JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

DESPEYROUS

Mémoire sur la théorie générale des permutations

Journal de mathématiques pures et appliquées 2^e série, tome 6 (1861), p. 417-439.
<http://www.numdam.org/item?id=JMPA_1861_2_6__417_0>

MÉMOIRE

SUR

LA THÉORIE GÉNÉRALE DES PERMUTATIONS;

PAR M. DESPEYROUS,

Professeur à la Faculté des Sciences de Dijon.

INTRODUCTION.

Les phénomènes périodiques étant les plus nombreux dans la nature, il doit être intéressant d'étudier *l'ordre périodique indépendamment de toute considération de grandeur* : « théorie, dit Poinsot [*], » neuve et profonde dont les éléments sont à peine connus, mais » qu'on doit regarder comme le premier fondement de l'algèbre et la » source naturelle des principales propriétés des nombres. »

D'ailleurs cette théorie se rattache à d'autres considérations dont nous parlerons dans une autre circonstance, considérations qui simplifieront notablement plusieurs théories importantes et feront naître des résultats nouveaux.

La théorie de l'ordre périodique est une géométrie spéciale qui ne considère que la situation des choses, la disposition des lieux dans l'espace et fait partie de la *géométrie de position* entrevue par Leibniz.

Cette théorie fait retrouver les polygones étoilés [**] de Poinsot et fournit une méthode très-directe pour partager toutes les permutations d'un nombre quelconque de lettres en plusieurs groupes de permutations associées de telle manière, que, malgré tous les échanges qu'on voudrait faire de ces lettres, les permutations d'un même groupe ne puissent jamais se séparer; pour constituer avec ces derniers groupes de permutations d'autres groupes de permutations également insépa-

[*] *Mémoires de l'Institut pour les années* 1813, 1814, 1815, p. 382.

[**] *Journal de l'École Polytechnique*, X^e cahier, p. 16.

rables, et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après *certains* diviseurs du nombre total des permutations.

La même méthode partage les racines de toute *équation abélienne* [*] en plusieurs groupes de racines *inséparables*, quel que soit l'échange que l'on considère, associe ces groupes eux-mêmes en de nouveaux groupes de racines également inséparables, et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après *tous* les diviseurs du degré de l'équation.

Telles sont les deux lois générales de classification que notre travail démontre. Le profond géomètre dont nous avons déjà parlé, Poinsot, avait, dès l'année 1817, entrevu une partie de ces résultats, et avait promis sur cette matière plusieurs Mémoires. Les géomètres regretteront sans doute qu'il n'ait pas réalisé sa promesse : loin de nous la prétention d'y suppléer. Mais nous croyons avoir trouvé deux lois importantes et nous les soumettons au jugement des géomètres.

Le rapprochement de la première de ces deux lois du théorème général de Lagrange relatif au nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme, ce rapprochement, dis-je, fait naître la pensée que cette loi offrira des ressources nouvelles à la solution de cette double question d'abord mise au concours pour le grand prix des sciences mathématiques de l'année 1860 et puis retirée au mois de mars dernier : « 1° Quel est le nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme; 2° comment peut-on former les fonctions primitives pour lesquelles les nombres de valeurs distinctes soient les nombres trouvés. »

C'est effectivement ce que nous démontrerons dans une autre occa-

---

[*] Une équation est dite *abélienne* lorsque ses n racines $x_1, x_2, x_3, \ldots, x_n$ sont telles, que

$$x_2 = \theta(x_1), \quad x_3 = \theta(x_2), \ldots, \quad x_n = \theta(x_{n-1}), \quad x_1 = \theta(x_n),$$

θ désignant une fonction rationnelle.

Cette dénomination tire son nom du célèbre géomètre Abel, qui le premier a étudié cette classe d'équations à laquelle il a été conduit en généralisant une idée de Gauss.

sion. Nous prouverons aussi que la deuxième loi démontrée dans notre Mémoire permet d'établir, en quelques lignes et de la manière la plus simple, les beaux théorèmes de Gauss et d'Abel sur la résolution des équations binômes et en général sur celle des équations abéliennes. Enfin nous ferons connaître les résultats indiqués seulement par Poinsot et les résultats nouveaux que produit l'application de ces deux lois à la théorie générale des équations.

I.

Suites périodiques.

Considérons une suite périodique et indéfinie dans les deux sens

$$(1) \qquad \ldots abc,.. kl,\ abc\ldots kl,\ abc\ldots kl,\ldots$$

dont la période est composée d'un nombre quelconque de lettres marqué par n, a, b, c,..., k, l écrites dans un ordre déterminé, $abc\ldots kl$ par exemple, et examinons, s'il est possible, en prenant les lettres de cette suite par *intervalles constants* à partir de la première a, de déduire de cette suite périodique d'autres suites également périodiques, la période étant composée des *mêmes* lettres, mais dans un ordre différent.

D'abord en prenant les lettres de cette suite (1) successivement, on retrouve cette suite qui satisfait aux conditions énoncées, et si nous les prenons à partir de a de p en p, p étant un sous-multiple de n, $pq = n$, il est clair qu'on ne prendra de chaque période que q lettres, et que par suite on aura une nouvelle suite périodique qui ne satisfera pas aux conditions données, puisque la période se composera seulement de q lettres.

Mais si nous prenons les lettres de la suite (1) à partir de la première a, de p en p, et si p est premier à n, je dis qu'on obtiendra une nouvelle suite satisfaisant à toutes les conditions demandées.

En effet, à partir de la lettre a de l'une quelconque des périodes de la suite (1) prenons, en marchant toujours de gauche à droite, les lettres de cette suite de p en p. Nous retomberons nécessairement sur la lettre a de départ après avoir parcouru p périodes consécutives, puisque p est un sous-multiple du nombre pn de lettres qui entrent dans

ces p périodes consécutives, et par suite nous formerons une nouvelle suite périodique. Il y a plus : nous prendrons les n lettres données avant de retomber pour la première fois sur cette lettre a : car les rangs des lettres d'une période quelconque $abc\ldots kl$ étant respectivement désignés par 0, 1, 2, 3,..., $n-1$, et ceux des lettres des périodes suivantes par n, $n+1$, $n+2$, etc., nous prendrons, en marchant de p en p, les lettres de ces p périodes consécutives dont les rangs sont marqués par les multiples

$$p,\ 2p,\ 3p,\ldots,\ (n-1)p;$$

et par conséquent les lettres de la *première* période dont les rangs sont marqués par les résidus à n de ces mêmes multiples.

Or p étant premier à n, ces $n-1$ résidus sont différents les uns des autres et aucun d'eux n'est nul. Car si l'un quelconque de ces multiples kp, k étant un nombre entier inférieur à n, avait pour résidu à n zéro, kp serait égal à un multiple de n, ce qui est absurde, puisque p est premier à n et k inférieur à n. De même si deux quelconques de ces mêmes multiples kp, $k'p$ avaient leurs résidus à n égaux entre eux, leur différence $(k-k')p$ serait égal à un multiple de n, ce qui ne peut être, puisque p est premier à n et $k-k'$ inférieur à n. Ces $n-1$ résidus étant différents et aucun d'eux ne pouvant être nul, seront égaux, dans un ordre déterminé, aux nombres 1, 2, 3,..., $n-1$. Donc la période de la nouvelle suite formée se compose des n lettres données, et, par suite, en prenant les lettres de la suite (1) de p en p, p étant inférieur et premier à n, on formera une nouvelle suite périodique, la période commençant par a et étant composée des n lettres données. De là ce premier théorème :

THÉORÈME I. — *Si p_1, p_2, p_3,..., p_ν désignent les ν nombres inférieurs et premiers à n, parmi lesquels se trouvent l'unité et $n-1$, on peut, avec n lettres écrites dans un ordre déterminé mais quelconque, former ν [*] suites périodiques, la période de chacune d'elles commençant par la première et composée des mêmes n lettres.*

---

[*] Si $n = a^\alpha b^\beta c^\gamma \ldots k^\delta$, on sait que

$$\nu = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots k^{\delta-1} . (a-1)(b-1)(c-1)\ldots(k-1).$$

Remarque. — Si p_i est premier à n, $n - p_i$ sera aussi premier à n : donc si p_i fournit la période *abl... ch*, $n - p_i$ fournira la période *ahc... lb*. De là il suit que les ν périodes peuvent être partagées en deux groupes composés chacun de $\frac{\nu}{2}$ périodes telles, que chaque période appartenant à l'un des groupes ne soit autre que l'une des périodes de l'autre groupe lue à l'envers.

Premier exemple : $n = 4$, auquel cas $\nu = 2$, $p_1 = 1$, $p_2 = 3$. Donc la disposition *abcd* produira les deux suites périodiques

$$...abcd,\ abcd,\ abcd,...$$
$$...adcb,\ adcb,\ adcb,...$$

Second exemple : Pour $n = 5$, on aura $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 4$, $\nu = 4$, et par suite les quatre suites relatives à la disposition *abcde* :

$$...abcde,\ abcde,\ abcde,...$$
$$...acebd,\ acebd,\ acebd,...$$
$$...adbec,\ adbec,\ adbec,...$$
$$...aedcb,\ aedcb,\ aedcb,...$$

Ces deux exemples suffisent pour les applications de ce premier théorème.

THÉORÈME II. — *Le nombre de suites périodiques qu'on peut former par la loi précédente avec n lettres écrites dans tel ordre qu'on voudra, les périodes étant composées de ces lettres et commençant toutes par la première, est égal au nombre ν qui marque combien il y a de nombres inférieurs et premiers à ce nombre de lettres.*

En effet, le premier théorème démontre qu'on peut en former ν, il suffit donc de prouver qu'il n'y en a pas d'autres.

D'abord si nous répétons indéfiniment la permutation donnée qu'offrent ces n lettres, nous aurons une première suite périodique satisfaisant aux conditions énoncées. Mais l'intervalle constant p, par lequel on doit sauter d'une lettre à une autre, pour déduire de cette suite une nouvelle satisfaisant aux mêmes conditions, devant être inférieur à n, il ne pourra arriver que trois cas :

1° Cet intervalle constant p est un sous-multiple de n, et alors la suite périodique, déduite de la suite donnée (1), ne remplira pas les conditions énoncées.

2° Cet intervalle constant p est premier à n, et alors la suite obtenue satisfera aux conditions prescrites.

3° Enfin cet intervalle constant p aura avec n un plus grand commun diviseur θ, et alors si l'on pose

$$p = p'\theta, \quad n = n'\theta,$$

p' et n' seront premiers entre eux. Or si l'on prend les lettres de la suite (1) de θ en θ à partir de la première a, nous obtiendrons une nouvelle suite périodique dont la période commencera par a et sera formée de n' lettres seulement; et si dans cette nouvelle suite nous prenons les lettres à partir de a de p' en p', nous obtiendrons, p' étant premier à n', une troisième suite périodique dont la période commencera par a et sera formée de n' lettres. Mais prendre dans la suite (1) les lettres à partir de a, d'abord de θ en θ et puis de p' en p' dans le résultat obtenu, c'est évidemment prendre dans la suite (1) les lettres à partir de a de $\theta p'$ en $\theta p'$, c'est-à-dire de p en p, et comme cette troisième suite ne contient que n' des n lettres données, elle ne satisfait pas aux conditions énoncées.

Il n'y a donc qu'une seule manière de déduire, par intervalle constant, d'une suite périodique donnée une nouvelle suite périodique dont la période commence par la même lettre que dans la période donnée et soit formée des mêmes lettres. Cette manière consite à prendre pour intervalle constant un nombre quelconque inférieur et premier au nombre de lettres données, ce qui, d'après le premier théorème, démontre le second.

Corollaire I. — Il résulte évidemment de là que les ν suites dont il est question dans le premier théorème sont *rentrantes* sur elles-mêmes; c'est-à-dire que, l'une d'elles étant donnée, on en déduira, par le procédé de l'intervalle constant, les mêmes ν suites.

Considérons en effet l'une d'elles, celle qui est produite par le

nombre p_i par exemple, et marchons dans cette suite de p_h en p_h. Marcher dans la suite (1) d'abord de p_i en p_i et puis dans la suite produite de p_h en p_h, c'est évidemment marcher dans la suite (1) de $p_i.p_h$ en $p_i.p_h$ Or n étant premier à p_i et à p_h sera premier à leur produit $p_i.p_h$ et le résidu à n de $p_i.p_h$ sera aussi premier à n; donc ce résidu sera l'un des ν nombres $p_1, p_2, \ldots, p_\nu$, et par conséquent la suite ainsi obtenue coïncidera avec l'une des ν suites du premier théorème.

Corollaire II. — Si n a des racines *primitives*, c'est-à-dire si n est égal à un nombre premier quelconque supérieur à 2, ou à une puissance d'un nombre premier (excepté si $n = 2^\alpha$ et $\alpha > 2$), ou enfin au double d'un nombre premier élevé à un puissance quelconque, on peut obtenir les ν suites du premier théorème en sautant toujours d'un *même* intervalle.

Soit en effet ρ l'une des racines primitives de n, les résidus à n de la suite des puissances

$$\rho, \rho^2, \rho^3, \ldots, \rho^\nu$$

seront tous différents et ne seront autres que les ν nombres inférieurs et premiers à n. Si donc, ayant d'abord écrit les n lettres données dans un ordre quelconque, on prend ces lettres de ρ en ρ à partir de la première écrite, on aura, en écrivant le résultat indéfiniment, une première suite satisfaisant aux conditions requises, puisque ρ est premier à n. Et si sur cette suite on prend encore les lettres à partir de la première de ρ en ρ, ce qui revient évidemment à prendre les lettres de la suite donnée de ρ^2 en ρ^2 si $\rho^2 < n$ ou de p_i en p_i si $\rho^2 > n$, p_i étant le résidu à n de ρ^2, on aura une deuxième suite périodique ayant les conditions énoncées. De même en prenant sur cette dernière suite et à partir de la première les lettres de ρ en ρ, on aura une nouvelle suite et ainsi indéfiniment. Donc, d'après le deuxième théorème, on formera ainsi les ν suites du premier.

Polygones étoilés — Plaçons sur une circonférence de rayon quelconque et d'une manière régulière ou irrégulière les n lettres données $a, b, c, \ldots, k, l$ qui forment la période de la suite (1), et traçons le polygone régulier ou irrégulier de n côtés $abc\ldots kl$. Il est clair que ce po-

lygone lu un nombre indéfini de fois dans le même sens sera une représentation géométrique très-exacte de cette suite (1).

Généralement, si p_i est un nombre inférieur et premier à n et si à partir du point a on joint ces n points $a, b, c, \ldots, k, l$ de p_i en p_i, le nouveau polygone de n côtés obtenu, lu indéfiniment dans le même sens, représentera celle des ν suites du premier théorème relative à ce nombre p_i.

Il faut remarquer que puisque p_i périodes consécutives de la suite (1) sont nécessaires pour former la période de la suite relative à p_i, le polygone de n côtés qui remplace cette suite s'obtiendra en partant du point a et faisant p_i fois le tour de la circonférence.

De là et des théorèmes I et II, ce théorème dû à Poinsot :

THÉORÈME III. — *Avec n points régulièrement ou irrégulièrement espacés sur une circonférence, on ne peut former qu'un nombre ν de polygones réguliers ou irréguliers de n côtés marqué par le nombre qui exprime combien il y a de nombres inférieurs et premiers à ce nombre n de points donnés.*

Corollaire. — La remarque du premier théorème démontre qu'il y a $\frac{\nu}{2}$ polygones qu'on obtient en marchant dans un sens sur la circonférence et $\frac{\nu}{2}$ autres qui ne sont autres que les $\frac{\nu}{2}$ premiers lus en sens inverse.

Remarque. — A peine est-il besoin d'ajouter que les n points donnés auraient pu être portés sur toute autre courbe fermée que la circonférence de cercle : mais alors il faudrait effacer en général le mot *régulier.*

Note. — Le profond géomètre dont il est ici question a déduit de son théorème plusieurs conséquences remarquables : on les trouvera dans le Mémoire déjà cité du *Journal de l'Ecole Polytechnique* et dans le tome X du *Journal de Mathématiques* publié par M. Liouville.

Nous terminerons cette première section par un *nouveau* théorème qui nous sera utile dans la recherche des équations solubles par radicaux.

THÉORÈME IV. — *Si ρ est une des racines primitives du nombre entier n, et si p_i est un des ν nombres inférieurs et premiers à n, les ν permutations produites par les ν polygones de Poinsot des n choses x, x_{p_i}, x_{2p_i}, x_{3p_i},... , $x_{(n-1)p_i}$ considérées dans cet ordre, sont*

$$\begin{aligned}
&x\ x_{p_i}\ x_{2p_i}\ x_{3p_i}\cdots\ x_{(n-1)p_i},\\
&x\ x_{p_i\rho}\ x_{2p_i\rho}\ x_{3p_i\rho}\cdots\ x_{(n-1)p_i\rho},\\
&x\ x_{p_i\rho^2}\ x_{2p_i\rho^2}\ x_{3p_i\rho^2}\cdots\ x_{(n-1)p_i\rho^2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&x\ x_{p_i\rho^{\nu-1}}\ x_{2p_i\rho^{\nu-1}}\cdots\ x_{(n-1)p_i\rho^{\nu-1}},
\end{aligned}$$

les indices de x étant pris suivant le module n.

En effet, p_i étant premier à n et ρ étant une racine primitive de ce nombre n, aucun des indices de x, $p_i\rho^h$, $2p_i\rho^h$, $3p_i\rho^h$,..., $(n-1)p_i\rho^h$ relatifs à une quelconque de ces permutations ne sera divisible par n, et de plus je dis que les $n-1$ restes obtenus seront différents. Car si, chacun des nombres k, k' étant inférieur à n, les restes ou résidus à n de $kp_i\rho^h$ et de $k'p_i\rho^h$ pouvaient être égaux, la différence $k'p_i\rho^h - kp_i\rho^h$ serait un multiple de n. On aurait donc, M désignant un nombre entier quelconque,

$$(k'-k)p_i\rho^h = \mathrm{M}.n.$$

Or n divisant le second membre de cette égalité doit diviser le premier; mais n étant premier à p_i et à ρ, sera premier au produit $p_i\rho^h$; donc n devrait diviser le facteur $k'-k$, ce qui est impossible, puisque chacun des nombres k, k' est inférieur à ce nombre n.

1° Donc les résidus à n de tous les indices des termes d'une quelconque des lignes précédentes sont tous différents, et par suite ces résidus ne peuvent être que 1, 2, 3,..., $n-1$ dans tel ou tel ordre.

Les résidus à n des indices des seconds termes dans chacune de ces permutations p_i, $p_i\rho$, $p_i\rho^2$,..., $p_i\rho^{\nu-1}$ sont différents aussi, et chacun d'eux est premier à n. Car si les résidus à n de $p_i\rho^k$ et de $p_i\rho^{k+k'}$ étaient égaux, chacun des exposants de ρ, k et $k+k'$, étant inférieur à ν, la

différence $p_i \rho^{k+k'} - p_i \rho^k$ serait un multiple de n, et on aurait

$$p_i \rho^k (\rho^{k'} - 1) = \mathrm{M}.n.$$

Or n divisant le second membre de cette égalité doit diviser le premier; mais n est premier au produit $p_i \rho^k$; donc n devrait diviser $\rho^{k'} - 1$, ce qui est impossible, puisque k' est inférieur à ν [*].

Je dis de plus que chacun de ces résidus est premier à n; car l'équation

$$p_i \rho^k = \mathrm{M}.n + r$$

prouve que si r et n n'étaient pas premiers entre eux, un quelconque de leurs facteurs premiers communs, α par exemple, divisant le second membre de cette égalité, devrait diviser le premier; et par conséquent diviser ou p_i ou ρ^k. Or α ne peut diviser p_i, car autrement n et p_i ne seraient pas premiers entre eux; ce facteur α ne saurait non plus diviser ρ^k, car, si cela était, α diviserait ρ; et par suite ρ et n ne seraient pas premiers entre eux, ce qui ne peut être, puisque ρ est racine primitive de n.

2° Donc les résidus à n de p_i, $p_i \rho$, $p_i \rho^2$,..., $p_i \rho^{\nu-1}$ sont tous différents et chacun d'eux est premier à n. Ces deux résultats démontrent évidemment le théorème énoncé.

Remarque. — Les ν permutations de ce théorème forment une suite *rentrante* sur elle-même. Car la permutation suivante serait

$$x \; x_{p_i \rho^\nu} \; x_{2p_i \rho^\nu} \cdots \; x_{(n-1)p_i \rho^\nu},$$

qui n'est autre que la première. Car, en vertu du théorème de Fermat généralisé par Euler, on a

$$\rho^\nu = 1 + \mathrm{M}.n$$

---

[*] On sait que ρ étant racine *primitive* de n, la plus petite puissance de ρ qui soit telle, que $\rho^{k'} - 1$ soit divisible par n, est le nombre ν qui marque combien il y a de nombres inférieurs et premiers à n.

et par suite

$$kp_i\rho^{\nu} \equiv kp_i \pmod{n}.$$

Ces polygones étoilés jouissent de plusieurs autres propriétés; mais elles trouveront mieux leur place dans la recherche du nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme; ce qui précède suffit pour l'intelligence de la classification des permutations qu'offrent n lettres.

II.

Classification des permutations d'un nombre quelconque de lettres.

Loi de formation du premier tableau. — Soient a, b, c,..., k, l les lettres que l'on considère en nombre quelconque n; le nombre de permutations qu'elles produisent est égal au produit $1.2.3...(n-1).n$.

Parmi ces permutations, prenons toutes celles qui commencent par une même lettre, a par exemple. Pour les obtenir, il suffira de permuter les $n-1$ autres lettres b, c,..., k, l et d'écrire au commencement de chacune d'elles cette lettre a. Le nombre de ces permutations ainsi obtenues sera égal au produit $1.2.3...(n-1)$, et elles constituent la *première classe*. Considérons l'une d'elles, $abc...kl$ par exemple, et joignons à cette permutation toutes celles qui sont relatives aux polygones de Poinsot, c'est-à-dire toutes celles qu'on déduit de cette permutation en prenant successivement les lettres, à partir de la première, de p_1 en p_1, de p_2 en p_2, etc., et de p_ν en p_ν, p_1, p_2,..., p_ν étant les ν nombres inférieurs et premiers à n. On obtiendra ainsi un premier groupe de ν permutations, la première comprise,

$$abc...kl,\ adh...ig,\ ....$$

Supprimons ces ν permutations dans cette première classe et prenons parmi celles qui restent une permutation quelconque, $ahg...ci$ par exemple. Nous ferons sur elle ce que nous avons fait sur la première $abc...kl$, c'est-à-dire que nous prendrons successivement les lettres de cette nouvelle permutation, à partir de la première a, de p_1 en p_1, de p_2 en p_2, etc., et de p_ν en p_ν, et nous obtiendrons ainsi un deuxième

groupe de ν permutations

$$ahg\ldots ci,\ af l\ldots he,\ \ldots.$$

Otons encore ces ν nouvelles permutations de toutes celles que nous avions après la première suppression ; prenons parmi celles qui restent une permutation quelconque, *ald... ef* par exemple, et faisons sur elle ce que nous avons fait sur chacune des deux premières ; nous obtiendrons ainsi un troisième groupe de ν permutations

$$ald\ldots ef,\ a\ldots,\ \ldots,$$

et continuons ainsi cette même opération jusqu'à l'entier épuisement des $1.2.3\ldots(n-1)$ permutations de la première classe qui toutes commencent par la même lettre a. Cela sera toujours possible, puisque chaque permutation produit ν permutations seulement et que ν est un diviseur de ce produit $1.2.3\ldots(n-1)$.

Cette première classe de permutations sera donc décomposée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes formés chacun de ν permutations, ainsi qu'il suit :

$$1^{re}\text{ classe.}\begin{cases} abc\ldots kl,\ adh\ldots ig,\ldots, \\ ahg\ldots ci,\ af l\ldots he,\ldots, \\ ald\ldots ef,\ a\ldots,\quad \ldots, \\ \ldots\ldots\ldots\ldots\ldots \end{cases}$$

On pourrait actuellement prendre les $1.2.3\ldots(n-1)$ permutations des n lettres données qui commencent toutes par une autre lettre, b par exemple, et établir avec elles la même classification qu'on vient de faire sur celles de la première classe. Mais on arrivera évidemment au même résultat, et d'une manière plus simple, si l'on écrit les permutations de cette première classe ligne par ligne et dans le même ordre, en commençant chacune d'elles par cette lettre b et en marchant toujours dans le même sens, de gauche à droite, chaque permutation étant supposée écrite deux fois.

On aura ainsi la deuxième classe de permutations, commençant

toutes par la lettre b, partagée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes composés chacun de ν permutations relatives aux ν polygones de Poinsot :

$$2^{e}\text{ classe.}\begin{cases} b\ldots,\ b\ldots,\ \ldots, \\ b\ldots,\ b\ldots,\ \ldots, \\ \ldots\ldots\ldots\ldots \end{cases}$$

De même si l'on écrit les permutations de la première classe, ligne par ligne et dans le même ordre, en commençant chacune d'elles par la lettre c et en marchant toujours de gauche à droite, chaque permutation étant supposée écrite deux fois, on aura une troisième classe de $1.2.3\ldots(n-1)$ permutations commençant toutes par cette lettre c partagée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes composés chacun de ν permutations relatives aux polygones de Poinsot.

En continuant cette même opération jusqu'à l'entier épuisement des n lettres données, toutes les permutations de ces lettres seront distribuées en n classes, et chaque classe en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes formés chacun de ν permutations. Telle est la loi de formation du premier tableau.

Premier tableau.

$$1^{re}\text{ classe.}\begin{cases} abc\ldots kl,\ adh\ldots ig,\ \ldots, \\ ahg\ldots ci,\ afl\ldots he,\ \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

$$2^{e}\text{ classe.}\begin{cases} bc\ldots,\ b\ldots,\ \ldots, \\ b\ldots,\ b\ldots,\ \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$n^{ième}\text{ classe.}\begin{cases} l\ldots,\ l\ldots,\ \ldots, \\ l\ldots.\ l\ldots,\ \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Loi de formation du second tableau. — Prenons les premiers groupes de chacune des n classes du tableau précédent et formons un groupe de ces $n\nu$ permutations

$$abc\ldots kl,\ adh\ldots ig,\ \ldots,\ l\ldots,\ l\ldots,\ \ldots.$$

Prenons de même les seconds groupes de chacune des n classes du même tableau et formons un nouveau groupe de ces $n\nu$ permutations

$$ahg\ldots ci,\ afl\ldots he,\ \ldots,\ l\ldots,\ l\ldots,\ \ldots.$$

Prenons encore les troisièmes groupes de chacune des mêmes classes; nous en formerons un troisième groupe de $n\nu$ permutations, et continuons cette même série d'opérations jusqu'à ce qu'on ait épuisé les groupes de chaque classe. Nous obtiendrons ainsi un second tableau :

Second tableau.

$$abc\ldots kl,\ adh\ldots ig,\ldots,\ l\ldots,\ l\ldots,\ \ldots,$$
$$ahg\ldots,\ ci,\ afl\ldots he,\ldots,\ l\ldots,\ l\ldots,\ \ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

composé d'un nombre de groupes marqué par la formule

$$\frac{1\ 2.3\ldots(n-1)}{\nu},$$

formés chacun de $n\nu$ permutations assujetties à la même loi, savoir : de ν permutations relatives aux polygones de Poinsot sur un ordre quelconque des n lettres données, et des $(n-1)\nu$ permutations qu'on déduit de cet ordre en le lisant successivement à partir des lettres b, $c,\ldots, l$.

Prenons pour premier exemple $n=4$, auquel cas $\nu=2$ et $p_1=1$, $p_2=3$; le premier tableau sera :

CLASSE.	ORDRE.	PERMUTATIONS.
1	1	*abcd*, *adcb*
	2	*abdc*, *acdb*
	3	*adbc*, *acbd*
2	4	*bcda*, *badc*
	5	*bdca*, *bacd*
	6	*bcad*, *bdac*
3	7	*cdab*, *cbad*
	8	*cabd*, *cdba*
	9	*cadb*, *cbda*
4	10	*dabc*, *dcba*
	11	*dcab*, *dbac*
	12	*dbca*, *dacb*

Le second tableau relatif à ces quatre lettres sera, en désignant par les numéros d'ordre les permutations qui composent les divers groupes dont il se forme :

ORDRE.	PERMUTATIONS.
1	1, 4, 7, 10
2	2, 5, 8, 11
3	3, 6, 9, 12

Dans cette hypothèse en effet

$$\frac{1.2.3\ldots(n-1)}{\nu} = 3.$$

Prenons pour second et dernier exemple $n = 5$, auquel cas

$\nu = 4$, $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 4$ et $\frac{1.2.3\ldots(n-1)}{\nu} = 6$:

le premier tableau sera :

CLASSE.	ORDRE.	PERMUTATIONS.
1	1	*abcde*, *acebd*, *adbec*, *aedcb*,
	2	*abced*, *acdbe*, *aebdc*, *adecb*,
	3	*abecd*, *aedbc*, *acbde*, *adceb*,
	4	*aebcd*, *abdec*, *acedb*, *adcbe*,
	5	*abdce*, *adebc*, *acbed*, *aecdb*,
	6	*adbce*, *abedc*, *acdeb*, *aecbd*,
2	7	*bcdea*, *bdace*, *becad*, *baedc*,
	8	*bceda*, *beacd*, *bdcae*, *badec*,
	..	.....
3	13	*cdeab*, *cebda*, *cadbe*, *cbaed*,
	...	.....
4	19	*deabc*, *daceb*, *dbeca*, *dcbae*,
	...	.....
5	25	*eabcd*, *ebdac*, *ecadb*, *edcba*,
	...	.....

Le second tableau sera, d'après la notation déjà adoptée :

ORDRE.	PERMUTATIONS.
1	1, 7, 13, 19, 25
2	2, 8, 14, 20, 26
3	3, 9, 15, 21, 27
4	4, 10, 16, 22, 28
5	5, 11, 17, 23, 29
6	6, 12, 18, 24, 30

Propriétés générales des groupes et des classes des deux tableaux précédents.

THÉORÈME V. — *Les permutations d'un quelconque des groupes du premier tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des n lettres qui les forment, elles ne se séparent jamais.*

En effet, plaçons sur une circonférence de rayon arbitraire et à égales distances les unes des autres les n lettres données dans l'ordre qui produit la première des permutations du premier groupe, et formons les ν polygones réguliers relatifs aux ν permutations de ce groupe. Le premier polygone s'obtient en joignant les n points désignés par ces lettres un à un, ce qui exige qu'on parcoure une seule fois la circonférence considérée.

Généralement le polygone relatif au nombre inférieur et premier à n, p_i, s'obtient en joignant les mêmes points de p_i en p_i, à partir du point considéré comme origine, ce qui exige qu'on parcoure cette même circonférence p_i fois. Mais, *la théorie de l'ordre étant indépendante de la notion de grandeur,* ce même polygone peut être obtenu en parcourant une *seule* fois une circonférence p_i fois plus grande et en prenant sur elle n points à égale distance les uns des autres, comme pour le premier polygone. Et comme ce résultat est vrai pour toutes les valeurs de p_i, p_1, p_2, p_3,..., p_ν, il s'ensuit que les ν polygones réguliers relatifs au premier groupe du premier tableau ne sont autre chose qu'*un seul et même polygone,* qu'*un seul et même ordre.* Rien ne distingue donc une permutation quelconque de ce groupe d'une autre du même groupe.

Si donc par un échange quelconque de lettres une des permutations de l'un des groupes de ce tableau se change en une autre du même groupe, cet échange ne fera pas sortir de l'*ordre* de ce groupe, et, par suite, toutes les ν permutations de ce groupe ne feront que s'échanger entre elles, que se déplacer.

Si au contraire un échange quelconque de lettres transformait une des permutations de l'un des groupes du premier tableau en une autre

appartenant à un groupe différent, cet échange ferait passer de l'*ordre* relatif à ce premier groupe à l'*ordre* relatif à ce dernier, et dès lors toutes les permutations de ce premier groupe se changeraient en toutes celles du second. Donc, etc.

THÉORÈME VI. — *Les permutations d'une quelconque des classes du premier tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des n lettres qui les forment, elles ne peuvent jamais se séparer.*

Il résulte en effet de la loi de formation du premier tableau et de ce qui vient d'être dit dans la démonstration du théorème précédent, que les permutations de la deuxième classe ayant été obtenues en lisant celles de la première à partir de la lettre b, ces permutations ne sont autre chose que *les divers ordres de cette première classe vus d'un autre point*. De même les permutations de la troisième classe ayant été obtenues en lisant celles de la première à partir de la lettre suivante c, ces permutations ne sont autre chose que les *divers ordres* de cette première classe vus d'un nouveau point; et ainsi de suite pour les autres classes.

Il suit de là que si un échange de lettres données transforme une permutation d'une des n classes du premier tableau en une autre permutation de la même classe, cet échange ne fera pas sortir du point de vue de cette classe, et que, par suite, les autres permutations de la même classe ne feront que se déplacer par cet échange.

Si, au contraire, un échange des lettres données transformait une des permutations d'une des classes du même tableau en une des permutations d'une autre classe, cet échange ferait passer des divers ordres du point de vue relatif à cette première classe aux divers ordres du point de vue relatif à la seconde, et dès lors toutes les permutations de cette première classe se changeraient en celles de la seconde par suite de cet échange.

THÉORÈME VII. — *Les permutations d'un quelconque des groupes du second tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des n lettres qui les forment, elles ne peuvent jamais se séparer.*

En effet, d'après la loi de formation de ces groupes et d'après la démonstration du théorème V, il résulte que l'un quelconque de ces groupes constitue *un seul et même ordre* vu de chacun des n points a, b,..., k, l. On peut donc appliquer aux groupes de ce second tableau le même raisonnement que celui qu'on vient d'appliquer aux groupes et aux classes du premier. Le théorème VII est donc démontré.

III.

Examen d'un cas particulier.

Décomposer les permutations de n lettres en plusieurs groupes de permutations *inséparables* quel que soit l'échange de ces lettres, est une idée qui trouve des applications dans la théorie des nombres et dans la théorie générale des équations. C'est même en vue de cette dernière que nous examinerons spécialement le cas où ces n lettres ou choses sont représentées par les n quantités suivantes

$$(1) \qquad x \quad \theta x \quad \theta^2 x \quad \theta^3 x \ldots \quad \theta^{n-1} x,$$

dans lesquelles x désigne l'une quelconque de ces n lettres et θx une fonction arbitraire de x telle, que $\theta^n x = x$: la notation $\theta^2 x$, $\theta^3 x$,..., $\theta^n x$ indiquant qu'il faut répéter deux fois, trois fois,..., n fois les opérations désignées par cette fonction.

Cela posé, nous démontrerons le théorème suivant :

THÉORÈME VIII. — *Cette suite de n fonctions peut être partagée en plusieurs groupes de fonctions* inséparables *quel que soit l'échange des fonctions données : ces groupes eux-mêmes se subdivisent en d'autres groupes de fonctions* inséparables *par l'échange de ces mêmes fonctions; et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après* tous *les diviseurs de ce nombre n.*

En effet, supposons d'abord $n = \alpha q$. Cette hypothèse permet d'écrire la suite (1) de la manière suivante

$$(2) \qquad x \quad \theta^1(x) \quad \theta^2 x \ldots \quad \theta^{q-1} x \quad \theta^q x \ldots \quad \theta^{2q} x \ldots \quad \theta^{\alpha q-1} x.$$

Actuellement prenons ces fonctions de q en q et successivement à partir de x, θx, $\theta^2 x$,..., $\theta^{q-1} x$, on obtiendra les q groupes suivants composés chacun de α termes :

$$(A)\qquad \left\{\begin{array}{llll} x & \theta^q x & \theta^{2q} x \ldots & \theta^{(\alpha-1)q}(x), \\ \theta x & \theta^{1+q} x & \theta^{1+2q} x & \theta^{1+(\alpha-1)q} x, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\ \theta^{q-1} x & \theta^{q-1+q} x & \theta^{q-1+2q} x \ldots & \theta^{q-1+(\alpha-1)q} x. \end{array}\right.$$

Ces q groupes contiennent évidemment les n fonctions de la suite (2) et chacun d'eux est une suite *rentrante* sur elle-même. Ainsi, par exemple, le terme qui suivrait le dernier terme du premier groupe serait $\theta^{\alpha q} x$ ou $\theta^n x$ et $\theta^n x = x$; de même le terme qui suivrait le dernier terme du second groupe serait $\theta^{1+q\alpha} x$ ou $\theta^{1+n} x$; or $\theta^{1+n} x = \theta x$, puisque $\theta^n x = x$; et ainsi de suite pour les autres groupes.

Or si dans l'un de ces groupes, dans le premier par exemple, on change x en $\theta^q x$, le premier terme de ce groupe se change en le second, le second en le troisième, et ainsi de suite, le dernier en le premier ; donc les termes de ce groupe ne font que s'échanger entre eux.

Cet échange produira évidemment le même résultat dans chacun des autres groupes. Il en serait de même si x se changeait en $\theta^{kq} x$, k étant un nombre entier quelconque inférieur à α.

Mais si l'on change x en $\theta^2 x$ par exemple, on voit que tous les termes du premier groupe se changent respectivement en ceux du troisième, et qu'ainsi le premier groupe tout entier se substitue au troisième. De même, par cet échange, le second groupe se substitue tout entier au quatrième, et ainsi de suite pour les autres.

Généralement, si l'on change x en $\theta^h x$, h étant plus petit que α, il est clair que chacun de ces groupes se substitue tout entier à l'un des groupes du système.

Donc : 1° Si $n = \alpha q$, les termes de la suite (2) peuvent être partagés en q groupes *inséparables* composés chacun de α termes.

Soit de nouveau $q = q' \beta$, auquel cas $n = \alpha \beta q'$.

Si dans le groupe premier du tableau précédent (A) on change x en θx, on obtient le second. La même transposition change le deuxième

groupe en le troisième, le troisième en le quatrième, etc., et enfin le dernier en le premier. Donc si nous désignons le premier groupe de ce tableau par $F(x)$, les suivants seront successivement désignés par

$$F(\theta x),\ F(\theta^2 x),\ldots,\ F(\theta^{q-1} x)$$

et la suite

$$F(x),\ F(\theta x),\ F(\theta^2 x),\ldots,\ F(\theta^{q-1} x) \tag{3}$$

sera analogue à la suite (2) et comme elle rentrante sur elle-même. Et puisque $q = q'\beta$, on pourra faire sur celle-ci ce qui a été fait sur la première. Donc cette suite (3), et par suite la suite (2), pourra être partagée en q' groupes de termes *inséparables*, quel que soit l'échange des n quantités de la suite (1). Chacun de ces nouveaux groupes sera formé de β termes de la suite (3) et par conséquent de $\alpha\beta$ termes de la suite (2).

A nouveau, si l'on suppose encore $q' = q''\gamma$, auquel cas $n = \alpha\beta\gamma q''$, on pourra décomposer les q' groupes de termes obtenus et par conséquent les termes de la suite (2) en q'' groupes de termes inséparables, et ainsi de suite.

Comme aussi, en supposant le produit $\alpha\beta\gamma$ effectué, on pourra, d'après le 1°, partager les termes de la suite (2) en q'' groupes de termes inséparables composés chacun de $\alpha\beta\gamma$ termes, ou en $\gamma q''$ groupes de termes inséparables composés chacun de $\alpha\beta$ termes, et ainsi de suite pour tous les diviseurs de n.

Le théorème énoncé est donc démontré.

Remarque I. — Si l'on continue de désigner par $p_1, p_2, p_3, \ldots p_\nu$ les ν nombres inférieurs et premiers à n, on ne peut déduire de la suite (2) que ν suites composées chacune de tous les termes de cette suite, mais dans un ordre différent, en prenant successivement ces termes à partir du premier x de p_1 en p_1, de p_2 en p_2, etc., de p_ν en p_ν.

Or nous avons démontré dans la deuxième section que ces ν suites n'étaient autre chose qu'*un seul et même ordre;* donc, en faisant sur chacune d'elles les mêmes opérations qui ont été faites sur la suite (2), on obtiendra exactement les *mêmes* groupes inséparables.

Cette remarque peut être facilement vérifiée sur une valeur particulière, d'ailleurs quelconque, de n.

Remarque II. — Ce théorème VIII fait retrouver, de la manière la plus simple et la plus élémentaire, comme nous le démontrerons bientôt, tout ce que l'on sait sur les équations binômes et plus généralement sur les équations *abéliennes*.

Addition à la deuxième section.

Les deux tableaux de permutations relatifs aux cas où $n = 4$ peuvent être suivis d'un troisième jouissant de propriétés analogues.

Si l'on désigne en effet les groupes du premier tableau par les numéros d'ordre qui leur correspondent, le tableau suivant :

Nos d'ordre.	permutations.
1	1, 7
2	2, 11
3	3, 6
4	4, 10
5	5, 8
6	9, 12

formé de six groupes de permutations composés chacun de quatre permutations, se déduit du premier tableau en joignant à chacun de ses groupes celui qu'on obtient en échangeant 1° les lettres qui occupent la première et la troisième place, 2° celles qui occupent la deuxième et la quatrième.

On constate aisément que les groupes de ce dernier sont également inséparables.

Nous devons encore ajouter que les deux tableaux de permutations

relatifs au cas de trois lettres a, b, c se réduisent en un seul

$$abc,\ acb,$$
$$bca,\ bac,$$
$$cab,\ cba,$$

mais qu'elles produisent un nouveau tableau de deux groupes de permutations *inséparables* formés chacun de trois permutations

$$abc,\ bca,\ cab,$$
$$acb,\ bac,\ cba,$$

propriété facile à être vérifiée.