§1. Polynômes réduits et polynômes identiquement nuls

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **26.04.2024**

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

§ **1**: la classification des corps (commutatifs) finis (« champs de Galois ») remonte essentiellement à Galois (1830).

§ **2**: le fait que le groupe multiplicatif du corps $\mathbf{F}_p$ est cyclique est dû à Euler (1760); sa démonstration utilisait les propriétés de l'« indicatrice d'Euler ». Ce résultat est un ingrédient essentiel de la théorie des restes quadratiques (Euler, Legendre, Gauss), cubiques (Jacobi, Eisenstein), biquadratiques (Gauss, Jacobi), et plus généralement des restes de puissances quelconques (Kummer, etc.); à ce sujet, voir par exemple Dickson, *History of the Theory of Numbers.*

§ **3**: les propositions 9 et 10 sont des cas particuliers du *théorème* 90 de Hilbert relatif aux extensions cycliques (voir [**10**], pp. 213-215).

CHAPITRE 2

POLYNÔMES ET IDÉAUX DE POLYNÔMES

On sait que si K est un corps *infini*, et si F est un polynôme à une ou plusieurs variables, à coefficients dans K, et *identiquement nul* sur K, alors F est *nul*: tous ses coefficients sont nuls. Ceci n'est plus vrai pour un corps fini: ainsi, sur $k = \mathbf{F}_q$, le polynôme $X^q - X$, non nul, est pourtant identiquement nul (chap. 1, sect. 1.1 et 1.2); c'est à cette particularité des corps finis qu'est consacré le présent chapitre.

Dans tout le cours de ce chapitre (ainsi que dans les chapitres suivants), k désignera un corps fini à $q = p^f$ éléments, n un entier $\geqslant 1$, $X = (X_1, ..., X_n)$ une famille de n variables, et $k[X] = k[X_1, ..., X_n]$ l'anneau des polynômes en $X_1, ..., X_n$ à coefficients dans k; d'autre part, les éléments $\mathbf{a} = (a_1, ..., a_n)$ de k^n seront appelés *points* (ou *points rationnels sur* k, si cette précision est nécessaire); si $F \in k[X]$, si $\mathbf{a}$ est un point de k^n, et si $F(\mathbf{a}) = 0$, on dira que $\mathbf{a}$ est un *zéro* de F.

§ 1. *Polynômes réduits et polynômes identiquement nuls.*

1.1. Soit F un élément de $k[X]$.

DÉFINITION 1. — *Si le degré de F par rapport à chacune des n variables X_i est inférieur ou égal à $q-1$, on dit que F est un polynôme* réduit.

Les polynômes réduits forment évidemment un sous-espace vectoriel R de $k[X]$ (le corps des scalaires étant k); une base naturelle de ce sous-espace est l'ensemble des monômes $X_1^{d_1} \dots X_n^{d_n}$ tels que $0 \leqslant d_i \leqslant q-1$ pour $i = 1, \dots, n$; R est donc de dimension q^n sur k.

1.2. Soit encore F un élément de $k[X]$.

DÉFINITION 2. — *On appelle* fonction polynomiale associée à F *l'application* $\mathbf{x} \mapsto F(\mathbf{x})$ *de k^n dans k. Si cette fonction polynomiale est nulle (donc si $F(\mathbf{x}) = 0$ en tout point $\mathbf{x}$ de k^n), on dit que le polynôme F est* identiquement nul.

Les polynômes identiquement nuls forment un idéal I de $k[X]$; notons d'autre part Γ l'idéal de $k[X]$ engendré par les éléments $X_i^q - X_i$ $(i=1, \dots, n)$; comme chacun de ces polynômes est identiquement nul (chap. 1, § 1), il est clair que $\Gamma \subset I$: on va voir qu'en fait, il y a égalité.

1.3. THÉORÈME 1. — (i) *Dans $k[X]$, les idéaux I et Γ sont égaux.* (ii) *En tant qu'espace vectoriel sur k, $k[X]$ est somme directe de R (voir sect. 1.1) et de Γ :*

$$k[X] = R \oplus \Gamma . \tag{1.3.1}$$

Démonstration. — On aura besoin de deux lemmes.

LEMME 1. — *Si un polynôme F de $k[X]$ est à la fois réduit et identiquement nul, alors il est nul ; autrement dit :*

$$R \cap I = (0) . \tag{1.3.2}$$

Ce lemme se démontre par récurrence sur n. Tout d'abord, la propriété est vraie pour $n = 1$: si en effet F, polynôme à une variable, est réduit et identiquement nul, il est de degré $\leqslant q-1$ (déf. 1) et il possède d'autre part au moins q racines: les q éléments de k (déf. 2); et ceci n'est possible que si $F = 0$. Ensuite, si la propriété est vraie pour $n-1$ variables (avec $n \geqslant 2$), elle est encore vraie pour n variables: soit en effet F un polynôme *réduit* à n variables; en l'ordonnant suivant les puissances décroissantes de X_1, on peut le mettre sous la forme

$$F_1(X_2, \dots, X_n) X_1^{q-1} + \dots + F_{q-1}(X_2, \dots, X_n) X_1 + F_q(X_2, \dots, X_n),$$

les F_j ($1 \leqslant j \leqslant q$) étant q polynômes *réduits, à* $n-1$ *variables* $X_2, ..., X_n$. Supposons maintenant F *identiquement nul*: alors, quel que soit le point $(x_2, ..., x_n)$ de k^{n-1}, le polynôme $f_1 X_1^{q-1} + ... + f_{q-1} X_1 + f_q$ (où, par définition, $f_j = F_j(x_2, ..., x_n)$ pour $j = 1, ..., q$) est lui-même identiquement nul; mais c'est un polynôme réduit, à une seule variable X_1: la première partie de la démonstration prouve donc qu'il est nul, c'est-à-dire que $f_1 = ... = f_q = 0$, ou encore que $F_1(x_2, ..., x_n) = ... = F_q(x_2, ..., x_n) = 0$; or ceci a lieu, rappelons-le, quel que soit $(x_2, ..., x_n)$ dans k^{n-1}: ainsi, les q polynômes F_j sont identiquement nuls, et l'hypothèse de récurrence permet d'affirmer qu'ils sont nuls; mais alors, F est lui-même nul, C.Q.F.D.

LEMME 2. — *Pour tout polynôme* F *de* $k[X]$, *il existe un polynôme réduit* F^* *tel que* $F \equiv F^* \pmod{\Gamma}$; *autrement dit :*

$$k[X] = R + \Gamma . \tag{1.3.3}$$

Prouvons ce lemme: par linéarité, on peut se ramener au cas où F est un monôme $X_1^{d_1} ... X_n^{d_n}$; Γ étant un idéal, on peut même se limiter au cas où ce monôme ne contient qu'une seule variable, par exemple, au cas où $F = X_1^{d_1}$; mais alors, pour $d_1 \leqslant q-1$, il n'y a rien à démontrer (faire $F^* = 0$); et pour $d_1 \geqslant q$, il suffit de raisonner par récurrence sur d_1, en remarquant qu'on a la congruence $X_1^{d_1} \equiv X_1^{d_1-(q-1)} \pmod{\Gamma}$.

Démontrons maintenant le théorème 1 lui-même. Comme $\Gamma \subset I$, il résulte du lemme 1 que

$$R \cap \Gamma = (0) . \tag{1.3.4}$$

Les égalités (1.3.3) et (1.3.4) montrent alors que $k[X] = R \oplus \Gamma$: (ii) se trouve ainsi établi. Reste à prouver (i), et il suffit évidemment de montrer que $I \subset \Gamma$; mais si $F \in I$, on peut écrire (lemme 2)

$$F = F^* + G \quad (F^* \in R,\ G \in \Gamma) ; \tag{1.3.5}$$

comme $\Gamma \subset I$, $F^* = F - G$, différence de deux éléments de I, est un élément de I, donc un polynôme identiquement nul; le lemme 1 montre alors que F^* est nul, et (1.3.5) donne $F = G \in \Gamma$, ce qui prouve bien l'inclusion $I \subset \Gamma$. Le théorème est ainsi démontré.

1.4. D'après le théorème 1, tout polynôme $F \in k[X]$ s'écrit d'une façon et d'une seule $F = F^* + G$, avec F^* réduit et G identiquement nul.

DÉFINITION 3. — *On dit que* F^* *est le* polynôme réduit associé à F.

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

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

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

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 $f: k^n \to k$, 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

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

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

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

(voir chap. 1, sect. 1.1). Ceci démontre le lemme 3, et achève de prouver le théorème 3.