§2. Fonctions polynomiales.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **06.08.2024**

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 $\varphi\colon k\,[X] \to A$, 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*

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

(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 $\varphi_R^{-1}\big(\varphi(F)\big) = F^*$.*

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 $f\colon k^n \to k$, 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

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

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

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

(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 $\operatorname{card}(R) = q^{q^n}$ 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: