PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

GUY CHASSÉ

Applications d'un corps fini dans lui-même

Publications de l'Institut de recherche mathématiques de Rennes, 1985, fascicule 4
« Séminaires de mathématiques - science, histoire et société », , p. 207-219

<http://www.numdam.org/item?id=PSMIR_1985___4_207_0>

APPLICATIONS D'UN CORPS FINI DANS LUI-MÊME

Par Guy CHASSÉ

Le présent exposé est consacré à quelques problèmes concernant les applications d'un corps fini dans lui-même. Il pose beaucoup plus de questions qu'il n'en résout. Les démonstrations des quelques résultats obtenus ne sont pas reproduites : on les trouvera dans [1] et la bibliographie citée là, ainsi que dans [2] pour les résultats de la partie III de cet exposé. On n'a pas non plus cherché à se placer dans le cadre le plus général, parlant par exemple de corps finis lorsque l'on ne se préoccupe que de questions purement combinatoires où il aurait suffit de considérer des ensembles finis.

La motivation de ce travail a été fournie par l'algorithme "rho" de factorisation des nombres entiers dû à Pollard (cf. [3] et [4]). Traçons-en sommairement les grandes idées.

Soit n le nombre entier que l'on veut factoriser. On construit la suite $(x_i)_{i \in \mathbb{N}}$ de la manière suivante

x_0 est fixé au départ

$x_{i+1} = x_i^2 + d$ modulo n pour $i \geqslant 0$

d est une constante.

On obtient ainsi une suite récurrente d'ordre 1 à valeurs dans un ensemble fini. Il s'agit donc d'une suite périodique au-delà d'un certain rang. Soit p un facteur premier de n, la suite $(x_i \bmod p)_{i \in \mathbb{N}}$ est aussi périodique au-delà d'un certain rang. Sa période est un diviseur de la période de la suite modulo n. L'idée de l'algorithme consiste à trouver un couple (i,j) d'en-

tiers tel que n ne divise pas $x_i - x_j$ et que p divise $x_i - x_j$. On obtient alors un diviseur non trivial de n puisque le p.g.c.d. de n et $x_i - x_j$ est strictement inférieur à n et plus grand ou égal à p. Dans la pratique, on regarde la suite $(c_i)_{i \in \mathbb{N}}$ définie par $c_i = x_{2i} - x_i \bmod n$, et on calcule successivement les p.g.c.d. (n, c_i) jusqu'à la découverte d'un facteur non trivial de n.

La compréhension des propriétés algébriques de l'itération d'une application $x \longmapsto x^2+d$ sur un corps fini $\mathbb{Z}/p\mathbb{Z}$, p premier fournirait donc une information importante avec cet algorithme. C'est cette volonté de comprendre, d'un point de vue algébrique, le déroulement d'un tel algorithme qui est à l'origine du travail présenté ici.

Dans tout ce qui suit, on notera k le corps fini à q éléments de caractéristique p.

I - Présentation du cadre et du vocabulaire.

a) Forme polynômiale d'une application de k dans k.

On considère l'anneau k^k des applications de k dans lui-même. Tout élément de cet anneau a une forme polynômiale, plus précisément on a l'isomorphisme d'anneaux :

$$k^k \simeq \frac{k[X]}{(X^q - X)} .$$

Toute application $k \longrightarrow k$ se représente donc d'une manière unique par un polynôme à coefficients dans k, de degré strictement inférieur à q.

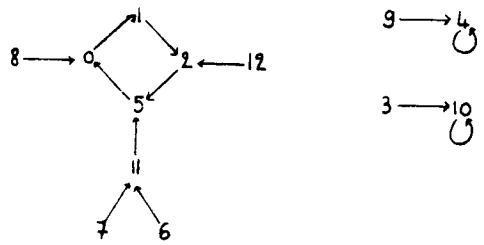
b) Graphe d'une application.

Soit $f : k \longrightarrow k$ une application. On peut lui associer un graphe orienté G(f) d'ensemble de sommets Som G(f) = k et d'ensemble d'arêtes

$$\text{Ar } G(f) = \{(x,f(x)) \ ; \ x \in k\} \ .$$

Un tel graphe se représente par un dessin.

Voici par exemple le graphe de l'application $f : x \longmapsto x^2+1$ dans le corps à 13 éléments.



On définit la relation $\sim$ sur l'ensemble des éléments de k (c'est-à-dire sur les sommets du graphe de f) par :

$$x \in k \ , \ y \in k \ : \ x \sim y \iff \{ \exists (m,n) \in \mathbb{N}^2 \text{ tel que } f^{\circ m}(n) = f^{\circ n}(x) \}$$

$f^{\circ m}$ désigne la $n^{\text{ième}}$ itérée de f.

On vérifie que $\sim$ est une relation d'équivalence dont les classes sont appelées composantes connexes.

Dans l'exemple représenté ci-dessus, sur le corps à 13 éléments, l'application $f : x \longmapsto x^2+1$ a un graphe de 3 composantes connexes, l'une de ces dernières étant formée des éléments 9 et 4.

Soit n un entier positif non nul, on appelle <u>cycle de longueur n</u> de f (ou du graphe de f) un ensemble ordonné $(x_1,\ldots,x_n)$ d'éléments de k tels que :

$$f(x_i) = x_{i+1} \quad \text{pour} \quad i \in \{1,\ldots,n-1\}$$

$$f(x_n) = x_1 \ .$$

Il y a un cycle par composante connexe. Dans l'exemple déjà cité on a

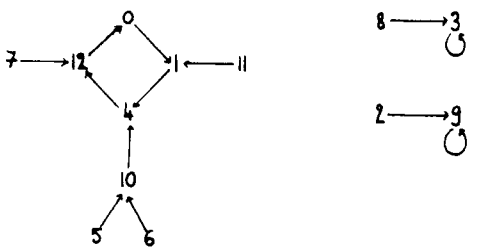
un cycle de longueur 4 : (0,1,2,5)

et deux cycles de longueur 1 : (4) et (10).

Soient f et g deux applications de k dans k, de graphes respectifs G(f) et G(g). On dit que ces graphes sont isomorphes si on peut trouver une bijection h : k ⟶ k telle que

$$f \circ h = h \circ g .$$

Voici par exemple le graphe de l'application g : $x \longmapsto x^2+2x+1$ dans le corps à 13 éléments



On constatera sans peine que ce graphe est isomorphe à celui de f : $x \longrightarrow x^2+1$ précédemment représenté. Il suffit de prendre pour h l'application $x \longmapsto x-1$.

II - Les rapports entre graphe et forme polynômiale d'une application.

Ce qui vient d'être dit nous amène aux questions suivantes : étant donnée une application $k \longrightarrow k$ sous forme polynômiale, quel est le nombre des composantes connexes de son graphe, quelles sont les longueurs de ses cycles ?

a) Cas des applications $x \longmapsto x^i$ (i entier naturel).

On restreint cette application à k^* (le groupe multiplicatif de k), ce qui donne un endomorphisme de ce groupe multiplicatif. On peut aussi, d'une manière évidente, considérer le graphe de l'application restreint à k^* (le graphe sur k sera la réunion du graphe restreint à k^* et de la composante connexe contenant le seul élément 0).

On a le résultat suivant (cf. [1], proposition de la page 58).

Proposition : Soit i un entier tel que $0 \leqslant i < q-1$ (q est le nombre d'éléments de k).
Soient r le plus grand diviseur de q-1 premier à i, et $d = (q-1)/r$.
Soit f l'endomorphisme du groupe multiplicatif k^* défini par $x \longmapsto x^i$.
s étant un diviseur de r, on note t_s l'ordre multiplicatif de i modulo s.
On convient que $t_1 = 1$.
Le graphe de f sur k^* a les propriétés suivantes :

(i) Tout diviseur s de r apporte une contribution de $\varphi(s)/t_s$ cycles de longueur t_s où φ est la fonction d'Euler.

(ii) Le nombre de cycles de f de longueur un entier quelconque n est est donné par la formule :

$$\frac{1}{n}\left(\sum_{u,u|n} \mu(n/u)(i^u-1,r)\right)$$

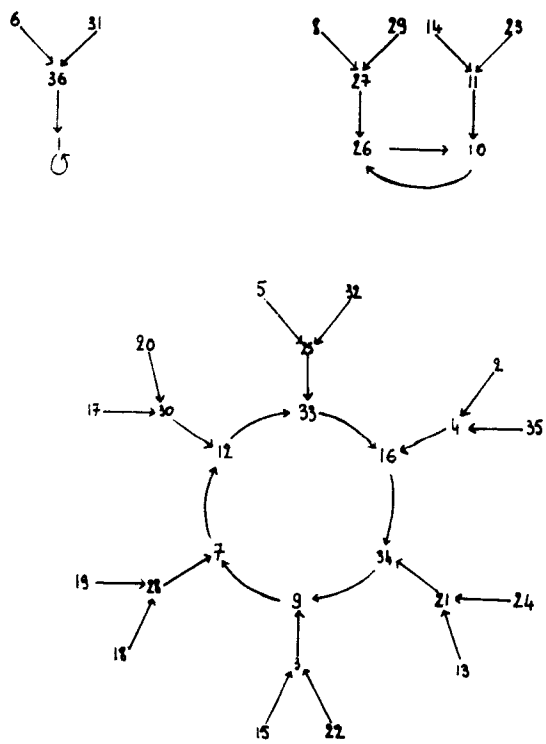
μ est la fonction de Möbius.

$\sum_{u,u|n}$ signifie que l'on fait la somme sur tous les diviseurs u de n.

(i^u-1,r) désigne le p.g.c.d. de i^u-1 et r.

(iii) Le nombre total de cycles (donc de composantes connexes) de f sur k^* est égal à $\sum_{s,s|r} \varphi(s)/t_s$ (la somme est faite sur tous les diviseurs s de r).

Voici à titre d'illustration, un dessin représentant le graphe de l'application $f : x \longmapsto x^2$ sur le groupe multiplicatif du corps à 37 éléments.



On a ici $i = 2$, $r = 9$.

Les diviseurs de 9 sont 1, 3 et 9.

On a

$t_1 = 1$

$t_3 = 2$ (ordre multiplicatif de 2 modulo 3)

$t_9 = 6$ (ordre multiplicatif de 2 modulo 9).

Ce qui donne :

1 cycle de longueur 1

$\varphi(3)/2$ = 1 cycle de longueur 2

$\varphi(9)/6$ = 1 cycle de longueur 6.

b) Applications du second degré.

On aimerait déterminer, à isomorphisme près, le graphe de l'application $f : x \longmapsto ax^2+bx+c$ où a,b,c sont trois éléments de k, $a \neq 0$. Il est facile de voir que l'on peut trouver une transformation affine $h : x \longmapsto \alpha x+\beta$, $\alpha \neq 0$ telle que

$$h^{-1} \circ f \circ h = x \longmapsto x^2+d \ , \ d \in k \ .$$

Les graphes de f et $h^{-1} \circ f \circ h$ sont alors isomorphes. Il suffit donc de regarder les graphes des applications $x \longmapsto x^2+d$, $d \in k$ pour avoir tous les graphes d'applications du second degré à isomorphisme près.

On peut vérifier, sur des exemples, que le graphe de $x \longmapsto x^2+d$, $d \neq 0$ ne dépend pas des propriétés de d en tant qu'élément de k^* (cf. [1]). Mais peut-on avoir deux graphes isomorphes pour d et d' distincts ou, ce qui revient au même, existe-t-il une bijection $\varepsilon : k \longrightarrow k$ telle que $x^2+d' = \varepsilon(\varepsilon^{-1}(x)^2+d)$ pour tout x dans k ? Une étude exhaustive montre que l'on peut répondre non dans les corps à 7 et 47 éléments. Y a-t-il une caractérisation des graphes d'applications du second degré à isomorphisme près ?

On établit facilement que le graphe d'une application du second degré a les propriétés suivantes ([1], proposition 2, page 106) :

(i) (q-1)/2 sommets ne sont l'extrémité d'aucune arête.

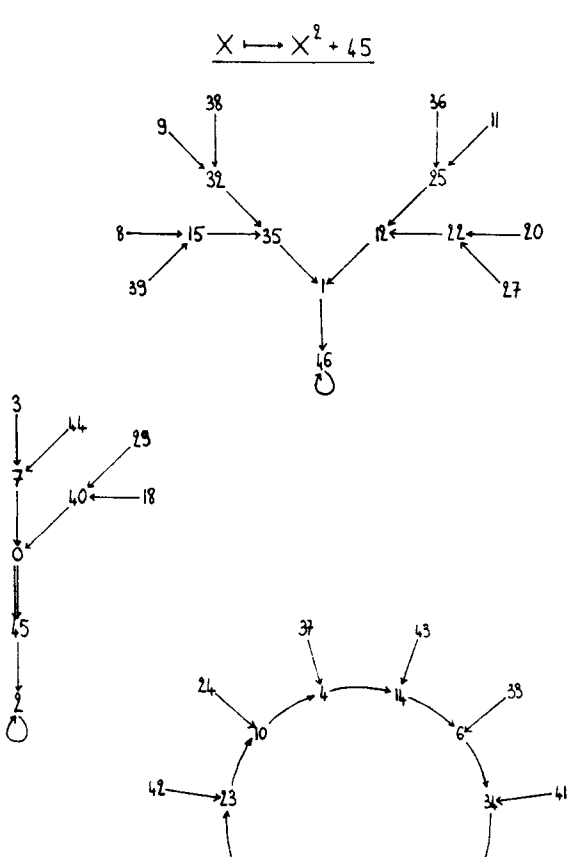
(ii) (q-1)/2 sommets sont l'extrémité de deux arêtes distinctes.

(iii) 1 sommet est l'extrémité d'une seule arête.

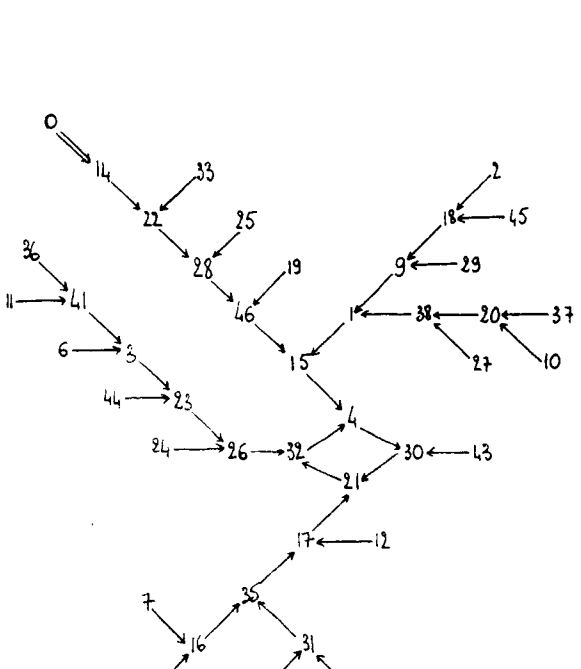
Ces propriétés ne suffisent pas à caractériser à isomorphisme près les graphes d'applications du second degré : dans le corps à 7 éléments, on peut trouver des graphes d'applications vérifiant ces propriétés qui ne sont isomorphes à aucun graphe d'application du second degré (cf. [1], pages 107-108).

Voici à titre d'illustration, les graphes de deux applications du second degré dans le corps à 47 éléments (la flèche double indique l'unique élément ayant un seul antécédent).

$X \longmapsto X^2 + 45$



$X \longmapsto X^2 + 14$



c) Un point de vue combinatoire.

Soient n un entier naturel strictement positif, E l'ensemble $\{1,2,\ldots,n\}$ et f une application de E dans E. On peut représenter f par la matrice carrée nxn

$$M_f = (m_{ij})_{1\leqslant i,j\leqslant n}$$

m_{ij} désignant le coefficient se trouvant sur la ligne i et la colonne j et

$$m_{ij} = 1 \quad \text{si} \quad i = f(j)$$
$$m_{ij} = 0 \quad \text{si} \quad i \neq f(j).$$

On désigne par E^E l'ensemble des applications de E dans E, et par $\mathcal{M}_n$ l'ensemble des matrices carrées nxn à coefficients dans $\{0,1\}$ ayant exactement un 1 dans chaque colonne. Ces deux ensembles munis respectivement de la composition des applications et de la multiplication matricielle, ont une structure de monoïde, et on a un isomorphisme de monoïdes :

$$E^E \longrightarrow \mathcal{M}_n$$
$$f \longmapsto M_f$$

f étant une application de E dans E, on note $P_f(T)$ le déterminant de la matrice $I-TM_f$ (I étant la matrice identité nxn). Ceci est un élément de $\mathbb{Z}[T]$.

On a la proposition suivante (cf. [1], proposition page 28).

Proposition : Les deux propriétés suivantes sont équivalentes :

(i) $P_f(T) = \prod_{i=1}^{r} (1 - T^{k_i})^{t_i}$

(ii) f a t_i cycles de longueur k_i pour $1 \leqslant i \leqslant r$.

Soit u le nombre de points de E qui sont dans des cycles de f (on appelle ces points des points récurrents), alors on a :

$$u = \sum_{i=1}^{r} k_i t_i = \text{degré de } P_f(T) .$$

Soit $Q_f(T)$ le polynôme caractéristique de la matrice M_f, on a formellement :

$$Q_f(T) = T^n P_f(\tfrac{1}{T})$$

et nous pouvons écrire :

$$Q_f(T) = T^{n-u} R_f(T)$$

$R_f(T)$ étant un polynôme de $\mathbb{Z}[T]$ à coefficient constant non nul. Ceci montre que la connaissance de la multiplicité de 0 en tant que racine du polynôme caractéristique de M_f nous donne le nombre u de points récurrents de f.

Venons-en à un corps fini à p éléments (p entier premier) et considérons

$$f : x \longrightarrow x^2+d$$

$$g : x \longmapsto x^2+d+1 .$$

Posons pour toute application h de ce corps dans lui-même :

$$M_h = (m_{ij})_{0\leqslant i,j\leqslant p-1}$$

$$m_{ij} = 1 \quad \text{si} \quad i = h(j)$$

$$m_{ij} = 0 \quad \text{si} \quad i \neq h(j) .$$

On passe de M_f à M_g en faisant agir une permutation circulaire sur les lignes qui envoie la ligne i sur la ligne i+1 pour i, $1 \leqslant i \leqslant p-1$ et la ligne p à la place de la première.

Peut-on trouver un algorithme permettant de passer de la multiplicité de 0 comme racine du polynôme caractéristique de M_f à la multiplicité de 0 comme racine du polynôme caractéristique de M_g ? Une réponse affirmative serait intéressante car on peut calculer la multiplicité de 0 dans $Q_f(T)$ pour d=0.

III - Extension du corps de base.

Soit f une application de k dans k. On peut, comme on l'a vu, représenter cette application par un polynôme f(X) de k[X] de degré inférieur à q. On cherche à répondre à la question suivante : que se passe-t-il du point de vue de la longueur des cycles lorsque l'on considère f sur une extension algébrique de k ? Le résultat, comme le montre la proposition suivante est que, si le degré du polynôme f(X) est supérieur ou égal à 2, la longueur des cycles de f sur une clôture algébrique de k n'est pas bornée.

Proposition ([2], proposition 2) : Soient K un corps commutatif algébriquement clos et $f : K \longrightarrow K$ une application polynômiale de degré plus grand ou égal à 2. Soit t un nombre premier, $t \neq p$ si K est de caractéristique $p \neq 0$, et t différent aussi des ordres multiplicatifs des racines de l'unité $u \neq 1$ de la forme $u = f'(\xi)$ (f' est la dérivée formelle de f) ξ étant un point fixe de f. Alors f a un cycle de longueur t dans K.

Remarque : Une telle application n'a pas nécessairement des cycles de n'importe quelle longueur (cf. la fin de [2]).

Liée à ce type de considérations, on a aussi la proposition suivante qui peut sembler surprenante (les notations sont identiques à celles de la proposition précédente).

Proposition : Soit ξ une racine de f(X)-X (c'est-à-dire un point fixe de f) de multiplicité $m > 1$. Soient n un entier positif et m' la multiplicité de ξ comme racine de $f^{\circ n}(X)-X$ ($f^{\circ n}(X)$ est le $n^{\text{ième}}$ itéré de f(X)). Alors :

(i) $m' = m$ si la caractéristique de K est nulle ou bien ne divise pas n.

(ii) $m' > m$ si la caractéristique de K est non nulle et divise n.

Remarques.

1) De curieuses suites de polynômes.

Les notations sont à nouveau les mêmes que dans les deux propositions précédentes. On peut montrer que l'on a deux suites de polynômes de

$$K[X] : (f^{\circ n}(X)-X)_{n\in\mathbb{N}} \quad \text{et} \quad ((f^{\circ n}(X)-X)/(f(X)-X))_{n\in\mathbb{N}}$$

qui sont des suites de divisibilité, c'est-à-dire que si m divise n, le $n^{\text{ième}}$ terme de la suite divise le $n^{\text{ième}}$ terme dans K[X]. Les suites de Lucas-Lehmer en théorie des nombres ont aussi cette propriété.

On peut enfin considérer une troisième suite $(\phi_n(X))_{n\in\mathbb{N}}$ définie par

$$\phi_n(X) = \prod_{d,d|n} (f^{\circ d}(X)-X)^{\mu(n/d)}$$

(μ est la fonction de Möbius).

Les $\phi_n(X)$ sont a priori des éléments de K(X), c'est-à-dire des fractions rationnelles. Mais sur de nombreux exemples, ils sont en fait dans K[X], cette propriété est-elle vraie en général ?

2) Action du groupe de Galois sur les cycles.

Soient k le corps à p éléments, p premier et k' une extension algébrique finie de k. Soit f un élément de k[X] que l'on considèrera comme une application $k' \longrightarrow k'$. Il est naturel de regarder l'action de l'automorphisme de Frobenius $\sigma : x \longmapsto x^p$ sur le graphe de f sur k'. σ est alors un automorphisme du graphe de f, mais parfois conserve globalement un cycle, parfois l'envoie sur un autre cycle de même longueur (cf. la dernière partie de [2]).

Bibliographie

[1] G. CHASSÉ : "Applications d'un corps fini dans lui-même". Thèse de troisième cycle. Université de Rennes 1984.

[2] G. CHASSÉ : "Combinatorial cycles of a polynomial map over a commutative field". Soumis pour publication à "Discrete Mathematics".

[3] D.E. KNUTH : "The art of computer programming, Vol. 2, Seminumerical algorithms". 2 nd. ed., Addison-Wesley, 1981.

[4] J.M. POLLARD : "A Monte Carlo method for factorization". B.I.T. 15 (1975) 331-334.

Guy CHASSÉ
C.C.E.T.T. - B. P. 59
Rue du Clos Courtel
35510 - CESSON SEVIGNÉ