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. Extensions algébriques d'un corps fini.
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: 09.07.2025

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

Pour $k = \mathbf{F}_p$, p impair, et $d = \delta = 2$, le corollaire 2 coïncide avec le *critère d'Euler* sur les restes et non-restes quadratiques modulo p.

§ 3. *Extensions algébriques d'un corps fini.*

Soit toujours k un corps fini à q éléments.

3.1. Soit K une extension algébrique de k, de degré fini m; il est clair que $\operatorname{card}(K) = q^m$, et donc que $K = \mathbf{F}_{q^m}$. Soit alors i un entier $\geqslant 0$; comme q^i est une puissance de la caractéristique de K, l'application σ_i: $K \to K$, définie par $\sigma_i(x) = x^{q^i}$ $(x \in K)$, est un automorphisme de K, et même, puisque $k = \mathbf{F}_q$, un k-automorphisme de K (prop. 2); si j est un autre entier $\geqslant 0$, on a évidemment $\sigma_{i+j} = \sigma_i \circ \sigma_j$; enfin, si (par exemple) $i \leqslant j$, l'ensemble des $x \in K$ tels que $\sigma_i(x) = \sigma_j(x)$, donc tels que $x^{q^{j-i}} = x$, est évidemment égal à $K \cap \mathbf{F}_{q^{j-i}}$, et ne peut par conséquent être égal à $K = \mathbf{F}_{q^m}$ que si $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^{j-i}}$, donc (prop. 4) si $i \equiv j \pmod{m}$; en particulier, les m k-automorphismes σ_i avec $0 \leqslant i < m$ sont distincts, et on peut affirmer:

PROPOSITION 8. — *L'extension K/k est galoisienne ; son groupe de Galois est cyclique, d'ordre m, engendré par l'automorphisme* (dit de Frobenius) $x \mapsto x^q$.

Le fait que K/k est galoisienne peut se voir plus directement: en effet, k étant évidemment parfait, K/k est séparable, et il suffit de prouver que K/k est normale, ce qui résulte du fait que K est le corps de décomposition, dans une clôture algébrique de k, du polynôme $X^{q^m} - X$ (prop. 2).

3.2. Mêmes données que ci-dessus. Soit $Tr : K \to k$, l'application *trace*. La proposition 8 montre que, pour tout élément x de K, on a

$$Tr(x) = x + x^q + \ldots + x^{q^{m-1}}. \tag{3.2.1}$$

En outre:

PROPOSITION 9. — *L'application $Tr : K \to k$, est surjective. Si $x \in K$, les deux assertions suivantes sont équivalentes :*

(a) $Tr(x) = 0$;

(b) *il existe $y \in K$ tel que $x = y^q - y$.*

Démonstration. — Considérons K comme espace vectoriel sur k; Tr est alors une forme linéaire, et cette forme linéaire n'est pas nulle (si elle l'était, (3.2.1) impliquerait que le polynôme $X + X^q + \ldots + X^{q^{m-1}}$, de

degré q^{m-1}, admet pour racines les q^m éléments de K: absurde): elle est donc surjective, ce qui prouve la première assertion, et ce qui montre en outre que le noyau de Tr est un hyperplan de K; comme $Tr\,(y^q - y) = 0$ pour tout élément y de K, il reste, pour établir l'équivalence de (a) et (b), à prouver que l'ensemble des éléments de la forme $y^q - y$ ($y \in K$) est également un hyperplan de K; et il suffit pour cela de remarquer que l'application $y \mapsto y^q - y$ de K dans K est k-linéaire et de rang $m - 1$, puisque son noyau (formé des $y \in K$ tels que $y^q = y$, donc égal à k: prop. 2, ou prop. 8) est de dimension 1.

3.3. Mêmes données et notations que ci-dessus. Soit maintenant $N: K \to k$, l'application *norme*. La proposition 8 montre que, pour tout élément x de K, on a

$$N(x) = x.x^q \dots x^{q^{m-1}} = x^{(q^m-1)/(q-1)}. \tag{3.3.1}$$

En outre:

PROPOSITION 10. — *L'application $N: K^* \to k^*$, est surjective. Si $x \in K^*$, les deux assertions suivantes sont équivalentes :*

(a) $N(x) = 1$;

(b) *il existe $y \in K^*$ tel que $x = y^{q-1}$.*

Démonstration. — N est un homomorphisme du groupe K^* dans le groupe k^*, et il résulte de (3.3.1) et de la proposition 7 (avec $d=(q^m-1)/(q-1)$) que le noyau de N est d'ordre $(q^m-1)/(q-1)$; comme l'ordre de K^* est égal à $q^m - 1$, l'image de N est nécessairement d'ordre $q - 1 = \text{card}\,(k^*)$, d'où la surjectivité de N. Le noyau de N contenant évidemment tous les éléments de K^* de la forme y^{q-1} ($y \in K^*$), qui en constituent un sous-groupe, il reste donc, pour établir l'équivalence de (a) et (b), à montrer que ce sous-groupe est précisément d'ordre $(q^m-1)/(q-1)$; mais il suffit pour cela de remarquer que l'application $y \mapsto y^{q-1}$ de K^* dans K^* est un homomorphisme dont le noyau (formé des $y \in K^*$ tels que $y^{q-1} = 1$, donc égal à k^*) est d'ordre $q - 1$, et dont l'image est alors effectivement d'ordre $(q^m-1)/(q-1)$, puisque K^* est lui-même d'ordre $q^m - 1$.

Notes sur le chapitre premier

Théorème de Wedderburn: pour la démonstration originale, voir Wedderburn (1905); l'idée d'utiliser (comme dans **[1]** ou **[19]**) les propriétés des polynômes cyclotomiques pour simplifier cette démonstration est due à Witt (1931).