Ann. sc. math. Québec, 1988, vol. 12, no 2, pp. 275-285

MOTS CIRCULAIRES ET POLYNÔMES IRRÉDUCTIBLES

Christophe Reutenauer

Abstract

This paper is a short survey on some results related to the following well-known fact: there are as many irreducible polynomials of degree n over the finite field with q elements as primitive circular words of length n over an alphabet with q elements. Several interpretations and bijections explaining this equality are given.

Résumé

Ce texte est celui d'un exposé au Séminaire de combinatoire de l'UQAM, le 9 mai 1986. Il ne s'agit pas de résultats originaux, mais d'une exposition de plusieurs résultats et techniques, centrés autour du fait remarquable et classique suivant: il y a le même nombre de polynômes irréductibles sur un corps fini à q éléments de degré n que de mots circulaires primitifs de longueur n sur un alphabet à q éléments.

Ces nombres interviennent encore dans plusieurs autres contextes: groupe libre, algèbre de Lie libre, identité cyclotomique. Il nous a semblé intéressant de rassembler les résultats relatifs à ces nombres dans un même article, en y ajoutant des références qui permettront au lecteur d'approfondir le sujet.

1. L'identité cyclotomique

C'est l'identité

$$\frac{1}{1-qx} = \prod_{n\geq 1} \frac{1}{(1-x^n)^{\alpha_n}}$$

où q est un nombre entier > 0 et où les α_n dépendent bien sûr de q.

Les α_n sont entièrement déterminés par cette relation. En effet, en passant aux dérivées logarithmiques, on obtient

$$\frac{q}{1-qx} = \sum_{n\geq 1} \frac{\alpha_n n x^{n-1}}{1-x^n}.$$

On multiplie par x et on développe

$$\sum_{\ell\geq 1} q^\ell x^\ell = \sum_{n,k\geq 1} n\alpha_n x^{nk} = \sum_{\ell\geq 1} x^\ell \Big(\sum_{n\mid\ell} n\alpha_n\Big).$$

Autrement dit

$$q^\ell = \sum_{n\mid\ell} n\alpha_n.$$

Grâce à Monsieur Möbius, on obtient

$$n\alpha_n = \sum_{d\mid n} \mu(d) q^{n/d}$$

ou encore

$$\alpha_n = \frac{1}{n} \sum_{d\mid n} \mu(d) q^{n/d}.$$

EXEMPLE. $(q = 2)$ $(\alpha_n)_{n\geq 1} = (2,1,2,3,6,9,18,30,56,\ldots)$.

2. Colliers

Soit A un alphabet à q lettres. Deux mots sur A sont dits *conjugués* si l'un s'écrit uv, et l'autre vu. Par exemple les mots abaab et aabab sont conjugués. Un *mot circulaire* est une classe de conjugaison, comme {aabab, ababa, babaa, abaab, baaba}. On peut représenter un mot circulaire par un mot écrit en

rond, avec un sens de lecture qui serait, disons, le sens des aiguilles des montres (celles qui ont encore des aiguilles...)

EXEMPLE. Voir Figure 1.

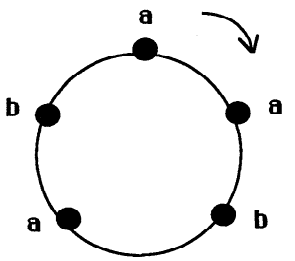

figure 1

Un *collier* est un mot circulaire *non périodique*. Il revient au même de dire qu'un collier est une classe de conjugaison de mots primitifs: un mot est *primitif* s'il n'est pas de la forme $u^n = u \cdot u \ldots u$ avec $n \geq 2$.

THÉORÈME. *Il y a* α_n *colliers de longueur* n.

PREUVE. Soit β_n le nombre de colliers de longueur n. Il suffit de montrer que

$$q^n = \sum_{d|n} d\beta_d .$$

En fait, cette relation exprime que l'ensemble des q^n mots de longueur n se partitionne en classes de conjugaison. Tout mot w de longueur n est une puissance d'un unique mot primitif: $w = u^k$; alors d = longueur (u) divise n et w possède d conjugués. □

3. Polynômes irréductibles

Soit $\mathbb{F}_q$ le corps à q éléments.

THÉORÈME. *Il y a* α_n *polynômes (en une variable) irréductibles et unitaires (i.e. de terme dominant* 1*) de degré* n *sur* F_q.

PREUVE. Soit γ_n le nombre de polynômes irréductibles et unitaires de degré n. Il y a q^n polynômes unitaires de degré n. Comme $\mathbb{F}_q[t]$ est factoriel, on obtient

$$\sum_{n\geq 0} q^n x^n = \prod_{n\geq 1} (1+x^n+x^{2n}+\ldots)^{\gamma_n}.$$

C'est encore l'identité cyclotomique. □

EXEMPLE. Voir Figure 2 (avec $q = 2$).

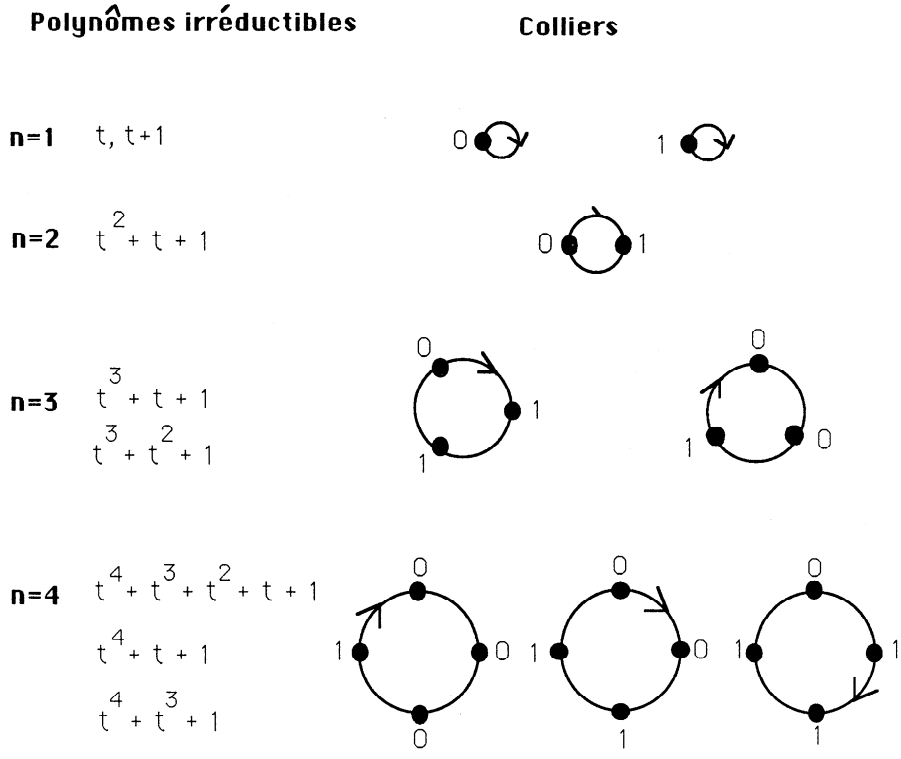

figure 2

4. Une autre interprétation

L'identité cyclotomique peut se relever en une identité sur les mots. Soit donc A un alphabet de q lettres, totalement ordonné. On ordonne A^* selon

l'ordre du dictionnaire. Un *mot de Lyndon* est un mot primitif qui est le plus petit parmi tous ses conjugués. Par exemple, aabab est un mot de Lyndon sur l'alphabet $\{a<b\}$. Un théorème de Lyndon affirme que tout mot w dans A^* s'écrit d'une et d'une seule manière comme $w = \ell_1 \cdot \ell_2 \ldots \ell_n$ où $n \geq 0$ et où les ℓ_i sont des mots de Lyndon décroissants: $\ell_1 \geq \ell_2 \geq \ldots \geq \ell_n$. Dans l'algèbre des séries formelles non commutatives sur A, ceci s'écrit

$$\sum_{w \in A^*} w = \prod_{\ell \text{ mot de Lyndon}} (1+\ell+\ell^2+\ldots)$$

où le produit Π est pris dans l'ordre décroissant. Mais le membre de gauche est $(1 - \sum_{a \in A} a)^{-1}$ et $1 + \ell + \ell^2 + \ldots = (1-\ell)^{-1}$.

En envoyant chaque lettre sur la même variable x, on obtient donc

$$\frac{1}{1-qx} = \prod_{n \geq 1} \left(\frac{1}{1-x^n}\right)^{\beta_n}$$

où β_n est le nombre de mots de Lyndon de longueur n, i.e. le nombre de colliers de longueur n.

REMARQUE. Si $A = \{1,2,\ldots,q\}$ et w est une permutation de A, i.e. $w = \sigma(1)\sigma(2)\ldots\sigma(q)$ avec $\sigma \in S_q$, alors sa décomposition en mots de Lyndon correspond à la transformée de Foata de σ. Par exemple, $w = 4\ 5\ 7\ 6\ 2\ 8\ 1\ 3 = (4576)(28)(13)$. Décomposer un mot en mots de Lyndon est donc très proche de décomposer une permutation en cycles. Cela est d'autant plus frappant que cycles et mots de Lyndon (i.e. colliers) sont des objets ayant une représentation naturelle en rond.

Pour les polynômes irréductibles, on a aussi une autre interprétation que la factorialité de $\mathbb{F}_q[t]$, comme utilisée à la Section 3. Ceci nous donnera une bonne transition vers les corps finis. On a en effet

$$t^{q^n} - t = \prod P,$$

où le produit est pris sur tous les polynômes irréductibles unitaires dont le degré divise n. Une variante du théorème de Fermat affirme en effet que tout élément du corps à q^n éléments vérifie $\alpha^{q^n} = \alpha$ (preuve: le groupe multiplicatif $\mathbb{F}_{q^n} \setminus 0$

a en effet q^n-1 éléments). Par suite,

$$t^{q^n} - t = \prod_{\alpha \in \mathbb{F}_{q^n}} (t-\alpha).$$

Mais tout α dans $\mathbb{F}_{q^n}$ est racine d'un unique polynôme unitaire dans $\mathbb{F}_q[t]$ de degré minimal, son *polynôme minimal*; si celui-ci est de degré r, alors $\mathbb{F}_q[\alpha]$ est le corps à q^r éléments, donc q^n est une puissance de q^r (puisque $\mathbb{F}_{q^n}$ est un espace vectoriel sur ce corps): donc r divise n. De plus, un polynôme minimal est toujours irréductible. Réciproquement, si P est un polynôme irréductible dont le degré r divise n et α une racine de P, alors $\mathbb{F}_q[\alpha]$ est un corps à q^r éléments; alors $r|n$ implique $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^n}$, et les autres racines de P, qui sont les $\alpha^q, \alpha^{q^2}, \ldots$ sont aussi dans $\mathbb{F}_{q^n}$. La relation ci-dessus exprime alors le fait que $\mathbb{F}_{q^n}$ a une partition dont les blocs sont formés des éléments ayant même polynôme minimal sur $\mathbb{F}_q$.

5. Corps finis

Pour toute puissance q d'un nombre premier, il existe un et un seul corps à q éléments. Si r, s sont deux entiers, on a $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^s}$ si et seulement si r divise s. Notons $\mathbb{F}_{q^\infty}$ la clôture algébrique de $\mathbb{F}_q$: c'est la réunion de tous les $\mathbb{F}_{q^r}$. De plus, on a pour $\alpha \in \mathbb{F}_{q^\infty}$:

$$\alpha \in \mathbb{F}_{q^r} \iff \alpha^{q^r} = \alpha.$$

L'application $\alpha \mapsto \alpha^{q^s}$ est un automorphisme de chacun de ces corps finis. Les éléments $\alpha, \alpha^q, \alpha^{q^2}, \ldots$ s'appellent les *conjugués* sur $\mathbb{F}_q$ de α: ce sont exactement les racines du polynôme minimal de α. L'ensemble des automorphismes

$$\alpha \to \alpha^{q^s} \qquad (s \in \mathbb{N})$$

est exactement le groupe de Galois sur $\mathbb{F}_q$ de chacun de ces corps finis; chacun d'eux laisse fixe $\mathbb{F}_q$, i.e. $\alpha \in \mathbb{F}_q \Rightarrow \alpha^q = \alpha$. Les conjugués d'un élément α sont donc les éléments de l'orbite de α sous l'action du groupe de Galois. Le groupe de Galois de $\mathbb{F}_{q^r}$ est cyclique d'ordre r, engendré par l'*automorphisme de*

Frobenius $\alpha \to \alpha^q$.

EXEMPLE: Voir Figure 3 (avec $q = 2$).

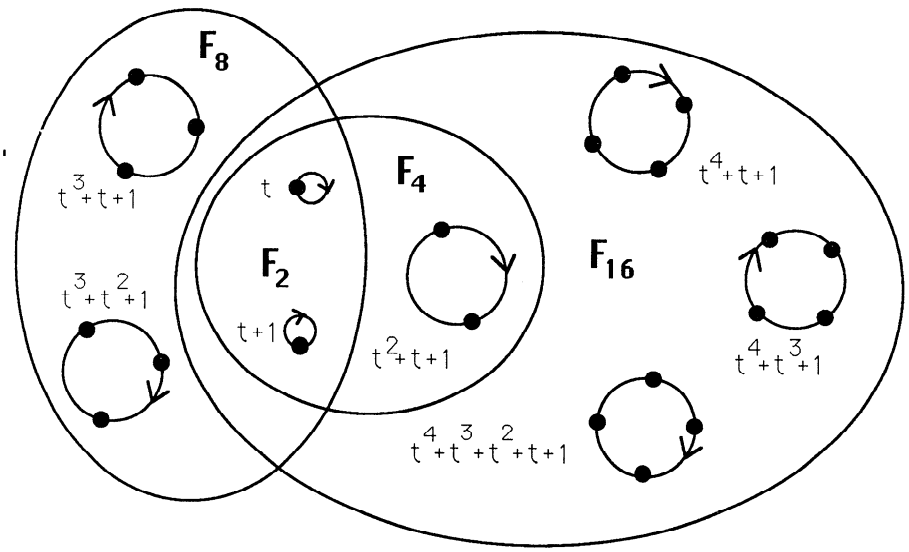

figure 3

Les corps $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$ et leurs orbites sous le groupe de Galois ($\overset{a}{\cdot} \to \overset{b}{\cdot}$ signifie que $b = a^2$). A chaque orbite, on a mis le polynôme irréductible correspondant.

6. Deux bijections

Je vais donner ici brièvement deux bijections entre polynômes irréductibles unitaires de degré n sur le corps à q éléments et colliers de longueur n sur un alphabet à q éléments.

En fait, on utilisera la bijection canonique entre polynômes irréductibles de degré n et orbites de cardinal n du groupe de Galois de $\mathbb{F}_{q^n}$.

Soit donc une bijection $a \to \underline{a}$ de $\mathbb{F}_q$ dans $[0,1,\ldots,q-1]$, qui nous permettra d'identifier les éléments de $\mathbb{F}_q$ comme des digits en base q. Un *élément primitif* α du corps $\mathbb{F}_{q^n}$ est un générateur du groupe multiplicatif (qui est cyclique) $\mathbb{F}_{q^n}\backslash 0$. On définit pour tout mot $w = a_o \ldots a_{n-1}$ sur l'alphabet $\mathbb{F}_q$ l'élément $G(w)$ par

$$G(w) = \alpha^b \quad \text{où} \quad b = \underline{a}_o + \underline{a}_1 q + \ldots + \underline{a}_{n-1} q^{n-1}.$$

On vérifie simplement que $G(a_{n-1}a_o \ldots a_{n-2}) = (G(a_o \ldots a_{n-1}))^q$, donc que les images par G de mots conjugués sont des éléments conjugués de $\mathbb{F}_{q^n}$. De plus, si w est primitif, alors ces n conjugués sont distincts, et l'on obtient ainsi une bijection entre colliers et orbites.

Pour l'autre bijection, nous utiliserons la notion de *base normale*. Une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est une base de la forme

$$\theta, \theta^q, \ldots, \theta^{q^{n-1}}.$$

Une telle base *existe toujours*.

REMARQUE. Les conjugués d'un élément ne sont pas toujours linéairement indépendants. Par exemple, l'élément θ de $\mathbb{F}_8$ ayant pour polynôme minimal $t^3 + t + 1$ sur $\mathbb{F}_2$ vérifie: $\theta^4 + \theta^2 + \theta = 0$, donc ses conjugués sont linéairement dépendants. Par contre, les racines de $t^3 + t^2 + 1$ forment une base normale de $\mathbb{F}_8$ sur $\mathbb{F}_2$.

Soit donc $\theta, \theta^q, \ldots, \theta^{q^{n-1}}$ une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. A un mot primitif $w = a_o \ldots a_{n-1}$ sur l'alphabet $\mathbb{F}_q$, associons l'élément β de $\mathbb{F}_{q^n}$ donné par

$$\beta = a_o\theta + a_1\theta^q + \ldots + a_{n-1}\theta^{q^{n-1}}.$$

Il est facile de voir qu'alors les conjugués de β correspondent aux conjugués de w, et qu'ils sont au nombre de n. On a en effet

$$\sum_{0 \le i \le n-1} a_i \theta^{q^i} = \sum_{0 \le i \le n-1} b_i \theta^{q^i}$$

si et seulement si $\forall i$, $a_i = b_i$. De plus

$$\beta^q = a_o\theta^q + a_1\theta^{q^2} + \ldots + a_{n-2}\theta^{q^{n-1}} + a_{n-1}\theta,$$

puisque $\theta^{q^n} = \theta$. Donc β^q correspond au mot $a_{n-1}a_o\ldots a_{n-2}$.

La bijection ci-dessus s'étend facilement en une bijection de $\mathbb{F}_q^\infty$ (la clôture algébrique de $\mathbb{F}_q$) sur l'ensemble des applications périodiques $\mathbb{Z} \to \mathbb{F}_q$. Pour cela, on considère une suite $(\theta_n)_{n\geq 1}$ telle que pour tout n

$$\theta_n, \theta_n^q, \ldots, \theta_n^{q^{n-1}}$$

soit une base normale de $\mathbb{F}_{q^n}$ et que pour toute factorisation $n = rs$ on ait

$$(*) \qquad \theta_s = \theta_n + \theta_n^{q^s} + \ldots + \theta_n^{q^{(r-1)s}}$$

D'après les théorèmes de non vacuité des limites projectives, une telle suite existe toujours. Soit alors

$$f: \mathbb{Z} \to \mathbb{F}_q$$

une fonction périodique et n une période de f. On lui associe l'élément de $\mathbb{F}_{q^n}$ égal à

$$f(0)\theta_n + f(1)\theta_n^q + \ldots + f(n-1)\theta_n^{q^{n-1}}.$$

A cause de $(*)$, cet élément ne dépend pas de la période n choisie. On obtient ainsi une bijection de l'ensemble des éléments périodiques de $\mathbb{F}_q^{\mathbb{Z}}$ sur $\mathbb{F}_q^\infty$: cette bijection est du reste $\mathbb{F}_q$-linéaire, comme on s'en rend compte aussitôt.

7. Encore les α_n

Ces nombres interviennent encore dans le contexte des algèbres de Lie libres et des groupes libres.

Soit $\mathbb{Z}\langle A\rangle$ l'algèbre des polynômes non commutatifs sur l'alphabet A à q éléments; soit $L\langle A\rangle$ la sous-algèbre de Lie de $\mathbb{Z}\langle A\rangle$ engendrée par les lettres.

On sait que c'est l'algèbre de Lie libre sur A. Alors l'espace des polynômes de Lie homogènes de degré n est un $\mathbb{Z}$-module libre de dimension α_n. On le voit par exemple en associant une base de $L\langle A\rangle$ aux mots de Lyndon.

EXEMPLE. $a \to a$, $b \to b$, $ab \to ab-ba$, $aab \to aab-2aba+baa = [a,ab-ba]$,
$abb \to abb-2bab+bba = [ab-ba,b]$.

Base des polynômes de Lie homogènes de degrés 1, 2, 3 sur l'alphabet $A = \{a,b\}$.

Soit F(A) le groupe libre engendré par A. La *série centrale* de F(A) est définie comme la suite de sous-groupes $F_0 = \{1\}$, $F_1 = F(A)$, $F_{n+1} = [F(A),F_n]$ où $[G,H]$ désigne le *commutateur* de G et H, i.e. le groupe engendré par les $ghg^{-1}h^{-1}$, $g \in G$, $h \in H$.

Alors F_n/F_{n-1} est un groupe abélien libre de rang α_n (formule de Witt).

Notes bibliographiques

Pour une preuve combinatoire de l'identité cyclotomique autre que celle de la Section 4, voir:

METROPOLIS, N., ROTA, G.C., Witt vectors and the algebra of necklaces, *Adv. in Math.* 50(1983), 95-125.

Pour mieux comprendre la Section 4 et les mots de Lyndon, on pourra consulter:

LOTHAIRE, M., *Combinatorics on Words* (1983), Chapitre 5.

On y trouvera aussi la construction des bases des algèbres de Lie libres, comme il en est question à la Section 7. Pour la transformée de Foata, voir aussi le Lothaire, Chapitre 10. Une référence solide pour les corps finis est:

LIDL, R., NIEDERREITER, H., Finite fields, *Encycl. of Maths* (1983), Addison-Wesley.

La première bijection de la Section 6 est due à:

GOLOMB, S.W., Irreducible polynomials, synchronization codes, primitive necklaces and the cyclotomic algebra, *Univ. of North Carolina Monograph Series in Probability and Statistics*, No 4 (1967), 358-370.

Pour ce qui touche le groupe libre, voir:

MAGNUS, W.A., KARASS, A., SOLITAR, D., *Combinatorial Group Theory* (1976), Dover.

Ni cette bijection, ni l'autre ne sont "naturelles", puisqu'on a choisi un élément primitif et une bijection $\mathbb{F}_q \to [0,q-1]$ pour l'une, et une base normale pour l'autre. La question qui demeure est donc: Existe-t-il une bijection naturelle entre colliers et polynômes irréductibles?

C. Reutenauer
Institut de Programmation
4, Place Jussieu
75005, Paris
France

Manuscrit reçu le 11 juin 1987.
Révisé le 29 septembre 1987.