Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: Chapitre 2 POLYNÔMES ET IDÉAUX DE POLYNÔMES
DOI: https://doi.org/10.5169/seals-46287

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 09.12.2025

ETH-Bibliothek Zürich, E-Periodica, https://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.

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

THÉORÈME 4. — *On a l'égalité*

$$I(V) = J + \Gamma . \tag{3.1.2}$$

Démonstration. — Considérons le polynôme

$$F = 1 - (1 - F_1^{q-1}) \dots (1 - F_s^{q-1}) ; \tag{3.1.3}$$

F appartient à l'idéal J: en effet, considéré comme polynôme par rapport à $F_1, \dots, F_s$, le second membre de (3.1.3) ne contient pas de terme constant; d'autre part, F prend constamment la valeur 0 sur V, et la valeur 1 en dehors de V (voir chap. 1, sect. 1.1). Soit alors H un élément de $I(V)$, donc un polynôme nul sur V; il est clair que le polynôme $G = H - HF$ est identiquement nul, et appartient donc à Γ; il est clair également, puisque J est un idéal contenant F, que HF appartient à J; on voit ainsi que $H = HF + G$ appartient à $J + \Gamma$, donc que $I(V) \subset J + \Gamma$, C.Q.F.D.

3.2. Le *théorème de la base finie* de Hilbert (voir **[10]**, p. 144) montre que tout idéal de $k[X]$ peut être engendré par un nombre fini de polynômes: le théorème 4 est donc en fait applicable à n'importe quel idéal J de $k[X]$ (dans le même ordre d'idées, on peut d'ailleurs remarquer que dans la démonstration du théorème 4, on a implicitement remplacé l'idéal J engendré par $F_1, \dots, F_s$, par l'idéal principal (F), contenu dans J, et dont l'ensemble des zéros dans k^n est le même que celui de J).

Notons d'autre part que le *théorème des zéros* de Hilbert (**[10]**, p. 256, **[12]**, p. 32, ou **[15]**, p. 4) implique que, dans l'anneau $k[X]$, l'idéal $J + \Gamma = I(V)$ est égal à sa racine, c'est-à-dire à l'intersection des idéaux premiers qui le contiennent; comme $\dim(V) = 0$ (V est un ensemble fini de points rationnels sur k), ces idéaux premiers sont d'ailleurs tous maximaux, ce sont exactement les idéaux de la forme $\mathfrak{M}_{\mathbf{a}} = (X_1 - a_1, \dots, X_n - a_n)$, $\mathbf{a} = (a_1, \dots, a_n)$ parcourant l'ensemble V.

Notes sur le chapitre 2

§ **1** et **2**: les résultats contenus dans ces deux paragraphes sont essentiellement dus à Chevalley (1935); ils donneront notamment (chap. 3, sect. 1.1) une démonstration immédiate du « théorème de Chevalley-Warning ».

§ **3**: le théorème 3 est dû à Terjanian (1966).