0 + j_1 + \ldots + j_{f-1} = \sigma(j); \tag{1.4.9}$$

l'égalité $s(j) = \sigma(j)$ résulte alors de (1.4.9), de la propriété (vi), et de l'égalité $\sum_{0 \leqslant j < q-1} \sigma(j) = f(p-1)(q-2)/2$, qui se vérifie facilement par récurrence sur f. La proposition 1 se trouve ainsi démontrée.

§ 2. *Démonstration du théorème* 1.

Cette démonstration se fera en quatre étapes.

2.1. *Introduction du polynôme* $C(Y)$. Soit T le sous-ensemble de B formé de 0 et des éléments de T^*; pour tout $t \in T$, soit $\bar{t}$ l'image de t dans $k = B/\mathfrak{P}$; l'application $t \mapsto \bar{t}$ est alors une bijection de T sur k (sect. 1.1 et 1.2), dont la bijection inverse est le caractère θ, prolongé comme toujours par $\theta(0) = 0$. Soit d'autre part β le caractère additif de k défini par $\beta(x) = \zeta^{Tr(x)}$ $(x \in k)$; comme card $(T) = q$, il existe évidemment un polynôme à une variable Y et un seul, soit $C(Y)$, de degré $q-1$, à coefficients dans L, et tel que $C(t) = \beta(\bar{t})$ pour tout $t \in T$; posons

$$C(Y) = c_0 + c_1 Y + \ldots + c_{q-1} Y^{q-1}. \tag{2.1.1}$$

Lemme 1. — *Avec les notations du paragraphe* 1, *on a*

$$c_0 = 1;\ c_{q-1} = -q/(q-1);\ \textit{et}\ c_j = \tau(j)/(q-1) \tag{2.1.2}$$
$$\textit{pour}\ 1 \leqslant j \leqslant q-2.$$

En effet, pour $0 \leqslant j \leqslant q-1$, on a, par définition de $\tau(j)$, de θ et de $C(Y)$,

$$\tau(j) = \sum_{x \in k^*} \theta^{-j}(x)\beta(x) = \sum_{t \in T^*} t^{-j}\beta(\bar{t}) = \sum_{t \in T^*} t^{-j} C(t);$$

il suffit alors, pour obtenir les relations (2.1.2), de remplacer, dans le membre de droite, $C(t)$ par son expression développée $c_0 + c_1 t + \ldots + c_{q-1} t^{q-1}$, et de remarquer comme au paragraphe 1 que

$$\sum_{t \in T^*} t^u = \begin{cases} q-1\,, \text{ si } u \equiv 0 \pmod{q-1}\,; \\ 0\,, \text{ sinon.} \end{cases} \tag{2.1.3}$$

LEMME 2. — *Avec les notations du paragraphe* 1, *on a, pour tout j tel que* $0 \leqslant j \leqslant q-1$, *l'égalité*

$$\operatorname{ord}(c_j) = \sigma(j)\,. \tag{2.1.4}$$

Si $0 \leqslant j < q-1$, il suffit d'appliquer le lemme 1, la proposition 1, et de remarquer que $\operatorname{ord}(1/(q-1)) = 0$. Si $j = q-1$, on a $j_0 = j_1 = \ldots = j_{f-1} = p-1$, donc $\sigma(j) = f(p-1)$; on a d'autre part (lemme 1) $\operatorname{ord}(c_j) = \operatorname{ord}(-q/(q-1)) = \operatorname{ord}(q) = \operatorname{ord}(p^f) = f \operatorname{ord}(p) = f(p-1)$ (sect. 1.3); d'où $\operatorname{ord}(c_j) = \sigma(j)$ également pour $j = q-1$.

2.2. *Evaluation de N à l'aide des* c_j. Commençons par introduire un supplément de notations; $\mathbf{x} = (x_0, \ldots, x_n)$ désignera un point quelconque de k^{n+1}; U désignera l'ensemble des suites $\mathbf{u} = (u_1, \ldots, u_n)$ d'entiers rationnels non négatifs telles que $\|\mathbf{u}\| = u_1 + \ldots + u_n \leqslant d = \deg(F)$; enfin, si $\mathbf{u} \in U$, $X^{\mathbf{u}}$ désignera le monôme $X_1^{u_1} \ldots X_n^{u_n}$, $\mathbf{u}'$ désignera la suite $(1, u_1, \ldots, u_n)$, et $X^{\mathbf{u}'}$ désignera le monôme $X_0 X_1^{u_1} \ldots X_n^{u_n} = X_0 X^{\mathbf{u}}$; convention analogue pour $\mathbf{x}^{\mathbf{u}}$ et $\mathbf{x}^{\mathbf{u}'}$ si $\mathbf{x} \in k^{n+1}$, etc.

Cela étant, on a (chap. 5, prop. 3)

$$N = q^{-1} \sum_{\mathbf{x} \in k^{n+1}} \beta\big(x_0 F(x_1, \ldots, x_n)\big)\,; \tag{2.2.1}$$

d'autre part, on peut écrire (en notant $a_{\mathbf{u}}\ (\mathbf{u} \in U)$ les coefficients de F) $F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}}$, donc $X_0 F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}'}$; comme β est un caractère additif, (2.2.1) peut se réécrire

$$N = q^{-1} \sum_{\mathbf{x} \in k^{n+1}} \prod_{\mathbf{u} \in U} \beta(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'})\,. \tag{2.2.2}$$

Posons alors, quels que soient $\mathbf{u} \in U$ et $x_i \in k$, $b_{\mathbf{u}} = \theta(a_{\mathbf{u}})$ et $t_i = \theta(x_i)$; posons également $\mathbf{t} = (t_0, \ldots, t_n)$; on a $b_{\mathbf{u}} \in T$, $t_i \in T$, $b_{\mathbf{u}} t^{\mathbf{u}'} \in T$, et $\overline{b}_{\mathbf{u}} \overline{\mathbf{t}}^{\mathbf{u}'} = a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'}$; ainsi,

$$\beta(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'}) = C(b_{\mathbf{u}} \mathbf{t}^{\mathbf{u}'}) = \sum_{0 \leqslant j \leqslant q-1} c_j b_{\mathbf{u}}^{\,j} \mathbf{t}^{j\mathbf{u}'}\,,$$

$\mathbf{t}^{ju'}$ signifiant évidemment ${t_0}^{j}{t_1}^{ju_1} \ldots {t_n}^{ju_n}$; et (2.2.2) devient

$$N = q^{-1} \sum_{t \in T^{n+1}} \prod_{u \in U} \sum_{0 \leq j \leq q-1} c_j {b_u}^{j} \mathbf{t}^{ju'} . \tag{2.2.3}$$

Soit M l'ensemble de toutes les applications de U dans $\{0, 1, \ldots, q-1\}$ (c'est-à-dire l'ensemble de toutes les « façons d'associer un j à chaque $\mathbf{u}$ »); la distributivité de la multiplication par rapport à l'addition permet de mettre le second membre de (2.2.3) sous la forme

$$q^{-1} \sum_{j \in M} \sum_{t \in T^{n+1}} \prod_{u \in U} c_{j(u)} {b_u}^{j(u)} \mathbf{t}^{j(u)u'} .$$

Pour chaque $j \in M$, posons $b^{(j)} = \prod_{u \in U} {b_u}^{j(u)}$ ($b^{(j)}$ est donc un élément de T), et désignons par $\mathbf{e}_j'$ la suite

$$\sum_{u \in U} j(\mathbf{u})\, \mathbf{u}' = \left(\sum j(\mathbf{u}), \sum j(\mathbf{u})\, u_1, \ldots, \sum j(\mathbf{u})\, u_n\right) .$$

L'égalité (2.2.3) peut alors s'écrire

$$N = q^{-1} \sum_{j \in M} b^{(j)} \prod_{u \in U} c_{j(u)} \sum_{t \in T^{n+1}} \mathbf{t}^{\mathbf{e}j'} . \tag{2.2.4}$$

2.3. *Réduction du problème.* Dans (2.2.4), tous les termes du membre de droite (abstraction faite du facteur q^{-1}) sont dans l'anneau B des entiers de L; il suffit donc pour prouver le théorème 1 de montrer ceci:

(2.3.1) *Quel que soit $j \in M$, l'entier algébrique $\prod_{u \in U} c_{j(u)} \sum_{t \in T^{n+1}} \mathbf{t}^{\mathbf{e}j'}$ est divisible (dans B) par q^{b+1}.*

Convenons d'écrire $q - 1 \mid \mathbf{e}_j'$ si $q - 1$ divise chacune des $n + 1$ composantes de $\mathbf{e}_j'$, et $q - 1 \nmid \mathbf{e}_j'$ dans le cas contraire; d'après (2.1.3), on a

$$\sum_{t \in T^{n+1}} \mathbf{t}^{\mathbf{e}j'} = \begin{cases} q^{n+1}, \text{ si } \mathbf{e}_j' = (0, 0, \ldots, 0); \\ 0, \text{ si } q - 1 \nmid \mathbf{e}_j'; \\ (q-1)^{s+1}\, q^{n-s}, \text{ si } \mathbf{e}_j' \neq (0, 0, \ldots, 0), \text{ si } q - 1 \mid \mathbf{e}_j', \\ \text{et si } \mathbf{e}_j \text{ (c'est-à-dire } \mathbf{e}_j' \text{ privé de sa première composante) possède exactement } s \text{ composantes non nulles;} \end{cases} \tag{2.3.2}$$

et il suffit en fait, pour établir (2.3.1), donc le théorème 1, de prouver ceci:

LEMME 3. — *Si $j \in M$ est tel que $\mathbf{e}_j'$ soit différent de $(0, 0, ..., 0)$, soit « divisible » par $q-1$, et que $\mathbf{e}_j$ possède exactement s composantes non nulles, alors l'entier algébrique $q^{n-s} \prod_{\mathbf{u} \in U} c_{j(\mathbf{u})}$ est divisible (dans B) par q^{b+1}.*

2.4. *Démonstration du lemme* 3. Pour tout $\mathbf{u} \in U$ et tout $j \in M$, écrivons l'entier $j(\mathbf{u})$ en base p:

$$j(\mathbf{u}) = j_0(\mathbf{u}) + j_1(\mathbf{u})\, p + \ldots + j_{f-1}(\mathbf{u})\, p^{f-1}$$

($0 \leqslant j_i(\mathbf{u}) \leqslant p-1$; $0 \leqslant i \leqslant f-1$); ceci définit $j_i(\mathbf{u})$ pour $0 \leqslant i < f$; étendons cette définition en convenant de poser, pour tout entier rationnel z, $j_z(\mathbf{u}) = j_{i(z)}(\mathbf{u})$, où $i(z)$ est le reste de division de z par f; enfin, pour tout entier rationnel h, posons

$$j^{(h)}(\mathbf{u}) = j_{-h}(\mathbf{u}) + j_{1-h}(\mathbf{u})\, p + \ldots + j_{f-1-h}(\mathbf{u})\, p^{f-1}$$

(les $j^{(h)}(\mathbf{u})$ sont les entiers rationnels déduits de $j(\mathbf{u})$ par permutation circulaire des chiffres de $j(\mathbf{u})$ en base p). Il est clair qu'on ne change rien aux égalités (2.3.2) en y remplaçant j par $j^{(h)}$, ce qui équivaut à effectuer sur T la permutation $t \mapsto t^{p^h}$; en particulier, cette substitution ne modifie pas la valeur de s; ainsi, sous les hypothèses du lemme 3, on a

$$(2.4.1) \qquad s(q-1) \leqslant \| \mathbf{e}_{j(h)} \| = \| \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u})\, u \| \leqslant d \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u}).$$

Mais $\sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u})$ est la première composante de $\mathbf{e}_{j(h)}'$: c'est donc (toujours avec les hypothèses du lemme 3) un entier strictement positif divisible par $q-1$; si $(s/d)^*$ désigne le plus petit entier supérieur ou égal à s/d, (2.4.1) implique alors

$$(q-1)(s/d)^* \leqslant \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u});$$

dans cette égalité, donnons à h les valeurs $0, 1, ..., f-1$, et additionnons; compte tenu de la définition de $j^{(h)}(\mathbf{u})$, il vient

$$f(q-1)(s/d)^* \leqslant \sum_{0 \leqq h \leqq f-1} \sum_{\mathbf{u} \in U} \sum_{0 \leqq i \leqq f-1} j_{i-h}(\mathbf{u})\, p^i,$$

ou encore (en intervertissant l'ordre des sommations, en utilisant la notation $\sigma(j)$, et en remplaçant q par p^f),

$$f(p^f-1)(s/d)^* \leqslant (p^{f-1} + \ldots + p + 1) \sum_{\mathbf{u} \in U} \sigma(j(\mathbf{u})).$$

Comme $\sum_{u \in U} \sigma(j(\mathbf{u})) = \operatorname{ord}\left(\prod_{u \in U} c_{j(u)}\right)$ (lemme 2 et première formule (1.3.1)), cette dernière inégalité peut s'écrire, après division par $p^{f-1} + \ldots + p + 1$,

$$f(p-1)(s/d)^* \leqslant \operatorname{ord}\left(\prod_{u \in U} c_{j(u)}\right);$$

compte tenu de (1.3.1) et (1.3.4), on a alors

$$f(p-1)(n-s+(s/d)^*) \leqslant \operatorname{ord}\left(q^{n-s} \prod_{u \in U} c_{j(u)}\right). \tag{2.4.2}$$

Mais le symbole ord est relatif à *n'importe quel* idéal premier $\mathfrak{P}$ de B divisant p, et on a (sect. 1.1, (1.1.3)) $pB = \prod_{\mathfrak{P}|p} \mathfrak{P}^{p-1}$, donc, puisque $q = p^f$, $qB = \prod_{\mathfrak{P}|p} \mathfrak{P}^{f(p-1)}$; ainsi, étant donné (2.4.2), il suffit, pour prouver le lemme 3 (donc le théorème 1), d'établir la propriété suivante:

(2.4.3) *Pour tout entier s tel que $0 \leqslant s \leqslant n$, on a l'inégalité*

$$n - s + (s/d)^* \geqslant b + 1.$$

Démontrons (2.4.3); il est clair que pour tout entier positif t, on a $t \geqslant ((s+t)/d)^* - (s/d)^*$: car, pour $t = 0$, les deux membres sont égaux, et d'autre part le membre de droite, considéré comme fonction de t, croît « moins vite » que t; dans cette inégalité, faisons alors $t = n - s$; il vient

$$n - s + (s/d)^* \geqslant (n/d)^*;$$

mais par définition même $(n/d)^* = b + 1$: ce qui prouve (2.4.3) et achève la démonstration du théorème 1.

§ 3. *Généralisations et compléments.*

3.1. Le théorème 1 s'étend sans difficulté au cas d'un système d'équations:

THÉORÈME 2. — *Soit $F_1, \ldots, F_s$ une famille de s polynômes de degrés respectifs $d_1, \ldots, d_s$, à n variables et à coefficients dans k; posons $d = d_1 + \ldots + d_s$, et soit b le plus grand entier strictement inférieur à n/d. Si alors N désigne le nombre de solutions dans k^n du système d'équations*

$$F_1 = 0, \ldots, F_s = 0, \tag{3.1.1}$$

N est divisible par q^b.

Démonstration. — On se sert du lemme combinatoire suivant:

LEMME 1. — *Soit $V_1, ..., V_s$ une famille de s ensembles finis. Posons $V = \bigcap_{i \leq j \leq s} V_j$, et, pour toute partie R de $S = \{1, ..., s\}$, posons $U_R = \bigcup_{j \in R} V_j$ (pour $R = \emptyset$, $U_R = \emptyset$). On a alors*

$$\text{card}(V) = \sum_{R \subset S} (-1)^{\text{card}(R)-1} \text{card}(U_R). \tag{3.1.2}$$

Ce lemme se prouve facilement par récurrence sur s. Appliquons-le à la démonstration du théorème 2: pour tout $j \in S = \{1, ..., s\}$, soit V_j l'ensemble des zéros dans k^n de l'unique polynôme F_j; avec les notations du lemme, V est alors l'ensemble des solutions dans k^n du système (3.1.1), on a $N = \text{card}(V)$, et (3.1.2) montre qu'il suffit de prouver que, pour chaque $R \subset S$, card (U_R) est divisible par q^b. Si $R = \emptyset$, $U_R = \emptyset$, card $(U_R) = 0$, et il n'y a rien à démontrer; sinon, posons $F_R = \prod_{j \in R} F_j$: U_R est alors l'ensemble des zéros dans k^n du polynôme F_R, et si b_R est le plus grand entier strictement inférieur à $n/\deg(F_R)$, le théorème 1 montre que card (U_R) est divisible par q^{bR}; mais $\deg(F_R) = \sum_{j \in R} \deg(F_j) \leqslant \sum_{j \in S} \deg(F_j) = d$, d'où $n/d \leqslant n/\deg(F_R)$ et $b \leqslant b_R$; card (U_R), divisible par q^{bR}, est divisible a fortiori par q^b, C.Q.F.D.

3.2. Le théorème 1, pour *une* équation, est « le meilleur possible » au sens suivant: *quels que soient n et d, il existe F, de degré d, à n variables et à coefficients dans k, tel que (avec les notations du théorème 1) q^b soit la plus haute puissance de q divisant N.* (Prendre par exemple pour F le polynôme $G_{n,d} = X_1 \ldots X_d + X_{d+1} \ldots X_{2d} + \ldots + X_{(b-1)d+1} \ldots X_{bd} + X_{bd+1} \ldots X_n$; pour ce polynôme, le nombre N peut être déterminé explicitement à l'aide du théorème 6 du chapitre 4: on laisse au lecteur le soin de faire les calculs en détail). En revanche, le théorème 2, pour un système de s équations, peut être amélioré; en fait, on a le résultat suivant, dû à Katz (1971):

THÉORÈME 3. — *Mêmes données et notations que dans le théorème 2. Si $\delta = \sup_{1 \leq j \leq s} d_j$, et si b_1 désigne le plus grand entier supérieur ou égal à $(n-d)/\delta$, alors N est divisible par q^{b1}.*

Ce théorème 3 (qui, pour $s = 1$, coïncide évidemment avec le théorème 1) est lui-même « le meilleur possible »; en fait, on peut montrer (en utilisant des polynômes du type $G_{n,d}$ ci-dessus et des polynômes normiques, et en raisonnant comme au chapitre 4, section 4.3) que, *quels que soient n, s, et $d_1, ..., d_s$, il existe une famille $F_1, ..., F_s$ satisfaisant aux hypothèses des*

théorèmes 2 et 3 et telle que N soit égal exactement à q^{b_1}. Pour la construction d'une telle famille de polynômes, et pour la démonstration du théorème 3, voir Katz (1971) (respectivement § 4 et § 3); voir également les Notes en fin de chapitre.

3.3. Pour des équations *de forme particulière*, le théorème 1 peut dans certains cas être amélioré. Ainsi, en combinant le théorème 1 du chapitre 6 avec les « relations de Stickelberger » (prop. 1), on obtient sans difficulté le résultat suivant:

THÉORÈME 4. — *Soit* $F = a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n}$ *un polynôme diagonal à coefficients dans le corps premier* $k = \mathbf{F}_p$. *Pour* $i = 1, \ldots, n$, *posons* $\delta_i = (p-1, d_i)$, *et soit* b_2 *le plus grand entier strictement inférieur à* $1/\delta_1 + \ldots + 1/\delta_n$. *Alors, si* $a \in k$, *et si N désigne le nombre de solutions dans* k^n *de l'équation* $F = a$, *N est divisible par* p^{b_2}.

Ce résultat reste d'ailleurs vrai sur un corps fini quelconque k à $q = p^f$ éléments, à condition de supposer que chaque $\delta_i = (q-1, d_i)$ divise $p - 1$: N est alors divisible par q^{b_2}; cet exposant b_2 peut encore être « amélioré » si $a = 0$ (voir Joly (1971)). On notera l'analogie entre le théorème 4 ci-dessus et le théorème 3 du chapitre 4.

Notes sur le chapitre 7

§ **1**: la démonstration de la proposition 1 donnée ici est due à Hilbert (« Zahlbericht »); cette proposition est en fait une conséquence d'un résultat plus précis (« congruences de Stickelberger »):

$$\tau(j) \equiv -\lambda^{\sigma(j)}/\rho(j) \pmod{\mathfrak{P}^{\sigma(j)+1}}$$

(avec par définition $\rho(j) = j_0!\, j_1!\, \ldots\, j_{f-1}!$); voir Stickelberger (1890), Davenport-Hasse (1934), ou [11], chap. IV, § 3. Pour une interprétation analytique p-adique de ces congruences, voir Dwork (1960).

§ **2-3**: dans Ax (1964), le cadre de la démonstration du théorème 1 est, non pas le corps de nombres $L = \mathbf{Q}(\omega, \zeta)$, mais le corps $\mathbf{Q}_p(\omega, \zeta)$ des racines $p(q-1)$-ièmes de l'unité dans une clôture algébrique du corps p-adique $\mathbf{Q}_p$ (avec les notations du § 1, ce corps $\mathbf{Q}_p(\omega, \zeta)$ est d'ailleurs isomorphe à $L_{\mathfrak{P}}$, complété $\mathfrak{P}$-adique de L); à cette différence près, la démonstration donnée ici est exactement celle d'Ax; elle est (selon Ax lui-même) « suggérée par certaines idées de Dwork [dans sa démonstration

de la rationalité des fonctions zêta des variétés algébriques] » (à ce sujet, voir chap. 9, § 2). La démonstration du théorème 3 donnée par Katz (1971) utilise également (et directement) les méthodes analytiques p-adiques de Dwork.

CHAPITRE 8

« HYPOTHÈSE DE RIEMANN »

Soient k un corps fini à q éléments, n un entier $\geqslant 1$, F un polynôme à n variables et à coefficients dans k, et N le nombre de solutions dans k^n de l'équation $F = 0$. On a remarqué aux chapitres 4 (sect. 4.2, th. 6, cor. 1) et 6 (sect. 1.2, th. 1, cor. 1, 2, 3; sect. 2.1, th. 2, cor. 1, 2) que, lorsque F est *multilinéaire* ou *diagonal* (et qu'il satisfait en outre à certaines hypothèses qui équivalent à supposer qu'il est absolument irréductible), alors N est de l'ordre de grandeur de q^{n-1}, l'exposant $n-1$ s'interprétant d'ailleurs comme dimension de l'hypersurface affine $F = 0$. Le but du présent chapitre est d'étendre ce résultat à n'importe quel ensemble algébrique, affine ou projectif, *absolument irréductible*, défini sur k — autrement dit, à n'importe quelle *variété* définie sur k; si V est une telle variété, et si N désigne maintenant le nombre de points de V rationnels sur k, on a en fait (§ 4, th. 4)

$$N = q^r + O(q^{r-(1/2)}),$$

q étant considéré comme « infiniment grand », et la constante impliquée par le symbole O ne dépendant que de $r = \dim(V)$, du degré de V, et de la dimension de l'espace affine ou projectif où V se trouve plongée.

Le théorème 4 (pour r quelconque) se déduit par récurrence sur r du cas particulier où $r = 1$, et où V est donc une *courbe*: ce cas est examiné en détail aux paragraphes 1 (courbes de genre 0), 2 (courbes de genre 1) et 3 (courbes de genre quelconque). Le résultat central de ce chapitre est d'ailleurs le théorème 3 (§ 3), dit « hypothèse de Riemann » pour la courbe V: on verra en effet (chap. 9, sect. 3.2) que ce théorème est équivalent au résultat suivant: tous les zéros de la fonction $\zeta(V; s)$ ont une partie réelle égale à 1/2.

Le langage géométrique utilisé dans ce chapitre (et dans le suivant) est essentiellement celui des Foundations de Weil, c'est-à-dire le langage « classique » (à une différence près: si V est un ensemble algébrique défini sur k, *on identifie V à l'ensemble de ses points algébriques sur k*; il en résulte

notamment que si V est une variété de dimension $\geqslant 1$ et si $\mathbf{x}$ est un *point générique* de V, $\mathbf{x}$ n'est pas considéré comme un *élément de* V: autrement dit, on n'a pas le droit d'écrire $\mathbf{x} \in V$). Pratiquement, pour la terminologie et les résultats de géométrie algébrique dont on aura effectivement besoin, le lecteur pourra se reporter au livre de Lang [**12**] ou à celui de Samuel [**15**].

Dans ce chapitre, k désigne (comme toujours) un corps fini à $q = p^f$ éléments, et $\bar{k}$ une clôture algébrique de k. $\mathbf{A}_n$ et $\mathbf{P}_n$ désignent respectivement l'espace affine et l'espace projectif de dimension n sur k. Enfin, si V est un ensemble algébrique défini sur k, *l'ensemble des points de* V *rationnels sur* k *est désormais noté* V_k.

§ 1. *Courbes de genre* 0 (*).

1.1. THÉORÈME 1. — *Si V est une courbe projective non singulière de genre* 0 *définie sur k, elle est birégulièrement équivalente (sur k) à la droite projective définie sur k.*

Démonstration. — D'après un théorème classique de Poincaré (voir [**18**], pp. 71-72), V, de genre 0, est birégulièrement équivalente sur k soit à une droite, soit à une conique (ceci, sans hypothèse sur k; ce théorème de Poincaré peut d'ailleurs se déduire facilement du théorème de Riemann-Roch: voir par exemple [**2**], chap. XVI, th. 6). On peut donc se borner à démontrer le théorème 1 lorsque V est une conique définie dans le plan projectif $\mathbf{P}_2$ par une équation homogène et de degré 2, $F(X_0, X_1, X_2) = 0$, à coefficients dans k: le théorème de Chevalley (chap. 3, th. 1, cor. 1) montre alors que cette équation admet une solution (a_0, a_1, a_2) non triviale dans k^3, donc que V admet un point $\mathbf{a}$ rationnel sur k. Soit maintenant Δ une droite projective du plan $\mathbf{P}_2$, définie sur k et ne passant pas par $\mathbf{a}$ (si par exemple $a_0 \neq 0$, on peut prendre pour Δ la droite d'équation $X_0 = 0$); pour tout point $\mathbf{y}$ de Δ, notons $\varphi(\mathbf{y})$ le second point d'intersection de V et de la droite joignant $\mathbf{a}$ à $\mathbf{y}$; alors l'application $\mathbf{y} \mapsto \varphi(\mathbf{y})$ est évidemment une équivalence birégulière $\Delta \to V$ définie sur k, et le théorème 1 est démontré.

1.2. COROLLAIRE 1. — *Si N désigne le nombre de points de V rationnels sur k, on a exactement $N = q + 1$.*

---

*) Pour un résumé rapide et élémentaire des propriétés des courbes algébriques (genre, théorème de Riemann-Roch), voir SAMUEL (1967).

Démonstration. — Le théorème 1 permet de se limiter au cas où $V = \Delta$ (la droite projective); mais l'ensemble Δ_k des points de Δ rationnels sur k comporte évidemment q éléments « à distance finie » (correspondant bijectivement aux éléments de k), plus un élément « à l'infini » — soit au total $q + 1$ éléments, C.Q.F.D.

§ 2. *Courbes de genre* 1.

Pour la géométrie des courbes de genre 1, voir [**4**], notamment pp. 209-233.

2.1. THÉORÈME 2 (théorème de Schmidt). — *Si V est une courbe projective non singulière de genre* 1 *définie sur k, V admet au moins un point rationnel sur k.*

Démonstration. — D'après un théorème de Châtelet (voir par exemple [**4**], pp. 230-233), il existe une courbe projective non singulière G (la jacobienne de V), définie sur k, ayant un point $\mathbf{o}$ rationnel sur k, et birégulièrement équivalente à V sur $\bar{k}$ (ce qui permet d'identifier $\bar{k}(G)$ à $\bar{k}(V)$). G est évidemment de genre 1, comme V, et on peut la munir d'une loi de groupe rationnelle, définie sur k, notée additivement, ayant $\mathbf{o}$ pour élément neutre, et faisant de G une variété abélienne de dimension 1 sur k ([**4**], pp. 210-211). De plus, l'identification $\bar{k}(G) = \bar{k}(V)$ permet de munir V d'une structure d'espace homogène principal sur G ([**4**], pp. 226-227), c'est-à-dire de construire deux applications rationnelles $\mu\colon V \times G \to V$, et $\upsilon\colon V \times V \to G$, définies sur k, et possédant les propriétés suivantes:

(i) quel que soit $\mathbf{x} \in V$, on a $\mu(\mathbf{x}, \mathbf{o}) = \mathbf{o}$;

(ii) quels que soient $\mathbf{x} \in V$ et $\mathbf{a}, \mathbf{b} \in G$, on a $\mu(\mu(\mathbf{x}, \mathbf{a}), \mathbf{b}) = \mu(\mathbf{x}, \mathbf{a}+\mathbf{b})$;

(iii) quels que soient $\mathbf{x}, \mathbf{y} \in V$, il existe un $\mathbf{a} \in G$ et un seul tel que $\mu(\mathbf{x}, \mathbf{a}) = \mathbf{y}$, et $\mathbf{a}$ est égal à $\upsilon(\mathbf{y}, \mathbf{x})$.

Concrètement, G opère sur V par translations: $\mu(\mathbf{x}, \mathbf{a})$ est le transformé de $\mathbf{x}$ par la translation $\mathbf{a}$, et $\upsilon(\mathbf{y}, \mathbf{x})$ est la translation qui transforme $\mathbf{x}$ en $\mathbf{y}$; ainsi, il n'y a aucun risque de confusion à écrire $\mathbf{x} + \mathbf{a}$ au lieu de $\mu(\mathbf{x}, \mathbf{a})$ et $\mathbf{y} - \mathbf{x}$ au lieu de $\upsilon(\mathbf{y}, \mathbf{x})$; on adoptera cette écriture dans le reste de la démonstration.

Convenons d'autre part, pour tout point $\mathbf{x} = (x_0, x_1, \ldots)$ d'un espace projectif de dimension quelconque sur k, de noter $\mathbf{x}^{(q)}$ le point $(x_0^q, x_1^q, \ldots)$. Il est clair que $\mathbf{x}$ est rationnel sur k si et seulement si $\mathbf{x}^{(q)} = \mathbf{x}$ (chap. 1, prop. 2 ou prop. 8). Il est clair également que si U est un ensemble algébrique

défini sur k et si $\mathbf{x} \in U$, alors $\mathbf{x}^{(q)} \in U$ (représenter U par un système d'équations à coefficients dans k, et remarquer que l'élévation à la puissance q-ième est un automorphisme de k qui laisse invariante lesdits coefficients).

Appliquons ceci à V et G. Soit $\mathbf{x}$ un élément quelconque de V, et posons $\mathbf{a} = \mathbf{x} - \mathbf{x}^{(q)}$. Considérons d'autre part l'application rationnelle $\mathbf{z} \mapsto \mathbf{z}^{(q)} - \mathbf{z}$ de G dans G; elle n'est certainement pas constante (sinon, on aurait $\mathbf{z}^{(q)} - \mathbf{z} = \mathbf{o}^{(q)} - \mathbf{o} = \mathbf{o}$, soit $\mathbf{z}^{(q)} = \mathbf{z}$, pour tout $\mathbf{z} \in G$; tout point de G serait rationnel sur k, et G serait de dimension 0: absurde); comme G est irréductible, projective (donc complète), non singulière et de dimension 1, cette application est surjective. En particulier, il existe $\mathbf{b} \in G$ tel que $\mathbf{a} = \mathbf{b}^{(q)} - \mathbf{b}$, donc, en revenant à la définition de $\mathbf{a}$, tel que $\mathbf{x} + \mathbf{b} = \mathbf{x}^{(q)} + \mathbf{b}^{(q)} = (\mathbf{x}+\mathbf{b})^{(q)}$ (cette dernière égalité parce que l'application rationnelle μ: $V \times G \to V$, qui à $(\mathbf{x}, \mathbf{b})$ associe $\mathbf{x} + \mathbf{b}$, est définie sur k); mais alors $\mathbf{x} + \mathbf{b}$ est un point de V rationnel sur k, C.Q.F.D.

2.2. COROLLAIRE 1 (théorème de Hasse). — *Si N désigne le nombre de points de V rationnels sur k, on a l'inégalité*

$$|q + 1 - N| \leqslant 2q^{1/2}. \tag{2.2.1}$$

Démonstration. — Soit $\mathbf{o}$ un point de V rationnel sur k (th. 2), et munissons V de sa structure de variété abélienne définie sur k et ayant $\mathbf{o}$ pour élément neutre. Soit M l'anneau des endomorphismes de V, et, pour tout $\lambda \in M$, soit $\deg(\lambda)$ le degré de l'application rationnelle λ ([**4**], pp. 215-216). Soit enfin F l'endomorphisme $\mathbf{x} \mapsto \mathbf{x}^{(q)}$ de V. Alors $F - 1$ (c'est-à-dire l'endomorphisme $\mathbf{x} \mapsto \mathbf{x}^{(q)} - \mathbf{x}$ de V) est un élément non nul de M (raisonner comme dans la sect. 2.1), donc une *isogénie* de V ([**4**], pp. 215-216) dont le noyau est exactement l'ensemble des points de V rationnels sur k (voir sect. 2.1). On peut démontrer que cette isogénie est *non ramifiée* ([**4**], p. 217), donc que l'ordre du noyau de $F - 1$ est égal au degré de $F - 1$; ainsi,

$$N = \deg(F - 1). \tag{2.2.2}$$

On peut démontrer également que M est un $\mathbf{Z}$-module libre de rang fini, sans diviseurs de zéro, et qu'il est muni d'un anti-automorphisme $\lambda \mapsto \lambda'$ tel que $\lambda\lambda' = \deg(\lambda)$ pour tout $\lambda \in M$ (voir par exemple Deuring (1941)); il en résulte notamment que, quel que soit $m \in \mathbf{Z}$, on a

$$\deg(F - m.1) = (F - m.1)(F - m.1)' = m^2 - tm + q, \tag{2.2.3}$$

avec $t = F + F' \in \mathbf{Z}$, et $q = FF' = \deg(F)$ (puisque $F(\mathbf{x}) = \mathbf{x}^{(q)}$). Etant

donné sa définition, le polynôme $m^2 - tm + q$ est toujours positif, d'où $t^2 - 4q \leqslant 0$, ou encore

$$|t| \leqslant 2q^{1/2}. \tag{2.2.4}$$

Mais faisons $m = 1$ dans (2.2.3) et utilisons (2.2.2); il vient

$$t = q + 1 - N, \tag{2.2.5}$$

et il suffit de porter (2.2.5) dans (2.2.4) pour obtenir l'inégalité (2.2.1).

2.3. La démonstration esquissée ci-dessus est essentiellement la démonstration originale de Hasse (voir Hasse (1933, 1934, 1936)). Manin en a donné une version « élémentaire » dont voici le principe (Manin (1956); pour les détails des calculs, voir [**6**], chap. 10, pp. 197-206). On suppose pour simplifier $p \neq 2, 3$ (mais cette restriction n'est pas essentielle). Comme V admet un point rationnel sur k, on peut supposer V écrite sous forme normale de Weierstrass

$$Y^2 = X^3 - aX - b, \tag{2.3.1}$$

$a, b \in k$, $4a^3 - 27b^2 \neq 0$. Soit alors ξ un élément transcendant sur k, et soit W la courbe définie sur $K = k(\xi)$ et ayant pour équation

$$Y^2 = \frac{X^3 - aX - b}{\xi^3 - a\xi - b}. \tag{2.3.2}$$

C'est une courbe de genre 1, dont on connaît (au moins) deux points rationnels sur K: $\mathbf{a}_0 = (\xi^q, \eta^{(q-1)/2})$ (avec $\eta = \xi^3 - a\xi - b$) et $\mathbf{b} = (\xi, 1)$. Munissons W de sa structure de variété abélienne définie sur K, ayant le point à l'infini $\mathbf{o}$ pour élément neutre, et pour laquelle trois points ont une somme nulle si, et seulement si, ils sont alignés ([**4**], pp. 211-214); pour tout $m \in \mathbf{Z}$, posons $\mathbf{a}_m = \mathbf{a}_0 - m.\mathbf{b}$, puis définissons un entier d_m de la façon suivante: si $\mathbf{a}_m = \mathbf{o}$, posons $d_m = 0$; si au contraire $\mathbf{a}_m \neq \mathbf{o}$, donc si le point $\mathbf{a}_m$ est « à distance finie », de coordonnées affines x_m, y_m, avec $x_m = P_m(\xi)/Q_m(\xi)$ et P_m, Q_m premiers entre eux, posons $d_m = \deg(P_m)$. On peut alors démontrer (à l'aide des formules d'addition sur une cubique de Weierstrass: voir [**4**], p. 214) les deux relations suivantes:

$$d_{-1} - d_0 = N - q\,; \quad d_{m-1} + d_{m+1} = 2d_m + 2\,;$$

ces deux formules permettent de calculer d_m:

$$d_m = m^2 - (q + 1 - N)\,m + q\,; \tag{2.3.3}$$

comme par définition $d_m \geqslant 0$, le polynôme en m figurant au second membre de (2.3.3) est positif; d'où

$$(q+1-N)^2 \leqslant 4q\,,$$

ce qui implique bien l'inégalité (2.2.1).

La parenté entre ces deux démonstrations tient au fait que $d_m = \deg(F - m.1)$.

2.4. On a vu au chapitre 6 (sect. 3.3, (1) et 3.5) que la courbe *affine* $Y^2 = 1 - X^3$ (qui est de genre 1 pour $p \neq 2, 3$) a un nombre de points rationnels sur k égal à q si $q \equiv -1 \pmod 6$ et à $q + \alpha + \bar{\alpha}$ (avec $\alpha = \pi(\varphi, \chi)$) si $q \equiv 1 \pmod 6$. Si on remarque que cette courbe, considérée maintenant comme *projective*, admet *un* point à l'infini rationnel sur k, on voit que le nombre total N de ses points rationnels sur k satisfait à $|q + 1 - N| = 0$ dans le premier cas, et à $|q + 1 - N| \leqslant |\alpha| + |\bar{\alpha}| = 2q^{1/2}$ dans le second cas (voir chap. 5, prop. 9, cor. 1): le théorème de Hasse se trouve ainsi vérifié directement pour cette courbe.

Raisonnement analogue pour la courbe $Y^2 = X - X^3$, qui admet *un* point à l'infini rationnel sur k, et pour la courbe $Y^3 = 1 - X^3$, qui admet un ou trois points à l'infini rationnels sur k selon que q est congru à -1 ou à 1 (mod 3) (on suppose naturellement $p \neq 3$).

Considérons enfin la courbe *affine* $Y^2 = 1 - X^4$ (qui est de genre 1 pour $p \neq 2$) et dont le nombre de points rationnels sur k est égal à $q + 1$ si $q \equiv -1 \pmod 4$ et à $q - 1 + \alpha + \bar{\alpha}$ (avec $\alpha = \pi(\varphi, \chi)$: chap. 6, sect. 3.3, (2), et 3.5) si $q \equiv 1 \pmod 4$. Dans le premier cas, cette courbe, envisagée maintenant comme *projective*, admet à l'infini *un point double* rationnel sur k, mais ce point est « isolé » (par désingularisation, il donnerait deux points conjugués sur k, mais non rationnels sur k): ce point ne doit donc pas être pris en considération; on a donc ici $N = q + 1$, ou $|q + 1 - N| = 0$. Dans le second cas, la courbe admet encore un point double à l'infini, rationnel sur k, mais « non isolé » (par désingularisation, il donnerait deux points rationnels sur k): ce point doit donc être compté deux fois, d'où maintenant $N = q + 1 + \alpha + \bar{\alpha}$, donc, comme précédemment, $|q + 1 - N| \leqslant 2q^{1/2}$: le théorème de Hasse se trouve également vérifié directement pour cette courbe *).

*) En fait, on a raisonné ici, non sur la courbe $Y^2 = 1 - X^4$, mais sur sa *normalisée* (voir d'ailleurs chap. 9, sect. 5.2, (2) et (4)).

§ 3. *Courbes de genre quelconque.*

3.1. L'égalité $N = q + 1$, pour une courbe de genre 0, et l'inégalité $|q + 1 - N| \leqslant 2q^{1/2}$, pour une courbe de genre 1 (th. 1, cor. 1, et th. 2, cor. 1), sont des cas particuliers du résultat suivant, dû à Weil (1940, 1948):

THÉORÈME 3 (« hypothèse de Riemann » pour V). — *Si V est une courbe projective non singulière de genre g définie sur k, et si N désigne le nombre de points de V rationnels sur k, on a*

$$|q + 1 - N| \leqslant 2gq^{1/2}. \tag{3.1.1}$$

Démonstration. — Soit $W = V \times V$ la surface produit de V par elle-même, c'est-à-dire le lieu sur k du point $(\mathbf{x}, \mathbf{y})$, où $\mathbf{x}$ et $\mathbf{y}$ sont deux points génériques de V, indépendants sur k (voir **[20]**, p. 29, ou Samuel (1967), § I et II). On appelle *correspondance sur V* ([**20**], p. 29) tout diviseur sur V, donc tout cycle de dimension 1 sur V; si X est une correspondance sur V, on appelle *symétrique de X* et on note X' la correspondance image de X par la symétrie $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{y}, \mathbf{x})$ de W; si X et Y sont deux correspondances sur V, on appelle *somme de X et Y* et on note $X + Y$ leur somme en tant que diviseurs sur V; on appelle *produit* (de composition: rien à voir avec le produit d'intersection) *de X et Y* et on note $X \circ Y$ la correspondance déduite de X et Y par l'opération de composition des graphes dans le produit $V \times V$ (pour une définition précise, voir [**20**], pp. 35-38); enfin, on écrit $X \equiv Y$ s'il existe deux diviseurs $\mathfrak{m}$ et $\mathfrak{n}$ sur la *courbe V* et une fonction rationnelle f sur la *surface W* tels que

$$X - Y = (\mathfrak{m} \times V) + (V \times \mathfrak{n}) + (f),$$

(f) désignant le diviseur de la fonction f. On peut alors montrer ([**20**], pp. 38-41) que la relation $\equiv$ est une relation d'équivalence dans l'ensemble des correspondances sur V, et qu'elle est compatible avec les opérations somme et produit introduites ci-dessus: l'ensemble quotient par $\equiv$ de l'ensemble des correspondances sur V se trouve ainsi muni d'une structure d'anneau; on le note $A(V)$, et on l'appelle *anneau des correspondances de V*; si $\xi, \eta \in A(V)$ sont les images de correspondances X et Y sur V, leur somme $\xi + \eta$ et leur produit $\xi\eta$ sont par définition les images dans $A(V)$ de $X + Y$ et de $X \circ Y$; noter que la symétrie $X \mapsto X'$ est évidemment compatible avec la relation $\equiv$; elle définit donc par passage au quotient une involution $\xi \mapsto \xi'$ de $A(V)$ qui est en fait un anti-automorphisme de $A(V)$: si $\xi, \eta \in A(V)$, on a $(\xi+\eta)' = \xi' + \eta'$ et $(\xi\eta)' = \eta'\xi'$; noter aussi que si Δ

désigne la diagonale de W, c'est-à-dire le lieu sur k du point $(\mathbf{x}, \mathbf{x})$, alors Δ est birégulièrement équivalente à V sur k, et δ, classe de la correspondance Δ sur V, est l'élément neutre de $A(V)$ pour la multiplication.

Pour toute correspondance X sur V, notons maintenant $d_1(X)$ et $d_2(X)$ les degrés des cycles $pr_1(X)$ et $pr_2(X)$, projections de X sur le premier et sur le second facteur de $W = V \times V$; notons d'autre part $i(X \cdot \Delta)$ le nombre d'intersection de X et Δ sur W (qui est défini même si Δ est une composante de X: voir par exemple Samuel (1967), p. 307), et posons

$$S(X) = d_1(X) + d_2(X) - i(X \cdot \Delta). \tag{3.1.2}$$

$S(X)$ est un entier rationnel, qui ne dépend que de la classe de la correspondance X; si alors $\xi \in A(V)$, et si X désigne n'importe quelle correspondance d'image ξ dans $A(V)$, on peut définir un entier rationnel $\sigma(\xi)$, ne dépendant que de ξ, par l'égalité $\sigma(\xi) = S(X)$; $\sigma(\xi)$ est dit *trace de* ξ; et on peut montrer ([**20**], pp. 41-54) que la trace possède les propriétés suivantes:

LEMME 1. — *Quels que soient* $\xi, \eta \in A(V)$, *on a* $\sigma(\xi+\eta) = \sigma(\xi) + \sigma(\eta)$, $\sigma(\xi\eta) = \sigma(\eta\xi)$, *et* $\sigma(\xi') = \sigma(\xi)$.

LEMME 2. — δ *désignant toujours la classe de* Δ, *on a* $\sigma(\delta) = 2g$.

LEMME 3. — *Quel que soit* $\xi \neq 0$ *dans* $A(V)$, *on a* $\sigma(\xi\xi') > 0$.

Le lemme 1 est immédiat; le lemme 2 résulte du fait que $d_1(\Delta) = d_2(\Delta) = 1$, de la formule classique $i(\Delta \cdot \Delta) = 2 - 2g$ (Samuel (1967), p. 307, (2)), et de la définition (3.1.2) de $\sigma(\delta) = S(\Delta)$. Le lemme 3 est la « clef de voûte » de la démonstration: c'est de l'inégalité $\sigma(\xi\xi') \geqslant 0$ convenablement appliquée que va résulter l'inégalité (3.1.1). Soit en effet Γ le lieu sur k du point $\mathbf{z} = (\mathbf{x}, \mathbf{x}^{(q)})$ (la notation $\mathbf{x}^{(q)}$ a été définie dans la sect. 2.1); Γ est une correspondance sur V (« correspondance de Frobenius »), et sa symétrique Γ' est le lieu sur k du point $\mathbf{z}' = (\mathbf{x}^{(q)}, \mathbf{x})$; on a évidemment $[k(\mathbf{x}): k(\mathbf{x})] = 1$ et $[k(\mathbf{x}): k(\mathbf{x}^{(q)})] = q$, donc $d_1(\Gamma) = 1$ et $d_2(\Gamma) = q$; on peut d'autre part montrer que chacun des points du cycle intersection $\Gamma \cdot \Delta$ a pour multiplicité 1: comme les composantes de ce cycle sont exactement les points $(\mathbf{a}, \mathbf{a})$ de $V \times V$ avec $\mathbf{a} = \mathbf{a}^{(q)}$, c'est-à-dire avec $\mathbf{a}$ *rationnel sur* k, on voit que $i(\Gamma \cdot \Delta) = N$; si alors γ désigne la classe de la correspondance Γ, la formule de définition (3.1.2) permet d'écrire

$$\sigma(\gamma) = q + 1 - N. \tag{3.1.3}$$

On peut démontrer par ailleurs que $\gamma\gamma' = q\delta$; soit maintenant m un entier rationnel et posons $\xi = \gamma - m\delta$; on a $\xi' = \gamma' - m\delta$, et

$$\xi\xi' = m^2\delta - m(\gamma+\gamma') + \gamma\gamma';$$

prenons les traces des deux membres, tenons compte de la valeur de $\gamma\gamma'$ et utilisons les lemmes 1 et 2; il vient:

$$\sigma(\xi\xi') = 2gm^2 - \sigma(\gamma+\gamma')\,m + 2gq;$$

mais $\sigma(\gamma+\gamma') = 2\sigma(\gamma) = 2(q+1-N)$ (lemme 1 et formule (3.1.3)); ainsi:

$$\sigma(\xi\xi') = 2gm^2 - 2(q+1-N)\,m + 2gq;$$

le lemme 3 montre que le polynôme en m figurant dans le membre de droite de cette dernière égalité est positif; on a donc

$$(q+1-N)^2 - 4g^2q \leqslant 0,$$

ce qui implique l'inégalité (3.1.1) et prouve le théorème 3.

3.2. On peut également démontrer le théorème 3 à l'aide de la théorie des variétés abéliennes (structure de l'anneau des endomorphismes, propriétés du polynôme caractéristique d'un endomorphisme, etc.; voir par exemple **[20]**, § VII à XI, ou **[9]**, chap. 5) appliquée à la jacobienne de la courbe V. Pour $g = 1$, cette seconde démonstration coïncide avec la démonstration du « théorème de Hasse » donnée dans la section 2.2 (dans ce cas en effet, V, admettant un point rationnel sur k par le théorème de Schmidt, s'identifie à sa propre jacobienne); dans le cas général (g quelconque), cette seconde démonstration n'est pas essentiellement différente de celle esquissée dans la section 3.1, du fait que l'anneau des correspondances sur V est isomorphe à l'anneau des endomorphismes de la jacobienne de V (**[20]**, pp. 161-163, th. 22 et cor. 2).

3.3. Revenons à l'inégalité (3.1.1). Considérons à titre d'exemple la courbe plane $X^4 + Y^4 = 1$, et supposons $q \equiv 1 \pmod 4$. Si ψ est un caractère d'ordre 4 de k^*, la proposition 3 du chapitre 6 montre que le nombre de points « à distance finie » sur cette courbe est égal à $q + \sum_{1 \leqslant j_i \leqslant 3} \pi(\psi^{j_1}, \psi^{j_2})$; la somme comprend neuf termes, dont trois sont des sommes de Jacobi triviales (pour $j_1 + j_2 = 4$) et valent -1 (chap. 5, prop. 9, (i)), les six autres (notons-les $\alpha_1, \ldots, \alpha_6$) étant des sommes de Jacobi non triviales, de module $q^{1/2}$: le nombre de points « à distance finie » est donc

$q - 3 + \alpha_1 + \ldots + \alpha_6$. Maintenant, la courbe étudiée, considérée comme projective, est non-singulière, de genre $g = (4-1)(4-2)/2 = 3$, par la formule de Plücker, et elle admet quatre points à l'infini; ainsi, $N = q - 3 + 4 + \alpha_1 + \ldots + \alpha_6$, et on a

$$|q + 1 - N| \leqslant |\alpha_1| + \ldots + |\alpha_6| = 6q^{1/2} = 2gq^{1/2},$$

ce qui vérifie directement le théorème 3 dans ce cas particulier.

La même vérification est possible plus généralement, grâce à la proposition 3 du chapitre 6, pour la courbe $X^{d_1} + Y^{d_2} = 1$, avec $q - 1$ divisible par d_1 et d_2: on laisse au lecteur le soin de faire les calculs, et notamment de montrer que le genre est égal à $((d_1-1)(d_2-1) - (d-1))/2$, avec $d = (d_1, d_2)$.

3.4. Le théorème 3 admet deux conséquences importantes:

COROLLAIRE 1. — *Soit N_m le nombre de points de V rationnels sur $k_m = \mathbf{F}_{q^m}$. Alors, quand m tend vers l'infini, N_m tend lui-meme vers l'infini; en particulier, pour tout m assez grand, $N_m \geqslant 1$.*

Démonstration. — En effet, le théorème 3 appliqué au corps de base k_m donne $N_m \geqslant q^m + 1 - 2gq^{m/2}$, et le membre de droite tend vers l'infini avec m.

COROLLAIRE 2. — *La courbe V possède un diviseur de degré 1 rationnel sur k.*

Démonstration. — Le corollaire 1 montre qu'on peut trouver deux entiers *successifs* m et $m + 1$ tels que V admette un point rationnel sur k_m et un point rationnel sur k_{m+1}; V admet donc un diviseur de degré m et un diviseur de degré $m + 1$ rationnels sur k, et il suffit de retrancher le premier du second pour obtenir un diviseur de degré $(m+1) - m = 1$ rationnel sur k.

Pour $g \geqslant 2$, V ne possède généralement pas de *point* rationnel sur k: le diviseur de degré 1 dont l'existence est affirmée par le corollaire 2 ne peut donc généralement pas (sauf pour $g = 0$ ou 1: th. 1, cor. 1, et th. 2) être supposé positif.

§ 4. *Variétés de dimension quelconque.*

4.1. Soit V une variété projective définie sur k, de dimension r, et supposée plongée dans $\mathbf{P}_n$, espace projectif de dimension n sur k; rappelons

qu'on appelle *degré de V* le nombre de points d'intersection de V avec une sous-variété linéaire de $\mathbf{P}_n$ de dimension $n - r$ « en position générique » (voir [**15**], chap. I, § 8.4); une variété projective plongée dans $\mathbf{P}_n$, de degré d et de dimension r sera dite « de type (n, d, r) ».

Cela étant, on a le théorème suivant, dû à Lang et Weil (1954) (voir aussi Nisnevich (1954): Nisnevich se limite au cas où le corps de base k est le corps premier $\mathbf{F}_p$):

THÉORÈME 4. — *Si V est une variété projective de type (n, d, r) définie sur k, et si $N = N_V$ désigne le nombre de points de V rationnels sur k, on a*

$$|N - q^r| \leqslant B(d)\, q^{r-(1/2)} + A(n, d, r)\, q^{r-1}, \tag{4.1.1}$$

$A(n, d, r)$ désignant une constante qui ne dépend que de n, d et r, et $B(d)$ désignant une constante qui ne dépend que de d (et qu'on peut prendre égale à $(d-1)(d-2)$).

Démonstration. — On raisonne par double récurrence, d'abord sur n, puis sur r. Si $n = 0$, on a $N \leqslant d$, et le théorème est évident; supposons donc $n \geqslant 1$: si V est contenue dans un hyperplan de $\mathbf{P}_n$ défini sur k, V peut être considérée comme de type $(n-1, d, r)$, et l'hypothèse de récurrence sur n permet d'écrire $|N - q^r| \leqslant B(d)\, q^{r-(1/2)} + A(n-1, d, r)\, q^{r-1}$: le théorème est également établi. Ainsi, on peut désormais supposer n fixé ($\geqslant 1$), faire l'hypothèse suivante:

(H) *V n'est contenue dans aucun hyperplan de $\mathbf{P}_n$ défini sur k,*

et raisonner par récurrence sur r. Pour $r = 0$, on a $N \leqslant d$, et le théorème est évident. Supposons maintenant $r = 1$; V est alors une courbe projective, éventuellement singulière: soit V_1 une courbe projective *non singulière* définie sur k et birationnellement équivalente à V sur k (via une équivalence birationnelle $\varphi: V_1 \to V$), et soit N_1 le nombre de points de V_1 rationnels sur k; le théorème 3 montre que $|q + 1 - N_1| \leqslant 2gq^{1/2}$, g désignant le genre de V_1, donc de V; mais le genre de V et le nombre de points singuliers de V sont tous deux majorés par $(d-1)(d-2)/2$ (projeter V sur un plan, ce qui ne modifie ni g, ni d, et ne peut qu'augmenter le nombre de points singuliers; puis appliquer la formule de Plücker à cette projection); d'autre part, la correspondance birationnelle $\varphi: V_1 \to V$ est bijective en dehors des points singuliers de V (et fait correspondre, à des points rationnels sur k, des points rationnels sur k, puisqu'elle est définie sur k), et elle associe, à chaque point

singulier de V, au plus d points de V_1; ainsi, $|N - N_1| \leqslant d(d-1)(d-2)/2$, et finalement $|N - q| \leqslant B(d)\, q^{1/2} + A(n, d, 1)$, avec $B(d) = 2g \leqslant (d-1)(d-2)$ et $A(n, d, 1) = d(d-1)(d-2)/2 + 1$: le théorème est établi pour les variétés de type $(n, d, 1)$.

Supposons alors $r \geqslant 2$, et le théorème démontré jusqu'à la dimension $r - 1$. Soit $\mathbf{P}'_n$ un second exemplaire de l'espace projectif $\mathbf{P}_n$ sur k; à tout point $\mathbf{w} = (w_0, \ldots, w_n)$ de $\mathbf{P}'_n$, associons l'hyperplan $H_{\mathbf{w}}$ de $\mathbf{P}_n$ d'équation $w_0X_0 + \ldots + w_nX_n = 0$; les hyperplans $H_{\mathbf{w}}$ définis sur k correspondent bijectivement aux points $\mathbf{w}$ de $\mathbf{P}'_n$ rationnels sur k, et il y en a exactement

$$Q_n = (q^{n+1} - 1)/(q - 1) = q^n + \ldots + q + 1 .$$

Calculons de deux manières différentes le nombre C des couples $(\mathbf{x}, H_{\mathbf{w}})$, où $\mathbf{x}$ est un point de V rationnel sur k, et où $\mathbf{w}$ est un point de $\mathbf{P}'_n$ rationnel sur k et tel que $\mathbf{x}$ appartienne à $H_{\mathbf{w}}$:

(1) V_k contient par définition N points, et par chacun d'eux passent Q_{n-1} hyperplans définis sur k: d'où $C = NQ_{n-1}$;

(2) pour chaque hyperplan $H_{\mathbf{w}}$ défini sur k, le cycle intersection $V \cdot H_{\mathbf{w}}$ (voir [**15**], chap. II, § 6.1) est, en un sens évident, de type $(n, d, r - 1)$, en vertu de l'hypothèse (H); notons $N_{\mathbf{w}}$ le nombre de points de $V \cdot H_{\mathbf{w}}$ (c'est-à-dire de $V \cap H_{\mathbf{w}}$) rationnels sur k; on a alors évidemment $C = \sum_{\mathbf{w}} N_{\mathbf{w}}$, $\mathbf{w}$ parcourant l'ensemble des Q_n points de $\mathbf{P}'_n$ rationnels sur k.

Le rapprochement des résultats de ces deux calculs donne $NQ_{n-1} = \sum_{\mathbf{w}} N_{\mathbf{w}}$, ou encore

$$N = Q_{n-1}^{-1} \sum_{\mathbf{w} \in I} N_{\mathbf{w}} + Q_{n-1}^{-1} \sum_{\mathbf{w} \in R} N_{\mathbf{w}} , \tag{4.1.2}$$

I (resp. R) désignant l'ensemble des points $\mathbf{w} \in \mathbf{P}'_n$ rationnels sur k et tels que le cycle $V \cdot H_{\mathbf{w}}$ soit (resp. ne soit pas) une variété. On posera $N_I = \text{card}(I)$ et $N_R = \text{card}(R)$; il est clair que $N_I + N_R = Q_n$.

On a alors ces deux lemmes:

LEMME 1. — *Il existe une constante $A_1(n, d, r)$ ne dépendant que de n, d et r et ayant la propriété suivante: quel que soit Z, cycle positif de type (n, d, r) rationnel sur k, on a*

$$N_Z \leqslant A_1(n, d, r)\, q^r , \tag{4.1.3}$$

N_Z désignant le nombre de points de Z rationnels sur k (un point de Z est un point de la réunion des composantes de Z).

LEMME 2. — *Il existe une constante $A_2(n, d, r)$ ne dépendant que de n, d et r et possédant la propriété suivante : quelle que soit V, variété de type (n, d, r) définie sur k et vérifiant* (H), *le nombre N_R défini ci-dessus satisfait à*

$$N_R \leqslant A_2(n, d, r)\, q^{n-1}. \tag{4.1.4}$$

Le lemme 1 est élémentaire; il se démontre par récurrence sur r, en coupant Z par les éléments rationnels sur k d'un faisceau d'hyperplans convenablement choisi dans $\mathbf{P}_n$. Le lemme 2 est plus technique; on le déduit du lemme 1 en construisant, grâce à la théorie de la *forme de Chow* (à ce sujet, voir par exemple [**15**], chap. I, § 9.4), un ensemble algébrique E défini sur k, de type $(n, e, n-1)$, plongé dans $\mathbf{P}'_n$, dont le degré $e = e(n, d, r)$ ne dépend que de n, d et r, et qui contient l'ensemble R; comme les points de R sont tous rationnels sur k, on a donc $N_R \leqslant N_E \leqslant A_1(n, e, n-1)\, q^{n-1}$, et la constante du lemme 2 est donnée par

$$A_2(n, d, r) = A_1\big(n, e(n, d, r), n-1\big).$$

(L'ensemble algébrique E dépend de V; pour une démonstration détaillée de ces deux lemmes, voir Lang-Weil (1954), pp. 820-821).

Achevons alors la démonstration du théorème 4. Dans le membre de droite de (4.1.2), chaque terme $N_{\mathbf{w}}$ de la première somme est le nombre de points rationnels sur k de $V \cdot H_{\mathbf{w}}$, qui est une *variété* de type $(n, d, r-1)$ définie sur k, puisque $\mathbf{w} \in I$; par hypothèse de récurrence (sur r), on a donc

$$|N_{\mathbf{w}} - q^{r-1}| \leqslant B(d)\, q^{r-(3/2)} + A(n, d, r-1)\, q^{r-2}.$$

D'autre part, le nombre de termes de cette première somme est $Q_n - N_R$; les valeurs de Q_{n-1} et Q_n sont connues, et celle de N_R est majorée par $A_2(n, d, r)$ (lemme 2); un calcul facile montre alors que

$$|Q_{n-1}^{-1} \sum_{\mathbf{w} \in I} N_{\mathbf{w}} - q^r - B(d)\, q^{r-(1/2)}| \leqslant A_3(n, d, r)\, q^{r-1}, \tag{4.1.5}$$

$A_3(n, d, r)$ étant une constante qui ne dépend que de n, d et r. Considérons maintenant la seconde somme figurant dans le membre de droite de (4.1.2); chacun des termes $N_{\mathbf{w}}$ qui y apparaissent est le nombre de points rationnels sur k d'un cycle, $V \cdot H_{\mathbf{w}}$, positif, rationnel sur k, et de type $(n, d, r-1)$; le lemme 1 donne donc $N_{\mathbf{w}} \leqslant A_1(n, d, r-1)\, q^{r-1}$; comme cette seconde somme comporte N_R termes, le lemme 2 montre qu'elle est majorée par $A_4(n, d, r)\, q^{n+r-2}$, avec $A_4(n, d, r) = A_1(n, d, r-1)\, A_2(n, d, r) =$ une constante qui ne dépend que de n, d et r. Mais $Q_{n-1} = q^{n-1} + \ldots + q + 1$; ainsi, $Q_{n-1}^{-1} \leqslant q^{1-n}$, et on arrive à la majoration

(4.1.6) $$|Q_{n-1}^{-1} \sum_{w \in R} N_w| \leqslant A_4(n, d, r)\, q^{r-1}.$$

Il suffit alors de porter les inégalités (4.1.5) et (4.1.6) dans la formule (4.1.2) et de poser $A(n, d, r) = A_3(n, d, r) + A_4(n, d, r)$ pour obtenir l'inégalité (4.1.1). Le théorème 4 se trouve ainsi établi.

4.2. Le théorème 4 admet la conséquence suivante, qui généralise le corollaire 1 du théorème 3, et se démontre de la même manière:

COROLLAIRE 1. — *Soit N_m le nombre de points de V rationnels sur $k_m = \mathbf{F}_{q^m}$. Alors, quand m tend vers l'infini, N_m tend lui-même vers l'infini; en particulier, pour tout m assez grand, $N_m \geqslant 1$.*

La propriété « $N_m \geqslant 1$ pour tout m assez grand », c'est-à-dire « V admet un point rationnel sur toute extension algébrique de k de degré assez grand », est évidemment fausse en général sur un corps de base quelconque. Ainsi, l'hyperquadrique projective $X_0^2 + \ldots + X_n^2 = 0$, définie sur le corps $\mathbf{Q}$, n'admet de point rationnel sur aucune extension de $\mathbf{Q}$ de degré *impair* m, si grand que soit m; en effet, $\mathbf{Q}$ est un corps formellement réel ([**10**], chap. XI, § 2); si $K/\mathbf{Q}$ est de degré impair, K est alors lui-même formellement réel (*ibid.*, prop. 2, (ii)), et une égalité $x_0^2 + \ldots + x_n^2$ avec $x_0, \ldots, x_n \in K$ n'est possible que si $x_0 = \ldots = x_n = 0$. Un argument de ramification montrerait de même que la variété $X_0^{n+1} + pX_1^{n+1} + \ldots + p^n X_n^{n+1} = 0$, définie sur le corps $\mathbf{Q}_p$ des nombres rationnels p-adiques, n'admet de point rationnel sur aucune extension de $\mathbf{Q}_p$ de degré *m non divisible par $n+1$*, si grand que soit m.

Cette propriété « $N_m \geqslant 1$ pour tout m assez grand » est également fausse en général, même sur un corps de base fini, si on ne suppose pas *V absolument* irréductible. Ainsi, considérons le polynôme P défini par (4.1.1) (chap. 4, § 4), et supposons $n \geqslant 2$; l'équation $P(X_0, \ldots, X_{n-1}) = 0$ définit alors une k-variété projective V (de type $(n-1, n, n-2)$), mais cette k-variété n'est pas absolument irréductible, donc n'est pas une variété (elle se décompose en n hyperplans définis sur $K = k_n$ et conjugués sur k); et il est facile de vérifier que si m est premier avec n, le nombre N_m de points de V rationnels sur k_m est nul, si grand que soit m (noter que si $(m, n) = 1$, k_m et k_n sont linéairement disjoints sur k (chap. 1, prop. 4, cor. 2); $\omega_1, \ldots, \omega_n$ est alors une base de k_{mn} sur k_m, et on peut raisonner comme au chapitre 4, section 4.1, en remplaçant k par k_m et $K = k_n$ par k_{mn}).

4.3. Remarquons enfin que le théorème 4 reste vrai pour des variétés *affines*, moyennant une modification de la constante $A(n. d, r)$. Soit en effet

$V \subset \mathbf{A}_n$ une variété affine de type (n, d, r); plongeons $\mathbf{A}_n$ dans $\mathbf{P}_n$ de manière que l'hyperplan « à l'infini » H_0 ait pour équation (par exemple) $X_0 = 0$; adjoignons alors à V ses points « à l'infini » de la façon habituelle, et notons W la variété projective ainsi obtenue; elle est de type (n, d, r), et on a, avec des notations évidentes, $N_V = N_W - N_{W.H_0}$; il suffit dans ces conditions d'appliquer le théorème 4 à N_W et le lemme 1 à $N_{W.H_0}$ pour obtenir

$$(4.3.1) \qquad |N_V - q^r| \leqslant B(d)\, q^{r-(1/2)} + A'(n, d, r)\, q^{r-1},$$

avec $A'(n, d, r) = A(n, d, r) + A_1(n, d, r) =$ une constante qui ne dépend que de n, d et r.

Notes sur le chapitre 8

§ **2**: le théorème 2 est dû à Schmidt (1931) (méthode analytique); ce théorème est un aspect d'un résultat général relatif aux espaces homogènes principaux sur un corps de base fini (Lang (1956); voir aussi Serre, *Groupes algébriques et corps de classes*, p. 119 (Hermann, 1959)). L'application $\mathbf{x} \mapsto \mathbf{x}^{(q)}$ utilisée dans la démonstration du théorème 2 est souvent dite « endomorphisme de Frobenius » (voir d'ailleurs chap. 1, prop. 8); le fait que les points fixes de cet endomorphisme sont exactement les points rationnels sur $k = \mathbf{F}_q$ est un trait caractéristique de la « géométrie diophantienne » sur un corps fini.

Un certain de nombre de cas particuliers du théorème de Hasse avaient déjà été remarqués au cours du XIX^{e} siècle; citons notamment la « dernière inscription du journal de Gauss » (« letzte Eintragung im Gauss'schen Tagebuch », reproduite dans *Deuring* (1941), pp. 197-198), relative au nombre de solutions de la congruence $X^2Y^2 + X^2 + Y^2 - 1 \equiv 0 \pmod{p}$, pour $p \equiv 1 \pmod 4$ (à ce sujet, voir également [**5**], p. 307, et [**4**], p. 242, note 3). Pour la démonstration originale du théorème de Hasse, voir Hasse (1933, 1934, 1936).

Les courbes (projectives, non singulières) de genre 1 sur un corps fini k ne sont autres (d'après le théorème de Schmidt) que les variétés abéliennes de dimension 1 définies sur k; les variétés abéliennes de dimension quelconque définies sur un corps fini ont été étudiées notamment par Honda, Milne, Serre, Tate, Waterhouse: pour une bibliographie sur ce sujet, voir Waterhouse (1969).

§ **3**: le théorème 3, annoncé par Weil en 1940, est démontré dans Weil (1948) (= [**20**], 1$^{\text{ère}}$ partie) par voie « géométrique »: c'est cette démonstration qu'on a résumée ici; pour des démonstrations « arithmétiques »,

voir Igusa (1949) et Roquette (1953) (voir aussi [**5**], chap. V, §§ 1-5); dans tous les cas, le point essentiel est l'inégalité $\sigma(\xi\xi') > 0$ (inégalité (23), p. 292, dans [**5**], par exemple); pour un commentaire sur cette inégalité (dite « de Castelnuovo »), voir Weil (1954), p. 553. Pour une application aux « sommes exponentielles », voir Weil (1948, b).

§ **4**: la constante $A_1(n, d, r)$ (lemme 1) peut être prise égale à $(2d)^r$ (en fait, elle ne dépend donc pas de n); en revanche, la constante $A_2(n, d, r)$ (lemme 2) et par conséquent la constante $A(n, d, r)$ (th. 4) dépendent de n; on ne sait d'ailleurs pas en général les majorer explicitement, faute de renseignements précis sur le degré $e(n, d, r)$ de l'ensemble algébrique E.

Pour d'autres remarques sur les résultats ci-dessus, voir également le chapitre 9.

CHAPITRE 9

FONCTIONS ZÊTA

Dans ce dernier chapitre, on se donne comme toujours un corps fini k à $q = p^f$ éléments, de clôture algébrique $\bar{k}$; pour tout entier $m \geqslant 1$, k_m désigne l'unique extension de degré m de k contenue dans $\bar{k}$ (chap. 1, § 1). A tout ensemble algébrique V défini sur k, on peut alors associer la série formelle $Z(V; t) = \exp\left(\sum_{m \geqq 1} N_m t^m/m\right)$, où N_m désigne le nombre de points de V rationnels sur k_m, et où t est une indéterminée. Il se trouve que cette série formelle est en fait une fraction rationnelle en t, et que, moyennant des hypothèses convenables sur V, cette fraction rationnelle peut être décrite avec précision. Le paragraphe 1 de ce chapitre énonce diverses définitions équivalentes de $Z(V; t)$, et justifie le nom de « fonction zêta de V » qui lui est attribué. Le paragraphe 2 donne une esquisse de la démonstration de la rationalité de $Z(V; t)$. Le paragraphe 3 montre comment le théorème de Riemann-Roch et le théorème 3 du chapitre 8 permettent d'obtenir une description très complète de $Z(V; t)$ quand V est une courbe projective non singulière. Le paragraphe 4 indique sans démonstration diverses généralisations des résultats du paragraphe 3. Enfin, le paragraphe 5 donne des exemples de calcul explicite de fonctions zêta; ce paragraphe peut d'ailleurs être lu directement après le paragraphe 2: on y utilise uniquement les défi-

nitions de $Z(V; t)$, l'énoncé (mais non la démonstration) du théorème 2, et le corollaire 1 de ce théorème 2 (on y utilise également les résultats des chapitres 5 et 6).

§ 1. *Definitions, propriétés élémentaires.*

1.1. Soit V un ensemble algébrique (affine ou projectif) défini sur k, et soit $\mathbf{M}$ l'ensemble des cycles de dimension 0, premiers rationnels sur k, et portés par V (voir [**15**], chap. I, §§ 9.2 et 9.3); rappelons qu'un tel cycle $\mathfrak{m}$ est une combinaison linéaire formelle $\mathbf{x}_1 + \ldots + \mathbf{x}_m$ de points de V (algébriques sur k) satisfaisant aux deux conditions suivantes:

(i) $k(\mathbf{x}_1) = \ldots = k(\mathbf{x}_m) = k_m$;

(ii) les $\mathbf{x}_j$ $(1 \leqslant j \leqslant m)$ sont permutés transitivement par le groupe de Galois de k_m/k;

l'entier m s'appelle *degré de* $\mathfrak{m}$, on le note $\deg(\mathfrak{m})$; l'entier $q^{\deg(\mathfrak{m})} = \mathrm{card}(k_m)$ est noté $N\mathfrak{m}$; cela étant:

DÉFINITION 1. — *On appelle fonction zêta (« minuscule ») de V la fonction d'une variable complexe s définie par*

$$\zeta(V; s) = \prod_{\mathfrak{m} \in \mathbf{M}} 1/(1 - N\mathfrak{m}^{-s}). \tag{1.1.1}$$

(On verra plus loin que ce produit infini converge quand la partie réelle de s est suffisamment grande.)

Si V est une k-variété affine, il existe une bijection canonique de $\mathbf{M}$ sur l'ensemble des idéaux maximaux de l'anneau de coordonnées $A = k[V]$ (conséquence facile du théorème des zéros de Hilbert); faisons l'identification correspondante; si alors $\mathfrak{m} \in \mathbf{M}$, $A/\mathfrak{m}$ est isomorphe à k_m, avec $m = \deg(\mathfrak{m})$, et on a $N\mathfrak{m} = \mathrm{card}(A/\mathfrak{m})$; la définition (1.1.1) de $\zeta(V; s)$ à partir de $A = k[V]$ et de l'ensemble $\mathbf{M}$ des idéaux maximaux de A est dans ce cas entièrement analogue à celle de la fonction $\zeta(K; s)$ d'un corps de nombres K à partir de l'anneau $A = O_K$ des entiers de K et de l'ensemble des idéaux maximaux de A. (Ces deux définitions sont en fait des cas particuliers de la notion générale de fonction zêta d'un schéma de type fini sur $\mathbf{Z}$: voir [**16**], pp. 82-86).

1.2. La relation $N\mathfrak{m} = q^{\deg(\mathfrak{m})}$ incite à faire le changement de variable $t = q^{-s}$ et à poser une seconde définition:

DÉFINITION 2. — *On appelle fonction zêta (« majuscule ») de V la fonction d'une variable complexe t définie par*

$$Z(V;t) = \prod_{\mathfrak{m}\in\mathbf{M}} 1/(1-t^{\deg(\mathfrak{m})}). \tag{1.2.1}$$

(On verra que ce produit infini converge quand $|t|$ est suffisamment petit.)

On a alors évidemment

$$\zeta(V;s) = Z(V;q^{-s}). \tag{1.2.2}$$

1.3. On va transformer la définition (1.2.1) de $Z(V;t)$. Pour tout $j \geqslant 1$, soit d_j le nombre de cycles $\mathfrak{m} \in \mathbf{M}$ tels que $\deg(\mathfrak{m}) = j$: le nombre de points $x \in V$ tels que $[k(\mathbf{x}):k] = j$ est évidemment égal à jd_j. Soit maintenant m un entier $\geqslant 1$; le nombre de points $\mathbf{x} \in V$ rationnels sur k_m (c'est-à-dire tels que $k(\mathbf{x}) \subset k_m$, donc que $[k(\mathbf{x}):k]$ divise m: chap. 1, prop. 4) est alors donné par

$$N_m = \sum_{j|m} jd_j. \tag{1.3.1}$$

D'autre part, l'égalité (1.2.1) peut s'écrire

$$Z(V;t) = \prod_{j\geqq 1} 1/(1-t^j)^{d_j}. \tag{1.3.2}$$

Considérons provisoirement t comme une indéterminée; dans l'anneau de séries formelles $\mathbf{Q}[[t]]$, le produit infini figurant au second membre de (1.3.2) est évidemment convergent, et il est de la forme $1 + tG(t)$, avec $G(t) \in \mathbf{Z}[[t]]$. Si D_j désigne le nombre de cycles positifs de dimension 0 et de degré d rationnels sur k (mais non nécessairement premiers) et portés par V, un calcul facile (analogue à celui qui permet de transformer en série de Dirichlet la fonction zêta de Riemann, supposée définie comme produit « eulérien » infini) montre d'ailleurs qu'on a de façon précise

$$Z(V;t) = 1 + \sum_{m\geqq 1} D_m t^m. \tag{1.3.3}$$

Prenons alors, dans $\mathbf{Q}[[t]]$, les logarithmes des deux membres de (1.3.2); il vient

$$\log Z(V;t) = \sum_{j\geqq 1} \sum_{n\geqq 1} d_j t^{nj}/n,$$

soit, en multipliant par j le numérateur et le dénominateur du terme général, en posant $m = nj$, et en tenant compte de (1.3.1),

$$\log Z(V;t) = \sum_{m \geqq 1} N_m t^m/m .$$

Ainsi:

PROPOSITION 1. — *Considérons $Z(V;t)$ comme élément de $\mathbf{Q}[[t]]$. Alors*

(i) *$Z(V;t)$ appartient à $1 + t\mathbf{Z}[[t]]$, et elle est donnée explicitement par la formule (1.3.3).*

(ii) *Si N_m désigne le nombre de points de V rationnels sur k_m, on a*

$$Z(V;t) = \exp\Big(\sum_{m \geqq 1} N_m t^m/m\Big). \tag{1.3.4}$$

La formule (1.3.4) est plus maniable que la formule (1.2.1), et c'est elle qu'on prend généralement comme *définition* de $Z(V;t)$; $\zeta(V;s)$ est alors *définie* par la formule (1.2.2).

1.4. Considérons à nouveau t comme une variable complexe, et $Z(V;t)$ comme une fonction de variable complexe. Si on suppose V affine, plongé dans $\mathbf{A}_n$, l'entier N_m est majoré par le nombre de points de $\mathbf{A}_n$ rationnels sur k_m; on a donc $N_m \leqslant (q^n)^m = (q^n)^m$, et la série entière $\sum_{m \geqq 1} N_m t^m/m$ admet pour majorante la série entière $\sum_{m \geqq 1} (q^n t)^m/m = \log 1/(1-q^n t)$, qui est holomorphe dans le disque $|t| < q^{-n}$; ainsi, $Z(V;t)$ est holomorphe (au moins) dans le disque $|t| < q^{-n}$. Même raisonnement et même conclusion si V est projectif, plongé dans $\mathbf{P}_n$; on a alors $N_m \leqslant (q^n)^m + (q^{n-1})^m + \ldots + q^m + 1$, et la série $\sum_{m \geqq 1} N_m t^m/m$ admet pour majorante la fonction $\log 1/(1-t)(1-qt)\ldots(1-q^n t)$, qui est holomorphe dans $|t| < q^{-n}$. Compte tenu de (1.2.2), on peut donc énoncer:

PROPOSITION 2. — *Si V désigne un ensemble algébrique défini sur k et plongé dans l'espace affine ou projectif de dimension n sur k, la fonction $Z(V;t)$ (supposée définie par (1.3.4)) est holomorphe (au moins) dans le disque $|t| < q^{-n}$; la fonction $\zeta(V;s)$ est holomorphe (au moins) dans le demi-plan $Re(s) > n$.*

On laisse au lecteur le soin de vérifier, en passant par l'intermédiaire de la formule (1.3.3), que le produit infini (1.2.1) converge pour $|t| < q^{-n}$ (au moins) et que le produit infini (1.1.1) converge alors pour $Re(s) > n$ (au moins). Notons d'autre part que les majorantes introduites ci-dessus ne sont autres que les logarithmes des fonctions zêta de $\mathbf{A}_n$ et $\mathbf{P}_n$; ainsi

PROPOSITION 3. — *Considérons* $\mathbf{A}_n$ *et* $\mathbf{P}_n$ *comme variétés définies sur* k *; alors*

$$Z(\mathbf{A}_n; t) = 1/(1-q^n t) ; \tag{1.4.1}$$

$$Z(\mathbf{P}_n; t) = 1/(1-t)(1-qt)\dots(1-q^n t) . \tag{1.4.2}$$

Si V est une *variété,* le théorème 4 du chapitre 8 permet d'en dire plus:

THÉORÈME 1. — *Soit* V *une variété (affine ou projective) de dimension* r*, définie sur* k*. Alors*

(i) $Z(V; t)$ *est holomorphe dans le disque* $|t| < q^{-r}$.

(ii) *Elle se prolonge analytiquement en une fonction méromorphe dans le disque* $|t| < q^{-r+(1/2)}$.

(iii) *Ainsi prolongée, elle n'admet aucun zéro, et elle a pour seule singularité un pôle simple en* $t = q^{-r}$.

Démonstration. — D'après le chapitre 8 (sect. 4.1, th. 1, pour le cas projectif; sect. 4.3, pour le cas affine), on peut, pour tout $m \geqslant 1$, écrire

$$N_m = (q^m)^r + B_m (q^m)^{r-(1/2)} , \tag{1.4.3}$$

et la suite B_m $(m = 1, 2, \dots)$ est alors *bornée*; posons

$$H(u) = \sum_{m \geqslant 1} B_m u^m / m ;$$

$H(u)$ est holomorphe dans le disque $|u| < 1$, et (1.4.3), joint à (1.3.4), permet d'écrire

$$Z(V; t) = \exp\left(H(q^{r-(1/2)}t)\right)/(1-q^r t) ; \tag{1.4.4}$$

le numérateur et le dénominateur du membre de droite sont holomorphes dans le disque $|t| < q^{-r+(1/2)}$, et le numérateur ne s'y annule évidemment pas; comme par ailleurs le dénominateur ne s'annule dans ce disque qu'en $t = q^{-r}$, qui est un zéro simple, le théorème 1 se trouve établi.

Les assertions (i) et (ii) du théorème 1 restent vraies pour un ensemble algébrique V quelconque (en ce qui concerne (ii), on a déjà annoncé, et on démontrera au paragraphe 2, que $Z(V; t)$ est une fraction rationnelle: elle se prolonge donc analytiquement à $\mathbf{C}$ tout entier !); tel n'est plus le cas pour l'assertion (iii): par exemple, si $q \equiv 3 \pmod 4$, la k-variété projective définie dans $\mathbf{P}_2$ (rapporté à un système de *trois* coordonnées homogènes x, y, z) par l'équation $X^2 + Y^2 = 0$, et qui est formée de deux droites définies sur

k_2 et conjuguées sur k, a pour fonction zêta $1/(1-t)(1-qt)(1+qt)$, fraction rationnelle qui admet, dans le disque $|t| < q^{-1/2}$, les *deux* pôles $t = q^{-1}$ et $t = -q^{-1}$.

§ 2. *Rationalité des fonctions zêta.*

2.1. THÉORÈME 2 (théorème de Dwork). — *Quel que soit V, ensemble algébrique défini sur k, $Z(V; t)$ est une fraction rationnelle en t.*

Démonstration. — Soient $\overline{\mathbf{Q}}_p$ la clôture algébrique du corps p-adique $\mathbf{Q}_p$, Ω le complété p-adique de $\overline{\mathbf{Q}}_p$, ord: $\Omega^* \to \mathbf{Q}$, la valuation p-adique de Ω, normalisée par ord $(p) = 1$, et $|\,.\,|_p$: $\Omega \to \mathbf{R}$, la valeur absolue p-adique de Ω, normalisée par $|p|_p = p^{-1}$; Ω est un corps algébriquement clos, complet pour $|\,.\,|_p$: c'est l'analogue p-adique de $\mathbf{C}$. Soit maintenant R un nombre réel positif (ou $+\infty$), et soit D le « disque » de Ω défini par $|t|_p < R$. Une fonction (définie dans une partie de Ω, à valeurs dans $\Omega \cup \{\infty\}$) sera dite *holomorphe dans D* si elle est représentable dans ce disque comme somme d'une série entière convergente; elle sera dite *méromorphe dans D* si elle est égale dans ce disque au quotient de deux fonctions holomorphes. Cela étant, la démonstration du théorème 2 repose essentiellement sur le résultat suivant:

PROPOSITION 1. — *$Z(V; t)$ est méromorphe dans Ω tout entier.*

Indiquons le principe de la démonstration (d'après Dwork (1960), et Serre (1959)). La formule (1.3.4) montre que si V_1 et V_2 sont deux sous-ensembles algébriques d'un même ensemble algébrique, et si on pose $V_3 = V_1 \cup V_2$, $V_4 = V_1 \cap V_2$, les fonctions zêta de ces quatre ensembles algébriques sont liées par $Z(V_1; t)\, Z(V_2; t) = Z(V_3; t)\, Z(V_4; t)$ (remarquer qu'on a, avec des notations évidentes, $N_{1,m} + N_{2,m} = N_{3,m} + N_{4,m}$). Un argument combinatoire simple prouve alors qu'on peut se ramener au cas où V est une hypersurface affine d'équation $F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}} = 0$ (notation analogue à celle du chapitre 7, section 2.2), et qu'on ne modifie pas le problème en remplaçant $Z(V; t)$ par $Z^*(V; t) = \exp\left(\sum_{m \geq 1} N_m^* t^m/m\right)$, N_m^* désignant le nombre de points $\mathbf{x} = (x_1, \ldots, x_n) \in V$, rationnels sur k_m et tels que $x_1 x_2 \ldots x_n \neq 0$. Soit β_m un caractère additif non trivial de k_m, *à valeurs dans Ω* (*); un calcul semblable à celui fait au chapitre 5, section 1.3, montre qu'on a

*) C'est-à-dire un homomorphisme non trivial ${k_m}^+ \to \Omega^*$.

$$(2.1.1) \qquad q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \beta_m(x_0 F(x_1, \ldots, x_n)),$$

la sommation étant étendue à tous les $\mathbf{x} = (x_0, \ldots, x_n) \in (k_m^*)^{n+1}$.

On va transformer le second membre de (2.1.1). Soit ζ une racine primitive p-ième de l'unité dans Ω, notons Tr_m la trace dans l'extension $k_m/\mathbf{F}_p$, et prenons pour β_m (comme d'habitude) le caractère défini par

$$\beta_m(y) = \zeta^{Tr_m(y)} = \zeta^{y + y^p + \ldots + y^{p^{fm-1}}}$$

($y \in k_m$). Ce caractère peut se « factoriser » grâce au résultat suivant:

LEMME 1. — *Il existe une fonction $B(t)$ holomorphe dans le disque* ord $(t) > -1/(p-1)$ *de Ω, et possédant les deux propriétés ci-dessous:*

(i) *Si $b_0 + b_1 t + \ldots + b_m t^m + \ldots$ est le développement en série entière de $B(t)$ dans ce disque, on a $b_0 = 1$, et* ord $(b_m) \geqslant m/(p-1)$ *pour tout m.*

(ii) *Si on identifie le corps résiduel de Ω à $\bar{k}$, et si, pour tout $y \in k_m^*$, on désigne par $\hat{y}$ l'unique racine (q^m-1)-ième de l'unité contenue dans Ω et ayant y comme image résiduelle dans $k_m \subset \bar{k}$, on a*

$$(2.1.2) \qquad \beta_m(y) = B(\hat{y})\, B(\hat{y}^p) \ldots B(\hat{y}^{p^{fm-1}}).$$

Une telle fonction $B(t)$ peut se construire directement (voir Serre (1959), pp. 4-5, ou Dwork (1960), pp. 634-636); on peut aussi la définir à partir de l'exponentielle d'Artin-Hasse (voir Dwork (1960), p. 636; pour les propriétés de l'exponentielle d'Artin-Hasse, voir par exemple Yamamoto (1959)) ou même à partir de l'exponentielle p-adique ordinaire: en fait, si $\pi \in \Omega$ est tel que $\pi^p = -p$, on peut prendre $B(t) = \exp(\pi t - \pi t^p)$.

Cela étant, (2.1.1) peut s'écrire successivement

$$q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \prod_{\mathbf{u} \in U} \beta_m(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'})$$

(pour la notation $X^{\mathbf{u}'}$, voir chap. 7, sect. 2.2), puis, compte tenu de (2.1.2),

$$(2.1.3) \qquad q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \prod_{\mathbf{u} \in U} \prod_{j=0}^{fm-1} B(\hat{a}_{\mathbf{u}} \hat{\mathbf{x}}^{\mathbf{u}' p^j})$$

($\hat{\mathbf{x}}$ signifie évidemment $(\hat{x}_0, \ldots, \hat{x}_n)$; si $a_{\mathbf{u}} = 0$, $\hat{a}_{\mathbf{u}}$ vaut par définition 0; enfin, la sommation est étendue à tous les $\mathbf{x} \in (k_m^*)^{n+1}$). Ici, faisons un changement de notation: pour tout $y \in k_m^*$, écrivons y au lieu de $\hat{y}$ (ce qui revient à identifier les éléments y de k_m^* avec leurs « représentants multi-

plicatifs » $\hat{y}$ dans Ω); notons par ailleurs T_m le groupe des racines (q^m-1)-ièmes de l'unité dans Ω. La relation (2.1.3) devient

$$(2.1.4) \qquad q^m N_m^* = (q^m-1)^n + \sum_{x \in T_m^{n+1}} \prod_{u \in U} \prod_{j=0}^{fm-1} B(a_u x^{u' p^j}).$$

Posons alors $C(t) = \prod_{i=0}^{f-1} B(t^{p^i})$ (si on a pris $B(t) = \exp(\pi t - \pi t^p)$, on a tout simplement $C(t) = \exp(\pi t - \pi t^q)$); on vérifie immédiatement (à l'aide de la partie (i) du lemme 1) que $C(t)$ est elle-même holomorphe dans le disque $\mathrm{ord}(t) > -1/(p-1)$ de Ω, et que son développement en série entière $c_0 + c_1 t + \ldots + c_m t^m + \ldots$ dans ce disque satisfait à

$$(2.1.5) \qquad c_0 = 1 \; ; \quad \mathrm{ord}(c_m) \geqslant m/(p-1) \quad \text{pour tout } m \; ;$$

comme $a_u^q = a_u$ pour tout $u \in U$ (le polynôme F est à coefficients dans $k = k_1$), la relation (2.1.4) peut s'écrire

$$(2.1.6) \qquad q^m N_m^* = (q^m-1)^n + \sum_{x \in T_m^{n+1}} \prod_{u \in U} \prod_{j=0}^{m-1} C(a_u x^{u' q^j}).$$

Introduisons alors la série formelle à $n+1$ variables

$$G(X) = \prod_{u \in U} C(a_u X^{u'}) = \sum g_v X^v$$

(v parcourant $\mathbf{N}^{n+1}$). La relation (2.1.6) devient

$$(2.1.7) \qquad q^m N_m^* = (q^m-1)^n + \sum_{x \in T_m^{n+1}} G(x)\, G(x^q) \ldots G(x^{q^{m-1}}),$$

et (2.1.5) permet d'autre part de vérifier que $G(X)$ possède la propriété suivante:

(2.1.8) *Il existe un nombre réel $M > 0$ tel que pour tout $v = (v_0, \ldots, v_n)$, on ait* $\mathrm{ord}(g_v) \geqslant M(v_0 + \ldots + v_n)$.

Soit alors E l'anneau de séries formelles à $n+1$ variables $\Omega[[X]]$, considéré comme espace vectoriel sur Ω, et définissons de la façon suivante deux endomorphismes Φ et Ψ de E: si $H(X) = \sum h_v X^v$ est un élément quelconque de E, on a $\Phi(H) = \sum h_{qv} X^v$, et $\Psi(H) = \Phi(GH)$; pour $m \geqslant 1$, soit également Ψ^m le m-ième itéré de Ψ. Alors

LEMME 2. — (i) *La série qui donne la trace $Tr(\Psi^m)$ de la matrice (infinie) de Ψ^m par rapport aux X^v ($v \in \mathbf{N}^{n+1}$) est convergente dans Ω et on a*

$$(2.1.9)\qquad (q^m-1)^{n+1}\,Tr(\Psi^m) = \sum_{x\in T_m^{n+1}} G(x)\,G(x^q)\ldots G(x^{q^m-1}).$$

(ii) *Le déterminant caractéristique de Ψ est donné par*

$$(2.1.10)\qquad \det(1-t\Psi) = \exp\Big(-\sum_{m\geqq 1} Tr(\Psi^m)\,t^m/m\Big).$$

(iii) *Enfin, $\Delta(t) = \det(1-t\Psi)$ est une fonction holomorphe dans Ω tout entier.*

Pour une démonstration de ce lemme, voir Serre (1959), pp. 7-9 (la démonstration utilise essentiellement la propriété (2.1.8) des coefficients de $G(X)$; la partie (i) du lemme est presque immédiate; la partie (ii) généralise une formule bien connue en dimension finie).

Démontrons alors la proposition 1. Les relations (2.1.7) et (2.1.9) donnent

$$q^m N_m^* = (q^m-1)^n + (q^m-1)^{n+1}\,Tr(\Psi^m);$$

si on développe $(q^m-1)^n$ et $(q^m-1)^{n+1}$ par la formule du binôme et si on utilise la définition de $Z^*(V;t)$ et la formule (2.1.10) (voir le lemme 2, (ii) et (iii)), on trouve

$$(2.1.11)\qquad Z^*(V;t) = K_1(t)\,K_2(t),$$

avec

$$K_1(t) = \prod_{i=0}^{n}(1-p^{n-i-1}t)^{(-1)^{i+1}\binom{n}{i}},$$

$$K_2(t) = \prod_{i=0}^{n+1}\Delta(p^{n-i}t)^{(-1)^{i+1}\binom{n+1}{i}}.$$

$K_1(t)$ est une fraction rationnelle; comme $\Delta(t)$ est holomorphe dans Ω tout entier (lemme 2, (iii)), $K_2(t)$ est évidemment méromorphe dans Ω tout entier; (2.1.11) montre alors que $Z^*(V;t)$ est elle-même méromorphe dans Ω tout entier, et la proposition 1 est établie.

La démonstration du théorème 2 utilise également le résultat suivant:

PROPOSITION 2 (critère de rationalité de Dwork). — *Soit $F(t)$ une série formelle en t à coefficients entiers rationnels, et supposons qu'il existe deux nombres réels positifs R et R_p tels que* (i) *$F(t)$ soit méromorphe dans le disque $|t| < R$ de $\mathbf{C}$;* (ii) *$F(t)$ soit méromorphe dans le disque $|t|_p < R_p$ de Ω;* (iii) *$RR_p > 1$. Alors $F(t)$ est une fraction rationnelle.*

On peut supposer $R_p \geqslant 1$. Si $R_p = 1$ (et par conséquent $R > 1$), on retombe sur le classique *critère de Borel* (voir Borel (1894)). Il suffit donc d'examiner le cas où $R_p > 1$. Si alors $F(t) = a_0 + a_1 t + \ldots + a_m t^m + \ldots$, et si on pose pour tout $h \geqslant 1$

$$D_{m,h} = \text{dét}\,(a_{m+i+j})_{0 \leqslant i,j < h},$$

le principe de la démonstration consiste à déduire de (i), (ii) et (iii) l'existence d'un entier h tel que $|D_{m,h}|\,|D_{m,h}|_p < 1$ pour tout m suffisamment grand; comme $D_{m,h}$ est un entier, ceci n'est possible que si $D_{m,h} = 0$ pour m suffisamment grand, donc si, à partir d'un certain rang, les a_m satisfont à une relation de récurrence linéaire de longueur h: mais ceci équivaut à dire que $F(t)$ est une fraction rationnelle. Pour les détails de la démonstration, voir par exemple Serre (1959), pp. 2-4.

Cela étant, le théorème 2 est immédiat: d'après la section 1.4, il existe un entier n tel que $Z(V;t)$ soit holomorphe dans le disque $|t| < q^{-n}$ de $\mathbf{C}$; posons $R = q^{-n}$ et (par exemple) $R_p = q^{n+1}$; on a $RR_p = q > 1$, et $Z(V;t)$ est évidemment méromorphe dans le disque $|t|_p < R_p$ de Ω (prop. 1); la proposition 2 est donc applicable à $Z(V;t)$, qui est effectivement une fraction rationnelle, C.Q.F.D.

2.2. On sait (voir Fatou (1906)) que si $F(t)$ est une fraction rationnelle en t à coefficients dans $\mathbf{Q}$, si $F(0) = 1$, et si le développement en série entière de $F(t)$ a tous ses coefficients *entiers*, alors les zéros et les pôles de $F(t)$ sont des inverses d'entiers algébriques. Ceci s'applique à $Z(V;t)$ et montre qu'on peut écrire

$$Z(V;t) = \prod_{i=1}^{r} (1 - \alpha_i t) / \prod_{j=1}^{s} (1 - \beta_j t), \tag{2.2.1}$$

les α_i et les β_j étant des entiers algébriques (respectivement les inverses des zéros et des pôles de $Z(V;t)$). Prenant les logarithmes des deux membres et utilisant la formule (1.3.4), on arrive alors au résultat suivant:

COROLLAIRE 1. — *Il existe deux familles $(\alpha_i)_{1 \leqslant i \leqslant r}$ et $(\beta_j)_{1 \leqslant j \leqslant s}$ d'entiers algébriques telles que pour tout $m \geqslant 1$, on ait*

$$N_m = {\beta_1}^m + \ldots + {\beta_s}^m - {\alpha_1}^m - \ldots - {\alpha_r}^m. \tag{2.2.2}$$

Remarquons qu'inversement, si V est un ensemble algébrique défini sur k et si $(\alpha_i)_{1 \leqslant i \leqslant r}$, $(\beta_j)_{1 \leqslant j \leqslant s}$ sont deux familles d'entiers algébriques telles

qu'on ait (2.2.2) pour tout $m \geqslant 1$, alors la fonction zêta de V est donnée par (2.2.1): on utilisera cette remarque à plusieurs reprises aux paragraphes 3, 4 et 5.

§ 3. *Fonction zêta d'une courbe projective non singulière.*

3.1. Si V est une courbe projective non singulière définie sur k, la fonction $Z(V;t)$ est décrite avec précision par le théorème suivant, dû à Weil (1940, 1948) (voir aussi [**19**], chap. VII, p. 130):

THÉORÈME 3. — *Si V est une courbe projective non singulière de genre g définie sur k, on a*

$$Z(V;t) = P(t)/(1-t)(1-qt), \tag{3.1.1}$$

P étant un polynôme à coefficients entiers rationnels vérifiant les propriétés suivantes :

(i) *Le degré de P est égal à $2g$; son coefficient dominant est égal à q^g et son terme constant à 1.*

(ii) *P satisfait à l'équation fonctionnelle*

$$P(1/qt) = q^{-g}t^{-2g}P(t). \tag{3.1.2}$$

(iii) *Les zéros de P (qui sont des inverses d'entiers algébriques, d'après* (i)*), ont tous pour module $q^{-1/2}$.*

Démonstration. — On utilise essentiellement le théorème 3 du chapitre 8 et le résultat suivant:

PROPOSITION 3. — *Mêmes hypothèses que dans le théorème 3 ; la fonction zêta de V satisfait à l'équation fonctionnelle*

$$Z(V;1/qt) = q^{1-g}t^{2-2g}Z(V;t). \tag{3.1.3}$$

Prouvons cette proposition (et convenons, pour simplifier, d'écrire $Z(t)$ au lieu de $Z(V;t)$, et de dire systématiquement *diviseur* au lieu de *diviseur rationnel sur k*). La formule (1.3.1) montre que $Z(t) = \sum_{m \geqq 0} D_m t^m$, D_m désignant ici (puisque V est une courbe) le nombre de diviseurs positifs de degré m sur V. Mais V possède un diviseur $\mathfrak{m}_0$ (non nécessairement positif) de degré 1 (chap. 8, th. 3, cor. 2); d'autre part, les diviseurs *positifs* de degré g sur V forment un ensemble fini, et l'équivalence linéaire entre divi-

seurs partage cet ensemble en classes d'équivalence: on peut donc trouver une famille $\mathfrak{m}_1, \ldots, \mathfrak{m}_h$ de diviseurs positifs de degré g sur V telle que tout diviseur positif $\mathfrak{m}$ de degré g sur V soit linéairement équivalent à un $\mathfrak{m}_j$ ($1 \leqslant j \leqslant h$) et un seul; et ceci reste d'ailleurs vrai *même si on ne suppose pas* $\mathfrak{m}$ *positif* (en effet, si $\deg(\mathfrak{m}) = g$, le théorème de Riemann-Roch donne $l(\mathfrak{m}) \geqslant 1$, de sorte que tout diviseur $\mathfrak{m}$ de degré g sur V est linéairement équivalent à un diviseur *positif* de degré g sur V).

Pour tout $m \geqslant 0$ et tout j ($1 \leqslant j \leqslant h$), posons alors

$$\mathfrak{m}_{j,m} = \mathfrak{m}_j + (m-g)\,\mathfrak{m}_0 . \tag{3.1.4}$$

Il est clair que, quel que soit le diviseur positif $\mathfrak{m}$ sur V, il existe un couple (j, m) et un seul tel que $\mathfrak{m} \sim \mathfrak{m}_{j,m}$ (m étant d'ailleurs égal à $\deg(\mathfrak{m})$). Calculons maintenant D_m; si $D_{j,m}$ est le nombre de diviseurs positifs sur V linéairement équivalents à $\mathfrak{m}_{j,m}$, il résulte de ce qui précède que

$$D_m = \sum_{j=1}^{h} D_{j,m} ; \tag{3.1.5}$$

par ailleurs, on sait que les diviseurs positifs sur V qui sont linéairement équivalents à un diviseur donné $\mathfrak{n}$ forment un espace projectif de dimension $l(\mathfrak{n}) - 1$ sur k (c'est la série linéaire complète $|\mathfrak{n}|$ associée à $\mathfrak{n}$); on a donc

$$D_{j,m} = \operatorname{card}(|\mathfrak{m}_{j,m}|) = (q^{l(\mathfrak{m}_{j,m})} - 1)/(q-1) . \tag{3.1.6}$$

(1.3.1), (3.1.5) et (3.1.6) donnent ainsi, après multiplication par $q - 1$:

$$(q-1)\,Z(t) = \sum_{m \geqslant 0} \sum_{j=1} (q^{l(\mathfrak{m}_{j,m})} - 1)\, t^m . \tag{3.1.7}$$

Posons alors

$$F(t) = \sum_{m=0}^{2g-2} \sum_{j=1}^{h} q^{l(\mathfrak{m}_{j,m})} t^m , \tag{3.1.8}$$

$$R(t) = -\sum_{m=0}^{2g-2} t^m + h^{-1} \sum_{m \geqslant 2g-1} \sum_{j=1}^{h} (q^{l(\mathfrak{m}_{j,m})} - 1)\, t^m ; \tag{3.1.9}$$

on a évidemment

$$(q-1)\,Z(t) = F(t) + hR(t) ; \tag{3.1.10}$$

mais le théorème de Riemann-Roch montre que pour $\deg(\mathfrak{m}) = m \geqslant 2g - 1$, on a $l(\mathfrak{m}) = m - g + 1$; ceci permet, dans $R(t)$, de remplacer chaque

somme $\sum_{j=1}^{h} (q^{l(\mathfrak{m}_{j,m})} - 1)\, t^m$ par $h\,(q^{m-g+1}-1)\, t^m$, et donne après sommation de deux séries géométriques

$$R(t) = -1/(1-t) + q^g t^{2g-1}/(1-qt)\,. \tag{3.1.11}$$

Un calcul direct prouve alors que

$$R(1/qt) = q^{1-g} t^{2-2g} R(t)\,. \tag{3.1.12}$$

D'autre part, si $\mathfrak{w}$ est un diviseur canonique sur V, le théorème de Riemann-Roch donne

$$l(\mathfrak{m}_{j,m}) = m - g + 1 + l(\mathfrak{w} - \mathfrak{m}_{j,m})\,;$$

en outre, pour toute valeur de m telle que $0 \leqslant m \leqslant 2g-2$, il est clair que les h nombres $l(\mathfrak{w}-\mathfrak{m}_{j,m})$ $(1 \leqslant j \leqslant h)$ sont les mêmes, à l'ordre près, que les h nombres $l(\mathfrak{m}_{j,2g-2-m})$ $(1 \leqslant j \leqslant h)$; il résulte de ces deux remarques (et de la définition (3.1.8) de $F(t)$) que

$$F(1/qt) = q^{1-g} t^{2-2g} F(t)\,. \tag{3.1.13}$$

Le rapprochement de (3.1.10), (3.1.12) et (3.1.13) donne immédiatement l'équation fonctionnelle (3.1.3), et la proposition 3 se trouve établie.

Démontrons alors le théorème 3. Posons par définition

$$P(t) = (1-t)\,(1-qt)\,Z(t)\,;$$

l'équation fonctionnelle (3.1.3) pour $Z(t)$ (prop. 3) implique l'équation fonctionnelle (3.1.2) pour $P(t)$, ce qui prouve (ii). Les formules (3.1.10), (3.1.8) et (3.1.11) (voir la démonstration de la prop. 3) montrent que $P(t)$ est un polynôme à coefficients entiers: (i) résulte alors de (ii), en ce qui concerne le degré de P et la valeur de son coefficient dominant; et du fait que $P(0) = Z(0) = 1$, en ce qui concerne son terme constant.

Reste à démontrer (iii). On a

$$\log P(t) = \log Z(t) - \log(1-t)\,(1-qt) = \sum_{m \geqq 0} (N_m - 1 - q^m)\, t^m/m\,;$$

le théorème 3 du chapitre 8 montre que la série entière de droite admet pour majorante la série $\sum_{m \geqq 0} 2q^{m/2} t^m$, qui est holomorphe dans le disque $|t| < q^{-1/2}$ de C; $\log P(t)$ est donc holomorphe dans ce disque, de sorte que $P(t)$ n'admet aucun zéro dans le disque $|t| < q^{-1/2}$; comme la transformation $t \mapsto 1/qt$ échange l'intérieur et l'extérieur de ce disque, (ii) montre

que $P(t)$ n'admet également aucun zéro dans le domaine $|t| > q^{-1/2}$: tous les zéros de $P(t)$ sont donc sur le cercle $|t| = q^{-1/2}$, ce qui prouve (iii) et achève la démonstration du théorème 3.

COROLLAIRE 1. — *Tous les zéros de la fonction $\zeta(V; s)$ sont sur la droite $Re(s) = 1/2$.*

Démonstration. — On a en effet $\zeta(V; s) = Z(V; q^{-s})$, et le changement de variable $t = q^{-s}$ transforme les t de module $q^{-1/2}$ en les s de partie réelle 1/2.

3.2. Ce corollaire 1 constitue l'analogue géométrique de l'hypothèse de Riemann, et résulte directement du théorème 3 du chapitre 8. Inversement, ce corollaire 1 (ou, ce qui revient au même, la partie (iii) du théorème 3 ci-dessus) implique le théorème 3 du chapitre 8: écrivons en effet $Z(V; t) = P(t)/(1-t)(1-qt)$, et soient α_i $(1 \leqslant i \leqslant 2g)$ les *inverses* des $2g$ zéros de $P(t)$; on a alors $Z(V; t) = (1-\alpha_1 t)\ldots(1-\alpha_{2g}t)/(1-t)(1-qt)$, donc (voir sect. 2.2), $N_m = q^m + 1 - {\alpha_1}^m - \ldots - \alpha_{2g}^m$; pour $m = 1$, ceci permet d'écrire $|q + 1 - N_1| \leqslant |\alpha_1| + \ldots + |\alpha_{2g}|$; si maintenant on suppose que les $2g$ zéros de P ont pour module $q^{-1/2}$, on a $|\alpha_i| = q^{1/2}$ pour $i = 1, \ldots, 2g$, et la dernière inégalité se réduit (puisque $N = N_1$) à

$$|q + 1 - N| \leqslant 2gq^{1/2}:$$

on retrouve bien l'inégalité (3.1.1) du chapitre 8.

3.3. Remarquons pour terminer que dans la démonstration du théorème 3 ci-dessus, la rationalité de $Z(V; t)$ a été établie directement (à l'aide du théorème de Riemann-Roch), indépendamment du théorème 2. Signalons d'autre part que l'entier h qui s'est introduit au cours de la démonstration de la proposition 3 est égal au nombre de classes de diviseurs de degré 0 du corps de fonctions algébriques $k(V)/k$, et qu'on a $P(1) = h$; ainsi, dans le cas géométrique comme dans le cas arithmétique, il y a un rapport étroit entre nombre de classes et comportement de la fonction ζ au point $s = 1$ (à ce sujet, voir par exemple **[19]**, chap. VII).

§ 4. *Conjectures de Weil.*

4.1. Soit maintenant V une variété projective non singulière de type (n, d, r) (voir chap. 8, § 4) définie sur k. Une description de $Z(V; t)$, généralisant le théorème 3 (qui correspond à $r = 1$), est donnée par les énoncés suivants, dits « conjectures de Weil » (voir Weil (1949), p. 507):

(CW1) (Théorème de Lefschetz). — *Il existe* $2r+1$ *familles d'entiers algébriques* $(\alpha_{ji})_{1\leq j\leq B_i}$, $0\leqslant i\leqslant 2r$, *telles qu'en posant, pour chaque* i, $P_i(t)=\prod_{j=1}^{B_i}(1-\alpha_{ji}t)$, *on ait*

$$Z(V;t)=\frac{P_1(t)\,P_3(t)\ldots P_{2r-1}(t)}{P_0(t)\,P_2(t)\ldots P_{2r}(t)}; \tag{4.1.1}$$

de plus, $P_0(t)=1-t$ et $P_{2r}(t)=1-q^rt$.

(CW2) (Equation fonctionnelle). — *Si on pose* $\chi=\sum_{i=0}^{2r}(-1)^i B_i$, *on a*

$$Z(V;1/q^rt)=\pm q^{r\chi/2}t^{\chi}Z(V;t)\,. \tag{4.1.2}$$

(CW3) (« Hypothèse de Riemann »). — *Pour tout couple d'indices* j, i, *on a*

$$|\alpha_{ji}|=q^{i/2}\,. \tag{4.1.3}$$

(CW4) (Rationalité des « polynômes de Weil » P_i). — *Chacun des polynômes* P_i *est à coefficients entiers rationnels, de terme constant égal à* 1.

(CW5) (Interprétation des entiers B_i comme nombres de Betti). — *Si* V *se relève en caractéristique* 0 *(autrement dit, s'il existe un anneau de valuation discrète* $\mathfrak{O}$, *contenu dans* $\mathbf{C}$, *et dont le corps résiduel s'identifie à* k, *et une variété projective non singulière* V_0, *définie sur* $\mathfrak{O}$, *et dont la variété réduite modulo l'idéal maximal de* $\mathfrak{O}$ *s'identifie à* V*), alors les* B_i *sont égaux aux nombres de Betti de* V_0, *considérée comme variété topologique complexe compacte de dimension complexe* r, *donc de dimension réelle* $2r$. *(L'exposant* χ, *dans l'équation fonctionnelle* (4.1.2), *est alors la caractéristique d'Euler-Poincaré de* V_0*).*

On remarquera que, compte tenu de la définition des P_i, (4.1.1) équivaut (voir th. 2, cor. 1 et remarque) à la collection d'égalités

$$N_m=\sum_{i,\,j}(-1)^i\alpha_{ji}^m\quad(m=1,2,\ldots);$$

de même, (4.1.2) équivaut à l'assertion suivante: quel que soit i $(0\leqslant i\leqslant 2r)$, les deux familles $(\alpha_{ji})_{1\leq j\leq B_{2r-i}}$ et $(q^r\alpha_{ji}^{-1})_{1\leq j\leq B}$ sont identiques (à une permutation près).

4.2. L'ensemble de ces conjectures a été démontré par Weil lui-même lorsque V est une *courbe* (th. 3), et lorsque V est une *variété abélienne* (voir

par exemple [9], notamment p. 140). Le cas où V est une *hypersurface* (c'est-à-dire où $r = n - 1$) a été traité par Dwork (1962, 1964; 1966, a) qui a montré, en perfectionnant les méthodes p-adiques de son article de 1960, qu'on a alors

$$(4.2.1) \qquad Z(V;t) = P(t)^{(-1)^n}/(1-t)(1-qt)\dots(1-q^{n-1}t),$$

$P(t)$ étant un polynôme de degré $d^{-1}((d-1)^{n+1} + (-1)^{n+1}(d-1))$: ceci prouve (CW1), (CW2) et (CW5) pour les hypersurfaces.

4.3. Les conjectures (CW1), (CW2) et (CW5) ont été démontrées en toute généralité par Artin et Grothendieck (voir Grothendieck (1964, a; b)) et, de deux manières différentes, par Lubkin (1967, 1968). Le principe de ces démonstrations est la construction, pour les variétés algébriques (ou plus précisément les schémas), d'une cohomologie à coefficients dans un corps K de caractéristique 0 (« cohomologie de Weil »), consistant en la donnée, pour tout $i \geqslant 0$, d'un foncteur H^i de la catégorie des schémas projectifs non singuliers dans la catégorie des espaces vectoriels de dimension finie sur K, cette famille de foncteurs possédant (entre autres) les propriétés suivantes:

(4.3.1) *Si* $\dim(V) = r$, *alors* $H^i(V) = 0$ *pour* $i > 2r$.

(4.3.2) (Formule « des traces », ou « des points fixes », de Lefschetz). — *Si f est un morphisme $V \to V$, et si $f_i = H^i(f)$ est l'endomorphisme correspondant dans $H^i(V)$, alors le nombre d'intersection $i(\Gamma \cdot \Delta)$ du graphe Γ de f avec la diagonale Δ de $V \times V$ est donné par*

$$i(\Gamma \cdot \Delta) = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i).$$

(4.3.3) (Formule de dualité). — *L'espace vectoriel $H^{2r}(V)$ est isomorphe à K (r désignant toujours la dimension de V), et il existe pour tout i tel que $0 \leqslant i \leqslant 2r$ une application bilinéaire $H^i(V) \times H^{2r-i}(V) \to H^{2r}(V) \simeq K$ mettant $H^i(V)$ et $H^{2r-i}(V)$ en dualité.*

(4.3.4) *Si V se relève en caractéristique 0 selon une variété complexe V_0, la « cohomologie de Weil » de V s'identifie à la cohomologie ordinaire de V_0 (à coefficients dans K).*

La « cohomologie de Weil » d'Artin-Grothendieck est la cohomologie l-adique étale, pour laquelle $K = \mathbf{Q}_l$, l désignant n'importe quel nombre premier différent de la caractéristique p du corps de base k; les « cohomologies de Weil » de Lubkin utilisent respectivement comme corps de

coefficients $K = \mathbf{Q}_l$, $l \neq p$ (Lubkin (1967)) et $K = \mathbf{Q}_p$ (Lubkin (1968)). A titre d'exemple, montrons comment la formule (4.1.1) peut se déduire de la formule des traces de Lefschetz: k et V étant fixés, soit f l'endomorphisme de V défini par $f(\mathbf{x}) = \mathbf{x}^{(q)}$ ($\mathbf{x} \in V$; voir chap. 8, § 2) et soit Γ le graphe de f dans $V \times V$; on peut montrer que tous les points du cycle intersection $\Gamma \cdot \Delta$ ont pour multiplicité 1; comme ces points correspondent bijectivement aux points de V invariants par f, donc rationnels sur k, la formule de Lefschetz donne

$$N_1 = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i);$$

appliquant le même raisonnement au corps de base k_m et à l'endomorphisme f^m, on trouve plus généralement, pour tout $m \geqslant 1$,

$$N_m = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i^m),$$

et par conséquent

$$\log Z(V;t) = \sum_{i=0}^{2r} (-1)^i \sum_{m \geqslant 1} Tr(f_i^m) \, t^m/m . \tag{4.3.5}$$

Mais K étant de caractéristique 0, on a, dans $K[[t]]$,

$$\det(1 - tf_i) = \exp\Big(-\sum_{m \geqslant 1} Tr(f_i^m) \, t^m/m\Big) \tag{4.3.6}$$

(c'est un résultat qui a déjà été mentionné au § 2, et qu'on peut prouver en triangularisant f_i sur la clôture algébrique $\overline{K}$ de K); si alors on pose $P_i^*(t) = \det(1 - tf_i)$, (4.3.5) et (4.3.6) donnent

$$Z(V;t) = \frac{P_1^*(t) \, P_3^*(t) \ldots P_{2r-1}^*(t)}{P_0^*(t) \, P_2^*(t) \ldots P_{2r}^*(t)}; \tag{4.3.7}$$

ceci prouve (CW1), moins le caractère algébrique des α_{ji}; mais il suffit de mettre le second membre de (4.3.7) sous forme irréductible, de noter $P_i(t)$ « ce qui reste » de $P_i^*(t)$ après cette simplification, et d'utiliser le théorème 2 et son corollaire 1, pour démontrer la totalité de (CW1).

Les conjectures (CW2) et (CW5) se démontrent de même à partir de (4.3.3) et (4.3.4). A l'heure actuelle, en revanche, les conjectures (CW3) et (CW4) ne semblent pas avoir été démontrées en toute généralité. Notons qu'il résulte de (CW3) que les polynômes de Weil P_i ne dépendent que de k

et V, et non du procédé, cohomologique ou autre, utilisé pour établir la formule (4.1.1).

§ 5. *Calcul explicite de certaines fonctions zêta.*

5.1. Ce dernier paragraphe donne, à titre d'illustration de ce qui précède, le calcul explicite des fonctions zêta de certaines variétés algébriques (courbes ou hypersurfaces) définies par des équations diagonales. On utilise essentiellement les résultats du chapitre 5, du chapitre 6 (§ 3), et le théorème suivant, dû à Davenport et Hasse (1934), qui permet de comparer les sommes de Gauss relatives à k et celles relatives à k_m ($m \geqslant 1$):

THÉORÈME 4 (Davenport-Hasse). — *Soient β et χ un caractère additif et un caractère multiplicatif non triviaux de k; pour $m \geqslant 1$, soient d'autre part $T^{(m)}$ et $N^{(m)}$ la trace et la norme dans l'extension k_m/k, et posons $\beta^{(m)} = \beta \circ T^{(m)}$, $\chi^{(m)} = \chi \circ N^{(m)}$. Alors*

(i) *$\beta^{(m)}$ est un caractère additif non trivial de k_m; $\chi^{(m)}$ est un caractère multiplicatif non trivial de k_m, et $\chi^{(m)}$ a même ordre que χ.*

(ii) *Si on désigne par τ et $\tau^{(m)}$ les sommes de Gauss $\tau(\chi \mid \beta)$ et $\tau(\chi^{(m)} \mid \beta^{(m)})$ relatives à k et k_m respectivement, on a*

$$\tau^{(m)} = (-1)^{m-1} \tau^m . \tag{5.1.1}$$

Démonstration. — (i) Il suffit de noter que $T^{(m)}: k_m^+ \to k^+$, et $N^{(m)}: k_m^* \to k^*$, sont des homomorphismes surjectifs (chap. 1, prop. 9 et 10).

(ii) (D'après Weil (1949), pp. 503-505). Pour tout polynôme unitaire $P(U) = U^h + a_1 U^{h-1} + \ldots + a_h$ appartenant à $k[U]$ (resp. à $k_m[U]$), posons $\varphi(P) = \beta(a_1)\chi(a_h)$ (resp. $\varphi^{(m)}(P) = \beta^{(m)}(a_1)\chi^{(m)}(a_h)$); φ et $\varphi^{(m)}$ sont évidemment des caractères multiplicatifs sur les anneaux principaux $k[U]$ et $k_m[U]$, et on peut leur associer, « à la Dirichlet », les « séries L » suivantes:

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

$$L_m(t) = \sum_{\substack{P \\ \text{unit.}}} \varphi^{(m)}(P)\, t^{\deg(P)} = \prod_{\substack{P \text{ unit.} \\ \text{irréd.}}} 1/(1 - \varphi^{(m)}(P)\, t^{\deg(P)}),$$

(P étant supposé appartenir à $k[U]$ et $k_m[U]$ respectivement, bien entendu.)

LEMME 1. — *On a* $L(t) = 1 + \tau t$, $L_m(t) = 1 + \tau^{(m)} t$.

Vérifions par exemple la première égalité. On a $L(t) = 1 + c_1 t + \ldots + c_h t^h + \ldots$, avec $c_h = \sum \varphi(P)$, cette somme étant étendue à tous les $P \in k[U]$ unitaires et de degré h, donc de la forme $U^h + a_1 U^{h-1} + \ldots + a_n$, les $a_i \in k$; pour $h = 1$, on trouve ainsi $c_1 = \sum_{a_1 \in k} \beta(a_1)\chi(a_1) = \tau$ (noter que $\bar{\chi}(0) = 0$); pour $h \geqslant 2$ au contraire, on trouve

$$c_h = q^{h-2}\Big(\sum_{a_1 \in k} \beta(a_1)\Big)\Big(\sum_{a_h \in k} \chi(a_h)\Big),$$

donc $c_h = 0$, chacune des deux sommes étant nulle (chap. 5, prop. 2 et 5).

LEMME 2. — *Si ω désigne une racine primitive m-ième de l'unité dans* **C**, *on a*

$$L_m(t^m) = \prod_{j=0}^{m-1} L(\omega^j t). \tag{5.1.2}$$

Pour chaque $P \in k[U]$, irréductible et unitaire, considérons le produit *fini*

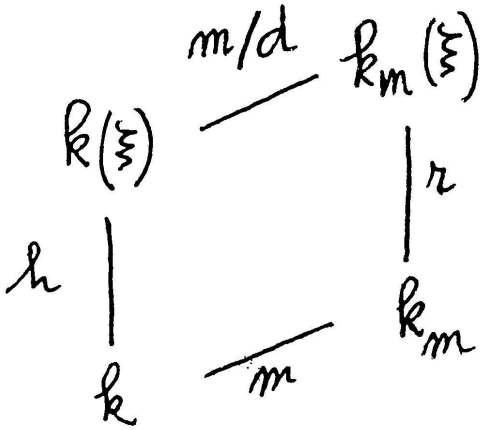
$$L_{m,P}(t^m) = \prod_{Q} 1/(1 - \varphi^{(m)}(Q)\, t^m),$$

Q parcourant seulement l'ensemble des facteurs irréductibles et unitaires de P dans $k_m[U]$; on a évidemment

$$L_m(t^m) = \prod_{\substack{P \text{ unit.} \\ \text{irréd.}}} L_{m,P}(t^m). \tag{5.1.3}$$

Transformons maintenant $L_{m,P}(t^m)$, P étant supposé fixé. Posons $h = \deg(P)$, et soit ξ une racine de P dans k; on a $[k(\xi):k] = h$, et bien entendu $[k_m:k] = m$; si alors $d = (h, m)$, le p.p.c.m. de h et m est égal à hm/d, et on a (chap. 1, prop. 4, cor. 1) $[k_m(\xi):k] = hm/d$, donc $[k_m(\xi):k_m] = h/d$. Il en résulte que la décomposition de P en facteurs irréductibles et unitaires de P dans $k_m[U]$ est de la forme

$$P = Q_1 Q_2 \ldots Q_d,$$



chacun des facteurs Q_i étant de degré $r = h/d$. Soit alors Q celui des Q_i dont ξ est racine, et calculons $\varphi^{(m)}(Q)$. Notons a_1 et a_n la trace et la norme de $-\xi$ dans l'extension $k(\xi)/k$, et b_1 et b_r la trace et la norme de $-\xi$ dans l'extension $k_m(\xi)/k_m$; on a $P(U) = U^h + a_1 U^{h-1} + \ldots + a_h$ et $Q(U) = U^r + b_1 U^{r-1} + \ldots + b_r$, et par conséquent

(5.1.4) $\varphi(P) = \beta(a_1)\,\chi(a_h)\,, \quad \varphi^{(m)}(Q) = \beta^{(m)}(b_1)\,\chi^{(m)}(b_r)\,.$

L'utilisation de la transitivité de la trace et de la norme dans le diagramme de corps ci-dessus donne d'autre part

(5.1.5) $T^{(m)}(b_1) = (m/d)\,a_1\,, \quad N^{(m)}(b_r) = a_h^{m/d}\,.$

(5.1.4), (5.1.5) et la définition de $\varphi^{(m)}$ permettent alors d'écrire

(5.1.6) $\varphi^{(m)}(Q) = \beta\big((m/d)\,a_1\big)\,\chi(a_h^{m/d}) = \varphi(P)^{m/d}\,.$

Les d facteurs irréductibles Q_i de P dans $k_m[U]$ donnent donc la même valeur à $\varphi^{(m)}$, d'où

(5.1.7) $L_{m,P}(t^m) = 1/(1-\varphi(P)^{m/d}t^{mh/d})^d\,.$

Mais, quel que soit $\alpha \in \mathbf{C}$, on a

(5.1.8) $(1-\alpha^{m/d}t^{mh/d})^d = \prod_{j=0}^{m-1}(1-\alpha(\omega^j t)^h)\,;$

les deux membres sont en effet des polynômes unitaires en t, à coefficients complexes, de même degré mh, et ayant les mêmes racines (toutes multiples d'ordre d). Dans (5.1.8), faisons $\alpha = \varphi(P)$, et portons dans (5.1.7); comme $h = \deg(P)$, il vient $L_{m,P}(t^m) = \prod_{j=0}^{m-1} 1/1(-\varphi(P)(\omega^j t)^{\deg(P)})$, ce qui, compte tenu de (5.1.3) et de la définition de $L(t)$, donne (5.1.2) et prouve le lemme 2.

Démontrons alors le théorème 4. Les lemmes 1 et 2 permettent d'écrire

$$1 + \tau^{(m)}t^m = \prod_{j=0}^{m-1}(1+\tau\omega^j t)\,;$$

la comparaison des termes de plus haut degré en t donne donc

$$\tau^{(m)} = \prod_{j=0}^{m-1}\tau\omega^j = \omega^{m(m-1)/2}\tau^m = (-1)^{m-1}\tau^m\,,$$

C.Q.F.D.

COROLLAIRE 1. — *Soient χ et ψ deux caractères multiplicatifs non triviaux de k, et supposons également $\chi\psi$ non trivial. Alors, si $\chi^{(m)} = \chi \circ N^{(m)}$ et si $\psi^{(m)} = \psi \circ N^{(m)}$, on a*

(5.1.9) $\pi(\chi^{(m)}, \psi^{(m)}) = (-1)^{m-1}\,\pi(\chi,\psi)^m\,.$

Démonstration. — Il suffit d'appliquer le théorème 4 et la proposition 9, (ii) du chapitre 5.

5.2. Appliquons alors le théorème 4 et son corollaire 1 au calcul des fonctions zêta des courbes de genre 1 étudiées au chapitre 6, sections 3.3 à 3.5 (dont on conserve les notations).

(1) *La courbe V_1 d'équation $Y^2 = 1 - X^3$ ($p \neq 2, 3$).*

Supposons d'abord $q \equiv 1 \pmod 6$; la formule (3.3.1) (chap. 6) appliquée au corps de base k_m donne $N_{1,m}^{\mathrm{aff}} = q^m + \pi(\varphi^{(m)}, \chi^{(m)}) + \pi(\varphi^{(m)}, \bar{\chi}^{(m)})$ $N_{1,m}^{\mathrm{aff}}$ étant évidemment le nombre de points de V_1 « à distance finie » et rationnels sur k_m; posons $\alpha = -\pi(\varphi, \chi)$, utilisons le corollaire 1 du théorème 4, et remarquons que V_1 admet exactement un point à l'infini, rationnel sur k; il vient alors $N_{1,m} = q^m + 1 - \alpha^m - \bar{\alpha}^m$, d'où finalement (th. 2, cor. 1):

$$Z(V_1; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt), \tag{5.2.1}$$

ce qui est évidemment conforme au théorème 3.

Supposons maintenant $q \equiv -1 \pmod 6$ (donc $p \equiv -1 \pmod 6$ et f impair). On aura besoin du lemme suivant:

LEMME 1. — *Soit $p \equiv -1 \pmod 6$, et soient φ_2 et χ_2 deux caractères multiplicatifs de $K = \mathbf{F}_{p^2}$, respectivement d'ordre 2 et d'ordre 3 (noter que $p^2 \equiv 1 \pmod 6$). Alors $\pi(\varphi_2, \chi_2) = p$.*

Démonstration. — Comme K contient six racines 6-ièmes de l'unité, il est facile de voir que le nombre N de solutions dans K^2 de l'équation $Y^2 = 1 - X^3$ satisfait à $N \equiv 5 \pmod 6$ (comparer avec le chap. 6, sect. A.1, exemple 2). Posons $\pi = \pi(\varphi_2, \chi_2)$; on a $N = p^2 + \pi + \bar{\pi}$ (chap. 6, (3.3.1)), et la congruence relative à N donne

$$\pi + \bar{\pi} \equiv 4 \pmod 6. \tag{5.2.2}$$

Mais $\pi, \bar{\pi} \in \mathbf{Z}[\rho]$ ($\rho = e^{2\pi i/3}$), $\pi\bar{\pi} = p^2$ (chap. 5, prop. 9, cor. 1), et p est *inerte* dans $\mathbf{Z}[\rho]$; ainsi, $\pi = \varepsilon p$, $\bar{\pi} = \bar{\varepsilon} p$, ε étant une racine 6-ième de l'unité. (5.2.2) donne alors $(\varepsilon + \bar{\varepsilon})p \equiv 4 \pmod 6$, puis $\varepsilon + \bar{\varepsilon} \equiv -4 \equiv 2 \pmod 6$, ce qui implique $\varepsilon = 1$ (examiner les six valeurs possibles de ε). Finalement, $\pi = \varepsilon p = p$, C.Q.F.D.

Calculons alors $N_{1,m}^{\mathrm{aff}}$. Si m est impair, on a $q^m \equiv -1 \pmod 3$, donc $N_{1,m}^{\mathrm{aff}} = q^m$. Supposons maintenant m pair, $m = 2m'$, et soient φ et χ deux caractères multiplicatifs de k_2, respectivement d'ordre 2 et d'ordre 3; le lemme 1 et le corollaire 1 du théorème 4 (appliqué à $k_2/\mathbf{F}_{p^2}$) donnent d'abord $\pi(\varphi, \chi) = (-1)^{f-1}p^f = q$; le corollaire 1 du théorème 4, appliqué à k_m/k_2, donne d'autre part $\pi(\varphi^{(m')}, \chi^{(m')}) = (-1)^{m'-1}q^{m'} = -(-q)^{m'}$,

donc (chap. 6, (3.3.1)) $N_{1,m}^{\mathrm{aff}} = q^m - 2(-q)^{m/2}$. Posons alors $\alpha = iq^{1/2}$; les calculs précédents montrent que, quelle que soit la parité de m, on a $N_{1,m}^{\mathrm{aff}} = q^m - \alpha^m - \bar{\alpha}^m$, donc $N_{1,m} = q^m + 1 - \alpha^m - \bar{\alpha}^m$; finalement, on trouve encore

$$Z(V_1; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt); \tag{5.2.3}$$

compte tenu de la valeur explicite $\alpha = iq^{1/2}$, on a même, dans ce cas,

$$Z(V_1; t) = (1+qt^2)/(1-t)(1-qt). \tag{5.2.4}$$

(2) *La courbe V_2 d'équation $Y^2 = 1 - X^4$ ($p \neq 2$).*

Supposons d'abord $q \equiv 1 \pmod 4$; la formule (3.3.2) (chap. 6) appliquée au corps de base k_m, combinée au corollaire 1 du théorème 4, donne, comme en (1), $N_{2,m}^{\mathrm{aff}} = q^m - 1 - \alpha^m - \bar{\alpha}^m$, avec $\alpha = -\pi(\varphi, \psi)$; d'autre part, V_2 admet à l'infini un point double rationnel sur k: comptons-le pour *deux* (ce qui revient à remplacer V_2 par sa normalisée V_2^* : voir d'ailleurs chap. 8, sect. 2.4); on trouve ainsi $N_{2,m}^* = q^m + 1 - \alpha^m - \bar{\alpha}^m$, donc

$$Z(V_2^*; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt), \tag{5.2.5}$$

ce qui est toujours conforme au théorème 3. Remarquer que la fonction zêta de V_2 *non normalisée* est $Z(V_2; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-qt)$.

Si on suppose au contraire $q \equiv -1 \pmod 4$, un calcul analogue à celui fait en (1) (pour $q \equiv -1 \pmod 6$) donnerait encore

$$Z(V_2^*; t) = (1+qt^2)/(1-t)(1-qt). \tag{5.2.6}$$

(3) *La courbe V_3 d'équation $Y^3 = 1 - X^3$ ($p \neq 3$).*

On laisse au lecteur le soin de vérifier que les formules (5.2.5) et (5.2.6) restent valides pour la normalisée V_3^* de V_3, respectivement pour $q \equiv 1 \pmod 3$ (et avec $\alpha = -\pi(\chi, \chi)$: voir chap. 6, (3.3.3)), d'une part; et pour $q \equiv -1 \pmod 3$, d'autre part.

(4) *La courbe V_4 d'équation $Y^2 = X - X^3$* (pour $q \equiv 1 \pmod 4$).

Il résulte des calculs faits au chapitre 6 (sect. 3.4) que

$$Z(V_4; t) = Z(V_2^*; t). \tag{5.2.7}$$

(En fait, V_4 est un modèle projectif non singulier de V_2, de sorte qu'on peut choisir pour V_2^* la courbe V_4.) L'égalité (5.2.7) reste d'ailleurs vraie pour $q \equiv -1 \pmod 4$.

5.3. Terminons par deux exemples simples d'hypersurfaces (dans $\mathbf{P}_3$).

(5) *La quadrique d'équation homogène* $X^2 + Y^2 + Z^2 + T^2 = 0$ $(p \neq 2)$.

Le nombre $N_m{}^c$ de points rationnels sur k_m du *cône* défini dans $\mathbf{A}_4$ par l'équation ci-dessus est donné (chap. 6, th. 1) par

$$N_m{}^c = q^{3m} + q^{-m}(q^m - 1)\,\tau(\varphi^{(m)})^4\,,$$

φ désignant le caractère de Legendre de k; mais $\tau(\varphi^{(m)})^2 = q^m\,\varphi^{(m)}(-1)$, et $(q^m - 1)\,N_m + 1 = N_m{}^c$ (N_m étant le nombre de points de la quadrique rationnels sur k_m); d'où immédiatement $N_m = q^{2m} + 2q^m + 1$, et (th. 2, cor. 1)

$$Z(V_5; t) = 1/(1-t)\,(1-qt)^2\,(1-q^2t)\,, \tag{5.3.1}$$

V_5 désignant la quadrique étudiée. (On aurait pu calculer $N_m{}^c$ à l'aide des formules du chap. 6, prop. 2). Ce résultat est évidemment conforme à (4.2.1) (sect. 4.2), c'est-à-dire au théorème de Dwork pour les hypersurfaces: on a $P(t) = 1 - qt$, de degré 1, et $(-1)^n = (-1)^3 = -1$, ce qui « envoie » $P(t)$ au dénominateur.

(6) *La surface cubique d'équation homogène* $X^3 + Y^3 + Z^3 + T^3 = 0$ $(p \neq 3)$.

On se limitera pour simplifier au cas où $q \equiv 1 \pmod 3$. On pourrait procéder comme en (5), et utiliser le théorème 1 du chapitre 6. Il est plus commode de remarquer que (avec des notations évidentes) $N_m = N_m^{\mathrm{aff}} + N_m^{\mathrm{inf}}$; N_m^{aff} est le nombre de solutions rationnelles sur k_m de l'équation $X^3 + Y^3 + Z^3 = -1$; si χ est un caractère multiplicatif d'ordre 3 de k, le théorème 2 du chapitre 6, la proposition 10 du chapitre 5 et le théorème 4 ci-dessus donnent

$$N_m^{\mathrm{aff}} = q^{2m} + (-\pi_1)^m + (-\bar{\pi}_1)^m + 3\,\pi_2{}^m + 3\,\bar{\pi}_2{}^m\,, \tag{5.3.2}$$

avec $\pi_1 = \pi(\chi, \chi) = -\pi(\chi, \chi, \chi)$ (chap. 5, prop. 10, (i)) et $\pi_2 = \pi(\chi, \chi, \bar{\chi})$; quant à N_m^{inf}, c'est le nombre de points rationnels sur k_m de la cubique d'équation projective $X^3 + Y^3 + Z^3 = 0$; d'où

$$N_m^{\mathrm{inf}} = q^m + 1 - (-\pi_1)^m - (-\pi_1)^m \tag{5.3.3}$$

(chap. 6, (3.3.3); tenir compte des trois points à l'infini !): au total,

$$N_m = q^{2m} + q^m + 1 + 3\,\pi_2{}^m + 3\,\bar{\pi}_2{}^m\,, \tag{5.3.4}$$

et (th. 2, cor. 1, une dernière fois)

(5.3.5) $\quad Z(V_6; t) = 1/(1-t)(1-qt)(1-q^2t)(1-\pi_2 t)^3(1-\bar{\pi}_2 t)^3$,

V_6 désignant la surface cubique étudiée. Ce résultat est conforme aux conjectures de Weil: on a $P_0(t) = 1 - t$, $P_1(t) = P_3(t) = 1$, $P_4(t) = 1 - q^2t$, et $P_2(t) = (1-qt)(1-\pi_2 t)^3(1-\pi_2 t)^3$; l'hypothèse de Riemann se réduit à $|\pi_2| = |\bar{\pi}_2| = |\pi(\chi, \chi, \bar{\chi})| = q$ (chap. 5, prop. 10, cor. 1, (ii)); la « caractéristique d'Euler-Poincaré » est égale à $1 + 7 + 1 = 9$, et l'équation fonctionnelle s'écrit $Z(V_6; 1/q^2t) = -q^9t^9Z(V_6; t)$.

Notes sur le chapitre 9

§ **1-2-3-4**: l'idée d'étudier arithmétiquement un corps de fonctions algébriques d'une variable sur un corps fini semble apparaître nettement pour la première fois chez Dedekind (1857). Mais c'est dans la thèse d'Artin (1924), puis dans les travaux de Schmidt (1931) et Hasse (1933, 1934, 1936), qu'est définie la notion de fonction zêta (« Kongruenzzetafunktion ») et formulée l'« hypothèse de Riemann » en caractéristique p (Artin, Schmidt, Hasse utilisent le langage des corps de fonctions algébriques d'une variable, et non celui des courbes: mais ces deux langages sont équivalents, ou plutôt, le sont devenus depuis les « Foundations » de Weil; voir d'ailleurs Weil (1949), *Introduction*). L'équation fonctionnelle pour $\zeta(V; s)$ (c'est-à-dire, aux notations près, la proposition 3) est due à Schmidt (1931); la démonstration de l'hypothèse de Riemann pour $g = 1$ est due à Hasse (1933, 1934), et, pour g quelconque, à Weil (1940; 1948, a). Les diverses définitions de $Z(V; t)$ données au paragraphe 1 figurent, pour une courbe, dans Weil (1948, a), et, pour une variété projective non singulière de dimension quelconque, dans Weil (1949); cet article contient également l'énoncé (et, pour des cas particuliers, la vérification) des « conjectures de Weil ». L'existence d'une « formule de Lefschetz » en géométrie algébrique est conjecturée dans Weil (1954) (p. 556): d'où la notion de « cohomologie de Weil » — cette terminologie étant d'ailleurs considérée par Weil lui-même comme « tout à fait inadéquate » (*wholly unsuitable*). Au sujet du lien formel entre théories cohomologiques des variétés algébriques et propriétés des fonctions zêta, voir Demazure (1969), notamment §§ 7 et 9. Au sujet du lien entre méthodes p-adiques et méthodes cohomologiques, voir Katz (1972) (cet exposé contient une abondante bibliographie).

Signalons qu'à côté des fonctions zêta, on peut (comme en arithmétique) construire, pour les variétés algébriques, des « séries L »; pour une définition générale (en langage des schémas, et englobant d'ailleurs les séries L de la théorie des nombres), voir [**16**], pp. 86-91. La rationalité des séries L des

variétés algébriques a été établie par Grothendieck (1964, b); voir également Dwork (1966, b). Pour l'application de ce résultat à l'étude des sommes exponentielles, voir notamment Bombieri (1966).

§ **5**: les exemples de ce paragraphe sont empruntés essentiellement à Davenport-Hasse (1934) et à Weil (1949). Signalons que le lemme 1 (sect. 5.2) peut aussi se démontrer à l'aide de la proposition 9, (ii) (chap. 5), et du résultat suivant, dû à Stickelberger (1890): si χ est un caractère multiplicatif de $\mathbf{F}_{p^2}$, et si θ est un élément primitif de $\mathbf{F}_{p^2}/\mathbf{F}_p$, on a $\tau(\chi \mid \beta) = \chi(\theta)\, p$, si $p \neq 2$, et $\tau(\chi \mid \beta) = p$ si $p = 2$; pour une démonstration de ce dernier énoncé, voir aussi Carlitz (1956, a).

Pour $V = V_1$ et $q \equiv -1 \pmod 6$, ou $V = V_2{}^*$ et $q \equiv -1 \pmod 4$, ou $V = V_3{}^*$ et $q \equiv -1 \pmod 3$, on a trouvé la même expression

$$Z(V; t) = (1+qt^2)/(1-t)\,(1-qt);$$

ceci résulte (1) du fait que, dans les trois cas, on a $N_1 = q + 1$, et (2) de la relation $Z(V; t) = (1 + (N_1 - q - 1)\, t + qt^2)/(1-t)\,(1-qt)$, valable pour toute courbe V (projective, non singulière) de genre 1, définie sur k et ayant N_1 points rationnels sur k (cette relation se déduit facilement du théorème 3 et du théorème 2, corollaire 1 et remarque). En fait, si deux courbes de genre 1, définies sur k, ont même nombre N_1 de points rationnels sur k, alors, elles ont le même nombre N_m de points rationnels sur k_m pour tout m, puisqu'elles ont même fonction zêta (appliquer la formule ci-dessus !): on peut prouver que ceci se produit si et seulement si les deux courbes sont isogènes sur k (voir [**4**], p. 242, pour la partie « si », et Tate (1966), pour la partie « seulement si ».)

BIBLIOGRAPHIE

1. *Ouvrages généraux, monographies.*

[1] Artin, E. *Geometric Algebra*, Interscience Publishers (1957).

[2] —— *Algebraic Numbers and Algebraic Functions*, Gordon and Breach (1967).

[3] Borevich, Z. I. and I. R. Shafarevich. *Number Theory*, Academic Press (1966).

[4] Cassels, J. W. S. *Diophantine equations with special reference to elliptic curves* (survey article), J. London Math. Soc., 41 (1966), pp. 193-291.

[5] Eichler, M. *Introduction to the theory of algebraic numbers and functions*, Academic Press (1966).

[6] Gel'fand, A. et I. Linnik. *Méthodes élémentaires dans la théorie analytique des nombres*, Gauthier-Villars (1965).

[7] Greenberg, M. J. *Lectures on forms in many variables*, Benjamin (1969).

[8] HASSE, H. *Vorlesungen über Zahlentheorie*, Springer (1950).
[9] LANG, S. *Abelian Varieties*, Interscience Publishers (1959).
[10] —— *Algebra*, Addison-Wesley (1965).
[11] —— *Algebraic Number Theory*, Addison-Wesley (1970).
[12] —— *Introduction to Algebraic Geometry*, Interscience Publishers (1958).
[13] LEVEQUE, W. J. (editor). *Studies in Number Theory*, MAA Studies, vol. 6 (1969).
[14] MORDELL, L. J. *Diophantine Equations*, Academic Press (1969).
[15] SAMUEL, P. *Méthodes d'algèbre abstraite en géométrie algébrique*, Springer (1967).
[16] SCHILLING, O. F. G. (editor). *Arithmetical Algebraic Geometry*, Harper & Row (1965).
[17] SERRE, J. P. *Cours d'arithmétique*, Presses Universitaires de France (1970).
[18] SKOLEM, T. *Diophantische Gleichungen*, Springer (1938).
[19] WEIL, A. *Basic Number Theory*, Springer (1967).
[20] —— *Courbes algébriques et variétés abéliennes*, Hermann (1970).

2. *Articles, mémoires.*

ARTIN, E. (1924). Quadratische Körper im Gebiet der höheren Kongruenzen, I, II, *Math. Z.*, **19**, pp. 153-206, 207-246.
AX, J. (1964). Zeroes of polynomials over finite fields, *Amer. J. Math.*, **86**, pp. 255-261.
—— (1965, a). A field of cohomological dimension 1 which is not (C_1), *Bull. Amer. Math. Soc.*, **71**, p. 717.
—— (1965, b). Proof of some conjectures in cohomological dimension, *Proc. Amer. Math. Soc.*, **16**, pp. 1214-1221.
—— (1968). The elementary theory of finite fields, *Ann. of Math.*, **88**, pp. 239-271.
BATEMAN, P. T. and R. M. STEMMLER (1962). Waring's problem for algebraic number fields and primes of the form $(p^r-1)/(p^d-1)$, *Illinois J. Math.*, **6**, pp. 142-156.
BIRCH, B. J. and H. P. F. SWINNERTON-DYER (1965). Notes on elliptic curves, II, *J. reine angew. Math.*, **218**, pp. 79-108.
BOMBIERI, E. (1966). On exponential sums in finite fields, *Amer. J. Math.*, **88**, pp. 71-105.
BOREL, E. (1894). Sur une application d'un théorème de M. Hadamard, *Bull. Sci. Math.*, **18**, pp. 22-25.
CARLITZ, L. (1953). Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.*, **75**, pp. 405-427.
—— (1954). Invariant theory of systems of equations in a finite field, *J. Analyse Math.*, **3**, pp. 382-413.
—— (1956, a). The number of solutions of a particular equation in a finite field, *Publ. Math. Debrecen*, **4**, pp. 379-383.
—— (1956, b). Solvability of certain equations in a finite filed, *Quart. J. Math. (Oxford)*, **7**, pp. 3-4.
CASSELS, J. W. S. (1970). On Kummer sums, *Proc. London Math. Soc.*, **21**, pp. 19-27.
CHEVALLEY, C. (1935). Démonstration d'une hypothèse de M. Artin, *Abh. Math. Sem. Hamburg*, **11**, pp. 73-75.
CHOWLA, S. (1961). On the congruence $\Sigma\, a_i x_i^k \equiv 0\ (p)$, *J. Indian Math.Soc.*, **25**, pp. 47-48.
—— H. B. MANN and E. G. STRAUS (1959). On diagonal forms over finite fields, *Norske Vid. Selsk. Forh. (Trondheim)*, **32**, pp. 74-80.
COHEN, E. (1956). Congruences in algebraic number fields involving sums of similar powers, *Trans. Amer. Math. Soc.*, **83**, pp. 547-556.
DAVENPORT, H. und H. HASSE (1934). Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. reine angew. Math.*, **172**, pp. 151-182.
—— and D. J. LEWIS (1963). Homogeneous additive equations, *Proc. Royal Soc. (London)*, **274**, pp. 443-460.

DEDEKIND, R. (1857). Abriss einer Theorie der höheren Kongruenzen in Bezug auf einer reellen Primzahl-Modulus, *J. reine angew. Math.*, **54**, pp. 1-26.

DEMAZURE, M. (1969). Motifs des variétés algébriques, Séminaire Bourbaki, 1969/70, exposé n° 365.

DEMYANOV, V. B. (1956). Sur la représentation de zéro par des formes du type $\Sigma a_i X_i^n$ (en russe), *Dokl. Akad. Nauk SSSR*, **105**, pp. 203-205.

DEURING, M. (1941). Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg*, **14**, pp. 197-272.

DICKSON, L. E. (1909). Sets of solutions of $x^e + y^e + z^e \equiv 0 \pmod{p}$, *J. reine angew. Math.*, **135**, pp. 181-188.

DWORK, B. (1960). On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.*, **82**, pp. 631-648.

—— (1962). On the zeta function of a hypersurface, I, Inst. Hautes Etudes Sci., *Publ Math.* n° 12, pp. 5-68.

—— (1964). On the zeta function of a hypersurface, II, *Ann. of Math.*, **80**, pp. 227-299.

—— (1966, a). On the zeta function of a hypersurface, III, *Ann. of Math.*, **83**, pp. 457-519.

—— (1966, b). On the rationality of the zeta functions and L series, Proceedings of a Conference on Local Fields (Driebergen, 1966), Springer Verlag (1967).

EULER, L. (1760). Demonstratio circa residua ex divisione potestatum per numeros primos resultantia, *Novi Comm. Acad. Petrop.*, 1760, pp. 74-104.

FATOU, P. (1906). Etude de la série de Taylor sur son cercle de convergence, *Acta Math.*, **30**, pp. 364-400.

GALOIS, E. (1830). Sur la théorie des nombres, *Bull. Sci. Math. Férussac*, XIII, § 218.

GRAY, J. F. (1960). Diagonal forms of odd degree over a finite field, *Michigan Math. J.*, **7**, pp. 297-301.

GROTHENDIECK, A. (1964, a). Cohomologie l-adique et fonctions L, Séminaire de Géométrie Algébrique, 1964/65, Inst. Hautes Etudes Sci., Bures-sur-Yvette.

—— (1964, b). Formule de Lefschetz et rationalité des fonctions L, Séminaire Bourbaki, 1964/65, exposé n° 279.

HARDY, G. H. and J. E. LITTLEWOOD (1922). Some problems of Partitio Numerorum, IV, *Math. Z.*, **12**, pp. 161-188.

HASSE, H. (1933). Beweis des Analogons der Riemannschen Vermutung..., *Nachr. Ges. Wiss. Göttingen, Math. Phys. Kl.*, 1933, pp. 253-262.

—— (1934). Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörper, *Abh. Math. Sem. Hamburg*, **10**, pp. 325-348.

—— (1936). Zur Theorie der abstrakten elliptischen Funktionenkörper, I, II, III, *J. reine angew. Math.*, **175**, pp. 55-62, 69-88, 193-208.

HUA, L. K. and H. S. VANDIVER (1948). On the existence of solutions of certain equations in finite fields, *Proc. Nat. Acad. Sci. USA*, **34**, pp. 258-263.

—— (1949, a). Characters over certain types of rings, with applications to the theory of equations in a finite field, *Proc. Nat. Acad. Sci. USA*, **35**, pp. 94-99.

—— (1949, b). On the nature of the solutions of certain equations in a finite field, *Proc. Nat. Acad. Sci. USA*, **35**, pp. 481-487.

HURWITZ, A. (1909). Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod{p}$, *J. reine angew. Math.*, **136**, pp. 272-292.

IGUSA, J. (1949). On the theory of algebraic correspondences and its application to the Riemann hypothesis in function fields, *J. Math. Soc. Japan*, **1**, pp. 147-201.

JACOBSTHAL, E. (1907). Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate, *J. reine angew. Math.*, **132**, pp. 238-245.

JOLY, J. R. (1968). Sommes de puissances m-ièmes dans les anneaux P-adiques et les anneaux d'entiers algébriques, *Enseign. Math.*, **14**, pp. 197-204.

—— (1971). Nombre de solutions de certaines équations diagonales sur un corps fini, *C. R. Acad. Sci. Paris*, **272**, pp. 1549-1552.

KATZ, N. M. (1971). On a theorem of Ax, *Amer. J. Math.*, **93**, pp. 485-499.

—— (1972). Travaux de Dwork, Séminaire Bourbaki, 1971/72, exposé nº 409.

LANG, S. (1952). On quasi-algebraic closure, *Ann. of Math.*, **55**, pp. 373-390.

—— (1956). Algebraic groups over finite fields, *Amer. J. Math.*, **78**, pp. 555-563.

—— and A. WEIL (1954). Number of points of varieties in finite fields, *Amer. J. Math.*, **76**, pp. 819-827.

LEBESGUE, V. A. (1837). Recherches sur les nombres, I, *J. Math. Pures Appl.*, **2**, pp. 253-292.

—— (1838). Recherches sur les nombres, II, III, *J. Math. Pures Appl.*, **3**, pp. 113-131, 132-144.

LEWIS, D. J. (1960). Diagonal forms over finite fields, *Norske Vid. Selsk. Forh. (Trondheim)*, **33**, pp. 61-65.

LIBRI, G. (1832). Mémoire sur la théorie des nombres, *J. reine angew. Math.*, **9**, pp. 261-276.

LUBKIN, S. (1967). On a conjecture of A. Weil, *Amer. J. Math.*, **89**, pp. 443-548.

—— (1968). A p-adic proof of Weil's conjectures, *Ann. of Math.*, **87**, pp. 105-255.

MANIN, I. (1956). Sur les congruences cubiques selon un module premier (en russe), *Izv. Akad. Nauk SSSR*, **20**, pp. 673-678.

MORDELL, L. J. (1922). Three lectures on Fermat's last theorem, London Univ. Press.

MORLAYE, B. (1971). Equations diagonales non homogènes sur un corps fini, *C. R. Acad. Sci. Paris*, **272**, pp. 1545-1548.

—— (1972). Démonstration élémentaire d'un théorème de Davenport et Hasse, *Enseign. Math.*, à paraître.

NAGATA, M. (1957). Note on a paper of Lang concerning quasi-algebraic closure, Mem. Univ. Kyoto, **30**, pp. 237-241.

NISNEVICH, L. (1954). Sur le nombre de points d'une variété algébrique sur un corps fini premier (en russe), *Dokl. Akad. Nauk SSSR*, **99**, pp. 17-20.

PORTER, A. D. (1966). Special equations in a finite field, *Math. Nachr.*, **32**, pp. 277-279.

RAJWADE, A. R. (1970). A note on the number N_p of solutions of the congruence $y^2 \equiv x^3 - Dx \pmod{p}$, *Proc. Cambridge Philos. Soc.*, **67**, pp. 603-605.

REDEI, L. (1846). Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged*, **11**, pp. 63-70.

ROQUETTE, P. (1953). Arithmetische Beweis der Riemannschen Vermutung, *J. reine angew. Math.*, **191**, pp. 199-252.

SAMUEL, P. (1967). Courbes algébriques, *Enseign. Math.*, **13**, pp. 305-311.

SCHMIDT, F. K. (1931). Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Z.*, **33**, pp. 1-32.

SCHUR, I. (1916). Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod{p}$, *Jahresbericht DMW*, **25**, pp. 114-120.

SCHWARZ, S. (1948, a). On Waring's problem for finite fields, *Quart. J. Math. (Oxford)*, **19**, pp. 123-128.

—— (1948, b). On the equation $a_1 x_1{}^k + a_2 x_2{}^k + \ldots + a_k x_k{}^k = 0$ in finite fields, *Quart. J. Math. (Oxford)*, **19**, pp. 160-163.

—— (1950). On universal forms in finite fields, *Casopis Pest. Mat. Fys.*, **75**, pp. 45-50.

—— (1956). On a type of universal forms in discretely normed fields, *Acta Univ. Szeged*, **17**, pp. 5-19.

SERRE, J. P. (1959). Rationalité des fonctions ζ des variétés algébriques (d'après Dwork), Séminaire Bourbaki, 1959/60, exposé nº 198.

STICKELBERGER, L. (1890). Über eine Verallgemeinerung von der Kreistheilung, *Math. Annalen*, **37**, pp. 321-367.

TATE, J. (1966). Endomorphisms of abelian varieties over finite fields, *Inventiones Math.*, **2**, pp. 134-144.

TERJANIAN, G. (1966). Sur les corps finis, *C. R. Acad. Sci. Paris*, **262**, pp. 167-169.
—— (1972). Dimension arithmétique d'un corps, à paraître.
TIETÄVÄINEN, A. (1968). On diagonal forms over finite fields, *Ann. Univ. Turku, Ser. A I*, n° 118, 10 p.
TORNHEIM, L. (1938). Sums of n-th powers in fields of prime characteristic, *Duke Math. J.*, **4**, pp. 359-362.
TSEN, C. C. (1933). Divisionsalgebren über Funktionenkörpern, *Nachr. Ges. Wiss. Göttingen*, 1933, pp. 335-339.
WARNING, E. (1935). Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Hamburg*, **11**, pp. 76-83.
WATERHOUSE, W. C. (1969). Abelian varieties over finite fields, *Ann. Sci. Ec. Norm. Sup., Sér.* 4, **2**, pp. 521-560.
(MACLAGLAN-) WEDDERBURN, J. H. (1905). A theorem on finite algebras, *Trans. Amer. Math. Soc.*, **6**, pp. 349-352.
WEIL, A. (1940). Sur les corps de fonctions algébriques à corps de constantes fini, *C. R. Acad. Sci. Paris*, **210**, pp. 592-594.
—— (1948, a). Sur les courbes algébriques et les variétés qui s'en déduisent, *Actual. Sci. Ind.*, n° 1041, Hermann, Paris (=[20], 1re partie).
—— (1948, b). On some exponential sums, *Proc. Nat. Acad. Sci. USA*, **34**, pp. 204-207.
—— (1949). Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55**, pp. 497-504.
—— (1954). Abstract versus classical algebraic geometry. *Proc. Intern. Cong. Math.* (Amsterdam), vol. III, pp. 550-558.
WITT, E. (1931). Über die Kommutativität endlicher Schiefkörper, *Abh. Math. Sem. Hamburg*, **8**, p. 413.
YAMAMOTO, K. (1959). The Artin-Hasse-Shafarevich function, *Japan J. Math.*, **29**, pp. 165-172.

(Reçu le 25 septembre 1972)

Jean-René Joly
Université Scientifique et Médicale de Grenoble
Institut de Mathématiques Pures
B. P. 116
F-38 — Saint Martin d'Hères