Chapitre 7 THÉORÈME D'AX

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.04.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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 ord (α) 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 $\operatorname{ord}\big(1/(q-1)\big) = 0$. 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) $\operatorname{ord}(c_j) = \operatorname{ord}\big(-q/(q-1)\big) = \operatorname{ord}(q) = \operatorname{ord}(p^f) = f \operatorname{ord}(p) = f(p-1)$ (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

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

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,

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

$\mathbf{t}^{ju'}$ signifiant évidemment ${t_0}^{j}{t_1}^{ju1} \ldots {t_n}^{ju_n}$; 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