

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

ANDRÉ WARUSFEL

Corps finis

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 1 (1967-1968), exp. n° 9, p. 1-7.

http://www.numdam.org/item?id=SDPP_1967-1968__9_1_A9_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1967-1968, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

CORPS FINIS

par André WARUSFEL

1. Préliminaires.

Tout corps fini a une caractéristique non nulle p qui est un nombre premier. Son cardinal est de la forme p^v .

(a) Soit k le cardinal du corps K et a un élément non nul. Il engendre un groupe G_a d'ordre γ , diviseur de k . De $\gamma \cdot a = 0$ on déduit $k \cdot a = 0$, pour tout a de K et $k \cdot 1 = 0$. La caractéristique p existe donc.

(b) Si l'on avait $p = mn$, alors on pourrait écrire

$$p \cdot 1 = 0 \implies m \cdot (n \cdot 1) = m \cdot a = 0,$$

ou bien $a = n \cdot 1 = 0$, ou bien $m \cdot a = 0$, c'est-à-dire $m \cdot 1 = 0$ en multipliant par $a^{-1} = (n \cdot 1)^{-1}$, ce qui est contradictoire.

(c) K contient donc le corps de Galois

$$F_p = \mathbb{Z}/p\mathbb{Z}$$

qui est son corps premier. Etant espace vectoriel (nécessairement de dimension finie v) sur F_p , son cardinal $|K|$ est égal à

$$k = p^v.$$

2. Polynômes cyclotomiques dans le corps \mathbb{C} .

(a) Soit R_n l'ensemble des racines n -ièmes de l'unité telles que

$$0 < m < n \implies x^m \neq 1$$

$$m = n \implies x^n = 1$$

(racines primitives de 1). On peut alors écrire

$$x = \exp \frac{2ik\pi}{n} \quad \text{avec} \quad \text{p. g. c. d.}(k, n) = 1.$$

(b) Soit

$$\varphi_n(X) = \prod_{x \in R_n} (X - x) \quad (\text{polynôme cyclotomique})$$

et $\varphi(n) = d^0 \varphi_n$ (fonction d'Euler : nombres d'entiers inférieurs à n premiers avec n). φ_n divise

$$\omega_n = X^n - 1.$$

(c) Soit d un diviseur de n . φ_d divise ω_n , car

$$x \in R_d \implies x^d = 1 \implies x^n = 1.$$

Toute racine x de ω_n est du type $\exp \frac{2ik\pi}{n}$. Si p. g. c. d. $(k, n) = \delta$, $d = \frac{n}{\delta}$ et $k' = \frac{k}{\delta}$, on voit que $x = \exp \frac{2ik'n}{d}$ et que p. g. c. d. $(k', d) = 1$, d'où $x \in R_d$.

Deux polynômes φ_d et $\varphi_{d'}$, étant premiers entre eux si $d' \neq d$, on voit donc que l'on peut écrire

$$X^n - 1 = \prod_{d|n} \varphi_d(X).$$

(d) Soit $P_n(X) = \prod_{\substack{d|n \\ d < n}} \varphi_d(X)$ (ex : $P_1 = 1$, $P_2 = X - 1$). Si $\varphi_m \in \mathbb{Z}[X]$, pour

tout $m < n$ et si φ_m est unitaire, il en est de même de P_n et de

$$\varphi_n = \frac{\omega_n}{P_n}.$$

Donc φ_n est unitaire, et

$$\varphi_n(X) \in \mathbb{Z}[X].$$

(e) Si d divise strictement n , φ_n et ω_d étant alors premiers entre eux, on en déduit que φ_n divise $\frac{\omega_n}{\omega_d}$ qui est un polynôme unitaire de $\mathbb{Z}[X]$. Le quotient

$$\frac{X^n - 1}{(X^d - 1)\varphi_n} \quad (d|n, d < n)$$

est lui-même unitaire et à coefficients entiers.

(f) Soit $q \geq 2$ un entier, et $n > 1$:

$$\begin{aligned} |\varphi_n(q)|^2 &= \prod_{x \in R_n} |q - x|^2 = \prod_{\theta} |q - \cos \theta - i \sin \theta|^2 \\ &= \prod [(q - \cos \theta)^2 + \sin^2 \theta] > \prod (q^2 - 2q + 1) \\ &= \prod (q - 1)^2 = (q - 1)^{2\varphi(n)}. \end{aligned}$$

Donc $|\varphi_n(q)| > q - 1$ (l'inégalité est stricte puisque $1 \notin R_n$, d'où $\theta \neq 0$ et $\cos \theta < 1$).

3. Théorème de Wedderburn.

(a) Soit H un sous-corps de K . Sa caractéristique est encore p , et $h = |H| = p^\mu$.

Comme $H - \{0\}$ est un sous-groupe de $K - \{0\}$, $(h - 1)$ divise $(k - 1)$. Si $v = \alpha\mu + \beta$ ($0 \leq \beta < \mu$), on a

$$p^\mu - 1 \mid p^v - 1 = (p^{\alpha\mu} - 1)p^\beta + (p^\beta - 1)$$

d'où

$$p^\mu - 1 \mid p^\beta - 1 < p^\mu - 1, \text{ et } \beta = 0$$

Le cardinal d'un sous-corps de K est une racine exacte de $k = h^\alpha$.

(b) Si $a \in K - \{0\}$ et $M_a = \{x \mid x \in K, xa = ax\}$, M_a est un sous-corps de K , ainsi que le centre

$$\Gamma = \cap M_a = \{x \mid x \in K, \forall y \in K, xy = yx\},$$

$q = |\Gamma| \geq 2$, car $\{0, 1\} \subset \Gamma$.

(c) Γ étant un sous-corps de M_a et de K , on a

$$|M_a| = q^s, \quad |K| = k = q^t.$$

De plus, q^t est une puissance exacte de q^s , et t est multiple de s .

(d) La relation d'équivalence sur $K - \{0\}$

$$a \sim a' \iff \exists x \in K, a' = x^{-1}ax = \theta_a(x)$$

définit une partition P de $K - \{0\}$. Soit λ_a le nombre d'équivalents de a , c'est-à-dire le nombre d'éléments b tels que les éléments $b^{-1}ab$ soient distincts ($\lambda_a = 1 \iff a \in \Gamma - \{0\}$).

(e) La relation

$$b \equiv c \iff b^{-1}ab = c^{-1}ac$$

équivalent à

$$a(bc^{-1}) = (bc^{-1})a,$$

c'est-à-dire à

$$bc^{-1} \in N_a = M_a - \{0\} .$$

Il y a donc $n_a = |N_a|$ éléments c tels que $b \equiv c$, d'où

$$\lambda_a = \frac{k-1}{n_a} = \frac{q^t - 1}{q^s - 1} .$$

(f) Dénombrant les cardinaux des classes de la partition P , en comptant d'abord les éléments de $\Gamma - \{0\}$ pour lesquels $\lambda_a = 1$, on obtient

$$q^t - 1 = q - 1 + \sum \frac{q^t - 1}{q^s - 1} ,$$

où $s|t$ et $s < t$. Si K n'est pas commutatif, $\Gamma \neq K$ et $t > 1$. Mais $\varphi_t(q)$, divisant $q^t - 1$ et tous les termes de la forme $\frac{q^t - 1}{q^s - 1}$, doit alors diviser $q - 1$. Ceci est contradictoire avec la relation

$$n > 1 \implies |\varphi_n(q)| > q - 1 .$$

Tout corps fini est commutatif.

4. $K - \{0\}$ est cyclique.

(a) Pour tout $a \in K$, il est clair que

$$a^k = a$$

(soit que $a = 0$, soit que l'ordre de a divise $k - 1$). $X^k - X$ n'ayant que des racines simples dans K , on a donc

$$X^k - X = \prod_{a \in K} (X - a) .$$

(b) Il est bien connu en théorie des groupes commutatifs qu'étant donnés des éléments d'ordres $\alpha, \beta, \gamma, \dots$, il existe un élément ω d'ordre

$$\tau = \text{p. p. c. m.} (\alpha, \beta, \gamma, \dots) .$$

Appliqué à $K - \{0\}$, ce théorème montre que les ordres de ses éléments sont des diviseurs du plus grand d'entre eux. Pour tout $a \neq 0$, on a donc $a^\tau = 1$ et

$$X^k - X = \prod_{a \in K} (X - a) \mid X^{\tau+1} - X .$$

(c) Donc $k \leq \tau + 1$. Mais comme τ divise $k - 1$, il est clair que $\tau = k - 1$. Il existe donc $\omega \in K - \{0\}$ d'ordre $k - 1$, et tous les éléments de $K - \{0\}$ sont des puissances exactes de ω .

5. Existence d'un corps de cardinal p^ν .

Il existe un sur-corps Ω de F_p dans lequel le polynôme $X^k - X \in F_p[X]$ est totalement décomposé. Dans Ω , les racines de $X^k - X$ forment un sous-corps K de Ω de cardinal k . En effet,

$$x^k = x \text{ et } y^k = y \implies x^k y^{-k} = xy^{-1} \in K.$$

D'autre part, on montre par récurrence sur ν (tel que $k = p^\nu$) que

$$(x - y)^k = x^k - y^k,$$

ce qui est bien connu pour $k = p$, puis résulte de la relation

$$(x - y)^{p^\nu} = (x^{p^{\nu-1}} - y^{p^{\nu-1}})^p = x^{p^\nu} - y^{p^\nu}.$$

Donc

$$x^k = x \text{ et } y^k = y \implies (x - y)^k = x - y \in K.$$

Pour tout nombre premier p et tout entier ν , il existe donc au moins un corps K de cardinal p^ν : le corps F_k de décomposition de $X^k - X$ dans F_p , appelé champ de Galois ou corps de Galois.

6. Construction de F_k

(a) L'ensemble des polynômes de $F_p[X]$ s'annulant pour un élément a de K est un idéal engendré par un diviseur Q de $X^k - X$. Le plus petit sous-corps de K contenant a , contenant évidemment $F_p(a) = F_p[X]/Q$, est donc $F_p(a)$ lui-même.

(b) Si ω engendre cycliquement $K - \{0\}$, et si $H = F_p(\omega)$, on a $\omega^{|H|} = \omega$, d'où $|H| \geq k$ et $H = K = F_p(\omega)$.

(c) Il existe donc un polynôme irréductible Q_0 de $F_p[X]$ tel que $Q_0(\omega) = 0$ et $K = F_p[X]/Q_0$. Si Q_0 est de degré n , on a $|K| = p^n$, d'où $n = \nu$.

(d) On sait que $X^k - X = X \prod_{d|k-1} \varphi_d(X)$. Si $\varphi_d(a) = 0$, alors $a^d = 1$. ω , racine de $X^k - X$, est donc racine de φ_{k-1} et non d'un φ_d avec $d < k - 1$. Il suffit donc, pour construire F_k , de décomposer $\varphi_{k-1}(X) \in \mathbb{Z}[X]$ en polynômes

irréductibles dans $F_p[X]$: on a vu qu'il en existait au moins un de degré v , soit Q_0 . Dès lors, $K = F_p[X]/Q_0$.

(e) Exemple : $p = 2$, $v = 4$, $k = 16$.

$$\varphi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \equiv (X^4 + X^3 + 1)(X^4 + X + 1),$$

d'où deux polynômes Q_0 possibles engendrant F_{16} .

7. Unicité de F_k .

(a) Soient K et K' deux corps de même cardinal k . K est engendré par une racine ω d'un polynôme Q_0 tel que

$$X^k - X = Q_0 R \quad (\text{degré de } Q_0 = v).$$

Cette égalité, vraie dans $F_p[X]$, l'est a fortiori dans $K'[X]$. $X^k - X$ y étant totalement décomposé, il en est de même de Q_0 .

(b) Soit alors $\omega' \in K'$ une racine de Q_0 . Elle engendre K' car le plus petit sous-corps de K' contenant ω' est de cardinal $p^v = k$.

Tout élément de $K = F_p[X]/Q_0$ peut s'écrire de façon unique sous la forme

$$a = \sum_{i=0}^{v-1} x_i \omega^i \quad (x_i \in F_p).$$

La bijection

$$a = \sum x_i \omega^i \longleftrightarrow a' = \sum x_i \omega'^i$$

est un isomorphisme de corps entre K et K' , puisque ω et ω' sont racines du même polynôme Q_0 de $F_p[X]$. Tout corps fini de cardinal k est donc isomorphe au champ de Galois F_k .

AnnexePolynômes engendrant F_k pour $k \leq 121$

k =	4	p =	2	$Q_0 = X^2 + X + 1$
	8		2	$X^3 + X + 1$
	9		3	$X^2 + X - 1$
	16		2	$X^4 + X + 1$
	25		5	$X^2 + X + 2$
	27		3	$X^3 - X + 1$
	32		2	$X^5 + X^2 + 1$
	49		7	$X^2 + X + 3$
	64		2	$X^6 + X + 1$
	81		3	$X^4 + X - 1$
	121		11	$X^2 + X - 3$
