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

S. BAYS

Recherche des systèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme $6n + 1$

Journal de mathématiques pures et appliquées 9^e série, tome 2 (1923), p. 73-98.
<http://www.numdam.org/item?id=JMPA_1923_9_2__73_0>

Gallica NUMDAM

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

Recherche des systèmes cycliques de triples de Steiner différents pour N *premier (ou puissance de nombre premier) de la forme* $6n + 1$;

Par S. BAYS.

INTRODUCTION.

Dans un premier travail sur les systèmes cycliques de triples de Steiner (¹), nous avons obtenu tous les systèmes cycliques de triples de Steiner possibles pour les premières valeurs de N de la forme $6n + 1$: $N = 7, 13, 19, 25, 31$ éléments.

Nous en rappelons les données essentielles :

1° Un ensemble de triples (combinaisons trois à trois) de N éléments, contenant *une fois et une seule fois* chaque couple de ces éléments, est un *système de triples de Steiner* (²). Il existe des systèmes de triples de Steiner pour chaque N de la forme $6n + 1$ et $6n + 3$, et seu-

(¹) S. Bays, *Sur les Systèmes cycliques de triples de Steiner* (*Annales de l'École Normale*, 1923). Les deux Mémoires paraissent à quelques jours d'intervalle. Nous prions le lecteur que le sujet intéresse et qui veut entreprendre la lecture du présent travail d'une manière aisée et complète, de bien vouloir prendre d'abord connaissance du Mémoire des *Annales*. Les résultats essentiels des deux Mémoires ont fait l'objet de deux Notes aux *Comptes rendus* (t. 165, 22 octobre 1917, p. 543, et t. 171, 27 décembre 1920, p. 1361).

(²) Le triple 123 contient les trois couples 12, 13, 23, et le système de triples de Steiner 123, 145, 167, 246, 257, 347, 356 contient une fois et une seule fois chaque couple des sept éléments 1, 2, ..., 7. Tout l'exposé nécessaire pour lire aisément ce travail se trouve dans notre premier travail. On peut consulter aussi Netto, *Combinatorik*, p. 202-228.

lement pour ces N. Deux systèmes de triples sont *différents*, s'ils ne peuvent provenir l'un de l'autre par une permutation quelconque des N éléments.

2° Soit $N = 6n + 1$ et les éléments 0, 1, 2, ..., $6n$. Un système de triples de Steiner de ces éléments est *cyclique* (1) lorsque ses $n(6n-1)$ triples sont répartis en n *séries cycliques* de la forme x, $a + x$, $b + x$ ($x = 0, 1, 2, \ldots, 6n$), a et b étant deux des entiers 1, 2, ..., $6n$, $b > a$ et $\neq 2a$, $N - a$, $\frac{N+a}{2}$. Nous entendons par les entiers $a + x$, $b + x$, comme par tous les entiers $\gtrless N$ qui interviennent dans les substitutions suivantes, leur plus petit reste positif ou nul (mod N).

3° Les séries cycliques vont par *paires* de séries dites *conjuguées*. Deux séries conjuguées contiennent les mêmes couples, bien que sans triple commun; elles sont déductibles l'une de l'autre par la substitution $|x, N - x|$. Les éléments associés à 0 dans un triple, dans chacune d'elles, sont :

$$a, \quad b - a, \quad b, \quad N - b, \quad N - (b - a), \quad N - a.$$

Trois de ces éléments sont inférieurs à $\frac{1}{2}N$; ils constituent la *caractéristique* de ces deux séries. L'ensemble des caractéristiques est l'ensemble des triples des éléments 1, 2, ..., $3n$, ayant la propriété : la somme de deux de leurs éléments est égale au troisième, ou la somme des trois éléments est égale à N.

4° Soit $N = 6n + 1$ premier (ou de la forme p^m), et les éléments 0, 1, 2, ..., $6n$. Le groupe *métacyclique* est produit par les deux substitutions $|x, 1 + x|$ et $|x, \alpha x|$, α étant racine primitive de N [appartenant à l'exposant $\varphi(N)$, mod N]. La substitution $|x, 1 + x|$ est génératrice de la série cyclique. La substitution $|x, \alpha x|$ change une série cyclique en une autre série cyclique, les trois triples de la première série qui contiennent l'élément 0 en ceux de la seconde qui

(1) Il existe également des systèmes *cycliques* de triples pour $N = 6n + 3$ éléments. Ils sont constitués de n séries cycliques de la forme x, $a + x$, $b + x$ ($x = 0, 1, 2, \ldots, 6n + 2$), et d'une série cyclique supplémentaire de $2n + 1$ triples. Nous ne nous en sommes pas occupés jusqu'ici.

contiennent l'élément o, et deux séries cycliques conjuguées en deux séries cycliques conjuguées.

5° Pour un système cyclique de triples de Steiner, il faut n séries cycliques telles que les $6n$ éléments associés à l'élément o dans les $3n$ triples qui le contiennent soient les $6n$ autres éléments 1, 2, ..., $6n$. Les n caractéristiques correspondant à ces séries contiendront les $3n$ éléments 1, 2, ..., $3n$, une fois chacun. Elles détermineront 2^n systèmes cycliques de triples de Steiner, puisque, pour constituer un système de triples, une série cyclique peut indifféremment être remplacée par la série conjuguée. Obtenir les systèmes cycliques de triples de Steiner de N éléments revient donc à déterminer d'abord tous les ensembles de n caractéristiques contenant les $3n$ éléments 1, 2, ..., $3n$. Nous appellerons un tel ensemble de n caractéristiques sans élément commun, un *système de caractéristiques* (1).

Dans notre premier travail, cette recherche des systèmes de caractéristiques a été faite directement, jusqu'à N = 31, sur l'ensemble des caractéristiques. Les substitutions métacycliques nous ont servi ensuite à répartir les systèmes cycliques de triples obtenus en classes de systèmes équivalents, et enfin le procédé des *trains de White* (2) nous a montré que les systèmes de deux classes différentes étaient toujours différents. Le théorème suivant était donc vérifié pour ces premières valeurs de N (premier ou de la forme p^m) : *deux systèmes cycliques équivalents sont déductibles l'un de l'autre par une substitution métacyclique.*

Ce théorème ne fait aucun doute pour nous, pour des raisons de la théorie des groupes que nous ne pouvons développer ici; mais nous ne sommes pas encore en état de le démontrer sous sa forme générale : *deux fonctions cycliques de n variables* $x_1, x_2, \ldots, x_n$ [possédant le groupe cyclique $\{(x_1 x_2 \ldots x_n)\}$, $n = p$ ou p^m] *équivalentes, sont*

---

(1) Une *solution du problème de Heffter* ou du *tableau des caractéristiques*, dans notre premier travail. D'autre part, pour abréger, par *système de triples*, ou *système cyclique*, nous entendrons toujours, dans la suite, un système cyclique de triples de Steiner.

(2) H.-S. White, *Trans. of the A. M. S.*, t. XIV, 1913, p. 13.

déductibles l'une de l'autre par une substitution métacyclique (¹). Nous l'admettrons pour la suite, jusqu'à démonstration ultérieure. On ne peut plus songer en effet à la vérification au moyen des trains de White pour un système de triples de chaque classe, comme elle a été faite dans notre premier travail, à cause du trop grand nombre des classes. D'autre part, il ne paraît pas possible d'aborder cette recherche des systèmes cycliques de triples différents par une autre voie, en tout cas, pas par une voie plus courte. C'est pourquoi à l'alternative d'abandonner cette recherche, nous avons préféré celle qui va suivre.

Les résultats d'ailleurs ont justifié notre peine. Pour N = 7, 13, 19, 25 et 31 éléments, la recherche directe des systèmes de caractéristiques et l'application du groupe $\{|x, \alpha x|\}$ aux systèmes cycliques de triples qui s'en déduisent, nous ont fourni les systèmes cycliques différents, *mais sans rendre compte des groupements très particuliers de ces systèmes*. Pour N = 31, les 2048 systèmes de triples existants donnaient 80 systèmes cycliques différents (80 classes de systèmes équivalents par les substitutions métacycliques); trois groupements de 16 systèmes étaient d'un même type, trois autres groupements de 8 systèmes d'un même type également, et deux groupements à part donnaient les 8 systèmes offrant le plus d'intérêt. Pour N = 19, les 4 systèmes de triples différents formaient deux groupements différents; de même les 12 systèmes différents pour N = 25 (²). A partir de N = 31, la recherche directe des systèmes de caractéristiques n'était plus possible. L'introduction du groupe que nous notons $\{|\underline{x}, \underline{\alpha x}|\}$ nous a du coup simplifié considérablement cette recherche, et rendu compte des groupements des systèmes cycliques différents. Nous ne cherchons

(¹) Je ne serais même pas surpris que le théorème soit déjà démontré, étant donné son importance en théorie des groupes. Je ne connais malheureusement pas assez la littérature de la théorie des groupes pour en décider. Quoi qu'il en soit, sa démonstration serait d'un intérêt essentiel dans le présent travail.

(²) Également dans la constitution des trains de White, apparaissaient nettement les groupements particuliers de ces systèmes. Les trains de White, appartenant aux systèmes d'un même groupement, semblaient dériver plus ou moins d'une même forme initiale, caractéristique de ce groupement [*voir* par exemple, dans les figures des trains pour N = 19 (fin du mémoire), les trains des systèmes a et a_1 d'une part et d et d_3 d'autre part].

plus que les systèmes de caractéristiques *non déductibles l'un de l'autre par les substitutions du groupe* $\{|\underline{x}, \underline{\alpha x}|\}$ et chacun d'eux se trouve déterminer directement *une famille de systèmes de triples différents à symétrie propre* (les groupements précédents pour $N = 31$, 19 et 25). Ces systèmes de caractéristiques fondamentaux (1) dont dépendent ainsi entièrement la répartition des systèmes de triples différents, et les groupes qu'ils possèdent apparaissent maintenant comme les éléments irréductibles du problème.

Dans un premier Chapitre, nous introduisons ce groupe $\{|\underline{x}, \underline{\alpha x}|\}$ et étudions son effet sur l'ensemble des caractéristiques. Dans un second Chapitre, nous faisons la recherche des systèmes de triples différents pour $N = 37$. Enfin, dans un dernier paragraphe, nous donnons les résultats de cette recherche pour $N = 43$.

Le groupe $|\underline{x}, \underline{\alpha x}|$ et son effet sur l'ensemble des caractéristiques.

1. La substitution $|x, \alpha x|$ des $6n$ éléments 1, 2, ..., $6n$, α racine primitive de N [appartenant à l'exposant $\varphi(N)$, mod N], transforme les trois triples d'une série qui contiennent l'élément o dans les trois triples contenant l'élément o de la série transformée.

Par suite, la substitution $|x, \alpha x|$ des $3n$ éléments 1, 2, ..., $3n$, dans laquelle nous remplaçons, non seulement chaque entier αx par son plus petit reste positif (mod N), mais encore chaque reste ainsi trouvé *a supérieur à* $\frac{1}{2}$N, *par son complément* $N - a$ (2) *inférieur à* $\frac{1}{2}$N, transforme *une caractéristique en une caractéristique.*

Nous noterons dorénavant par $\underline{a}$ l'élément a, chaque fois que nous entendons ainsi *la valeur absolue de son plus petit reste positif ou négatif* (mod N). Conséquemment, nous noterons par $|\underline{x}, \underline{\alpha x}|$ la substitution précédente.

---

(1) Nous les appelons dans la suite « systèmes de caractéristiques *différents* ».

(2) Pour un entier a compris entre o et N, nous appellerons *complément* de a le nombre $N - a$.

2. Si nous introduisons un signe quelconque, par exemple $\underline{=}$, pour cette relation entre les entiers a et $\underline{a}$ (mod N), $a \underline{=} \underline{a}$ (mod N), cette relation a en partie les propriétés d'une congruence ordinaire (mod N), c'est-à-dire, si $a \underline{=} b$ et $b \underline{=} c$,

$$a \underline{=} c \quad (\text{mod N})$$

et vis-à-vis de la multiplication, si $a \underline{=} b$ et $c \underline{=} d$,

$$(1) \qquad ac \underline{=} bd \quad (\text{mod N}),$$

et comme cas particulier, si $a \underline{=} b$, $m \underline{=} m$,

$$ma \underline{=} mb \quad (\text{mod N}).$$

En effet, $a \underline{=} b$ (mod N) équivaut à $a \equiv \pm b$ (mod N), les deux autres congruences $\pm a \equiv b$ ne différant pas de ces deux premières.

De $a \equiv \pm b$ et $b \equiv \pm c$, il suit

$$a \equiv \pm c \quad (\text{mod N}).$$

De $a \equiv \pm b$ et $c \equiv \pm d$, il suit

$$ac \equiv \pm bd \quad (\text{mod N}).$$

Par contre, vis-à-vis de l'addition, la relation n'a plus nécessairement la propriété de la congruence (mod N) : si $a \equiv \pm b$ et $c \equiv \pm d$,

$$a + c \equiv \pm b \pm d,$$

mais la valeur absolue du second membre n'est pas toujours égale à $b + d$.

De la propriété (1) nous avons, s'appliquant plus directement à l'usage que nous allons en faire :

$$a \underline{=} \underline{a}, \quad b \underline{=} \underline{b}, \quad ab \underline{=} \underline{a}.\underline{b}, \quad \underline{ab} \underline{=} \underline{a.b}$$

ou enfin

$$\underline{ab} = \underline{\underline{a.b}}.$$

Autrement dit, les deux opérations $\underline{\underline{a.b}}$ et $\underline{ab}$ donnent le même

résultat, et sont indifférentes à remplacer l'une par l'autre. D'où

$$\underline{a^n} \equiv (\underline{a})^n; \qquad \underline{\underline{a^n}} = \underline{\underline{(a)^n}} = \underline{\underline{(a)^{n-1}}}.\underline{a}, \qquad \ldots.$$

3. La substitution $|x, \alpha x|$ des $6n$ éléments 1, 2, ..., $6n$ est le cycle

$$(1\,\alpha^1\alpha^2\alpha^3 \ldots \alpha^{6n-1}) \quad \text{ou} \quad (\alpha^0\alpha^1\alpha^2 \ldots \alpha^{6n-1}).$$

La substitution $|\underline{x}, \underline{\alpha x}|$ des $3n$ éléments 1, 2, ..., $3n$ est le cycle

$$(1\,\underline{\alpha}\,\underline{\alpha^2}\,\underline{\alpha^3} \ldots \underline{\alpha^{3n-1}}) \quad \text{ou} \quad (\underline{\alpha^0}\,\underline{\alpha^1}\,\underline{\alpha^2} \ldots \underline{\alpha^{3n-1}}).$$

On a en effet :

$$\alpha^{3n} \equiv -1, \quad \alpha^{3n+\nu} \equiv -\alpha^\nu \pmod{N};$$

les petits restes positifs des puissances α^{3n}, α^{3n+1}, ..., α^{6n-1} sont les compléments des plus petits restes positifs des $3n$ premières puissances. Les entiers $1, \underline{\alpha}, \underline{\alpha^2}, \ldots, \underline{\alpha^{3n-1}}$ sont donc les $3n$ éléments 1, 2, ..., $3n$.

Les $6n$ premières puissances de la substitution cyclique $s = |x, \alpha x|$ forment le groupe cyclique d'ordre $6n$: $\{|x, \alpha x|\}$. Celles de ces puissances dont l'exposant est premier avec $6n$ sont formées d'un seul cycle; elles sont évidemment les substitutions $|x, \alpha x|$ correspondant aux autres racines primitives de N. On sait d'ailleurs que les puissances α^ν, dont l'exposant ν est premier avec $6n$, sont congrues aux autres racines primitives de N.

Les $3n$ premières puissances de la substitution cyclique $\sigma = |\underline{x}, \underline{\alpha x}|$ forment le groupe cyclique d'ordre $3n$: $\{|\underline{x}, \underline{\alpha x}|\}$. Seules les puissances de σ, dont l'exposant est premier avec $3n$, sont formées d'un seul cycle, et correspondent aux autres racines primitives de N. Dans le cas où deux racines primitives de N, α et β sont complémentaires, $\beta = N - \alpha$, $\underline{\alpha} = \underline{\beta}$, $\underline{\alpha^2} = \underline{\beta^2}$, etc., et les deux substitutions correspondantes sont identiques (1).

---

(1) Les racines primitives sont complémentaires deux à deux ou non complémentaires, selon que le nombre premier est de la forme $4n + 1$ ou $4n - 1$. Cette remarque que je n'ai pu retrouver dans les *Disquisitiones arithmeticæ*, de GAUSS, se trouve démontrée ici très simplement, en passant, pour les nombres

4. Les deux groupes cycliques $\{|x, \alpha x|\}$ et $\{|\underline{x}, \underline{\alpha x}|\}$ sont *réguliers transitifs :* leur ordre est égal à leur degré, chacune de leurs substitutions est formée de cycles égaux (contenant le même nombre d'éléments) et déplace tous les éléments, et par les substitutions du groupe, chaque élément se trouve successivement transformé en tous les autres. On sait qu'un groupe régulier transitif d'ordre N est *imprimitif;* chacune de ses substitutions donne une répartition des N éléments en systèmes imprimitifs, constitués directement par les éléments de chaque cycle.

5. Le groupe cyclique d'ordre $3n$: $\{|\underline{x}, \underline{\alpha x}|\}$ contient la substitution suivante, qui est la puissance n de la substitution $\sigma = |\underline{x}, \underline{\alpha x}|$:

$$(2) \qquad (\underline{\alpha^0\,\alpha^n\,\alpha^{2n}})(\underline{\alpha^1\,\alpha^{n+1}\,\alpha^{2n+1}}) \cdots (\underline{\alpha^{n-1}\,\alpha^{2n-1}\,\alpha^{3n-1}}).$$

Le système imprimitif constitué par chacun de ces cycles est une *caractéristique.* En effet, α étant toujours une racine primitive de N, les trois triples formés avec l'élément o :

$$o\,\alpha^\nu\,\alpha^{n+\nu}, \quad o\,\alpha^{2n+\nu}\,\alpha^{3n+\nu}, \quad o\,\alpha^{4n+\nu}\,\alpha^{5n+\nu} \qquad (\nu = 0, 1, \ldots, n-1)$$

appartiennent à la même série cyclique (¹). Trois des six éléments α^ν, $\alpha^{n+\nu}$, $\alpha^{2n+\nu}$, $\alpha^{3n+\nu}$, $\alpha^{4n+\nu}$, $\alpha^{5n+\nu}$ sont les compléments des trois autres et inférieurs à $\frac{1}{2}$N (d'après 3°, introduction); ils ne peuvent être que les trois éléments $\underline{\alpha^\nu}$, $\underline{\alpha^{n+\nu}}$, $\underline{\alpha^{2n+\nu}}$, puisque $\alpha^{3n+\nu} \equiv -\alpha^\nu$, $\alpha^{4n+\nu} \equiv -\alpha^{n+\nu}$, $\alpha^{5n+\nu} \equiv -\alpha^{2n+\nu}$, et le triple $\underline{\alpha^\nu}\,\underline{\alpha^{n+\nu}}\,\underline{\alpha^{2n+\nu}}$ est la caractéristique de cette

---

premiers de la forme $6n+1$, par le fait que les racines primitives seront complémentaires ou non, selon que

$$\varphi(3n) = \tfrac{1}{2}\varphi(6n) \qquad \text{ou} \qquad \varphi(3n) = \varphi(6n).$$

Or on a $\varphi(3n) = \frac{1}{2}\varphi(6n)$ pour n pair, c'est-à-dire pour les nombres premiers $6n+1$ de la forme $12n'+1 = 4n''+1$, et $\varphi(3n) = \varphi(6n)$ pour n impair, c'est-à-dire pour les nombres premiers $6n+1$ de la forme $12n'-5 = 4n''-1$.

(¹) La construction du système cyclique de Netto est déjà l'application directe de cette propriété (*voir* notre premier travail, page 57). Il est d'ailleurs facile et court de répéter ici la démonstration. Les trois triples contenant l'élément o dans

série cyclique. Les cycles de la substitution (2) sont donc des caractéristiques, et constituent un système de n caractéristiques sans élément commun. Nous l'appellerons le *système des caractéristiques imprimitives*.

6. La démonstration donnée ne fait aucune restriction sur l'entier positif ν, et le triple $\underline{\alpha^\nu}\,\underline{\alpha^{n+\nu}}\,\underline{\alpha^{2n+\nu}}$ est encore une caractéristique quel que soit $\nu \gtrless n$. Cette caractéristique est aussi toujours l'une des caractéristiques imprimitives (2). En effet soit ν' un entier positif $\gtrless n$; l'élément $\underline{\alpha^{\nu'}}$ est contenu dans l'une des caractéristiques (2). Supposons par exemple $\underline{\alpha^{\nu'}} = \underline{\alpha^{2n+\nu}}$ $(\nu = 0, 1, \ldots, n-1)$, ce qui signifie

$$\alpha^{\nu'} \equiv \pm\, \alpha^{2n+\nu};$$

on aura

$$\alpha^{n+\nu'} \equiv \pm\, \alpha^{3n+\nu} \equiv \mp\, \alpha^{\nu}; \qquad \alpha^{2n+\nu'} \equiv \pm\, \alpha^{4n+\nu} \equiv \mp\, \alpha^{n+\nu} \pmod{N},$$

c'est-à-dire

$$\underline{\alpha^{n+\nu'}} = \underline{\alpha^{\nu}}; \qquad \underline{\alpha^{2n+\nu'}} = \underline{\alpha^{n+\nu}}. \qquad \text{C. Q. F. D.}$$

Dans ce cas,

$$\underline{\alpha^{\nu'}},\ \underline{\alpha^{n+\nu'}},\ \underline{\alpha^{2n+\nu'}};\quad \underline{\alpha^{\nu'+1}},\ \underline{\alpha^{n+\nu'+1}},\ \underline{\alpha^{2n+\nu'+1}};\quad \ldots;\quad \underline{\alpha^{\nu'+n-1}},\ \underline{\alpha^{\nu'+2n-1}},\ \underline{\alpha^{\nu'+3n-1}}$$

sont évidemment de nouveau les n caractéristiques imprimitives différentes.

7. La substitution $|x,\ \alpha^{2n}x|$ transforme la série cyclique qui contient les trois triples

$$0,\ \alpha^{\nu},\ \alpha^{n+\nu};\quad 0,\ \alpha^{2n+\nu},\ \alpha^{3n+\nu};\quad 0,\ \alpha^{4n+\nu},\ \alpha^{5n+\nu}$$

en elle-même. On a donc le théorème :

---

la série déterminée par $0,\ \alpha^{\nu},\ \alpha^{n+\nu}$ sont :

$$0,\ \alpha^{\nu},\ \alpha^{n+\nu};\quad -\alpha^{\nu},\ 0,\ -\alpha^{\nu}+\alpha^{n+\nu};\quad -\alpha^{n+\nu},\ -\alpha^{n+\nu}+\alpha^{\nu},\ 0.$$

Au moyen des congruences, faciles à établir,

$$\alpha^{3n+\nu} \equiv -\alpha^{\nu}, \qquad \alpha^{n+\nu} - \alpha^{\nu} \equiv \alpha^{2n+\nu} \pmod{N};$$

on voit immédiatement qu'ils peuvent s'écrire :

$$0,\ \alpha^{\nu},\ \alpha^{n+\nu};\quad 0,\ \alpha^{2n+\nu},\ \alpha^{3n+\nu};\quad 0,\ \alpha^{4n+\nu},\ \alpha^{5n+\nu}. \qquad \text{C. Q. F. D.}$$

Les 2^n systèmes cycliques, déterminés par le système des caractéristiques imprimitives, possèdent chacun le diviseur métacyclique d'ordre $3n$:

$$\{|x, 1+x|, |x, \alpha^{2n}x|\}.$$

De ce résultat découlera plus loin une conséquence importante.

8. Soit maintenant une *autre* caractéristique quelconque. Nous pouvons l'écrire

$\underline{\alpha^a}, \underline{\alpha^b}, \underline{\alpha^c}$ $[a, b, c = 0, 1, 2, \ldots, 3n-1$, et incongrus entre eux $(\mathrm{mod}\, n)]$ (1).

Les puissances de la substitution $|x, \alpha x|$ la transforme en $3n$ caractéristiques *différentes :*

$$(3) \qquad \underline{\alpha^a}, \underline{\alpha^b}, \underline{\alpha^c}; \quad \underline{\alpha^{a+1}}, \underline{\alpha^{b+1}}, \underline{\alpha^{c+1}}; \quad \ldots; \quad \underline{\alpha^{a+3n-1}}, \underline{\alpha^{b+3n-1}}, \underline{\alpha^{c+3n-1}}.$$

En effet, si la même caractéristique se retrouvait deux fois dans cet ensemble, il y aurait deux puissances différentes de $|x, \alpha x|$ transformant $\underline{\alpha^a}$, $\underline{\alpha^b}$, $\underline{\alpha^c}$ dans la même caractéristique. Par suite, une puissance autre que l'identité transformerait $\underline{\alpha^a}$, $\underline{\alpha^b}$, $\underline{\alpha^c}$ en elle-même, et contiendrait donc le cycle $(\underline{\alpha^a}\,\underline{\alpha^b}\,\underline{\alpha^c})$ ou son inverse. Or il n'y a que deux puissances de $|x, \alpha x|$ contenant des cycles de trois éléments, la substitution (2) et son inverse, qui ont pour cycle les caractéristiques imprimitives. Mais, par hypothèse, $\underline{\alpha^a}$, $\underline{\alpha^b}$, $\underline{\alpha^c}$ n'est pas une caractéristique imprimitive.

9. Les $3n$ caractéristiques (3) se répartissent en n *ensembles* ou *carrés* de trois caractéristiques chacun, qui sont imprimitifs vis-à-vis des substitutions du groupe cyclique $\{|x, \alpha x|\}$. Ces carrés sont :

$$(4) \quad \begin{cases} \underline{\alpha^a}, & \underline{\alpha^b}, & \underline{\alpha^c}; & \underline{\alpha^{a+1}}, & \underline{\alpha^{b+1}}, & \underline{\alpha^{c+1}}; & \ldots; & \underline{\alpha^{a+n-1}}, & \underline{\alpha^{b+n-1}}, & \underline{\alpha^{c+n-1}}; \\ \underline{\alpha^{a+n}}, & \underline{\alpha^{b+n}}, & \underline{\alpha^{c+n}}; & \underline{\alpha^{a+n+1}}, & \underline{\alpha^{b+n+1}}, & \underline{\alpha^{c+n+1}}; & \ldots; & \underline{\alpha^{a+2n-1}}, & \underline{\alpha^{b+2n-1}}, & \underline{\alpha^{c+2n-1}}; \\ \underline{\alpha^{a+2n}}, & \underline{\alpha^{b+2n}}, & \underline{\alpha^{c+2n}}; & \underline{\alpha^{a+2n+1}}, & \underline{\alpha^{b+2n+1}}, & \underline{\alpha^{c+2n+1}}; & \ldots; & \underline{\alpha^{a+3n-1}}, & \underline{\alpha^{b+3n-1}}, & \underline{\alpha^{c+3n-1}}. \end{cases}$$

(1) a, b, c peuvent d'ailleurs aussi bien être pris *quelconques:* ils sont seulement les trois incongrus entre eux (mod n).

Dans chacun de ces carrés, trois éléments disposés verticalement forment de nouveau une caractéristique imprimitive (§ 6). Si nous représentons chacune des n caractéristiques imprimitives :

$$\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}: \quad \underline{\alpha^1}, \underline{\alpha^{n+1}}, \underline{\alpha^{2n+1}}; \quad \ldots: \quad \underline{\alpha^{n-1}}, \underline{\alpha^{2n-1}}, \underline{\alpha^{3n-1}},$$

par le chiffre de son rang d'ordre :

$$\mathbf{1}, \mathbf{2}, \ldots, \mathbf{n},$$

les carrés précédents, en commençant par celui où, par exemple dans la troisième rangée verticale, se trouve la première caractéristique imprimitive $\underline{\alpha^0}$, $\underline{\alpha^n}$, $\underline{\alpha^{2n}}$, sont représentés par :

$$\text{(5)} \qquad \mathbf{p}, \mathbf{q}, \mathbf{1}; \quad \mathbf{p}+\mathbf{1}, \mathbf{q}+\mathbf{1}, \mathbf{2}; \quad \ldots; \quad \mathbf{p}+\mathbf{n}, \mathbf{q}+\mathbf{n}, \mathbf{n},$$

p et **q** étant deux des nombres **1**, **2**, ..., **n**, et en entendant par chacun de ces entiers son plus petit reste positif (mod n).

Le groupe des permutations des carrés (4) ou des nouveaux triples (5), par les substitutions du groupe cyclique $\{|\underline{x}, \underline{\alpha x}|\}$, est isomorphe au groupe cyclique $\{(\mathbf{123}\ldots\mathbf{n})\}$.

Remarquons de suite que, lorsque dans les triples (5) les trois éléments sont différents, les neuf éléments dans les carrés correspondants sont différents et peuvent servir à construire un système de caractéristiques. Cela se produit chaque fois que les trois éléments de la première caractéristique $\underline{\alpha^a}$, $\underline{\alpha^b}$, $\underline{\alpha^c}$ sont choisis dans trois caractéristiques imprimitives différentes. Par contre, lorsque deux des éléments de la caractéristique $\underline{\alpha^a}$, $\underline{\alpha^b}$, $\underline{\alpha^c}$ appartiennent à la même caractéristique imprimitive, dans les triples (5) deux éléments sont égaux, et dans un système de caractéristiques, il ne pourra pas entrer deux caractéristiques appartenant au même carré (4).

Recherche des systèmes cycliques de triples différents pour $N = 37$.

10. La recherche des systèmes de caractéristiques est maintenant considérablement simplifiée. Sans chercher à exprimer le procédé sous une forme générale, nous allons l'appliquer directement au cas de $N = 37$ éléments.

Pour $N = 37$, $n = 6$, le nombre des caractéristiques est

$$\frac{(N-1)(N-5)}{12} = 96 \quad (^1).$$

2 est racine primitive de 37. La substitution $|\underline{x}, \underline{2x}|$ est (²)

$$(1\,2\,4\,8\,6'\,5\,0'\,7'\,3\,6\,2'\,3'\,1'\,5'\,7\,4'\,9\,8').$$

Si nous disposons ces caractéristiques en *colonnes* de $3n = 18$ caractéristiques, invariante chacune par les substitutions du groupe cyclique $\{|\underline{x}, \underline{2x}|\}$, comme il a été dit aux paragraphes **8** et **9**, nous avons le tableau suivant (³) :

Caractéristiques imprimitives : 1 0′ 1′, 2 7′ 5′, 4 3 7, 8 6 4′, 6′ 2′ 9, 5 3′ 8′.

Colonnes.....		I.	II.	III.	IV.	V.
(6)	1	2′ 3′ 1	5′ 4′ 1	7 8 1	7 6 1	0′ 9 1
	7	9 8′ 0′	2 8 0′	4 6 0′	4 4′ 0′	1′ 6′ 0′
	3′	6′ 5 1′	7′ 6 1′	3 4′ 1′	3 8 1′	1 2′ 1′
	2	3′ 1′ 2	7 9 2	4′ 6′ 2	4′ 2′ 2	7′ 8′ 2
	8	8′ 1 7′	4 6′ 7′	8 2′ 7′	8 9 7′	5′ 5 7′
	4′	5 0′ 5′	3 2′ 5′	6 9 5′	6 6′ 5′	2 3′ 5′
	3	1′ 5′ 4	4′ 8′ 4	9 5 4	9 3′ 4	3 1 4
	9	1 2 3	8 5 3	6′ 3′ 3	6′ 8′ 3	7 0′ 3
	5′	0′ 7′ 7	6 3′ 7	2′ 8′ 7	2′ 5 7	4 1′ 7
	4	5′ 7 8	9 1 8	8′ 0′ 8	8′ 1′ 8	6 2 8
	0′	2 4 6	6′ 0′ 6	5 1′ 6	5 1 6	4′ 7′ 6
	6′	7′ 3 4′	2′ 1′ 4′	3′ 1 4′	3′ 0′ 4′	8 5′ 4′
	5	7 4′ 6′	8′ 2 6′	1 7′ 6′	1 5′ 6′	2′ 4 6′
	1′	4 8 2′	5 7′ 2′	0′ 5′ 2′	0′ 2 2′	9 3 2′
	7′	3 6 9	3′ 5′ 9	1′ 2 9	1′ 7′ 9	6′ 7 9
	6	4′ 9 5	1 4 5	2 3 5	2 7 5	3′ 8 5
	2′	8 6′ 3′	0′ 3 3′	7′ 7 3′	7′ 4 3′	8′ 6 3′
	8′	6 2′ 8′	1′ 7 8′	5′ 4 8′	5′ 3 8′	5 4′ 8′

(¹) Voir notre premier travail, première partie, p. 60. Le nombre des caractéristiques est égal au nombre des triples situés à l'intérieur du triangle AOC′. Le nombre des triples situés sur une médiane est $\frac{N-1}{2}$. Celui des triples situés à l'intérieur du triangle AOB est $\frac{(N-1)(N-2)}{6} - \frac{N-1}{2} = \frac{(N-1)(N-5)}{6}$. Celui des caractéristiques sera $\frac{(N-1)(N-5)}{12}$.

(²) Les éléments 10, 11, ..., 18 sont notés 0′, 1′, ..., 8′.

(³) Nous indiquons par les chiffres placés à gauche de la barre verticale le rang d'ordre des caractéristiques, dans leur déduction de la caractéristique de tête correspondante par les puissances de $|\underline{x}, \underline{2x}|$.

et en représentant chaque caractéristique imprimitive par son rang d'ordre, comme plus haut :

(7)

Colonnes.....	I.	II.	III.	IV.	V.
	561	241	341	341	151
	612	352	452	452	262
	123	463	563	563	313
	234	514	614	614	424
	345	625	125	125	535
	456	136	236	236	646

Nous avons disposé ici verticalement les carrés (4) et les triples (5) écrits horizontalement dans le paragraphe **9**. A cela près, nous avons suivi *en tout* l'ordre des notations précédentes, en faisant $\alpha = 2$, par exemple pour l'ordre des éléments dans les caractéristiques imprimitives, etc.

Nous avons commencé, dans chaque colonne, la rangée verticale de droite par la caractéristique imprimitive $\underline{2^0}$, $\underline{2^6}$, $\underline{2^{12}}$, comme dans les triples (5).

11. L'existence et les propriétés de ces colonnes sont, en principe, *indépendantes* du nombre $N = 6n + 1$, premier (ou de la forme p^m). En effet, les puissances de la substitution $|\underline{x}, \underline{\alpha x}|$ sont les substitutions $|\underline{x}, \underline{mx}|$, m entier positif quelconque, et une caractéristique $a, b, a + b$ $(a + b \leqq 3n)$, pour N éléments, est encore une caractéristique pour un N supérieur. Cette étude des propriétés de l'ensemble des caractéristiques, au moyen du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, fera l'objet d'un autre travail. Nous remarquons ici seulement que :

La colonne V a deux éléments appartenant à la même caractéristique imprimitive dans la caractéristique de tête [ou deux éléments égaux dans les triples (7)]; dans un système de caractéristiques, il n'entrera donc pas deux caractéristiques appartenant au même de ses carrés.

Les colonnes III et IV ne diffèrent que par le déplacement d'un élément dans la rangée verticale du milieu ($\underline{2^3} = 8$ et $\underline{2^9} = 6$); leurs carrés homologues ont ainsi les mêmes éléments et peuvent se substituer l'un à l'autre pour construire un système de caractéristiques.

La colonne I présente, pour le moment du moins, le plus d'intérêt. Ses deux premières rangées verticales contiennent les $3n$ couples qui n'entrent qu'une fois dans une caractéristique, tandis que les autres couples des éléments $1, 2, \ldots, 3n$ entrent chacun dans deux caractéristiques de l'ensemble. Cela permet déjà d'établir quelques théorèmes relatifs au groupe de substitutions qui appartient à l'ensemble des caractéristiques. Nous indiquerons le premier :

Pour $N = 6n + 1$ *premier, pour lequel* $3n$ *est le plus petit exposant qui rend* $2^{3n} = 1 \pmod N$, *le groupe qui appartient à l'ensemble des caractéristiques est le groupe* $\{|x, \alpha x|\}$, α *racine primitive de* N.

12. Tout système de caractéristiques qui contient une caractéristique imprimitive, ou une caractéristique de l'une des colonnes, se transforme par une puissance de $|x, 2x|$ en un système qui contient une caractéristique imprimitive donnée, ou une caractéristique fixée de cette colonne. Il nous suffira donc d'obtenir, par exemple, les systèmes contenant la caractéristique imprimitive $10'1'$, et pour chaque colonne ceux contenant la caractéristique de tête; avec les substitutions du groupe $\{|x, 2x|\}$, nous en déduirons tous les systèmes de caractéristiques possibles. Nous appellerons systèmes de caractéristiques *différents*, ceux qui ne sont pas équivalents par les substitutions du groupe $\{|x, 2x|\}$; nous verrons que, aussi dans la suite, ce sont les seuls qu'il nous importe de connaître.

13. Voici le tableau de ces systèmes différents pour notre cas de $N = 37$. Le procédé suivi pour les obtenir découle à peu près déjà de l'ordre dans lequel ils sont écrits; nous donnons d'ailleurs en Note plus bas le détail de la recherche. Les systèmes 1, 2, 3, 4, 5, 12, 13 et 14 s'obtiennent et s'écrivent sans autre; pour les autres, nous notons les caractéristiques par le chiffre de leur colonne et en indice leur rang d'ordre [écrit à gauche dans le tableau (6)] dans leur déduction de la caractéristique de tête par les puissances de $|x, 2x|$. Le groupe $\{(123\ldots3n)\}$ est isomorphe au groupe $\{|x, 2x|\}$. Lorsque, dans une

colonne, deux caractéristiques appartiennent au même carré, elles sont entre parenthèses.

A. — *Systèmes contenant des caractéristiques imprimitives.*

								Systèmes équivalents.
1.	Le système des caractéristiques imprimitives							1
2.	Trois caractéristiques imprimitives et le carré de la colonne I contenant les trois autres							6
3, 4, 5.	Même formation avec un carré des colonnes II, III et IV							18
6.	Deux caractéristiques imprimitives	$10'1'$, $27'5'$, I_5, $I_{8'}$, $II_{9'}$, IV_3						18
7.		$10'1'$, $864'$, II_5, $II_{1'}$, III_3, $III_{2'}$						9
8.	Une caractéristique imprimitive	$10'1'$	I_6	–	$III_{2'}$	$IV_{8'}$	V_4V_5	18
9.		–	–	$II_{4'}$	–	$IV_{2'}$	$V_4V_7V_{8'}$	18
10.		–	I_5	$II_{1'}$	–	$IV_3IV_{8'}$	V_4	18
11.		–	–	$II_{5'}$	$(III_2III_8)III_3$	$IV_{8'}$	–	18

B. — *Systèmes ne contenant pas de caractéristiques imprimitives.*

12.	Le système des premier et quatrième carrés de la colonne I						3
13, 14.	Les deux systèmes formés du premier carré de II et du troisième carré de III ou IV						12
15.	Systèmes contenant au moins deux caractéristiques de la colonne V	$I_{3'}$	$II_3II_{4'}$	$III_{2'}$	–	V_1V_4	18
16.		–	$II_9II_{8'}$	–	–	$V_1V_{0'}V_5V_4$	9
17.		$I_{0'}I_{2'}$	–	$III_{3'}III_{5'}$	–	V_1V_8	18
18.		$I_{1'}$	$II_5II_{5'}$	$III_{3'}$	–	V_1V_8	18
19.		$I_3I_{2'}$	–	$III_6III_{5'}$	–	$V_1V_{0'}$	9
20.	Systèmes contenant deux caractéristiques de la colonne I, et non obtenus dans les précédents	$(I_3I_{5'})I_1I_6$	–	–	IV_9	V_4	18
21.		I_1I_4	$II_{0'}$	$III_3III_{3'}$	–	V_2	18
22.		I_1I_5	$II_3II_{0'}$	III_6	$IV_{7'}$	–	18
23.		I_1I_5	$(II_7II_{3'})$	III_3	$IV_{8'}$	–	18
24.	Systèmes contenant deux caractéristiques de la colonne II, non encore obtenus	–	II_1II_5	$III_8III_{0'}$	IV_3	V_9	18
25.		$I_{8'}$	$II_1II_2II_{1'}$	–	$IV_{2'}$	V_7	18
26.		–	$II_1II_2II_9$	III_7III_9	IV_4	–	18
27.		–	$II_4II_{0'}$	–	$(IV_3IV_{5'})IV_{3'}$	V_2	18
28.	Systèmes contenant deux caractéristiques de la colonne III, non encore obtenus	I_7	$II_{4'}$	$III_1III_2III_{0'}$	$IV_{2'}$	–	18
29.		I_2	–	$III_1III_3III_{1'}$	IV_9	$V_{0'}$	18
30.		I_7	$II_{6'}$	III_1III_6	$IV_2IV_{4'}$	–	18
31.	Systèmes contenant deux caractéristiques de la colonne IV, non encore obtenus	$I_{3'}$	$II_{2'}$	$III_{8'}$	$IV_1(IV_2IV_8)$	–	18
32.		$I_{4'}$	–	III_2	$IV_1IV_4IV_{2'}$	$V_{1'}$	18
						Total.....	445

Nous indiquons à droite, pour chaque système différent, le nombre des systèmes équivalents par les 18 substitutions du groupe $\{|x, 2x|\}$. Dès qu'un système n'a qu'une caractéristique dans l'une des colonnes,

il a nécessairement 18 systèmes équivalents; dans les quelques autres cas (2, 3, 4, 5, 7, 12, 13, 14, 16, 19), le nombre des systèmes équivalents est ou immédiatement donné, ou immédiatement déterminable par les caractéristiques d'une colonne (*voir* la Note).

Note contenant le détail de la recherche. — **1.** Un système ne peut contenir *cinq caractéristiques imprimitives* sans contenir la sixième.

2. Un système ne peut contenir *quatre caractéristiques imprimitives*, car les deux autres caractéristiques ne pourraient être prises que dans la colonne V, les deux dans le même carré, ce qui est impossible, ou chacune dans un carré différent, ce qui est également impossible [deux triples (7) dans la même colonne ont toujours au moins trois éléments différents].

3. Un système qui contient *trois caractéristiques imprimitives* ne peut être complété qu'avec le carré, qui contient les trois autres caractéristiques imprimitives, si ce carré existe. Car, dans le cas contraire, il faudrait le compléter avec des caractéristiques prises dans deux ou trois carrés différents des colonnes I à V, et n'ayant aucun des éléments des trois caractéristiques imprimitives données. Il faudrait donc que les triples (7), représentant ces deux ou trois carrés, ne contiennent que les mêmes trois éléments. Or, dans les colonnes (7), il n'y a :

Deux triples contenant les mêmes éléments que dans la troisième et la quatrième, chaque triple de l'une avec l'homologue de l'autre, et dans ce cas, il n'est possible que d'y prendre deux caractéristiques sans élément commun;

Deux ou trois triples formés des mêmes trois éléments que dans la dernière, les trois triples **151**, **313**, **535** ou **262**, **424**, **646**, et dans ce cas encore, on voit immédiatement qu'on ne peut y trouver une caractéristique dans chacun des trois triples, sans avoir deux fois le même élément.

4. Inversement, un système construit avec un carré de l'une des colonnes I, II, III, IV ne peut être complété qu'avec trois caractéristiques imprimitives, ou avec le carré constitué de ces trois caractéristiques imprimitives, si ce carré existe. Autrement le système est impossible, pour les mêmes raisons que celles de la démonstration précédente.

5. La recherche des systèmes différents contenant *deux caractéristiques imprimitives* se réduit à ceci : les couples des éléments **1**, **2**, **3**, **4**, **5**, **6**, représentant les caractéristiques imprimitives, se répartissent en trois séries imprimitives :

12, **23**, **34**, **45**, **56**, **61**,
13, **24**, **35**, **46**, **51**, **62**,
14, **25**, **36**,

par les substitutions du groupe $\{(123456)\}$, triplement isomorphe au

groupe $\{|x, 2x|\}$. Il nous suffit donc d'obtenir les systèmes possibles avec les couples de caractéristiques imprimitives **12**, **13**, **14**.

6. La recherche des systèmes contenant *une caractéristique imprimitive*, $10'1'$, est un peu plus longue. Il suffit naturellement d'essayer avec $10'1'$ une seule caractéristique de chaque carré, dont le triple (7) ne contient pas l'élément **1**.

7. Un système, qui ne contient plus de caractéristiques imprimitives, contient nécessairement *deux caractéristiques* de l'une au moins des colonnes I à V. *Représentons les caractéristiques* d'une colonne *par leur rang d'ordre*, dans leur déduction de la caractéristique de tête. Les substitutions du groupe $\{(1\,2\,3\ldots8')\}$, isomorphe au groupe $\{|x, 2x|\}$, laissent imprimitifs les couples suivants des éléments $1, 2, \ldots, 8'$, contenant l'élément **1** :

$$12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 10'.$$

De ces couples de caractéristiques, les seuls à prendre en considération dans notre recherche, parce que contenant six éléments différents, sont :

$$(8)\qquad \begin{cases} \text{Pour la colonne I.....} & 13,\ 14,\ 15,\ 16,\ 17,\ 10'. \\ \text{» II....} & 12,\ 15,\ 17,\ 18,\ 19,\ 10'. \\ \text{» III...} & 12,\ 13,\ 16,\ 17,\ 19,\ 10'. \\ \text{» IV...} & 12,\ 13,\ 14,\ 17,\ 18,\ 19. \\ \text{» V....} & 12,\ 14,\ 15,\ 16,\ 18,\ 10'. \end{cases}$$

Nous avons effectué la recherche avec les colonnes dans cet ordre : V, I, II, III, IV, en essayant donc successivement chacun des couples précédents de caractéristiques de la colonne V, puis de la colonne I, II, etc. Dès que l'on a deux caractéristiques données, il est vite fait d'éliminer (dans la même colonne et dans les quatre autres) les caractéristiques ayant avec elles un élément commun ; il ne reste jamais qu'un nombre restreint de caractéristiques, et la recherche pour chacun des couples (8) est l'affaire de quelques instants.

Le procédé a en outre l'avantage de se vérifier lui-même. En effet, chaque système doit être trouvé plus d'une fois dans cette recherche. Par exemple, le système 16 doit être trouvé quatre fois dans la recherche pour la colonne V [car la combinaison d'indices $10'5\,4'$, par les substitutions du groupe $\{(1\,2\,3\ldots8')\}$, prend les deux formes contenant 1, $10'5\,4'$ et $10'6\,5'$, et le système doit être trouvé deux fois avec le couple (8) $10'$, une fois avec le couple 15 et une fois avec le couple 16] et une fois dans la recherche pour la colonne II. Il est aisé d'établir combien de fois et où chaque système doit être trouvé, et si, la recherche faite, chaque système a été trouvé en place et le nombre de fois voulu, on peut être sûr de l'opération.

La recherche des systèmes contenant des caractéristiques imprimitives a été

vérifiée également, en la répétant une seconde fois avec des caractéristiques imprimitives différentes.

14. Soit maintenant l'un quelconque des 32 systèmes de caractéristiques différents, que nous venons d'obtenir. Représentons ses six caractéristiques par les lettres

(9) $$a,\ b,\ c,\ d,\ e,\ f.$$

Chacune de ces caractéristiques détermine les deux séries cycliques conjuguées correspondantes, et le système donne 2^6 systèmes cycliques de triples de Steiner. Soit l'un quelconque de ces systèmes :

(10) $$A,\ B,\ C,\ D,\ E,\ F.$$

Nous représentons par A, B, ..., F ses séries cycliques. Rappelons que les substitutions $|x,\ \alpha x|$ et $|\underline{x},\ \underline{\alpha x}|$ changent respectivement une série cyclique en une série cyclique et la caractéristique de la première dans la caractéristique de la seconde.

Lorsque la substitution $|\underline{x},\ \underline{2x}|$ transforme le système de caractéristiques (9) en un système de caractéristiques :

(11) $$a',\ b',\ c',\ d',\ e',\ f',$$

la substitution $|x,\ 2x|$ transforme le système de triples (10) en un système de triples :

(12) $$A',\ B',\ C',\ D',\ E',\ F',$$

dont les caractéristiques sont les caractéristiques précédentes. Inversement, lorsque la substitution $|x,\ 2x|$ transforme le système de triples (10) en un système de triples (12), la substitution $|\underline{x},\ \underline{2x}|$ transforme les caractéristiques (9) dans les caractéristiques (11).

Admettons maintenant le théorème que deux systèmes cycliques de triples équivalents sont déductibles l'un de l'autre par une substitution métacyclique, et rappelons les données de l'introduction (1). Nous avons les résultats suivants :

---

(1) Le groupe métacyclique est produit par les deux substitutions $|x,\ 1+x|$ et $|x,\ \alpha x|$. La substitution $|x,\ 1+x|$ laisse invariable le système cyclique de

1° Deux systèmes de triples déterminés par deux systèmes de caractéristiques différents sont *différents*. Autrement, une puissance de $|x, 2x|$ transformerait l'un des systèmes de triples dans l'autre, et une puissance de $|\underline{x}, \underline{2x}|$ transformerait l'un dans l'autre les deux systèmes de caractéristiques correspondants.

2° Si la première puissance de $|\underline{x}, \underline{2x}|$ qui transforme le système de caractéristiques (9) en lui-même, est

$$|\underline{x}, \underline{2x}|^{3n} = |\underline{x}, \underline{2^{3n}x}| = |\underline{x}, \underline{x}|,$$

la première puissance de $|x, 2x|$, qui transforme le système de triples (10) en un système de mêmes caractéristiques, est

$$|x, 2x|^{3n} = |x, -x| = |x, \mathrm{N}-x|.$$

Cette puissance $|x, 2x|^{3n}$ transforme le système (10) dans le système conjugué (1), et la puissance $|x, 2x|^{6n}$ le transforme en lui-même. Le système de triples (10) ne possède alors que le diviseur cyclique $\frac{1}{3}|x, 1+x|\frac{1}{3}$ (2) et 2^5 *systèmes de triples* déterminés par les caractéristiques (9) sont nécessairement *différents*.

3° Si la première puissance de $|\underline{x}, \underline{2x}|$, qui transforme le système de caractéristiques (9) en lui-même, est $|\underline{x}, \underline{2x}|^d$, $d < 3n$ et diviseur de $3n$, $|x, 2x|^d$ est la première puissance de $|x, 2x|$, qui transforme le système de triples (10) en un système de mêmes caractéristiques. Ce système de triples transformé n'est pas le système (10) lui-même, d étant diviseur de $3n$, car $|x, 2x|^{3n}$ transformerait le système (10) en

---

triples. Par suite, avec le théorème admis, deux systèmes cycliques équivalents sont déductibles l'un de l'autre par une puissance de $|x, \alpha x|$. Autrement dit, les systèmes de triples qui ne se trouvent pas dans les transformées de (10), par les puissances de $|x, 2x|$, sont *différents* du système (10).

(1) Nous appelons systèmes *conjugués*, les deux systèmes de triples formés des séries respectivement conjuguées. Rappelons encore qu'une substitution métacyclique change deux séries conjuguées en deux séries conjuguées (Introduction, 4°), et donc deux systèmes cycliques conjugués en deux systèmes conjugués.

(2) En tant que substitutions du groupe métacyclique, mais je ne puis pas assurer qu'il n'y a pas de substitutions, autres que métacycliques, qui transforment le système (10) en lui-même.

lui-même, ce qui n'est pas. Il n'est pas non plus le conjugué du système (10), si $2d$ est diviseur de $3n$, pour la même raison qu'avant, puisque dans ce cas $|x,\ 2x|^{2d}$ transformerait le système (10) en lui-même.

Pour $n=6$, $3n=18$, $2d$ est diviseur de $3n$ pour les diviseurs $d=1, 3, 9$. Donc le 1er, le 3^{e} et le 9^{e} transformé d'un système (10) par la substitution $|x,\ 2x|$, ne peuvent être le conjugué de ce système (10). Il reste les diviseurs 2 et 6; seuls le 2^{e} et le 6^{e} transformé d'un système (10), peuvent être, avant le 18^{e}, le conjugué de (10) (1).

15. Par conséquent, pour les systèmes de caractéristiques suivants, le système (9) étant successivement chacun de ces systèmes, nous aurons :

Systèmes 7, 16, 19; $d=9$. — Le 9^{e} transformé d'un système (10) par $|x,\ 2x|$ est de mêmes caractéristiques que (10), mais $|x,\ 2x|^{18}$ est la première puissance qui donne le conjugué de (10). Chacun de ces systèmes détermine donc 2^{1} *systèmes de triples différents*, possédant uniquement le diviseur cyclique $\{|x,\ 1+x|\}$.

Systèmes 2, 3, 4, 5; $d=6$. — Le 6^{e} transformé d'un système (10) peut être son conjugué. Avec chacun de ces systèmes (9), nous trouvons que, pour huit systèmes (10), le 6^{e} transformé est le conjugué, et pour huit autres, $|x,\ 2x|^{18}$ est la première puissance qui donne le conjugué (2). Chacun de ces systèmes détermine 2^{4} *systèmes de triples*

(1) Si le 2^{e} transformé est le conjugué du système (10), naturellement le 6^{e}, le 10^{e} et le 14^{e} le seront également, avant le 18^{e}.

(2) Cette recherche ne demande plus qu'un temps minime pour chaque système de caractéristiques en question. Nous l'effectuerons comme exemple avec le système 2.

Le premier système de triples que détermine le système 2, c'est-à-dire le système des six séries cycliques *directes* (prises dans le triangle AOC'; *voir* notre premier travail, p. 60), est

(13) $$013',\ 027',\ 037,\ 056',\ 064',\ 099'.$$

Nous n'écrivons que le triple de tête de chaque série. Formons la puissance $|x,\ 2x|^{6}$; par cette substitution, ces six triples se changent en six autres

différents; huit d'entre eux possèdent le diviseur métacyclique d'ordre $3 \times 37 = 111$

$$\{|x, 1+x|, |x, 2^{12}x|\},$$

et les huit autres n'ont que le diviseur cyclique $\{|x, 1+x|\}$.

Systèmes 13 *et* 14; $d = 6$. — Le 6^e transformé d'un système (10) peut encore être le conjugué. Avec chacun de ces systèmes (9), nous trouvons que, pour deux systèmes (10), le 6^e transformé est le conjugué, et pour dix autres, $|x, 2x|^{18}$ est la première puissance qui donne le conjugué. Chacun de ces systèmes détermine donc 12 *systèmes de triples différents;* deux d'entre eux possèdent le diviseur

---

contenant encore l'élément o, et qui nous donnent sans autre la série transformée de chacune des précédentes. Cette série transformée ne peut d'ailleurs être que l'une de ces mêmes séries (13) ou l'une des conjuguées. En remarquant toujours que la substitution métacyclique $|x, 2x|^6$ change deux séries conjuguées en deux séries conjuguées, *cette première transformation suffit pour notre tableau,* que nous écrirons en omettant l'élément o et faisant ressortir les séries conjuguées :

Système direct.		13′.	27′.	37.	56′.	64′.	99′.	B_0.	B_1.	B_2.	B_3.	B_4.	B_5.
Transformés.	6^e...	99′	**22″**	**33‴**	13′	**69″**	**56″**	B'_{16}	B'_1	B'_{126}	B'_{361}	B'_6	B'_{156} ...
	12^e...	**56″**	27′	37	99′	64′	**15″**	B_{11}		B_{124}	B_{134}	B_{116}	B_{145} ...
	18^e...	**15″**	**22″**	**33‴**	**56″**	**69″**	**97″**	B'_0		B'_2	B'_3	B'_4	B'_5 ...

Pour écrire le 12^e transformé, par exemple, 99′ devient **56″**, **22″** devient 27′ puisque 27′ devient **22″**, etc.

Désignons par B_0 le système (13), par $a_1, a_2, a_3, a_4, a_5, a_6$ ses séries cycliques, par B_i, B_{ik}, B_{1ik} ($i, k = 1, 2, 3, 4, 5, 6$) les systèmes obtenus en remplaçant, dans B_0, respectivement la série a_i; les deux séries a_i, a_k; les trois séries a_1, a_i, a_k; par les conjuguées; enfin par B'_i, B'_{ik}, B'_{1ik}, les systèmes conjugués respectifs (B_1 a pour conjugué $B_{23456} = B'_1$, etc.).

Les quatre systèmes précédents sont ainsi B_0, B'_{16}, B_{11}, B'_0. Prenons maintenant B_1, c'est-à-dire remplaçons la première rangée verticale du tableau par les séries conjuguées. *Sans rien écrire,* nous voyons que le 6^e transformé est déjà B'_1. Nous prenons ensuite B_2, c'est-à-dire nous remplaçons la deuxième rangée verticale par les conjuguées, nous trouvons B'_{126}, B_{124}, B'_2, puis nous prenons B_3, B_4, etc., c'est-à-dire chaque fois un système qui n'a pas encore été obtenu, *lui* ou *son conjugué*, et nous continuons ainsi jusqu'à épuisement des 2^5 systèmes *directs* B_i, B_{ik} et B_{1ik}.

métacyclique

$$\{|x,\ 1+x|,\ \ |x,\ 2^{12}x|\},$$

et les dix autres n'ont que le diviseur cyclique $\{|x,\ 1+x|\}$.

Système 12; $d=3$. — Le 3e transformé d'un système (10) ne peut pas être le conjugué, mais le 6e transformé pourra être le conjugué de (10). Pour cinq systèmes (10), $|x,\ 2x|^{18}$ est la première puissance qui donne le conjugué, et pour un seul, le 6e transformé est son conjugué. Ce système détermine *six systèmes de triples différents;* cinq n'ont que le diviseur cyclique $\{|x,\ 1+x|\}$, et le sixième a le diviseur métacyclique

$$\{|x,\ 1+x|,\ \ |x,\ 2^{12}x|\}.$$

Systèmes des caractéristiques imprimitives, $d=1$. — Tous les transformés d'un système (10) sont des systèmes de mêmes caractéristiques. D'autre part, on sait (§ **7**), que ce système (10) possède le diviseur métacyclique d'ordre 3N

$$\{|x,\ 1+x|,\ \ |x,\ \alpha^{2n}x|\},$$

c'est-à-dire que la puissance $|x,\ \alpha x|^{2n}$ le transforme en lui-même. On aura donc pour $N=6n+1$ *premier, au moins* $\left[\frac{2^n}{2n}\right]=\left[\frac{2^{n-1}}{n}\right]$ *systèmes de triples différents, fournis par le système des caractéristiques imprimitives*, en entendant ici par ces crochets le premier entier égal ou *supérieur* à $\frac{2^{n-1}}{n}$. Dans notre cas, $\left[\frac{2^{n-1}}{n}\right]=6$; nous trouvons en effet cinq systèmes (10), pour qui la puissance $|x,\ 2x|^6$ est la première qui donne le conjugné, ayant donc le diviseur métacyclique

$$\{|x,\ 1+x|,\ \ |x,\ 2^{12}x|\},$$

et un système pour lequel la puissance $|x,\ 2x|^2$ donne déjà le conjugué et qui a le diviseur métacyclique d'ordre $9\times 37=333$

$$\{|x,\ 1+x|,\ \ |x,\ 2^4x|\}.$$

La recherche des systèmes cycliques de triples différents pour $N=37$ est ainsi terminée. Nous obtenons

$21\times 2^5+3\times 2^4+4\times 2^3+2\times 12+6+6=820$ *systèmes cycliques différents.*

Recherche des systèmes cycliques de triples différents pour N = 43.

16. Nous avons appliqué également le procédé au cas N = 43 éléments en suivant une marche en tout pareille à celle qui vient d'être exposée. Nous ne donnerons maintenant plus que les résultats :

Pour N = 43, $n = 7$, le nombre des caractéristiques est

$$\frac{(N-1)(N-3)}{12} = 133.$$

La recherche a été faite avec la substitution $|x, \underline{3x}|$, 3 étant racine primitive de 43. Nous obtenons 157 *systèmes de caractéristiques différents*.

140 *systèmes* ne possèdent que l'identité (¹) : $d = 3n = 21$. Ils déterminent donc chacun 2^6 systèmes de triples différents, ne possédant que le groupe cyclique $\{|x, 1+x|\} = \{s\}$.

15 *systèmes* ont le diviseur $\{|x, \underline{3^7x}|\}$: $d = 7$. $2d$ n'est pas diviseur de $3n$; donc le 7ᵉ transformé d'un système de triples peut être son conjugué. Autrement dit un système de triples déterminé par l'un de ces systèmes de caractéristiques peut posséder un diviseur du groupe métacyclique autre que le groupe $\{s\}$. Ces systèmes de caractéristiques sont *de deux types*, comme plus haut (§ 15) ceux pour lesquels $d = 6$. Cinq d'entre eux donnent chacun 32 systèmes de triples différents : 16 n'ayant que le diviseur cyclique $\{s\}$ et 16 ayant le diviseur métacyclique

$$\{|x, 1+x|, \ |x, 3^{14}x|\}.$$

Les dix autres donnent chacun 24 systèmes de triples différents : 20 n'ayant que le groupe cyclique $\{s\}$ et 4 le diviseur métacyclique précédent.

1 *système* a le diviseur $\{|x, \underline{3^3x}|\}$: $d = 3$. $2d$ n'est pas diviseur

(¹) En tant que substitutions du groupe cyclique $\{|x, \underline{3x}|\}$, mais de nouveau je ne puis pas assurer qu'il n'y a pas de substitutions, autres que celles de ce groupe, qui transforment l'un de ces systèmes de caractéristiques en lui-même.

de $3n$: un système de triples déterminé par ce système pourra posséder le diviseur métacyclique

$$\{|x, 1+x|, \quad |x, 3^6 x|\}.$$

On trouve 10 systèmes de triples différents, 9 n'ayant que le groupe $\{s\}$, et 1 possédant le diviseur métacyclique indiqué.

1 *système* (système des caractéristiques imprimitives) a le groupe entier $\{|\underline{x}, \underline{3x}|\}$; $d=1$. Il donne au moins $\left[\frac{2^{n-1}}{n}\right] = 10$ systèmes de triples différents. On trouve en effet dix systèmes différents, neuf n'ayant que le groupe $\{s\}$ et le dixième le diviseur métacyclique

$$\{|x, 1+x|, \quad |x, 3^2 x|\}.$$

Nous obtenons ainsi pour $N = 43$:

$140 \times 2^6 + 5 \times 2^5 + 10 \times 24 + 10 + 10 = 9380$ *systèmes de triples différents.*

Conclusion.

Nous résumerons dans le tableau suivant, nos résultats obtenus jusqu'ici dans cette recherche des systèmes cycliques de triples différents pour $N = 6n + 1$.

Nous désignons par :

S le nombre des systèmes cycliques de triples différents;
S′ le nombre des systèmes de caractéristiques;
S″ le nombre des systèmes de caractéristiques différents.

Ce tableau est :

$N = 6n+1$.	n.	S″.	S′.	S.
7	1	1	1	1
13	2	1	1	1
19	3	2	4	4
31	5	8	64	80
37	6	32	745	820
43	7	157	3049	9380
25 (1)	4	2	15	17

(1) Nous mettons à part le cas $N = 25$, parce que non premier.

La recherche des systèmes cycliques différents pour les premières valeurs de N, jusqu'à $N = 31$, laborieuse dans notre premier travail, n'aurait été qu'un jeu avec l'introduction du groupe $\{|\underline{x}, \underline{\alpha x}|\}$. Même pour $N = 31$, l'existence des 8 systèmes de caractéristiques différents, déterminant immédiatement les 80 systèmes de triples différents (en 8 groupements distincts; *voir* fin de l'Introduction), se reconnaît très vite dans le tableau (6) correspondant, à quatre colonnes de caractéristiques.

Nous avons donc un procédé permettant d'obtenir encore, avec un peu de temps, les systèmes cycliques de triples différents pour les valeurs immédiatement suivantes de N : 49, 61, 67, etc., et surtout, fournissant déjà, *pour* $N = 6n + 1$ *premier*, indéfiniment grand, un nombre *indéfini* de systèmes de triples différents. Nous entendons par là, non seulement les $\left[\frac{2^{n-1}}{n}\right]$ systèmes de triples différents, déterminés par le système des caractéristiques imprimitives, mais, par exemple, également les systèmes de triples différents déterminés par les systèmes de caractéristiques différents constitués d'un carré d'une des $n - 1$ colonnes du tableau (6) (1) et des $n - 3$ caractéristiques imprimitives restantes (2), les systèmes de triples différents déterminés par les systèmes de caractéristiques différents, constitués de deux carrés d'une colonne du tableau (6) (3) et des $n - 6$ caractéristiques imprimitives restantes, etc. Ainsi l'étude du tableau (6) des colonnes de caractéristiques, engendrées par le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ donnera déjà, avec N croissant, un nombre très grand de systèmes de caractéristiques différents *immédiats*, et comme il a été dit au paragraphe **11**,

(1) Il faut excepter de ce raisonnement les colonnes (colonne V) ayant dans la caractéristique de tête deux éléments appartenant à la même caractéristique imprimitive.

(2) Ces systèmes de caractéristiques ont le diviseur $\{|\underline{x}, \underline{\alpha^n x}|\}$. Chacun détermine donc encore au moins $\left[\frac{2^{n-1}}{n}\right]$ systèmes de triples différents.

(3) Dès que $n > 7$, dans chaque colonne du tableau (7), il y a certainement deux triples entièrement différents; les deux carrés correspondants contiendront les éléments de six caractéristiques imprimitives. Dès que $n > 14$, il y aura dans chaque colonne de (7) trois triples entièrement différents, etc.

elle fera l'objet d'un travail ultérieur. Nous devons seulement reconnaître, encore une fois, en terminant, que la démonstration du théorème à la base de l'obtention des *systèmes de triples différents* est encore à faire (¹); cependant, même indépendamment de ce théorème et de la question des systèmes de triples différents, les résultats obtenus dans ce travail pour la construction des *systèmes de caractéristiques*, autrement dit pour la solution du problème de Heffter (*voir* notre premier travail, p. 58), ont déjà leur intérêt.

(¹) Quoique, nous le répétons encore, pour des raisons de la théorie des groupes, le théorème *doit exister*, si ce n'est sous la forme générale que nous lui avons donnée, du moins, dans le cas de deux systèmes cycliques de triples équivalents.

BIBLIOTHÈQUE NATIONALE R F IMPRIMÉS