Sur la transitivité et la primitivité des groupes de substitutions.

Autor(en): **Bays, S.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **22 (1949)**

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-19187

Sur la transitivité et la primitivité des groupes de substitutions[1)]

Par S. Bays, Fribourg

Introduction

Ce travail est le développement d'une communication présentée à la Société mathématique suisse (réunion de Sils, 1944) et parue en résumé dans les Actes de la S.H.S.N., 1944, p. 82. Jusqu'ici on a toujours envisagé la transitivité et l'intransitivité dans les groupes de substitutions non seulement par rapport aux éléments, mais aussi par rapport aux couples, aux triples, ou d'une façon générale, par rapport aux *i-uples* des éléments. Par contre la primitivité et l'imprimitivité des mêmes groupes n'ont jamais été considérées que par rapport aux *éléments*. Il nous a paru que cette restriction n'avait pas sa raison d'être et qu'il y avait un intérêt à chercher si la primitivité et l'imprimitivité avaient un sens aussi par rapport aux couples, aux triples, etc., des éléments ou des variables du groupe. Dans ce travail nous nous limitons au cas de la primitivité ou de l'imprimitivité par rapport aux *couples*.

§ 1. Les groupes de substitutions transitifs et intransitifs

Soit un groupe de substitutions ou de permutations G. Nous appellerons indifféremment éléments ou variables les n objets soumis aux permutations de G et nous les noterons respectivement $0, 1, 2, \ldots, n-1$ ou $x_1, x_2, \ldots, x_n$. Sur la simple notion de *groupe* de *substitutions* on établit les faits suivants :

[1)] C'est l'appellation française et celle de *Netto* (Gruppen und Substitutionentheorie, Sam. Schubert LV et Substitutionentheorie und ihre Anwendungen auf die Algebra, Leipzig, Teubner, 1882). *Speiser* (Die Theorie der Gruppen von endlicher Ordnung, Berlin, Springer, 1923) les appelle groupes de permutations, réservant le mot de substitutions aux groupes des substitutions linéaires. Nous emploierons indifféremment les deux termes.

I. Fixons l'une des variables du groupe G, soit x_1[2]). Cette variable x_1 par les permutations de G est changée en elle-même d'abord, puisque le groupe contient l'identité, et en un certain nombre d'autres variables, soit $x_2, \ldots, x_r$. Je prétends d'abord que cet ensemble $x_1, x_2, \ldots, x_r$ par les substitutions de G est *fermé*, c'est-à-dire que les substitutions du groupe G ne peuvent qu'échanger entre elles les variables de cet ensemble. En effet, admettons que la permutation S, appartenant à G, change x_i en x_k, où i est l'un des indices $1, 2, \ldots, r$. Soit T une permutation de G qui change x_1 en x_i ; une telle permutation existe d'après l'hypothèse. Par suite la permutation TS, qui appartient à G, change x_1 en x_k. Donc par l'hypothèse k est aussi l'un des indices $1, 2, \ldots, r$, c. q. f. d.

Je prétends ensuite que cet ensemble $x_1, x_2, \ldots, x_r$ par les substitutions de G est *transitif*, c'est-à-dire que par les substitutions de G chaque variable devient chaque variable. En effet soit x_i et x_k deux quelconques de ces variables. Les permutations S et T changeant respectivement x_1 en x_i et x_1 en x_k existent par l'hypothèse. Donc la permutation $S^{-1}T$, qui appartient à G, change x_i en x_k, c. q. f. d.

Ainsi cet ensemble $x_1, x_2, \ldots, x_r, (\alpha)$, qui a été déterminé par x_1 d'après l'hypothèse, reste le même en prenant comme point de départ l'une quelconque des autres variables $x_2, \ldots, x_r$. Il est donc indépendant de la variable $x_1, x_2, \ldots, x_r$ choisie comme point de départ. Nous exprimons ce fait, qui est le résultat des deux démonstrations précédentes, en disant que l'ensemble (α) est *lié transitivement* par les substitutions du groupe. Si cet ensemble (α) n'absorbe pas toutes les variables du groupe G, une variable x_{r+1}, en dehors de (α), détermine un second ensemble lié transitivement (β), et ainsi de suite. Nous appelons les ensembles (α), $(\beta), \ldots$, simplement *transitifs* ; le groupe G lui-même dans le cas où (α) contient toutes les variables du groupe, est dit *transitif* ; dans le cas contraire il est dit *intransitif*.

II. Le nombre des permutations de G qui changent deux variables quelconques de l'ensemble (α) l'une dans l'autre, x_i et x_k, $i \neq$ ou $= k$, est indépendant de ces variables, c'est-à-dire il est le même pour tous les couples $x_i\, x_k$ de l'ensemble (α). Cela résulte sans autre de la décomposition du groupe G en complexes-adjoints relativement au sous-groupe H des permutations de G qui changent x_i en lui-même.

---

[2]) Le raisonnement que nous employons ici est celui de *Speiser*, p. 65 de l'ouvrage mentionné dans la note 1 et qui fait partie de la Collection: Die Grundlehren der Mathematischen Wissenschaften, Bd. V.

Soit $G = H + Ht_2 + \cdots + Ht_r$, (1), cette décomposition. Chacun des r complexes-adjoints Ht_k, $k = 2, \ldots, r$, change x_i dans le même x_k, t_k étant une substitution de G qui change x_i en x_k. Chaque complexe a le même nombre de substitutions et l'ensemble de toutes ces substitutions différentes constitue le groupe G. Il y a donc le même nombre de permutations qui changent un x_i fixé en un x_k quelconque de l'ensemble (α), $i \neq$ ou $= k$. Mais si nous changeons le x_i de l'ensemble (α) relativement auquel est faite la décomposition (1), comme le nombre des termes de la somme de droite ne peut pas changer, le H correspondant reste du même ordre et le fait ci-dessus est entièrement établi. D'ailleurs on sait que si H est le sous-groupe de G qui laisse x_i en place et t_k est une substitution de G qui change x_i en x_k, $t_k^{-1} H t_k$ est le groupe qui laisse x_k en place ; il est isomorphe au groupe H, etc.

III. Fixons l'un des *couples* de variables du groupe H, soit $x_1 x_2$[3]). Ce couple de variables par les permutations de G est changé en lui-même d'abord, puisque le groupe contient l'identité, et en un certain nombre des autres couples de variables, soit par exemple $x_1 x_3$, $x_2 x_4$, $x_4 x_5, \ldots,$. L'ensemble complet $x_1 x_2$, $x_1 x_3$, $x_2 x_4$, $x_4 x_5, \ldots, (\alpha')$ des couples de variables en lesquels est changé $x_1 x_2$ par les substitutions de G est de nouveau *fermé* et *transitif*, comme plus haut ; autrement dit les substitutions de G ne peuvent qu'échanger entre eux les couples de cet ensemble et par ces substitutions chaque couple devient chaque couple. Les démonstrations sont exactement pareilles ; il n'y a qu'à remplacer la variable par le couple de variables. Ainsi cet ensemble (α'), déterminé d'après l'hypothèse par le couple $x_1 x_2$, reste encore le même en prenant comme point de départ l'un quelconque des autres couples (α'). Il est indépendant du couple (α') choisi comme point de départ. Nous exprimons encore ce fait en disant que l'ensemble (α') est *lié transitivement* par les substitutions du groupe. Si maintenant cet ensemble n'absorbe pas tous les couples de variables, un couple en dehors de (α') détermine un second ensemble (β') lié transitivement, et ainsi de suite.

Nous appelons les ensembles (α'), (β'), etc., simplement *transitifs*[4]). Nous appelons le groupe G lui-même, selon que (α') contient tous les couples de variables du groupe ou non, *transitif* ou *intransitif pour les*

---

[3]) Il s'agit des couples-*arrangements* et non des couples-*combinaisons*. Autrement dit le couple $x_2 x_1$ est différent du couple $x_1 x_2$.

[4]) Chacun est *transitif* considéré en lui-même; mais l'un vis-à-vis de l'autre, les ensembles (α'), (β'), etc. sont *intransitifs*.

couples, tandis que la transitivité et l'intransitivité du cas I sont alors relatives aux *éléments*[5]).

Nous remarquons immédiatement que si l'on a l'ensemble transitif (α') vis-à-vis du groupe G, on a aussi l'ensemble transitif (α'') correspondant à (α') : $x_2\,x_1, x_3\,x_1, x_4\,x_2, x_5\,x_4, \ldots,$. Il peut évidemment se présenter que ces deux ensembles soient séparés. Si le groupe est doublement transitif, comme nous venons de le dire, ils sont réunis en un seul et unique ensemble (α') qui contient $n(n-1)$ couples. Nous remarquons aussi que la transitivité pour les couples exige la transitivité pour les éléments, mais que l'inverse n'a pas lieu.

IV. De nouveau le nombre des permutations de G qui changent deux couples quelconques de l'ensemble (α'), l'un dans l'autre, est indépendant de ces couples ; il est le même pour toutes les paires de couples de l'ensemble (α'). Cela résulte encore sans autre de la décomposition du groupe G relativement au sous-groupe H des permutations de G qui changent le couple $x_i\,x_k$ en lui-même, c'est-à-dire (note 3) qui laissent en place séparément x_i et x_k. La démonstration est encore exactement celle qui est sous II ; nous remplaçons seulement la variable par le couple de variables.

V. Il est clair maintenant que le raisonnement sous III et sous IV s'applique d'une façon exactement correspondante aux *i-uples* (arrangements i à i, note 3) des variables du groupe G. Si tous les i-uples de ces variables se trouvent dans un seul ensemble transitif (α'''), le groupe G est *transitif pour les i-uples* ou *i-fois transitif* (note 5) ; dans le cas contraire il est intransitif pour les i-uples. Le nombre des permutations de G qui changent deux i-uples quelconques de l'ensemble (α''') l'un dans l'autre est le même pour toutes les paires de i-uples de cet ensemble. Si l'on a vis-à-vis du groupe G l'ensemble transitif (α'''), on a aussi les $i!$ ensembles transitifs qui en proviennent en faisant chaque fois sur chaque i-uple de (α''') la même permutation. Si le groupe est i-fois transitif, ces $i!$ ensembles sont réunis en un seul qui contient $n(n-1)(n-2)\ldots(n-i+1)$ i-uples. Enfin le groupe ne peut être i-fois transitif s'il ne l'est pas $(i-1)$-fois ; mais l'inverse n'a pas lieu.

§ 2. Les groupes de substitutions primitifs et imprimitifs

Soit un groupe de substitutions *transitif pour les éléments*. Par les permutations du groupe chaque élément devient chaque élément. Mais il peut se faire qu'à cette faculté le groupe impose une certaine modalité,

[5]) Nous dirons aussi, comme *Netto* par exemple, au lieu de transitif pour les éléments, pour les couples, pour les i-uples, $i = 1, 2, \ldots, n$, *simplement, doublement, i-fois* transitif.

celle que cet échange des variables entre elles se produise par *ensembles particuliers* de plusieurs variables. Dans le cas où cette modalité n'existe pas, le groupe G est dit *primitif*; si elle existe, il est dit *imprimitif* et les ensembles en question sont appelés *ensembles* ou *systèmes imprimitifs* constitués par les éléments. Il est évident que le nombre des variables dans chaque ensemble doit être le même, puisque les variables d'un ensemble doivent devenir les variables d'un autre ensemble.

Soit $S_1, S_2, \ldots, S_l$ les ensembles imprimitifs de variables qui doivent permuter entre eux, chacun de i variables. Lorsque $i = 1$, le groupe est primitif; lorsque $i > 1$ le groupe est imprimitif [6]). Soit H les substitutions de G qui laissent chaque S_k en place, $k = 1, 2, \ldots, l$; ces substitutions constituent évidemment un groupe. Soit g_2 une substitution de G qui effectue une permutation des S_k. Les substitutions de l'ensemble $g_2 H$ ou de l'ensemble $H g_2$ effectuent la même permutation des S_k. D'autre part soit g une substitution *quelconque* de G qui effectue la permutation des S_k en question; les substitutions $g_2^{-1} g$ et $g g_2^{-1}$ appartiennent à H. Donc $g = g_2 h_\alpha = h_\beta g_2$, h_α et h_β étant deux substitutions de H. Ainsi H est un diviseur *normal* en G [7]) et les complexes-adjoints de H dans G:

$$H_i = g_i H = H g_i \qquad G = H + H_2 + H_3 + \cdots + H_s$$

donnent chacun l'ensemble des substitutions de G produisant une même permutation des S_k. Le groupe *quotient* G/H est le groupe des permutations des S_k; il est isomorphe au groupe G, etc.

A cause de la répartition en systèmes imprimitifs, un groupe imprimitif pour les éléments ne peut évidemment pas être transitif pour les couples. Autrement dit le groupe transitif pour les éléments peut être primitif ou imprimitif pour les éléments; s'il est imprimitif, il n'est transitif que pour les éléments.

Soit maintenant un groupe G *transitif pour les couples*. Par les permu-

---

[6]) Les cas $i = 1$ et $i > 1$ s'excluent; ils caractérisent des groupes de nature différente. Par contre dans le cas $i > 1$ le groupe imprimitif peut l'être de plusieurs manières; il y a en général plusieurs répartitions possibles des éléments en systèmes imprimitifs. Chaque répartition correspond à un sous-groupe particulier du groupe G; en effet une condition nécessaire et suffisante pour l'imprimitivité de G est la suivante. Si H_1 est le sous-groupe de G qui laisse en place l'une des variables, x_1 par exemple, et s'il y a dans G un sous-groupe intermédiaire K plus étendu contenant H_1, le groupe G est imprimitif. A chaque tel diviseur intermédiaire K correspond une répartition des éléments de G en systèmes imprimitifs (*Speiser*, l. c. § 30).

[7]) C'est l'appellation de *Speiser* (l. c.). *Netto* appelle *self-conjugué* le sous-groupe transformé en lui-même par toutes les substitutions de G, c'est-à-dire celui pour lequel, g étant une substitution quelconque de G, $g^{-1} H g = H$ ou $H g = g H$.

tations du groupe chaque couple devient chaque couple. Mais il peut se faire aussi que cet échange des couples entre eux doive se produire par ensembles *particuliers* de plusieurs couples. S'il en est ainsi le groupe peut être dit *imprimitif pour les couples* ; les ensembles de couples qui doivent s'échanger entre eux sont des *systèmes imprimitifs* de *couples*, etc. Dans ce cas, puisque ces ensembles imprimitifs doivent permuter entre eux, ils ne peuvent avoir que *la même constitution*, c'est-à-dire avoir le même nombre de couples et dans ces couples les répétitions d'éléments, en mêmes nombres de fois.

Soit encore $S_1, S_2, \ldots, S_m$ ces ensembles imprimitifs de couples qui doivent permuter entre eux par les substitutions de G. Chacun a donc le même nombre de couples. L'ensemble des substitutions de G qui laissent en place chaque S_k, $k = 1, 2, \ldots, m$, est de nouveau un diviseur normal en G et ce qui est dit plus haut relativement aux éléments, se répète ici identiquement pour les couples.

Toutefois il intervient une différence essentielle entre le cas des éléments et celui des couples. D'abord s'il existe une répartition imprimitive des couples :

$$(a\,b, c\,d, \ldots), (a'\,b', c'\,d', \ldots), \ldots ,$$

$a\,b, c\,d, \ldots, a'\,b', c'\,d', \ldots$. étant simplement des couples différents (note 3), il existe par le fait même la répartition suivante correspondante :

$$(b\,a, d\,c, \ldots), (b'\,a', d'\,c', \ldots), \ldots, .$$

Ces deux répartitions, qui ne vont pas l'une sans l'autre et qui peuvent évidemment n'en former qu'une seule, seront dites *conjuguées* l'une de l'autre.

Ensuite il existe une première répartition imprimitive *nécessaire* des couples qui est la suivante :

$$(a\,b, b\,a), (c\,d, d\,c), \ldots, \tag{1}$$

$a\,b, c\,d, \ldots$. étant toujours simplement des couples différents. Nous appelons cette répartition *nécessaire* parce qu'elle existe indépendamment du groupe G. Elle est conjuguée à elle-même ; on peut la noter simplement par son système général (ab, ba).

Puis il existe deux autres répartitions imprimitives également *nécessaires* qui sont les suivantes :

$$(ab, ac, \ldots, al), (ba, bc, \ldots, bl), \ldots, (la, lb, \ldots, lk) , \tag{2}$$

$$(ba, ca, \ldots, la), (ab, cb, \ldots, lb), \ldots, (al, bl, \ldots, kl) , \tag{3}$$

$a, b, c, \ldots, l$ étant les variables du groupe G. Ces deux répartitions existent encore indépendamment du groupe G ; elles sont conjuguées l'une de l'autre ; elles peuvent être notées simplement par leurs systèmes généraux (ax) et (xa), en convenant que pour chaque variable a, x parcourt toutes les autres variables.

Le fait que ces répartitions (1), (2) et (3) sont nécessaires, c'est-à-dire existent quel que soit le groupe G doublement transitif, ressort immédiatement de leur constitution. Elles n'empêchent pas une transitivité supérieure du groupe G ; on voit immédiatement en effet qu'elles ne gênent en rien un i-uple donné $abc\ldots f$, $i>2$, de devenir le i-uple *quelconque* $a'b'c'\ldots f'$.

Par contre toute répartition en systèmes imprimitifs *autre* que les trois ci-dessus, exclut dans un premier cas la transitivité quadruple, dans un second cas la transitivité triple, donc dans les deux cas la transitivité *quadruple*. C'est la démonstration que nous allons faire dans le paragraphe suivant.

§ 3. La caractéristique de la répartition (1) est le fait de n'avoir que deux éléments différents par système. La caractéristique des répartitions (2) et (3) est le fait d'avoir un élément commun à tous les couples du système, associé à chacun des autres éléments. Une autre répartition imprimitive quelconque des couples doit alors forcément rentrer dans l'un des deux cas qui suivent :

1er cas. Le système imprimitif général contient *au moins* deux couples avec quatre éléments différents $(ab, cd, \ldots)$. Dans ce cas on est assuré de trouver dans un second système de la répartition $(a'b', \ldots)$ un couple $a'b'$ dont les variables diffèrent de a et b *ou* de c et d. En effet, s'il n'en était pas ainsi, les couples de ce second système devraient tous contenir non seulement a ou b, ou a et b, mais aussi c ou d, ou c et d ; ces couples ne pourraient donc être constitués que des quatre éléments a, b, c, d. Dans ce cas il est évidemment impossible que le premier système $(ab, cd, \ldots)$ contienne des couples avec des éléments autres que ces quatre a, b, c, d, à cause de la transitivité. Par conséquent, à moins d'être dans le cas du groupe symétrique de quatre variables, nous pouvons admettre que a' et b' diffèrent en tout cas de l'un des couples a et b ou c et d. Admettons que ce soit a et b. Dans ce cas le quadruple $abcd$ ne peut pas devenir le quadruple $aba'b'$ par les permutations du groupe G, en vertu de la propriété de la répartition imprimitive. Donc dans ce cas le groupe G *n'est pas transitif pour les quadruples.*

Nous reviendrons sur le cas du groupe symétrique des quatre éléments a, b, c, d.

2e cas. Le système imprimitif général contient *au plus* [8]) deux couples avec trois éléments différents $(ab, ac, \ldots)$. Dans ce cas, il n'y a que deux alternatives : ou bien tous les couples contenant un même élément a se trouvent dans le même système, ou bien, dans plusieurs systèmes différents. La première alternative est celle des répartitions imprimitives nécessaires (2) et (3). Dans la seconde alternative nous avons un premier système $(ab, ac, \ldots)$ et un second système $(ad, \ldots)$. Mais alors aucune permutation du groupe ne peut changer, à cause de l'imprimitivité, le quadruple avec élément répété $abac$ dans le quadruple avec élément répété $abad$, et donc le triple abc dans le triple abd. Dans ce cas le groupe *G n'est pas transitif pour les triples* et par suite non plus pour les quadruples.

Ainsi une répartition imprimitive autre que les trois répartitions nécessaires n'est possible en tout cas que pour les groupes doublement ou triplement transitifs. Dès que le groupe a une transitivité supérieure à trois, il ne peut avoir relativement aux couples que les imprimitivités nécessaires ; on peut l'appeler *primitif* par rapport aux *couples*. D'autre part, s'il existe des groupes avec les transitivités double ou triple et possédant une répartition imprimitive des couples autre que les trois nécessaires, on peut les appeler *imprimitifs* par rapport aux *couples*. Nous verrons que ces groupes existent effectivement. Pour cela nous prenons successivement les quatre groupes généraux de degré n bien connu, cyclique, métacyclique, alterné et symétrique et nous fixons pour chacun la question de leur transitivité et de leur primitivité par rapport aux éléments et par rapport aux couples.

§ 4. Le groupe de substitutions cyclique

Nous employerons pour le groupe cyclique la notation par cycles. Soit la substitution génératrice du groupe s ; nous noterons le groupe lui-même $\{s\}$ et les éléments $0, 1, 2, \ldots, n-1$ (§ 1).

Il est évident d'abord que nous pouvons admettre que le ou les cycles

---

[8]) Ce *au plus* est opposé à *au moins* du premier cas. Naturellement les deux cas s'excluent l'un l'autre. Le premier cas est celui où le système général contient en tout cas deux couples avec quatre éléments différents; le second cas est celui où il ne contient pas deux couples avec quatre éléments différents, mais au plus deux couples avec trois éléments différents. D'autre part il les contient effectivement, sinon il ne contiendrait que deux couples avec deux éléments différents, ce qui est la caractéristique de la répartition nécessaire (1).

de s n'ont pas d'élément répété ; en effet le cycle par sa définition même est constitué d'éléments différents et une permutation formée de plusieurs cycles avec des éléments qui se répéteraient, se compose en une permutation de cycles sans élément répété. Nous envisageons maintenant les deux cas :

1er cas. La substitution s est formée *d'un seul* cycle. Elle peut donc se noter $s = (012\ldots\overline{n-1})$. La puissance a de s est la permutation suivante $s^a = (0, a, 2a, \ldots)(1, a+1, 2a+1, \ldots)\ldots$ Si a est premier à n, les entiers $0.a, 1.a, 2.a, \ldots, (n-1)a$ forment un système complet de restes mod. n[9]) et le premier cycle de s^a absorbe les n éléments. Si a a avec n un diviseur commun $d > 1$, alors $\frac{a}{d} = a'$ et $\frac{n}{d} = n'$ sont premiers entre eux et les restes mod. n des entiers $0.a, 1.a, 2.a, \ldots, (n-1)a$ se répartissent dans les d systèmes suivants du même nombre d'entiers n'

$$(0.a, 1.a, 2.a, \ldots, (n'-1)a), (1, a+1, 2a+1, \ldots, (n'-1)a+1), \ldots,$$
$$(d-1, a+d-1, 2a+d-1, \ldots, (n'-1)a+d-1) . \quad (1)$$

Ainsi pour le cas général $d \gtreqless 1$, la permutation s^a est constituée des d *cycles égaux* de n' *éléments* constitués par (1). Elle est donc une substitution dite *régulière* ; en particulier pour les puissances a premières à n, elle n'a qu'un cycle ; elle est alors dite *cyclique* ou *circulaire*. Pour la suite remarquons que chacun des cycles (1) est *fixé* par l'un quelconque de ses éléments ; en effet chaque élément est toujours le précédent augmenté de a, le premier étant consécutif au dernier.

Ajoutons maintenant 1 à tous les éléments des cycles (1). Ils deviennent respectivement

$$(1, a+1, 2a+1, \ldots, (n'-1)a+1), (2, a+2, 2a+2, \ldots, (n'-1)a+2), \ldots,$$
$$(d, a+d, 2a+d, \ldots, (n'-1)a+d) . \quad (2)$$

On voit que le premier cycle (1) devient le second, que le second devient le troisième, et ainsi de suite. Le dernier cycle de (1) devient le premier ; en effet la congruence $ax + d \equiv 0 \pmod{n}$ est toujours résoluble et

---

[9]) C'est un théorème simple de la théorie élémentaire des congruences. Voir par exemple *Landau*, Vorlesungen über Zahlentheorie, 1927, Bd. 1, Th. 62. La démonstration de l'énoncé pour le cas général où a et n ont un diviseur commun $d > 1$, qui vient ensuite, ne se trouve pas dans Landau, mais ne fait pas de difficultés. Le cas général redonne d'ailleurs le cas particulier où a est premier à n pour $d = 1$.

par un seul x allant de 0 à $n' - 1$[10]) et ainsi l'un des éléments du dernier cycle devient l'élément 0 du premier.

2e cas. La substitution s est formée de *plusieurs* cycles. Il est évident dans ce cas que chacun des cycles se comporte dans les puissances de s comme s'il était seul. Donc le cas se ramène au précédent. Si les cycles sont égaux, l'ordre du groupe est celui de chaque cycle ; si les cycles sont inégaux, l'ordre du groupe est le p. p. c. m. des ordres de chaque cycle. D'ailleurs pour ce que nous cherchons ici, la réponse dans ce second cas est très simple : le groupe est *intransitif* déjà *pour les éléments*, puisque les cycles de s constituent des systèmes intransitifs d'éléments l'un vis-à-vis de l'autre (note 4).

Il suffit donc d'étudier le groupe du premier cas $\{(012\ldots\overline{n-1})\}$. Il est *transitif* pour *les éléments*, puisque 0 devient a par la puissance s^a. Il est *intransitif* pour *les couples*, puisque le nombre n des permutations est inférieur au nombre $n(n-1)$ des couples.

Si n est *composé*, il est *imprimitif* pour *les éléments*, d'après ce que nous venons d'établir ci-dessus, car ajouter 1 aux éléments de (1), c'est effectuer la substitution s. Donc les puissances de s ne peuvent que permuter entre eux, et d'ailleurs cycliquement, les cycles de la substitution s^a. Ces cycles constituent ainsi une répartition des éléments en systèmes imprimitifs ; pour chaque a ayant avec n le même commun diviseur d, cette répartition est la même ; d'autre part à chaque diviseur d de n correspond une répartition différente. Le groupe H des substitutions de $G = \{s\}$ (voir § 2) qui laissent en place chacun des cycles (1) est formé des puissances $s^a, s^{2a}, \ldots, s^{(n'-1)a}, s^{n'a} = I$[11]) ; ce groupe $\{s^a\}$ d'ordre n' est, comme il doit être, diviseur normal de G, puisque G est abélien. Le groupe des permutations des cycles (1) par les substitutions de G, c'est-à-dire le groupe quotient G/H est le groupe d'ordre d engendré par la substitution cyclique $\sigma = (012\ldots\overline{d-1})$; ce dernier est lui-même homomorphe au groupe $\{s^{n'}\}$, diviseur de G ; en effet $s^{n'}$ est constituée de n' cycles égaux de d éléments et les deux groupes $\{s^{n'}\}$ et $\{\sigma\}$ sont homomorphes[12]).

Si n est *premier*, il est *primitif* pour *les éléments*. Toutes les puissances de s n'ont qu'un cycle de n éléments ; il n'y a pas de répartition des

---

[10]) *Landau* (l. c.), Bd. 1, Th. 65.

[11]) Nous noterons par I majuscule la substitution-identité.

[12]) Ce qui est dit à la note 6 se vérifie ici. Le diviseur de G qui laisse en place un élément, 0 par exemple, est l'identité. Chaque diviseur propre du groupe $\{s\}$ joue le rôle du sous-groupe intermédiaire K et donne lieu à une répartition des éléments en systèmes imprimitifs.

éléments en systèmes imprimitifs. Cela correspond d'ailleurs à l'observation de la note 12, le groupe $\{s\}$ n'ayant dans ce cas pas de diviseur propre.

La question de la primitivité ou de l'imprimitivité par rapport *aux couples* ne se pose pas ici, puisque le groupe n'est pas transitif pour les couples.

§ 5. Le groupe de substitutions métacyclique

Nous employons pour ce groupe la notation analytique. Nous entendons par le groupe *métacyclique*[13]) l'ensemble des substitutions $w = |\, x, a + bx \,|$, où $a = 0, 1, 2, \ldots, n-1$ et $b =$ les $\varphi(n)$ entiers positifs premiers à n et $< n$ ou, autrement dit, un système réduit de restes mod. n [14]). Il est simple de montrer par des congruences élémentaires que $|\, x, a + bx \,|$ est une substitution lorsque b est premier à n et seulement dans ce cas et que ces substitutions constituent un groupe.

Le groupe métacyclique est l'ensemble des substitutions du groupe symétrique permutables au groupe cyclique $\{s\}$, $s = (012\ldots\overline{n-1})$ [15]); ou énoncé autrement, il est dans le groupe symétrique le sous-groupe maximum dans lequel le groupe cyclique est diviseur normal.

Pour $n = 2$, le groupe cyclique, le groupe métacyclique et le groupe symétrique ne font qu'un seul et même groupe, constitué des deux substitutions I et (01). Pour $n = 3$, le groupe cyclique est le groupe alterné : I, (012), (021) ; le groupe métacyclique est le groupe symétrique I, (012), (021), (01), (02), (12) ; il est évidemment comme tel *triplement* transitif.

Pour n *premier* > 3 le groupe métacyclique a $n(n-1)$ permutations. Il peut donc être au plus *doublement* transitif et il l'est en effet ; la permutation suivante $|\, x, \alpha + (\beta - \alpha)\, x \,|$ change le couple 01 dans le couple *quelconque* $\alpha\beta$. Il est donc *primitif* pour *les éléments* (§ 2), mais par contre

---

[13]) Cette appellation que nous avons employée déjà dans plusieurs travaux antérieurs est simplement une extension de celle de Kronecker (*Netto*, Gruppen und Substitutionentheorie, p. 133) qui désigne par ce mot ce même groupe lorsque n est *premier*. On appelle aussi *métacycliques* (*Weber*, Lehrbuch der Algebra, Bd. 1, p. 647) les groupes dits résolubles par Frobenius et Hölder, c'est-à-dire les groupes correspondants aux équations résolubles par radicaux, et dont la série des indices de composition est constituée uniquement de nombres premiers. C'est là aussi une extension, mais dans un autre sens, du mot de Kronecker, puisque, lorsque le degré est premier, les équations les plus générales résolubles par radicaux, sont celles dont le groupe est métacyclique au sens de Kronecker.

[14]) *Landau* (l. c., définition 16).

[15]) *S. Bays*, Sur les systèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme $6n + 1$. Commentarii mathematici helvetici, vol. 3, fasc. I, p. 25.

il est *imprimitif* pour *les couples*. En effet une répartition des couples en systèmes imprimitifs autre que les trois nécessaires est la suivante :

$$(01, 12, 23, \ldots, \overline{n-1}\,0),\quad (02, 24, 46, \ldots, \overline{n-2}\,0), \ldots,$$
$$(0\,\overline{n-1}, \overline{n-1}\,\overline{n-2}, \ldots, 10)\ ,$$

c'est-à-dire, en n'écrivant que le système général de la répartition :

$$(0, b\,;\, b, 2b\,;\, 2b, 3b\,;\ldots;\quad (n-1)\,b, 0),\quad b = 1, 2, 3, \ldots, n-1\ . \quad (1)$$

Pour le voir, constatons d'abord que les entiers b, $2b$, $3b, \ldots, (n-1)b$, b étant premier à n, forment un système complet de restes mod.n (note 9) et ensuite que par la permutation $|\ x, a + bx\ |$ le système général (1) devient :

$$\left(a, a + b^2\,;\, a + b^2, a + 2b^2\,;\, a + 2b^2, a + 3b^2\,;\ldots;\, a + (n-1)\,b^2, a\right) \quad (2)$$

Or c'est encore là l'un des systèmes de la répartition (1). En effet la congruence $a + b^2x \equiv 0$ (mod.n) a une et une seule solution puisque b est premier à n. Soit α cette solution. Le système (2) qui peut s'écrire en commençant par n'importe lequel de ses couples, ici par le couple $a + \alpha b^2$, $a + (\alpha + 1)b^2$ revient à celui-ci :

$$\left(0, b^2\,;\, b^2, 2b^2\,;\, 2b^2, 3b^2\,;\ldots;\, (n-1)\,b^2, 0\right)\ .$$

Comme b^2 est aussi bien que b congru à l'un des entiers $1, 2, 3, \ldots, n-1$ (mod.n), on a c. q. f. d.

Pour n *composé*, le groupe métacyclique a $n\,\varphi(n)$ permutations. $\varphi(n)$ étant dans ce cas $< n-1$, le groupe n'a pas assez de permutations pour être doublement transitif. Il est transitif pour *les éléments* seulement. La question de la primitivité ou de l'imprimitivité pour les couples ne se pose donc pas ; par contre du fait que le groupe est permutable au groupe cyclique, il est comme ce dernier *imprimitif* pour *les éléments* et a les mêmes répartitions que lui en systèmes imprimitifs d'éléments.

Pour $n = 3$ le groupe est, comme nous l'avons dit, triplement transitif. Il est donc primitif pour les éléments ; il est imprimitif pour les couples ; il possède la seule répartition imprimitive *non* nécessaire suivante : (01, 12, 20), (02, 21, 10), qui est celle ci-dessus du groupe métacyclique.

§ 6. Le groupe alterné

Le groupe alterné est, comme on le sait, l'ensemble des permutations de première classe, c'est-à-dire qui comportent un nombre pair d'inversions. Il est d'ordre $\frac{n!}{2}$; il peut donc être *au plus* $(n-2)$ fois transitif puisque le nombre des $(n-2)$-uples (note 3) est le même nombre $n(n-1)(n-2)\ldots 3$. Il est effectivement *transitif* pour *les* $(n-2)$-*uples*. En effet, des deux permutations suivantes :

$$\begin{pmatrix} 1, 2, \ldots, n-2, n-1, n \\ i_1, i_2, \ldots, i_{n-2}, i_{n-1}, i_n \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1, 2, \ldots, n-2, n-1, n \\ i_1, i_2, \ldots, i_{n-2}, i_n, i_{n-1} \end{pmatrix}$$

qui changent chacune le $(n-2)$-uple $1, 2, \ldots, n-2$ dans le $(n-2)$-uple *quelconque* $i_1, i_2, \ldots, i_{n-2}$, l'une des deux est de *première* classe, puisque les deux permutations des éléments $1, 2, \ldots, n$ écrites dans les rangées inférieures ont l'une ou l'autre un nombre pair d'inversions. Il y a donc toujours une permutation du groupe alterné qui change un $(n-2)$-uple fixé en un $(n-2)$-uple quelconque, c. q. f. d.

Pour $n = 2$, le groupe alterné se réduit à l'identité. Pour $n = 3$, le groupe alterné est le groupe cyclique (§ 5). Pour $n = 4$, le groupe alterné est constitué des 12 substitutions suivantes :

$$\begin{aligned} &\mathrm{I},\ (234),\ (243),\ (12)\,(34),\ (123),\ (124), \\ &(132),\ (134),\ (13)\,(24),\ (142),\ (143),\ (14)\,(23)\ . \end{aligned}$$

D'après la démonstration précédente il est transitif pour les couples ; il est donc primitif pour les éléments (§ 2). Pour les couples, il donne lieu à des répartitions imprimitives *non* nécessaires, qui sont les suivantes :

$$(01, 23)\,;\ (02, 31)\,;\ (03, 12)\,;\ (10, 32)\,;\ (20, 13)\,;\ (30, 21)\ , \qquad (1)$$

$$(01, 12, 20)\,;\ (13, 32, 21)\,;\ (30, 02, 23)\,;\ (31, 10, 03)\ , \qquad (2)$$

et la conjuguée de (2) qui est différente ; en plus une troisième répartition, identique encore à sa conjuguée, obtenue de (1) en remplaçant le premier *ou* le second couple de chaque système par son inverse. Il est donc *imprimitif* pour *les couples*.

Pour $n = 5$, le groupe alterné est constitué de 60 substitutions. Il est triplement transitif ; il est donc primitif pour les éléments. Par une vérification très courte, on constate qu'il est *primitif* aussi pour *les couples*. Il suffit pour cela de s'appuyer sur le fait que le second cas du § 3 est exclu pour ce groupe triplement transitif ; par conséquent le système général d'une répartition imprimitive éventuelle des couples, doit contenir au moins deux couples avec quatre éléments différents. Sans restreindre la généralité, nous prenons pour ces deux couples, 01, 23. On effectue sur ces deux couples les 60 substitutions du groupe. Les couples qui résultent de 23 par celles de ces substitutions qui laissent 01 invariant, doivent figurer dans le système général (01, 23, . . .) ; de même les couples qui résultent de 01 par celles qui laissent 23 invariant. On trouve les couples (01, 23, 34, 42, 40, 14, . . .). On part ensuite de 01, 34 par exemple et on continue de la même manière ; on trouve très vite que le système doit contenir plus de 10 couples, c'est-à-dire qu'il doit contenir les 20 couples des 5 éléments. Une répartition imprimitive des couples autre que les nécessaires est donc impossible.

Pour $n \leqq 6$ le groupe alterné est transitif pour les quadruples ; en conséquence il est *primitif* pour *les éléments* et pour *les couples* (§ 3).

§ 7. Le groupe symétrique

Le groupe symétrique de n éléments est évidemment n-fois transitif. Donc pour $n > 4$ le groupe est en tout cas *primitif* pour *les éléments* et pour *les couples*. Pour $n = 2$ et $n = 3$ nous savons déjà ce qu'il en est (§ 5). Reste le cas $n = 4$; nous avons vu qu'il a dû être mis de côté dans la démonstration du premier cas du § 3. Le groupe est évidemment *primitif* pour *les éléments*. Il est *imprimitif* pour *les couples* au sens que nous avons fixé pour cette imprimitivité. Il a en effet, en plus des trois répartitions nécessaires, une quatrième répartition imprimitive des couples qui est la suivante, conjuguée à elle-même : (01, 23, 10, 32), (02, 13, 20, 31), (03, 12, 30, 21). Il est facile de vérifier, en appliquant séparément les deux cas du § 3, qu'il n'y a pas une autre répartition imprimitive possible, pour les couples.

(Reçu le 5 décembre 1947.)