

COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 3 Les théorèmes de Chevalley et Warning

Cours de l'institut Fourier, tome 4 (1971), p. 1-9

http://www.numdam.org/item?id=CIF_1971__4__A3_0

© Institut Fourier – Université de Grenoble, 1971, tous droits réservés.

L'accès aux archives de la collection « Cours de l'institut Fourier » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Chapitre 3

Les théorèmes de Chevalley et Warning

Nous conservons ici les notations et conventions adoptées au début du chapitre 2.

(3.1). Le théorème de Chevalley-Warning.

Théorème 1 (Chevalley-Warning). - Soit $F_1, F_2, \dots, F_r$ une famille de r polynômes appartenant à $K[X] = K[X_1, \dots, X_n]$ et de degrés respectifs $d_1, d_2, \dots, d_n$; désignons par V l'ensemble des solutions dans K^n du système d'équations

$$(\Sigma) \quad \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ \dots \\ F_r(X_1, \dots, X_n) = 0 \end{cases}$$

et posons $N = \text{card}(V)$. Alors, si

$$(1) \quad d = d_1 + d_2 + \dots + d_r < n,$$

on a la congruence

$$(2) \quad N \equiv 0 \pmod{p}.$$

Démonstration. Posons

$$(3) \quad F = (1 - F_1^{q-1})(1 - F_2^{q-1}) \dots (1 - F_r^{q-1}).$$

On vérifie sans peine que $F(x) = 1$ si et seulement si $F_1(x) = \dots = F_r(x) = 0$, autrement dit si $x \in V$, et que $F(x) = 0$ si au

contraire $x \notin V$; la fonction polynomiale $x \mapsto F(x)$ est donc égale à la fonction caractéristique de V à valeurs dans K , et comme K est de caractéristique p , la congruence à démontrer équivaut à l'égalité

$$(4) \quad \sum_{x \in K^n} F(x) = 0 ;$$

or, par définition même de F , et compte tenu de l'hypothèse (1),

$$\deg(F) \leq d(q-1) < n(q-1)$$

et (4) résulte du théorème 3 du chapitre 2 (attention: d n'a pas ici la même signification que dans le théorème 3 en question).

Corollaire 1 ("théorème de Chevalley"). - Mêmes données et hypothèses (y compris (1)) que dans le théorème 1. Si chacun des polynômes F_j est sans terme constant (et en particulier si chaque F_j est une forme de degré $d_j > 0$), alors le système (Σ) admet dans K^n une solution autre que la solution triviale $(x_1, \dots, x_n) = (0, \dots, 0)$.

Démonstration. L'absence de termes constants montre que l'origine de K^n appartient à V , donc que $N \geq 1$; le théorème 1 prouve par ailleurs que N est divisible par p ; on a donc $N \geq p$, et le nombre $N - 1$ de solutions non triviales de (Σ) est donc $\geq p - 1 \geq 2 - 1 = 1$, c.q.f.d.

Exemple d'application de ce corollaire: toute forme quadratique à 3 variables ou plus sur un corps fini est isotrope.

On laisse au lecteur le soin de se fabriquer d'autres exemples.

Corollaire 2 (Warning). - Mêmes données et hypothèses que dans le théorème 1. Soient G un polynôme, G^* le polynôme réduit correspondant à G .

Alors, si

$$(5) \quad \deg(G^*) < (n - d)(q - 1) ,$$

on a l'égalité

$$(6) \quad \sum_{x \in V} G(x) = 0 .$$

Démonstration. On sait (chapitre 2, théorème 1, (i) et (iii)) que les fonctions polynomiales associées à G et à G^* sont égales. Par ailleurs, le polynôme F défini par (3) vaut 1 sur V et 0 en dehors de V .

On a donc

$$(7) \quad \sum_{x \in V} G(x) = \sum_{x \in K^n} F(x) G^*(x) ;$$

or, d'après (5), $\deg(FG^*) < d(q - 1) + (n - d)(q - 1) = n(q - 1)$, et (6) résulte alors de (7) et du théorème 3 (chapitre 2) appliqué au polynôme FG^* .

(3.2). Intermède historico-technique.

Les résultats démontrés dans le paragraphe précédent (et obtenus par Chevalley et Warning en 1935) ont une histoire intéressante. En 1933, Tsen avait démontré ceci (voir [29] et [2]):

si $L = k(T)$ est le corps des fractions rationnelles à une variable T sur un corps algébriquement clos k , alors L possède la propriété suivante:

(B₀) Si M est un corps gauche (c'est-à-dire non nécessairement commutatif) de centre L et de degré fini sur L , alors $M = L$.

Artin remarqua que la méthode de Tsen consistait essentiellement

1°) à prouver que le corps L possède la propriété suivante:

(C₁) si $F(X_1, \dots, X_n)$ est un polynôme homogène à coefficients dans L et de degré $d < n$, alors l'équation $F(X_1, \dots, X_n) = 0$ admet au moins une solution non triviale dans L^n ,

puis

2°) à déduire directement la propriété (B₀) de la propriété (C₁) (en "oubliant" la définition particulière du corps L).

Comme les corps finis possèdent évidemment la propriété (B₀)^(*), Artin fut alors amené à conjecturer ("hypothèse de M. Artin")

les corps finis possèdent la propriété (C₁).

Cette conjecture fut immédiatement démontrée en caractéristique 2 par Völsch, puis en caractéristique quelconque par Chevalley (Chevalley, [2]) qui montra qu'on pouvait même remplacer l'hypothèse homogène par l'hypothèse plus faible sans terme constant et que la propriété s'étendait à des systèmes d'équations polynomiales: c'est le "théorème de Chevalley" (= corollaire 1 du théorème 1). La démonstration originale de Chevalley était la suivante:

supposons vérifiées les hypothèses du corollaire 1, et supposons que néanmoins les polynômes $F_1, F_2, \dots, F_r$ n'aient que $(0, \dots, 0)$ pour zéro commun; alors le polynôme

$$F = (1 - F_1^{q-1})(1 - F_2^{q-1}) \dots (1 - F_r^{q-1})$$

serait tel que $F(x) = 1$ pour $x = (0, \dots, 0)$ et $F(x) = 0$ pour tout autre point x de K^n ; mais le polynôme G défini par

(*) C'est le théorème de Wedderburn...

$$G(X) = (1 - X_1^{q-1})(1 - X_2^{q-1}) \dots (1 - X_n^{q-1})$$

possède évidemment la même propriété (sa fonction polynomiale associée est la fonction caractéristique de l'origine: voir chapitre 2, lemme 5, remarque); $F - G$ serait donc identiquement nul, et comme G est un polynôme réduit, on aurait $G = F^*$ (chapitre 2, théorème 1, (i) et (iii)), et en particulier

$$\deg(G) = n(q-1) = \deg(F^*) \leq \deg(F) \leq d(q-1),$$

ce qui est en contradiction avec l'hypothèse (1) : $d < n$; ceci achève la démonstration.

Analysant à son tour la démonstration de Chevalley, Warning remarqua ("Bemerkung zur vorstehenden Arbeit von Herrn Chevalley", Warning, [17]) que sous la seule hypothèse (1) : $d = d_1 + d_2 + \dots + d_r < n$, le nombre N de solutions du système (Σ) était divisible par $p = \text{car}(K)$ ("théorème de Chevalley-Warning" = théorème 1) et que le théorème de Chevalley n'est qu'un cas particulier de ce résultat. La démonstration de Warning était essentiellement la suivante:

(nous conservons les notations et aussi, évidemment, les hypothèses du théorème 1); posons, "comme chez Chevalley",

$$F = (1 - F_1^{q-1})(1 - F_2^{q-1}) \dots (1 - F_r^{q-1})$$

et formons d'autre part le polynôme

$$H(X) = \sum_{a \in V} (1 - (X_1 - a_1)^{q-1}) \dots (1 - (X_n - a_n)^{q-1}),$$

qui, comme F , prend la valeur 1 en tout point de V , et la valeur 0 partout ailleurs; comme H est réduit, on a ici encore $H = F^*$, et

par conséquent

$$\deg(H) = \deg(F^*) \leq \deg(F) \leq d(q-1) < n(q-1) ;$$

en particulier, le coefficient $(-1)^n N.1$ de $X_1^{q-1} X_2^{q-1} \dots X_n^{q-1}$ l'écriture développée de H doit être nul: autrement dit, on a $N.1 = 0$ dans K , donc $N \equiv 0 \pmod{p}$, c.q.f.d.

Les démonstrations originales de Chevalley et de Warning utilisaient donc essentiellement le théorème 1 du chapitre 2 (qui se trouve dans l'article de Chevalley déjà cité); la démonstration du théorème de Chevalley-Warning que nous avons donnée ici (et qu'on trouve par exemple dans l'article [1] , § 2 , "Quick proof of the Chevalley-Warning theorem") utilise le théorème 3 du chapitre 2, qui est indépendant du théorème 1 de ce même chapitre: l'idée de base de cette démonstration apparaîtra par la suite (estimation du nombre de solutions d'une équation ou d'un système d'équations à l'aide des caractères du corps K). A ce propos, signalons que dans l'article cité à l'instant, Ax obtient le résultat suivant, qui précise considérablement le théorème de Chevalley-Warning:

si b est le plus grand entier strictement inférieur à n/d , alors N est divisible par q^b (donc par p^{fb} , ce qui est en général beaucoup mieux que la simple divisibilité par p).

La démonstration de ce théorème d'Ax est assez technique: nous la donnerons plus loin, quand nous disposerons de l'outillage nécessaire (sommes de Gauss et relations de Stickelberger).

Indiquons pour terminer ce paragraphe que l'étude systématique de la propriété (C_1) définie plus haut (et plus généralement de la propriété dite (C_1)) a été entreprise vers 1950-1952 par Lang, et a connu depuis

lors un développement considérable: voir à ce sujet le très agréable petit livre de Greenberg [Gr]. Voir également la Note de Terjanian [24]

(3.3). L'"autre" théorème de Warning.

L'article de Warning cité plus haut contient un autre sympathique théorème que nous allons examiner maintenant.

Théorème 2 (Warning). - Mêmes données et hypothèses (y compris (1)) que dans le théorème 1. Alors, si $N > 0$ (autrement dit si le système (Σ) admet au moins une solution), on a en fait

$$(8) \quad N \geq q^{n-d},$$

(autrement dit, le système (Σ) admet au moins q^{n-d} solutions).

Démonstration. Elle repose sur des considérations géométriques simples dans l'espace affine K^n : dans tout ce qui suit, variété voudra dire sous-variété affine de K^n ; nous aurons besoin du lemme ci-dessous:

Lemme. - Soient W_1 et W_2 deux variétés parallèles de dimension d (le même d que précédemment). Alors

$$(9) \quad \text{card}(V \cap W_1) \equiv \text{card}(V \cap W_2) \pmod{p}.$$

Démontrons ce lemme. Quitte à faire un changement de repère dans K^n , on peut supposer que les variétés W_1 et W_2 sont définies respectivement par les deux systèmes d'équations

$$\left\{ \begin{array}{l} X_1 = 0 \\ X_2 = 0 \\ \dots \\ X_{n-d} = 0 \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} X_1 = 1 \\ X_2 = 0 \\ \dots \\ X_{n-d} = 0 \end{array} \right.$$

Soit H le polynôme à une variable T défini par

$$H(T) = T^{q-1} - 1 = \prod_{t \in K^*} (T - t),$$

et posons

$$G(X) = (-1)^{n-d} \left(\prod_{x_1 \neq 0,1} (X_1 - x_1) \right) H(X_2) \dots H(X_n).$$

G est évidemment un polynôme réduit de degré $(n-d)(q-1)$, de sorte que le corollaire 2 du théorème 1 nous permet d'écrire

$$(10) \quad \sum_{x \in V} G(x) = 0.$$

Par ailleurs, on vérifie sans peine que G possède la propriété suivante:

$G(x) = -1$ si $x \in W_1$; $G(x) = 1$ si $x \in W_2$; $G(x) = 0$ partout ailleurs; il résulte de là que

$$(11) \quad \sum_{x \in V} G(x) = (\text{card}(V \cap W_2) - (\text{card}(V \cap W_1))).1.$$

Le rapprochement de (10) et (11) montre que le second membre de (11) est nul en tant qu'élément de K , ce qui équivaut à la congruence (9).

Le lemme étant ainsi prouvé, démontrons le théorème 2. Il faut distinguer deux cas.

Premier cas. Il existe au moins une variété W de dimension d telle que $\text{card}(V \cap W) \not\equiv 0 \pmod{p}$. Le lemme montre alors qu'on a également $\text{card}(V \cap W') \not\equiv 0 \pmod{p}$ pour toute variété W' parallèle à W et de même dimension d ; comme il existe exactement q^{n-d} telles variétés W' , qu'elles forment une partition de K^n et que chacune d'elles contient évidemment au moins un point de V , il suffit de cueillir un point de V dans chaque W' pour se fabriquer un lot de q^{n-d} points distincts de V , ce qui règle ce premier cas.

Deuxième cas. Pour toute variété W de dimension d , on a la congruence $\text{card}(V \cap W) \equiv 0 \pmod{p}$. Puisque V contient au moins un point, on peut néanmoins affirmer ceci: il existe un entier s ($1 \leq s \leq d$) possédant la propriété suivante:

pour toute variété S de dimension s , on a $\text{card}(V \cap S) \equiv 0 \pmod{p}$, mais il existe une variété T de dimension $s - 1$ telle que $\text{card}(V \cap T) \not\equiv 0 \pmod{p}$.

Fixons une telle variété T , et désignons par a le reste de division de $\text{card}(V \cap T)$ par p : on a donc $1 \leq a \leq p - 1$; considérons maintenant le faisceau des variétés S de dimension s passant par T ; il existe exactement

$$\frac{q^n - q^{s-1}}{q^s - q^{s-1}} = q^{n-s} + \dots + q + 1$$

telles variétés S (petit exercice combinatoire; c'est d'ailleurs le nombre de points dans l'espace projectif à $n - s$ dimensions sur K); chacune d'elles contient au moins a points de V (ceux qui sont dans T), et comme pour chacune d'elles, on a par ailleurs $\text{card}(V \cap S) \equiv 0 \pmod{p}$, chaque différence ensembliste $S - T$ contient au moins $p - a$ points de V ; mais les $S - T$ forment une partition de $K^n - T$; il résulte au total de là que $\text{card}(V) = \text{card}(T) + \sum_S \text{card}(S - T) \geq a + (q^{n-s} + \dots + q + 1)(p - a) > q^{n-s} \geq q^{n-d}$, ce qui prouve le théorème 2 dans le second cas.