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: §3. 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: 10.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

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 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).