Zeitschrift: L'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Kapitel: §2. Groupe additif et groupe multiplicatif d'un corps fini.
Autor: Joly, Jean-René
DOI: https://doi.org/10.5169/seals-46287

1.2. Soient maintenant p un nombre premier, f un entier $\geqslant 1$, et posons $q = p^f$. Désignons par Ω une clôture algébrique de $\mathbf{F}_p$, et notons k l'ensemble des racines dans Ω du polynôme $X^q - X$. Ce polynôme ayant toutes ses racines simples (son dérivé vaut -1), on voit que card $(k) = q$; de plus, q étant une puissance de la caractéristique, on a, quels que soient a et b dans k, $(a+b)^q = a^q + b^q = a + b$; on a évidemment aussi $(ab)^q = a^q b^q = ab$, et k est un sous-corps de Ω; en particulier:

PROPOSITION 3. — *Quels que soient p premier et $f \geqslant 1$, il existe un corps fini possédant exactement $q = p^f$ éléments.*

Ce corps est unique à isomorphisme près (prop. 2); on le note généralement $\mathbf{F}_q$.

1.3. Mêmes données que dans la section précédente. Soient f_1 et f_2 deux entiers $\geqslant 1$, et posons, pour $i = 1, 2$,

$$q_i = q^{f_i}; \qquad k_i = \mathbf{F}_{q_i} \subset \Omega;$$

on a alors évidemment $[k_i : \mathbf{F}_q] = f_i$. Si $k_1 \subset k_2$, la multiplicativité du degré montre que f_1 divise f_2. Inversement, supposons que f_1 divise f_2; on peut écrire $f_2 = mf_1$, donc $q_2 = {q_1}^m$; si $a \in k_1$, on a alors $a^{q_1} = a$ (prop. 2), donc $a^{{q_1}^m} = a^{q_2} = a$, et par conséquent $a \in k_2$ (prop. 2); ainsi, $k_1 \subset k_2$. Au total (et en conservant ces notations):

PROPOSITION 4. — *L'inclusion $k_1 \subset k_2$ équivaut à la relation f_1 divise f_2, donc à la relation q_2 est une puissance de q_1.*

COROLLAIRE 1. — *Soient respectivement f' et f'' le p.g.c.d. et le p.p.c.m. de f_1 et f_2. Posons $q' = q^{f'}$, $q'' = q^{f''}$, $k' = \mathbf{F}_{q'}$, $k'' = \mathbf{F}_{q''}$. Alors l'intersection et le composé de k_1 et k_2 sont respectivement k' et k''.*

§ 2. *Groupe additif et groupe multiplicatif d'un corps fini.*

Soit k un corps fini à $q = p^f$ éléments.

2.1. L'extension $k/\mathbf{F}_p$ étant de degré f, k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, et a fortiori en tant que groupe additif, au produit direct de f exemplaires de $\mathbf{F}_p$; en conséquence:

PROPOSITION 5. — *Le groupe additif k^+ de k est un groupe de type $(p, ..., p)$ (f fois).*

2.2. Passons au groupe multiplicatif k^*; il est commutatif, d'ordre $q-1$; si N désigne le p.p.c.m. des ordres des éléments de k^*, on vérifie sans peine qu'il existe dans k^* un élément g d'ordre exactement égal à N (c'est là une propriété générale des groupes commutatifs d'ordre fini). Tout élément de k^* est évidemment racine du polynôme $X^N - 1$; ce polynôme, de degré N, possède donc au moins $q-1$ racines, d'où $N \geqslant q-1$; or, par construction même, N divise $q-1$; ainsi, $N = q-1$; mais alors g est d'ordre $q-1$, c'est un générateur de k^*, et on peut énoncer:

PROPOSITION 6. — *Le groupe multiplicatif k^* de k est un groupe cyclique d'ordre $q-1$.*

Pour une autre démonstration de ce résultat, utilisant les propriétés de l'indicatrice d'Euler, voir [**17**], pp. 12-13.

2.3. Soit d un entier $\geqslant 1$; on se propose d'étudier le groupe des puissances d-ièmes et le groupe des racines d-ièmes de l'unité dans k^*, c'est-à-dire l'image et le noyau de l'homomorphisme $u_d: k^* \to k^*$, défini par $u_d(x) = x^d$ $(x \in k^*)$. Posons $\delta = (q-1, d)$, $u_\delta(x) = x^\delta$ $(x \in k^*)$ et notons g un générateur de k^* (prop. 6). L'identité de Bezout $a(q-1) + bd = \delta$ montre que u_d et u_δ ont même noyau (noter que $x^{q-1} = 1$ pour tout $x \in k^*$); k^* étant fini, il en résulte que l'image de u_d et celle de u_δ ont même ordre; mais la première est évidemment contenue dans la seconde: u_d et u_δ ont donc aussi même image. Maintenant, comme δ divise $q-1$, il est clair que l'image de u_δ est le sous-groupe de k^* engendré par g^δ, et que le noyau de u_δ est le sous-groupe de k^* engendré par $g^{(q-1)/\delta}$ (pour le voir, identifier par exemple k^* à $\mathbf{Z}/(q-1)\,\mathbf{Z}$, g s'identifiant à la classe de 1 (mod $q-1$)). En résumé:

PROPOSITION 7. — *Soient k un corps fini à q éléments, g un générateur de k^*, d un entier $\geqslant 1$, et posons $\delta = (q-1, d)$. Alors:*

(i) *Dans k^*, les puissances d-ièmes et les puissances δ-ièmes forment un même sous-groupe, cyclique, engendré par g^δ, et d'ordre égal à $(q-1)/\delta$.*

(ii) *De même, les racines d-ièmes et les racines δ-ièmes de l'unité forment un même sous-groupe, cyclique, engendré par $g^{(q-1)/\delta}$, et d'ordre égal à δ.*

COROLLAIRE 1. — *Le groupe quotient k^*/k^{*d} est cyclique, d'ordre égal à δ.*

COROLLAIRE 2. — *Pour qu'un élément a de k^* soit une puissance d-ième, il faut et il suffit que $a^{(q-1)/\delta} = 1$.*

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 $\mathrm{card}\,(K) = q^m$, 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