MATHÉMATIQUES ET SCIENCES HUMAINES

G. HEUZÉ

Sur les corps finis

Mathématiques et sciences humaines, tome 47 (1974), p. 57-59
<http://www.numdam.org/item?id=MSH_1974__47__57_0>

Math. Sci. hum. (12e année, n° 47, 1974, p. 57-59)

SUR LES CORPS FINIS

par

G. HEUZÉ

RÉSUMÉ

La théorie des corps finis a été faite il y a longtemps et ne comporte plus de problèmes ouverts. Toutefois, quand l'utilisateur cherche à déterminer effectivement un corps fini d'ordre donné, il rencontre des difficultés : après avoir eu beaucoup de mal pour obtenir un polynome irréductible unitaire de degré convenable, il constate souvent que les racines de ce polynome n'engendrent pas le groupe multiplicatif des éléments non nuls, d'où des complications pour obtenir la table multiplicative du corps. Le présent papier met en lumière l'origine de cette situation et donne des tables pour tous les corps non premiers d'ordre inférieur à 1 000.

SUMMARY

The theory of finite fields was established long ago and no longer presents any open problems. Nonetheless, the person who attempts to determine effectively a finite field of a given order, encounters difficulties: after having painstakingly obtained an irreducible unit polynomial of a convenient degree, he often finds that the roots of this polynomial do not generate the multiplicative group of non-zero elements ; hence, the complications which arise in obtaining a multiplication table for this field. The present paper sheds some light on the origins of this situation and provides tables for all non-prime fields of an order less than 1 000.

Rappelons d'abord les résultats classiques (voir par exemple [1], [2], [3] ou [4]).

(1) *Tout corps fini est d'ordre p^n, p étant un nombre premier.*

(2) *Tout corps fini d'ordre p^n contient un sous-corps identifiable au corps F_p des entiers modulo p.*

(3) *Tout corps fini est commutatif.*

(4) *Deux corps finis de même ordre p^n sont isomorphes* (dans un isomorphisme laissant invariants les éléments de F_p).

(5) *Quels que soient le nombre premier p et l'entier n il existe un corps d'ordre p^n* (ce corps, unique en vertu de (4), est noté F_{p^n}).

(6) *Le groupe multiplicatif $F_{p^n} - \{0\}$ est cyclique* (nous noterons ce groupe $F^*_{p^n}$).

F_pn est donc une extension algébrique simple de F_p, c'est-à-dire qu'il existe au moins un polynome $f(X)$ irréductible unitaire de degré n de $F_p[X]$ tel que F_{p^n} soit isomorphe à $F_p[X]/(f(X))$.

Toute racine d'un tel $f(X)$ engendrant $F^*_{p^n}$, la connaissance de $f(X)$ permet la détermination effective de F_{p^n} de façon rapide. En effet si $f(X) = X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_o$ et si x désigne une racine de $f(X)$ on sait que tout élément de $F^*_{p^n}$ s'écrit x^n (où $0 \leqslant h \leqslant p^n - 2$) et que $x^n = -a_{n-1} x^{n-1} - \ldots - a_1 x - a_o$. D'où la table de multiplication de F_{p^n} (la table d'addition étant immédiate).

Montrons alors la proposition :

(7) *Le nombre* $\omega_p\ (n)$ *des polynomes irréductibles unitaires de degré* n *de* $F_p\ [X]$ *dont les racines engendrent* $F^*_{p^n}$ *est égal à* $\dfrac{1}{n}\ \varphi\ (p^n - 1)$ *où* φ *désigne l'indicateur d'Euler.*

En effet $F^*_{p^n}$ a $\varphi\ (p^n - 1)$ générateurs et, si un polynome irréductible de degré n a pour racine un de ces générateurs, il en est de même de ses $(n - 1)$ autres racines.

Malheureusement tout polynome irréductible de degré n de $F_p\ [X]$ n'a pas nécessairement des racines engendrant $F^*_{p^n}$. Ainsi $X^2 + 1$ est irréductible de $F_3\ [X]$ mais ses racines n'engendrent pas F^*_9 (elles ne sont que d'ordre 4). Pour préciser cette différence montrons :

(8) *Le nombre* $\psi_p\ (n)$ *des polynomes irréductibles unitaires de degré* n *de* $F_p\ [X]$ *est égal à* $\dfrac{1}{n}\ \sum\limits_{d|n} p^d\ \mu\ (\dfrac{n}{d})$ *où* μ *désigne la fonction de Möbius.*

Cela tient au fait que F_{p^n} est l'ensemble des racines du polynome $X^{p^n} - X$ de $F_p\ [X]$. Par ailleurs l'ensemble des facteurs irréductibles unitaires de $X^{p^n} - X$ s'identifie à l'ensemble des polynomes irréductibles unitaires de degré d où $d|n$ (conséquence du résultat classique : F_{p^d} est sous-corps de F_{p^n} si et seulement si $d|n$). On a donc $p^n = \sum\limits_{d|n} d\ \psi_p\ (d)$. D'où (8) par « inversion ».

Le tableau donne les valeurs de $\psi_p\ (n)$ et $\omega_p\ (n)$ pour tous les nombres p^n inférieurs à 1 000 avec $n \geqslant 2$. Dans la dernière colonne figure un exemplaire de polynome irréductible unitaire dont chaque racine engendre F_{p^n} ([1], table de Bussey). Bien entendu les coefficients de ces polynomes sont des entiers modulo p.

p^n	$\psi_p(n)$	$\omega_p(n)$	Un des $\omega_p(n)$ polynomes
$4 = 2^2$	1	1	$X^2 + X + 1$
$8 = 2^3$	2	2	$X^3 + X + 1$
$9 = 3^2$	3	2	$X^2 + 2X + 2$
$16 = 2^4$	3	2	$X^4 + X + 1$
$25 = 5^2$	10	4	$X^2 + 3X + 3$
$27 = 3^3$	8	4	$X^3 + 2X + 1$
$32 = 2^5$	6	6	$X^5 + X^3 + X^2 + X + 1$
$49 = 7^2$	21	8	$X^2 + 6X + 3$
$64 = 2^6$	9	6	$X^6 + X + 1$
$81 = 3^4$	18	8	$X^4 + X^3 + X^2 + 2X + 2$
$121 = 11^2$	55	16	$X^2 + 7X + 2$
$125 = 5^3$	40	20	$X^3 + 3X + 2$
$128 = 2^7$	18	18	$X^7 + X + 1$
$169 = 13^2$	78	24	$X^2 + 12X + 2$
$243 = 3^5$	48	22	$X^5 + 2X + 1$
$256 = 2^8$	30	16	$X^8 + X^4 + X^3 + X^2 + 1$
$289 = 17^2$	136	48	$X^2 + 16X + 3$
$343 = 7^3$	112	36	$X^3 + 6X + 2$
$361 = 19^2$	171	48	$X^2 + 18X + 2$
$512 = 2^9$	56	48	$X^9 + X^8 + X^4 + X^3 + X^2 + X + 1$
$529 = 23^2$	253	80	$X^2 + 22X + 7$
$625 = 5^4$	150	48	$X^4 + 4X^3 + 4X + 3$
$729 = 3^6$	116	32	$X^6 + 2X + 2$
$841 = 29^2$	406	96	$X^2 + 28X + 3$
$961 = 31^2$	465	128	$X^2 + 30X + 12$

On remarquera que, quand $p^n - 1$ est premier, on a nécessairement $p = 2$ et $\omega_2(n) = \frac{1}{n}(2^n - 2)$. (6) impose alors : $\psi_2(n) = \omega_2(n)$ et n premier. C'est le cas pour $n = 2, 3, 5, 7$, mais pas pour $n = 11$ (en effet $2^{11} - 1 = 23.89$, $\psi_2(11) = 186$, $\omega_2(11) = 176$).

BIBLIOGRAPHIE

[1] Albert A.-A., *Fundamental concepts of higher algebra,* Chicago, Ill., University of Chicago Press, 1956.

[2] Warusfel A., *Structures algébriques finies,* Paris, Hachette Université, 1971.

[3] Bussey W.-H., « Galois field tables for $p^n \leqslant 169$ », *Bull. amer. math. Soc.*, 1905 (12), pp. 22-38.

[4] Bussey W.-H., « Galois field tables for $p^n < 1\,000$ » *ibid.*, 1909 (16), pp. 188-206.