Condition nécessaire et suffisante pour qu'une bijection d'un ensemble fini (noté E) dans lui-même, soit un carré

par L. G. Vidiani, professeur en Mathématiques supérieures, lycée Carnot de Dijon.

L'épreuve du Concours Général du mercredi 20 avril 1983, très intéressante, mais décousue, demandait dans sa partie II, d'établir une condition nécessaire et suffisante pour qu'une bijection f d'un ensemble E fini dans lui-même soit un carré, c'est-à-dire qu'il existe une bijection g de E dans lui-même telle que

$$f = g \circ g.$$

Il me semble que les résultats obtenus peuvent intéresser les lecteurs de la Revue de Mathématiques spéciales.

Soit f une permutation de l'ensemble fini E; posons $f = g \circ g$. L'orbite $G(a)$ de a par g, formée des itérés d'ordre 0, 1, 2, 3... jusqu'à $(m - 1)$ de a, est stable par f; si la longueur de $G(a)$ est $m = 2p - 1$, l'orbite $F(a)$ de a par f est égale à $G(a)$ car f transforme successivement a en ses itérés par g d'ordres respectifs $2, 4, \ldots, 2p - 2, \quad 1, 3, 5, \ldots, (2p - 3)$; si $m = 2p$, f transforme $G(a)$ en deux orbites disjointes : $F(a)$ et $F(b)$ où $b = f(a)$ (les deux orbites $F(a)$ et $F(b)$ sont disjointes car $g^{2k}(a) = g^{2k'+1}(a)$ signifierait que $G(a)$ serait de longueur impaire).

Il en résulte une condition nécessaire pour qu'une permutation d'un ensemble fini soit un carré : il faut que, pour tout entier pair k, le nombre d'orbites de longueur k soit pair, car une orbite paire de f provient d'une orbite paire de g qui engendre deux orbites disjointes de même longueur.

Cette condition est également suffisante. On définit g par ses restrictions aux orbites de f. Une orbite $F(a)$ de longueur $2p - 1$ permet de définir la restriction de g à $F(a)$ par

$$g(x) = f^p(x);$$

si $F(a)$ est de longueur $2p$, on lui associe une orbite disjointe $F(b)$ de même cardinal et on transforme $f^i(a)$ en $f^i(b)$, lui-même transformé en $f^{i+1}(a)$. On notera que g n'est unique que si, et seulement si, f ne possède que des orbites impaires de longueurs distinctes.

Critère.

On a donc prouvé qu'une condition nécessaire et suffisante pour que f soit un carré est que pour tout entier pair $2p$ appartenant à $\mathbb{N} \cap [2, \operatorname{card} E]$ le nombre des orbites éventuelles, de cardinal $2p$, soit pair.

Ceci était prévisible car la signature d'un cycle de longueur L est $(-1)^{L-1}$, l'existence de g dont f soit le carré implique donc que la signature de f est plus un.

Par exemple si toutes les orbites sont de cardinal impair, alors f est un carré. Par contre si f est de signature -1, il ne peut être un carré car

$$\varepsilon g^2 = (\varepsilon g)^2 = +1.$$

Notons que la condition nécessaire de signature positive, ne suffit pas d'après le critère, comme le montre une bijection décomposée en deux cycles pairs d'ordres distincts.

Donnons maintenant quelques exemples d'application :

Premier exemple : Avec les notations usuelles considérons :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 3 & 1 & 2 & 6 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 4 & 3 & 5 \\ 4 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 7 & 6 \\ 7 & 6 & 2 \end{pmatrix}$$

f ne peut être un carré puisqu'il n'y a qu'une seule orbite paire.

Second exemple (celui du concours général 1983) : Soit m et p deux entiers naturels non nuls. On donne

$$E = \{1, 2, 3, \ldots m\} \times \{1, 2, \ldots p\}$$

et la bijection f de E définie par

$$\begin{cases} f(i, j) = (i + 1, \ p + 1 - j) & \text{si } i \neq m \\ f(m, j) = (1, p + 1 - j). \end{cases}$$

l'orbite de (a, j) est

$$\{(a, j), (a + 1, \ p + 1 - j), (a + 2, j) \ldots (a - 1, \ p + 1 - j)\} \ 1 \leqslant a \leqslant m.$$

• *Si m est pair*, l'orbite se ferme au premier tour, $\operatorname{Card}(O(i, j)) = m$ et comme il y a p valeurs de j, il y a p orbites. L'orbite n'est plate que si $j_0 = \dfrac{p + 1}{2}$ est entier, ce qui n'a lieu que pour p impair.

En effet les itérés de $(1, j)$ aboutissent à $(m, p + 1 - j)$ dont l'image est $(1, j)$.

Sur la figure 1 est représentée l'orbite de $(1, j)$ pour m pair.

Les traits légers fléchés, indiquent l'effet de f sur un point de E.

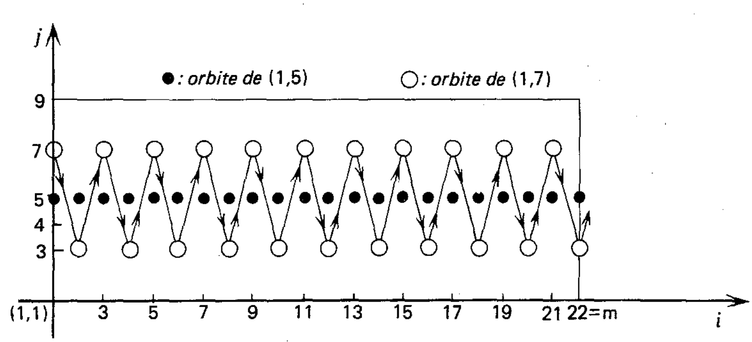

Fig. 1.

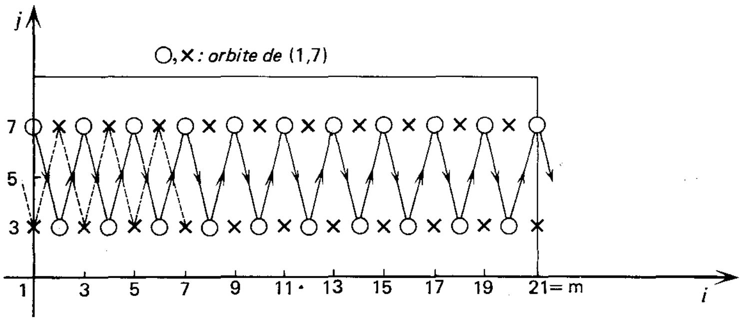

FIG. 2.

• *Si m est impair* et j différent de j_0 l'orbite de (i, j) ne se ferme pas au premier tour et dans ce cas card $O((i, j)) = 2m$.

Si p est pair, toutes les orbites sont de cardinal $2m$, leur nombre est $p/2$ puisque (i, j) a la même orbite que $(i, p + 1 - j)$.

Si p est impair, il y a une orbite de cardinal m impair, celle de $(1, j_0)$ et comme il y a $p - 1$ valeurs de j différentes de j_0, il y a $\frac{p-1}{2}$ orbites de cardinal $2m$. Sur la figure 2 ci-dessus est représentée l'orbite de (i, j) pour m impair : au premier tour les points sont marqués par O, au second par ×.

Résumons les résultats obtenus dans un tableau synthétique.

Les nombres indiqués dans une case ont la signification suivante :

Nombre des orbites de cardinal pair	
Cardinal des orbites de cardinal pair	Nombre des orbites de cardinal impair

p \ m	Impair $m = 2m' + 1$		Pair $m = 2m'$	
Impair $p = 2p' + 1$ $\frac{p}{2} = p' + \frac{1}{2}$	$\frac{p-1}{2} = p' = \left[\frac{p}{2}\right]$		$p = \left[\frac{p}{1}\right]$ f non carré (le nombre des orbites paires est impair)	
	$2m$	1	m	0
Pair $p = 2p'$ $\frac{p}{2} = p'$	$\frac{p}{2} = p' = \left[\frac{p}{2}\right]$		$p = 2p' = \left[\frac{p}{1}\right]$	
	$2m$	0	m	0

Ce qui permet de dresser le nouveau tableau, où les cases barrées indiquent les cas où f ne peut être un carré.

p \ m		Impair	Pair
Impair	$4q + 1$, $\left[\frac{p}{2}\right] = 2q$	$f = g^2$	
	$4q + 3$, $\left[\frac{p}{2}\right] = 2q + 1$		
Pair	$4q$, $\left[\frac{p}{2}\right] = 2q$	$f = g^2$	$f = g^2$
	$4q + 2$, $\left[\frac{p}{2}\right] = 2q + 1$		$f = g^2$

Apprécions, comme une baie rare, la possibilité de synthétiser la conclusion sous la forme réduite suivante :

f carré équivaut à $\left[\dfrac{p}{1 + \dfrac{1 - (-1)^n}{2}}\right]$ est un entier pair.

Pour établir le critère faisant l'objet de la présente note, nous aurions pu, bien évidemment, utiliser le théorème de Lagrange, mais il aurait masqué l'effet fonctionnel de g sur les orbites.

Ainsi si n est l'ordre de f, n' celui de g à un même ensemble stable par f et g, on a

$$f^n = e \quad \text{implique} \quad g^{2n} = e$$

et donc n' divise $2n$. En outre

$$g^{n'} = e \quad \text{implique} \quad f^{n'} = e$$

et donc d'après le théorème de Lagrange n divise n' :

$\left.\begin{array}{l} 2n = k'n' \\ n' = kn \end{array}\right\}$ ce qui donne $2n = kk'n$ soit $kk' = 2$

ce qui donne les deux situations que nous avons évoquées plus haut :

$k = 1$, $n' = n$ l'orbite de a par g est $F(a)$;

$k = 2$, $n' = 2n$ l'orbite de a par g est $F(a) \cup F(b)$.

Le problème pourrait se généraliser à la discussion de la recherche de racine k^e de f. Le problème de l'unicité ne se pose pas, ainsi que la finitude éventuelle de l'ensemble des solutions, comme on le voit dans le cas où $(\mathscr{L}(E), .)$ est un anneau fini à diviseurs de zéro, deux solutions devant vérifier

$$(g + g') \circ (g - g') = 0$$

ou encore comme le montre le cas particulier où $f = \mathrm{id}_E$ et où l'ensemble des solutions de $g^2 = \mathrm{id}_E$ n'est pas réduit à id_E et contient toutes les transpositions qui existent si card E supérieur à 2.

Une autre généralisation du problème est d'étudier l'équation fonctionnelle

$$f(f(x)) + af(x) + tx = 0$$

ce qui fait l'objet des trois premières références bibliographiques.

Bibliographie :

Revue de Mathématiques spéciales n° 2, 1982, page 120.

American Mathematical Monthly, Novembre 1981, page 711.

C. Berge : Graphes et hypergraphes, pages 37 et 38 (Dunod).

Comtet, Analyse combinatoire, tome 2, P.U.F., pages 99 et 102.

Gandemacher. Théorie des matrices, tome 1, pages 234 et 242.

Premier exercice, premier jour des Olympiades mercredi 6 juillet 1983.