Chapitre 3 THÉORÈMES DE CHEVALLEY ET WARNING

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).