JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIE JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

GUSTAVE CHOQUET

Application à la théorie des réseaux, d'un théorème sur la structure des permutations d'un ensemble

Journal de mathématiques pures et appliquées 9e série, tome 25 (1946), p. 161-172. http://www.numdam.org/item?id=JMPA_1946_9_25__161_0



 $\mathcal{N}_{\text{UMDAM}}$

Article numérisé dans le cadre du programme Gallica de la Bibliothèque nationale de France http://gallica.bnf.fr/

et catalogué par Mathdoc dans le cadre du pôle associé BnF/Mathdoc http://www.numdam.org/journals/JMPA

Application à la théorie des réseaux, d'un théorème sur la structure des permutations d'un ensemble;

PAR GUSTAVE CHOQUET.

Introduction.

Définitions. — Soit E un ensemble abstrait, fini ou infini, contenant au moins deux éléments. Et soit \mathcal{E} l'ensemble des couples non ordonnés (a, b) d'éléments distincts de E.

- 1. Si A est un sous-ensemble quelconque de & (A peut être vide ou identique à &), on dit que A définit un réseau sur E; on dit encore, par abus de langage, que A est un réseau défini sur E. On appelle ordre du réseau le nombre cardinal E de E.
- 2. Si $\mathcal{B} = \mathcal{E} \mathcal{A}$, on dit que \mathcal{B} est le réseau complémentaire de \mathcal{A} sur E.
- 3. Pour toute permutation P de E, désignons par \mathcal{Z} la permutation de \mathcal{E} associée à P. Si alors \mathcal{A}_1 et \mathcal{A}_2 sont deux réseaux définis sur E, on dit que \mathcal{A}_1 et \mathcal{A}_2 sont isomorphes s'il existe une permutation P de E telle que $\mathcal{A}_2 = \mathcal{Z}(\mathcal{A}_1)$.
- 4. Un réseau α défini sur E est dit réciproque lorsque α est isomorphe à son complémentaire β .

L'étude qui suit a pour but de montrer que pour qu'on puisse définir un réseau réciproque sur E, il faut et il suffit que E soit infini, ou composé de 4n ou (4n+1) éléments (n est un entier ≥ 1). Nous montrerons en même temps comment on peut définir tous les réseaux

réciproques sur E; puis nous ferons une brève étude de la structure de ces réseaux.

Cette étude est la réponse à une question posée par M. Germain Kréweras.

I. — Étude des permutations d'un ensemble.

1. Soit & une permutation d'un ensemble &.

Considérons une partition de \mathcal{E} en ensembles \mathcal{E}_i dont chacun soit globalement invariant par \mathcal{R} .

Il est évident que pour tout $a \in \mathcal{E}_i$, on a aussi

$$\mathfrak{L}^n(a) \in \mathcal{E}_i$$
 pour tout $n \geq 0$.

Il existe donc une partition de \mathcal{E} en ensembles \mathcal{E}_i plus fine que toutes les autres. C'est la partition de \mathcal{E} par la relation d'équivalence « $a \sim b$ si $b = \mathcal{Z}''(a)$ pour un certain n ».

Toute classe d'équivalence de cette partition sera désignée par e_i . Ou bien e_i se compose d'un nombre fini p d'éléments permutés circulairement par \mathfrak{A} . On dit alors que e_i est un cycle fermé d'ordre n.

Ou bien e_i se compose d'une suite d'éléments a_n (avec n = ..., -k), ..., -1, 0, +1...) telle que $a_{n+1} = \mathfrak{L}(a_n)$ pour tout n. On dit alors que e_i est un cycle ouvert.

Donc pour toute permutation \mathfrak{L} de \mathfrak{E} , il existe une partition de \mathfrak{E} en cycles e_i , ouverts ou fermés. Toute partition de \mathfrak{E} en ensembles \mathfrak{E}_k dont chacun est globalement invariant par \mathfrak{L} s'obtient en prenant pour tout \mathfrak{E}_k une réunion quelconque de cycles e_i .

Toute permutation de & s'obtient donc à partir d'une partition quelconque de & en ensembles finis ou dénombrables, dont chacun peut être organisé de façon quelconque en cycle.

L'ensemble des points invariants d'une permutation \mathfrak{L} est évidemment identique à l'ensemble des cycles fermés d'un élément. L'ensemble des points invariants de $\mathfrak{L}^{(n)}$ est identique à l'ensemble des éléments des cycles fermés de k éléments, où k est un diviseur quelconque de n.

2. Recherchons les permutations \mathcal{Z} d'un ensemble donné \mathcal{E} telles qu'il existe une partition de \mathcal{E} en deux ensembles \mathcal{A} et \mathcal{B} , avec $\mathcal{B} = \mathcal{Z}(\mathcal{A})$ (donc aussi $\mathcal{A} = \mathcal{Z}(\mathcal{B})$).

Plus généralement, cherchons les permutations \mathfrak{L} de \mathfrak{E} telles qu'il existe une partition de \mathfrak{E} en ensembles ε_i , de telle sorte que, pour tout ε_i , il existe une partition de ε_i en deux ensembles α_i , β_i , avec $\beta_i = \mathfrak{L}(\alpha_i)$ (donc aussi $\alpha_i = \mathfrak{L}(\beta_i)$).

Nous verrons que ces deux problèmes sont équivalents :

Remarquons que tout ε_i est globalement invariant par \mathfrak{T} , donc ε_i est une réunion de cycles.

Comme
$$\beta_i = \mathfrak{L}(\alpha_i)$$
 et $\alpha_i = \mathfrak{L}(\beta_i)$, on a, pour tout $a \in \alpha_i$, $\mathfrak{L}^{(2n)}(\alpha) \in \alpha_i$ et $\mathfrak{L}^{(2n+1)}(\alpha) \in \beta_i$ pour tout n entier.

Donc le cycle de ${\mathfrak L}$ défini par a est forcément d'ordre pair s'il est fermé.

Donc & ne doit contenir aucun cycle fermé d'ordre impair. Supposons qu'il en soit ainsi :

Tout cycle de \mathcal{Z} se partage alors d'une façon et d'une seule en deux ensembles donc chacun est l'image de l'autre par \mathcal{Z} .

Par exemple, si ce cycle est infini, soient $(\ldots a_k \ldots a_1, a_0, a_1 \ldots)$ ses éléments; les deux ensembles de sa partition sont :

$$\bigcup_{n} a_{2n}$$
 et $\bigcup_{n} a_{2n+1}$, où n est un entier quelconque.

On peut donc énoncer :

Théorème 1. — Pour que le problème général posé au début de ce paragraphe soit possible, il faut et il suffit que la permutation $\mathfrak L$ ne contienne pas de cycle fermé d'ordre impair. Dans ce cas, parmi les partitions de $\mathfrak E$ en ensembles ϵ_i , il en existe une plus fine que toutes les autres, c'est la partition de $\mathfrak E$ en cycles e_i ; pour cette partition, les ensembles α_i , β_i sont bien déterminés, à l'échange près de α_i en β_i .

Cas particulier. — \mathcal{L} ne contenant aucun cycle fermé d'ordre impair, on obtient de la façon suivante toutes les partitions de \mathcal{E} en deux ensembles \mathcal{A} , \mathcal{B} tels que $\mathcal{B} = \mathcal{L}(\mathcal{A})$.

Pour tout cycle e_i , soit $e_i = \alpha_i + \beta_i$ avec α_i . $\beta_i = 0$ et $\beta_i = \hat{\mathfrak{L}}(\alpha_i)$. On pose

$$\alpha = \bigcup_i \alpha_i$$
 et $\alpha = \bigcup_i \beta_i$

Lorsque & et 2 sont donnés, on peut évaluer aisément le nombre N de façons de choisir A:

Si & contient & cycles distincts, on a

$$N = 2^{\aleph}$$
.

En particulier, si & n'est pas dénombrable, on a

$$\aleph = \overline{\mathcal{E}}, \quad \text{donc} \quad N = 2^{\overline{\overline{\mathcal{E}}}}.$$

Si & est denombrable, on a $\aleph = \aleph_0$ ou un nombre fini. Donc $N = 2^{\aleph_0}$ ou un nombre fini.

II. — Recherche des réseaux réciproques définis sun un ensemble :

3. Soit & un réseau réciproque défini sur un ensemble E. On désigne par P une permutation de E dont l'associée & transforme & en son complémentaire &.

Comme $\mathcal{B} = \mathfrak{A}(\mathcal{A})$, en vertu du théorème 1, \mathcal{A} ne contient aucun cycle fermé d'ordre impair.

Voyons ce qu'il en résulte pour P. On va voir que P ne peut contenir aucun cycle fermé d'au moins deux éléments qui soit d'ordre n ou 2n, où n est un nombre impair > o.

En effet, supposons qu'il n'en soit pas ainsi.:

1° Si a, b sont deux éléments distincts d'un cycle d'ordre n impair de P, on a

$$P^n(a) = a$$
 et $P^n(b) = b$

Donc $\mathfrak{L}''(a, b) = (a, b)$ et \mathfrak{L} contient donc un cycle d'ordre impair.

2º Si a est un élément d'un cycle d'ordre 2n de P, posons $b = P^n(a)$. On a donc

$$b = \mathbf{P}^n(a)$$
 et $a = \mathbf{P}^n(b)$, 0

Donc $\mathfrak{A}^n(a, b) = (a, b)$ et \mathfrak{A} contient encore un cycle d'ordre impair.

Donc tous les cycles fermés de P sont d'ordre 1 ou d'ordre 4n (où n > 0).

Et il est évident que P contient au plus un cycle d'ordre 1, sinon C contiendrait aussi des cycles d'ordre 1.

Réciproquement, soit P une permutation quelconque de E dont tous les cycles fermés sont d'ordre divisible par 4, sauf un au plus qui peut être d'ordre 1.

Je dis que la permutation \mathscr{L} de \mathscr{E} associée à P a tous ses cycles fermés d'ordre pair. En effet, dans le cas contraire, \mathscr{L} posséderait un cycle d'ordre impair; il y aurait donc dans E un couple (a, b) d'éléments distincts tel que $\mathscr{L}^n(a, b) = (a, b)$ pour un n impair > 0. On aurait donc:

- 1° Soit $P^n(a) = a$, $P^n(b) = b$; donc P contiendrait, soit un cycle impair d'ordre > 1, soit au moins deux cycles d'ordre 1.
- 2º Soit $P^n(a) = b$, $P^n(b) = a$; d'où $P^{2n}(a) = a$. Donc a et b feraient partie d'un même cycle fermé. Soit r l'ordre de ce cycle; l'égalité $2n = \lambda r$, où n n'est pas un multiple de r montre que r = 2n.

Donc P contiendrait un cycle d'ordre 2n, où n est impair > 0.

Le théorème 1 montre que si $\mathscr L$ ne contient pas de cycle sermé d'ordre impair, on peut trouver une partition de $\mathscr E$ en $\mathscr A$ et $\mathscr B$, avec $\mathscr L(\mathscr A) = \mathscr B$.

On peut donc énoncer :

Théorème 2. — La condition nécessaire et suffisante pour que la permutation $\mathfrak L$ de $\mathfrak E$ associée à une permutation P d'un ensemble E soit telle qu'il existe une partition de $\mathfrak E$ en $\mathfrak L$ et $\mathfrak B$ avec $\mathfrak B=\mathfrak L(\mathfrak L)$, est que tout cycle fermé de P soit d'ordre divisible par $\mathfrak L$, sauf au plus un de ces cycles, qui peut être d'ordre $\mathfrak I$ (l'élément de ce cycle est alors le seul élément invariant de P).

4. On peut maintenant répondre à la question :

Étant donné un ensemble E, reconnaître si l'on peut définir sur E des réseaux réciproques, et déterminer ces réseaux.

Si l'on peut définir un réseau sur E, le théorème 2 montre que l'on doit avoir, soit \overline{E} infini, soit $\overline{E} = 4n$ ou (4n+1), où n est un entier > o.

Si E répond à cette condition simple, on prend une partition quelconque de E en ensembles e_i tels que, pour tout e_i , on ait, soit $\overline{e_i} = \aleph_0$, soit $\overline{e_i} = 4n_i$ (n_i entier positif quelconque), avec l'exception possible d'un seul e_i pour lequel $\overline{e_i} = 1$.

On définit sur chacun de ces e_i une permutation quelconque comprenant un seul cycle. Ces permutations partielles définissent sur E une permutation P; la permutation \mathfrak{L} de \mathfrak{L} associée à P ne contient aucun cycle fermé d'ordre impair.

Nous avons, dans la première partie, indiqué comment on trouvait alors toutes les partitions de \mathcal{E} en \mathcal{A} telles que $\mathcal{B} = \mathcal{R}(\mathcal{A})$.

L'ensemble des réseaux réciproques définis sur E et associés à P est identique à l'ensemble de tous les & ainsi trouvés.

Donc sur tout ensemble E tel que $\overline{E} = 4n$, (4n + 1) ou ∞ , on peut définir des réseaux réciproques et on peut les trouver tous par un procédé régulier.

5. Pour compléter ces indications, nous allons montrer comment on peut trouver les cycles de 2 connaissant ceux de P.

Soit (a, b) un élément de \mathcal{E} , et soit $\mathcal{C}(a, b)$ le cycle de \mathcal{Z} défini par (a, b); les éléments a et b peuvent appartenir à un même cycle, ou à deux cycles distincts de P.

Donc tout cycle de P est défini, soit à partir d'un seul cycle de P, soit à partir de deux cycles de P.

Premier cas. — Cycles de & désinis à partir d'un seul cycle de P: Soit C un cycle de P.

a. C est infini; soient a_i ses éléments, avec $a_{i+1} = P(a_i)$. Les cycles \mathcal{C} de \mathcal{L} définis à partir de C sont les cycles $\mathcal{C}_k(k=1,2,\ldots)$

$$\mathcal{C}_k = \bigcup_{-\infty < i < \infty} (a_i, a_{i+k}).$$

b. C est fini; soient 4p son ordre et $a_0, a_1, \ldots, a_{4p} \equiv a_0$ ses éléments, avec $a_{(i+1)} = P(a_i)$ (où $[i+1] \equiv (i+1) \mod 4p$).

Les cycles \mathcal{C} de \mathcal{Z} définis à partir de C sont les cycles \mathcal{C}_k $(k=1,2,\ldots,(2p-1))$ d'ordre 4p

$$k = \bigcup_{0 \leq i < k\rho} (a_i, a_{[i+k]}).$$

et le cycle \mathcal{C}_0 d'ordre 2 p

$$\mathcal{C}_0 = \bigcup_{0 \leq i < 2p} (a_i, a_{i+2p}).$$

Il y a donc ici 2p cycles \mathcal{C} attachés à C.

Deuxième cas. — Cycles de \mathfrak{A} définis à partir de deux cycles distincts de P: Soient C_1 et C_2 deux cycles de P.

a. C_1 et C_2 sont fermés; soient n_1 et n_2 leurs ordres respectifs, Δ le p. p. c. m. de n_1 et n_2 et δ leur p. g. c. d.

Les cycles \mathcal{C} de \mathcal{L} définis à partir de C_1 et C_2 sont tous d'ordre Δ et leur nombre est δ .

b. C₁ est d'ordre n fini, C₂ est d'ordre infini.

Les cycles \mathcal{C} de \mathcal{L} définis à partir de C_1 et C_2 sont d'ordre infini et leur nombre est n.

c. C_1 et C_2 sont d'ordre infini; soient (a_i) et (b_i) leurs éléments, rangés dans l'ordre canonique.

Les cycles \mathcal{C} de \mathcal{L} définis à partir de C_1 et C_2 sont d'ordre infini et en infinité dénombrable. Ce sont les cycles \mathcal{C}_k (k entier ≥ 0)

$$\mathcal{C}_k = \bigcup_{-\infty < i < +\infty} (a_i, b_{i+k}).$$

Cas particulier: E est fini. — Désignons par C_i les cycles de la permutation P de E (P satisfaisant aux conditions du théorème 2), et par β_i l'ordre de C_i .

Ce qui précède permet de montrer aisément que le nombre r de cycles de $\mathfrak L$ est donné par

$$r = \sum_{i} \left[\frac{\beta_{i}}{2} \right] + \sum_{i \neq j} \delta_{j,j},$$

en désignant par [x] la partie entière de x et par δ_{ij} le p. g. c. d. de β_i et β_i .

La remarque faite à la fin de la première partie montre alors que le nombre des parties \mathfrak{A} de \mathfrak{E} telles que $\mathfrak{L}(\mathfrak{A}) = \mathfrak{E} - \mathfrak{A}$ est égal à 2^r .

Toutesois ceci ne permet pas de résoudre le problème suivant qui semble difficile :

Trouver le nombre $\varphi(p)$ des réseaux réciproques définis sur un ensemble E de p éléments, en ne considérant pas comme distincts deux réseaux isomorphes [On peut trouver aisément $\varphi(p)$ pour $p \leq 8$: $\varphi(4) = 1$; $\varphi(5) = 2$; $\varphi(8) = 16$].

6. Exemple de Recherche d'un réseau réciproque. — Soit E un ensemble de neuf éléments a_0 , b_1 , b_2 , b_3 , b_4 , c_1 , c_2 , c_3 , c_4 .

Prenons pour P une permutation contenant trois cycles C1, C2, C3

$$C_1 \equiv (a_0);$$
 $C_2 \equiv (b_1, b_2, b_3, b_4);$ $C_3 \equiv (c_1, c_2, c_3, c_4),$

où les éléments sont rangés dans un ordre canonique :

$$\mathfrak{A}$$
 comprend alors r cycles, avec $r=(2+r)+(1+1+4)=10$.

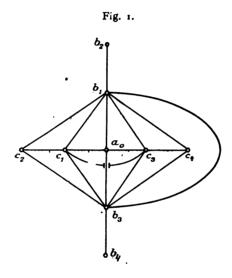
On peut donc définir 2¹⁰ réseaux réciproques à partir de P, mais ils ne sont évidemment pas tous isomorphiquement distincts.

Écrivons les cycles de & en respectant l'ordre canonique

Voici l'un des réseaux réciproques définis sur E et déduit de ce tableau :

$$(b_1b_2), (b_3b_4), (b_1b_3), (c_1c_2), (c_3c_4), (c_1c_3), (a_0b_1), (a_0b_3), (a_0c_1), (a_0c_3), (b_1c_1), (b_3c_3), (b_1c_2), (b_3c_4), (b_1c_3), (b_3c_1), (b_1c_4), (b_3c_2).$$

On peut donner de ce réseau le schéma indiqué dans la figure 1.



III. — Étude de la structure des réseaux réciproques.

- 7. DEFINITIONS. 1° Si α est un réseau défini sur E, on dit que α est connexe si : α . Pour tout- $a \in E$, il y a un élément de α de la forme (a, b); β . Il n'existe aucune partition de α : $\alpha = \alpha_1 + \alpha_2$ avec α_1 . α_2 = 0 telle que si $(a_1b_1) \in \alpha_1$ et $(a_2b_2) \in \alpha_2$, les points a_1 , b_1 , a_2 , b_2 soient toujours distincts deux à deux.
- Un réseau connexe α est dit compact s'il existe un nombre fixe n it tel que, quels que soient $a \in E$ et $b \in E$, il existe un ensemble de p éléments $(p \leq n)$: de $(a_0 a_1)$, de $(a_1 a_2)$, ..., $(a_{p-1} a_p)$, avec $a_0 \equiv a$ et $a_p \equiv b$.

La borne inférieure des nombres n est dite le coefficient de compacité de $\mathfrak A$.

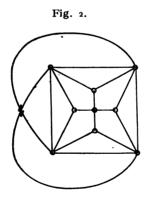
3° Soient α un réseau connexe défini sur E et a un élément de E. Soit $\lambda(a)$ l'ensemble des éléments de α de la forme (a, b).

On dit que a divise α si $(\alpha - \lambda(a))$ n'est pas connexe. On montre aisément les théorèmes suivants :

Théorème 3. — Tout réseau connexe compact possède au moins deux points qui ne le divisent pas. Quand un réseau connexe compact possède seulement deux points qui ne le divisent pas, il est de la forme $(a_0 a_1)$, $(a_1 a_2)$, ..., $(a_{n-1} a_n)$.

Théorème 4. — Tout réseau réciproque est connexe et compact et son coefficient de compacité est au plus égal à 3.

Il existe d'ailleurs des réseaux réciproques de coefficient de compacité égal à 2 (voir le réseau d'ordre 9 de la figure 2). Mais il n'en existe évidemment aucun ayant un coefficient de compacité égal à 1.



8. Étude des réseaux réciproques d'ordre (4n+1). — Pour construire un réseau $\mathfrak A$ d'ordre (4n+1) défini sur E à partir d'une permutation P de E, on fait jouer un rôle privilégié à un élément a_0 de E, qui est l'élément unique d'un des cycles de P.

Il est immédiat qu'en supprimant de α les 2n éléments de la forme (a_0b) , on obtiendrait un réseau réciproque α' défini sur $(E-a_0)$.

Inversement, tout réseau réciproque de 4n éléments est un sousréseau d'au moins un réseau réciproque de (4n + 1) éléments.

On pourra donc, dans beaucoup de cas, se borner à l'étude des réseaux réciproques d'ordre 4n.

9. RECHERCHE DES RÉSEAUX RÉCIPROQUES A IMPASSES. — La figure 1 donne l'exemple d'un réseau réciproque α défini sur un ensemble E, et tel qu'il existe un élément $a \in E$ pour lequel il existe dans α un seul élément de la forme (a, b).

Un tel élément a est dit une impasse du réseau. Indiquons comment on obtient les réseaux réciproques possédant des impasses.

Soit P la permutation de É à partir de laquelle est défini A. On voit aisément que A n'aura des impasses que si tout cycle de P est au plus d'ordre 4.

Plaçons-nous dans ce cas. Soit a_i une impasse de \mathfrak{A} ; il est immédiat que le cycle de P défini par a_i est d'ordre 4. Désignons les divers cycles de P, rangés chacun dans l'ordre canonique par $(a_ib_ic_id_i)$ (où $i=1,2,\ldots,n$), et le cycle éventuel d'ordre 1 par (a_0) .

Tout réseau réciproque admettant a_1 pour impasse se décompose ainsi :

$$\alpha = \alpha_1 + \alpha_2 + \alpha_3$$
.

 α_1 est entièrement déterminé, en voici les éléments :

$$(b_1b_i), (d_1d_i); (b_1c_i), (d_1a_i); (b_1d_i), (d_1b_i); (b_1a_i), (d_1c_i)$$

$$\bullet \quad \text{pour } i = 2, 3, \ldots, n;$$

et éventuellement

$$(a_0b_1), (a_0d_1).$$

 α_2 est une partie composée de, soit

$$(a_1b_1), (c_1d_1), (b_1d_1),$$

soit

$$(a_1d_1), (c_1b_1), (b_1d_1).$$

 α_3 est une partie qui contient uniquement des couples formés avec des éléments a_i d'indice différent de 1.

On voit donc que pour tout nombre p = 4n ou (4n + 1) il existe des réseaux ayant des impasses.

172 G. CHOQUET. — APPLICATION A: LA THÉORIE: DES RÉSEAUX.

On remarque ci-dessus que a_i et c_i jouent exactement le même rôle. D'autre part, pour $i \neq 1$, tout élément de E d'indice i intervient dans α_i et dans α_i .

D'où, en résumé:

Théorème 5. — Tout réseau réciproque contient au plus deux impasses. Lorsqu'il en contient une, il en contient aussi une autre et la permutation de ces deux impasses est une automorphie du réseau.

Pour tout nombre p = 4n ou (4n + 1), il existe des réseaux réciproques d'ordre p ayant deux impasses.