

# §4. Polynômes normiques et théorème de Terjanian.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **11.07.2024**

## **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.

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

(1) *Il existe au moins une variété  $W$  de dimension  $d$  telle que  $\text{card}(W \cap V) \not\equiv 0 \pmod{p}$* : le lemme 1 montre alors que pour toute variété  $W'$  parallèle à  $W$  et de même dimension  $d$ , on a également  $\text{card}(W' \cap V) \not\equiv 0 \pmod{p}$ ; 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  $N \geq q^{n-d}$  se trouve immédiatement établie dans ce premier cas.

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

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

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

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

(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  $\text{card}(M \cap V) \equiv 0 \pmod{p}$ , chaque différence ensembliste  $M - L$  contient au moins  $p - a \geq 1$  points de  $V$ ; mais les différences  $M - L$  forment une partition de  $k^n - L$ ; ainsi,

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

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  $N \geq q^{n-d}$  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  $n \leq d$ , 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  $\geq 1$ , et soit  $K$  l'unique extension de degré  $n$  de  $k$ , c'est-à-dire le corps  $\mathbb{F}_{q^n}$ ; soit  $\omega_1, \dots, \omega_n$  une base de  $K$  sur  $k$ , et posons

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

les  $\omega_i^{q^j}$  ( $0 \leq j \leq n-1$ ) étant les conjugués de  $\omega_i$  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  $\mathbf{x} = (0, \dots, 0)$ : en effet, si  $\mathbf{x} = (x_1, \dots, x_n)$  est un point de  $k^n$ , et si on pose  $\xi = \omega_1 x_1 + \dots + \omega_n x_n$ , il est évident (voir chap. 1, sect. 3.3) que  $P(\mathbf{x})$  est égal à la norme de  $\xi$  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  $x_1 = \dots = x_n = 0$ . 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  $n \leq d$ , mais qu'il perd alors tout intérêt, puisqu'il se réduit à l'énoncé suivant: si  $N > 0$ , on a  $N \geq 1/q^{d-n}$ ).

**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  $(0, \dots, 0)$  (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*

$$(4.2.1) \quad F(X) = G(X)$$

*admet au moins une solution dans  $k^n$ .*

**Démonstration.** — Introduisons  $nq$  variables notées  $X_{ij}$  ( $1 \leq i \leq n$ ,  $1 \leq j \leq q$ ), et, pour tout  $i$ , soit  $S_i \in k[X_{i1}, \dots, X_{iq}]$  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

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

Son degré  $d(R)$  est  $\leq nq$ , 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  $G(S_1, \dots, S_n)$  se trouve multiplié par  $Y^{q-1}$ . Le théorème de Chevalley montre alors que  $R$  admet dans  $k^{nq+1}$  un zéro non trivial  $(x_{11}, \dots, x_{nq}, y)$ ; si on pose  $s_i = S_i(x_{i1}, \dots, x_{iq})$ , on a

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

Mais  $y$  n'est certainement pas nul: sinon, on aurait  $F(s_1, \dots, s_n) = 0$ , donc ( $F$  étant normique)  $s_1 = \dots = s_n = 0$ , donc (les  $S_i$  étant eux-mêmes normiques)  $x_{11} = \dots = x_{nq} = 0$ , et en définitive  $(x_{11}, \dots, x_{nq}, y) = (0, \dots, 0, 0)$  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  $(s_1, \dots, s_n)$  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  $N \geq q^{n-d}$  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  $F(X_1, \dots, X_n) = P(X_1, \dots, X_d)$  (les variables  $X_{d+1}, \dots, X_n$  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  $q^{n-m}$ .*