ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

S. BAYS

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

Annales de la faculté des sciences de Toulouse 3^e série, tome 17 (1925), p. 23-61

<http://www.numdam.org/item?id=AFST_1925_3_17__23_0>

SUR LES SYSTÈMES CYCLIQUES DE TRIPLES DE STEINER DIFFÉRENTS

POUR N PREMIER

(ou puissance de nombre premier) de la forme $6n + 1$

PAR M. S. BAYS.

INTRODUCTION

[1] Dans notre second Mémoire sur les systèmes cycliques de triples de Steiner(1), nous avons ramené l'obtention des systèmes cycliques de triples de Steiner *différents*, pour $N = 6n + 1$ premier ou puissance de nombre premier, à l'obtention des systèmes de caractéristiques *différents*, c'est-à-dire non déductibles l'un de l'autre par une substitution du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, ($\alpha$ appartenant à l'exposant $\varphi(N)$ mod. N).

Dans le présent Mémoire, nous faisons l'étude des propriétés de l'ensemble des caractéristiques vis-à-vis du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, pour $N = 6n + 1$ premier ou puissance de nombre premier, et nous obtenons de ce fait une part importante de ces systèmes de caractéristiques différents.

[2] Nous rappelons les données essentielles du Mémoire précédent qui nous sont nécessaires pour notre exposé :

---

(1) 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, t. II, 1923, fascicule 1.

Notre premier Mémoire : *Sur les systèmes cycliques de triples de Steiner*, est dans les Annales de l'École normale supérieure (3), XL, février et mars, 1923.

La lecture préalable de ces deux Mémoires rendrait la lecture de celui-ci aisée et complète. Nous les désignerons dans la suite, pour nos références, simplement par les lettres A et J.

Un exposé du problème même des *triples de Steiner* est donné dans E. Netto, Lehrbuch der Combinatorik, 1901, p. 202 à 218. D'autre part toutes les références aux travaux essentiels sur la question sont données dans nos deux Mémoires, principalement dans A.

Les résultats du présent Mémoire ont été publiés dans une Note aux *Comptes Rendus* (t. CLXXV, p. 936, 20 novembre 1922).

1° L'ensemble des caractéristiques pour $N = 6n + 1$, premier ou puissance de nombre premier, est l'ensemble des triples des éléments $1, 2, \ldots, 3n$, sans répétition, dans lesquels ou bien la somme de deux éléments est égale au troisième élément, ou bien la somme des trois éléments est égale à N.

2° Un *système* de caractéristiques est un ensemble de n caractéristiques contenant les $3n$ éléments $1, 2, \ldots, 3n$, autrement dit, un ensemble de n caractéristiques sans élément commun. Un système de caractéristiques détermine 2^n systèmes cycliques de triples de Steiner, parmi lesquels 2^{n-1} sont éventuellement différents.

3° Nous avons désigné par $\underline{a}$ la valeur absolue du plus petit reste positif ou négatif de l'entier a mod. N. — α appartenant à l'exposant $\varphi(N)$ mod. N, $\underline{\alpha^0}, \underline{\alpha^1}, \ldots, \underline{\alpha^{3n-1}}$, sont les $3n$ éléments, $1, 2, \ldots, 3n$; $\underline{\alpha^{3n}}, \underline{\alpha^{3n+1}}, \underline{\alpha^{3n+2}}, \ldots$, les reproduisent indéfiniment dans le même ordre $\underline{\alpha^0}, \underline{\alpha^1}, \ldots, \underline{\alpha^{3n-1}}$; $\underline{\alpha^{-1}}, \underline{\alpha^{-2}}, \ldots$, les reproduisent indéfiniment dans l'ordre inverse.

La substitution $|\underline{x}, \underline{\alpha x}|$ est le cycle $(\underline{\alpha^0}\,\underline{\alpha^1} \ldots, \underline{\alpha^{3n-1}})$. Ses $3n$ premières puissances $|\underline{x}, \underline{\alpha x}|^\nu = |\underline{x}, \underline{\alpha^\nu x}|$, $\nu = 0, 1, \ldots, 3n-1$, constituent le groupe cyclique $\sigma = \{|\underline{x}, \underline{\alpha x}|\}$, *indépendant de la racine primitive choisie*(1) α. Ses autres puissances, positives ou négatives, reproduisent les mêmes substitutions.

4° Les substitutions du groupe σ transforment une caractéristique en une caractéristique. La substitution $|\underline{x}, \underline{m x}|$, où m est un entier quelconque, positif ou négatif, étant l'une des substitutions $|\underline{x}, \underline{\alpha^\nu x}|$, a la même propriété.

5° La puissance n (ou la puissance $2n$) de la substitution $|\underline{x}, \underline{\alpha x}|$ fournit un système immédiat de caractéristiques, que nous avons appelé (J. § 5) le système des caractéristiques *imprimitives*.

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

$\underline{\alpha^\nu}, \underline{\alpha^{n+\nu}}, \underline{\alpha^{2n+\nu}}$ est, quelque soit l'entier positif ou négatif ν, l'une de ces caractéristiques imprimitives, et $\underline{\alpha^\nu}, \underline{\alpha^{n+\nu}}, \underline{\alpha^{2n+\nu}}; \underline{\alpha^{\nu+1}}, \underline{\alpha^{n+\nu+1}}, \underline{\alpha^{2n+\nu+1}}; \ldots; \underline{\alpha^{\nu+n-1}}, \underline{\alpha^{\nu+2n-1}}, \underline{\alpha^{\nu+3n-1}}$ est encore le système des caractéristiques imprimitives rangées dans le même ordre cyclique (1). En d'autres termes, les substitutions $|\underline{x}, \underline{\alpha^\nu x}|$ transforment le système des caractéristiques imprimitives en lui-même, en permutant cycliquement les caractéristiques.

6° Les substitutions du groupe σ transforment une *autre* caractéristique quel-

(1) Notre exposé, dans ce Mémoire, à cause de l'existence *univoque* dans les deux cas des groupes $\{|x, \alpha x|\}$ et $\{|\underline{x}, \underline{\alpha x}|\}$, est constamment valable pour N *premier*, ou *puissance de nombre premier*, de la forme $6n+1$, avec peut-être dans le second cas une restriction ou l'autre qu'il faudrait encore étudier. Cependant, pour simplifier, nous entendrons dès maintenant par N, dans tout notre exposé, *uniquement un nombre premier de la forme* $6n+1$.

conque, $\underline{\alpha^a}, \underline{\alpha^b}, \underline{\alpha^c}$, $(a, b, c$ incongrus les trois entre eux mod. $n)$(1), en $3n$ caractéristiques *différentes* :

$$\underline{\alpha^a}, \underline{\alpha^b}, \underline{\alpha^c}; \quad \underline{\alpha^{a+1}}, \underline{\alpha^{b+1}}, \underline{\alpha^{c+1}}; \quad \ldots; \quad \underline{\alpha^{a+3n-1}}, \underline{\alpha^{b+3n-1}}, \underline{\alpha^{c+3n-1}}; \tag{2}$$

qui constituent une *colonne* de caractéristiques, se reproduisant indéfiniment de chacune d'elles par les substitutions du groupe σ. Ces $3n$ caractéristiques se répartissent en n *carrés* de trois caractéristiques, imprimitifs vis-à-vis des substitutions de σ, et que nous disposons ainsi :

$$\begin{array}{llll}
\underline{\alpha^a}, \underline{\alpha^b}, \underline{\alpha^c}; & \underline{\alpha^{a+1}}, \underline{\alpha^{b+1}}, \underline{\alpha^{c+1}}; & \ldots; & \underline{\alpha^{a+n-1}}, \underline{\alpha^{b+n-1}}, \underline{\alpha^{c+n-1}}; \\
\underline{\alpha^{a+n}}, \underline{\alpha^{b+n}}, \underline{\alpha^{c+n}}; & \underline{\alpha^{a+n+1}}, \underline{\alpha^{b+n+1}}, \underline{\alpha^{c+n+1}}; & \ldots; & \underline{\alpha^{a+2n-1}}, \underline{\alpha^{b+2n-1}}, \underline{\alpha^{c+2n-1}}; \\
\underline{\alpha^{a+2n}}, \underline{\alpha^{b+2n}}, \underline{\alpha^{c+2n}}; & \underline{\alpha^{a+2n+1}}, \underline{\alpha^{b+2n+1}}, \underline{\alpha^{c+2n+1}}; & \ldots; & \underline{\alpha^{a+3n-1}}, \underline{\alpha^{b+3n-1}}, \underline{\alpha^{c+3n-1}}.
\end{array} \tag{3}$$

Dans chaque carré, trois éléments disposés verticalement forment une caractéristique imprimitive. Les substitutions du sous-groupe de σ, $\{|\underline{x}, \underline{\alpha^n x}|\}$, changent chaque carré en lui-même. Les autres substitutions $|\underline{x}, \underline{\alpha^\nu x}|$ permutent cycliquement ces carrés entre eux.

[3] Les caractéristiques *contenant l'élément* $\underline{\alpha^0} = 1$, ne peuvent être que les $3n - 2$ caractéristiques suivantes :

$$1, 2, 3; \quad 1, 3, 4; \quad 1, 4, 5; \quad \ldots; \quad 1, 3n-1, 3n. \tag{4}$$

Il ne peut en effet en exister où la somme des trois éléments est égale à N, puisque les deux plus grands éléments qui peuvent être associés à 1 dans une caractéristique sont $3n - 1$ et $3n$, et que $1 + 3n - 1 + 3n < N$.

Chaque colonne de caractéristiques (2) a trois et trois seules de ses caractéristiques contenant l'élément $\underline{\alpha^0} = 1$, et une des caractéristiques imprimitives, $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$, contient l'élément 1. Par suite l'ensemble des caractéristiques est réparti par les substitutions du groupe σ en $\dfrac{3n-3}{3} + 1 = n$ séries de caractéristiques; $n - 1$ de ces séries sont des colonnes de caractéristiques de la forme (2); la dernière est le système des caractéristiques imprimitives.

Le nombre des caractéristiques pour $N = 6n + 1$ éléments se retrouve ainsi(2) :

$$(n-1)3n + n = 3n^2 - 2n = n(3n-2) = \frac{(N-1)(N-5)}{12}.$$

(1) C'est-à-dire que l'on n'a pas $a \equiv b \equiv c \pmod{n}$.

(2) Voir dans J la note au bas de la page 84.

[4] Avec les premières valeurs de N étudiées jusqu'ici(1), il est apparu, plus ou moins immédiatement, que certaines de ces $n-1$ colonnes de $3n$ caractéristiques présentaient des propriétés ou une construction particulières, indépendamment du nombre des éléments N. Pour fixer les idées et faciliter la manière de nous exprimer dans la suite, nous donnons le tableau de ces colonnes pour $N = 31$, avec, à droite, le système des caractéristiques imprimitives(2). Les éléments sont $1, 2, \ldots, 9, 0', \ldots, 5'$; le tableau est construit avec la racine primitive $\alpha = 3$, et dans les colonnes, les caractéristiques sont disposées en carrés comme dans (3). Nous avons seulement rangé verticalement ce qui est disposé horizontalement dans (1) et (3) :

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

(1) $N = 37$ et $N = 43$ dans J., $N = 7, 13, 19, 25$ et 31, dans A; mais dans A la recherche des systèmes de caractéristiques préalable à la recherche des systèmes cycliques de triples de Steiner différents, a été faite directement sur l'ensemble des caractéristiques. L'obtention des systèmes de caractéristiques *différents*, par l'introduction du groupe $\{|x, \alpha x|\}$, eût simplifié considérablement ce premier Mémoire. C'est précisément en cherchant une voie pour continuer notre recherche des systèmes cycliques de triples de Steiner différents pour $N = 37$, les méthodes du premier Mémoire n'étant plus applicables à cause du temps qu'elles auraient exigé, que nous avons eu l'idée du groupe $\{|x, \alpha x|\}$, et l'introduction de ce groupe, et la répartition des caractéristiques en colonnes *invariantes* par ses substitutions, nous ont du coup expliqué, ce qui nous était inexpliqué dans les résultats du premier Mémoire.

(2) Voir également le même tableau pour $N = 37$, J., page 84.

La colonne qui contient la caractéristique 123, contient des couples des éléments $1, 2, \ldots, 3n$, qui n'entrent qu'une fois dans une caractéristique, tandis que les autres couples de ces éléments entrent chacun dans deux caractéristiques. Nous appellerons cette colonne, *la colonne I*; nous établirons dans le *premier* chapitre que cette propriété est indépendante du nombre des éléments N, et nous en déduirons que le groupe de substitutions, qui appartient(1) à l'ensemble des caractéristiques pour N premier (ou puissance de nombre premier), est le groupe $\sigma = \{ |x, \alpha x| \}$.

La colonne que nous appellerons *la colonne II*, a, dans chacune de ses caractéristiques, deux éléments appartenant à la même caractéristique imprimitive. Nous établirons ce fait facilement, et que cette colonne est unique de son espèce. Les deux colonnes que nous désignerons *par les chiffres III et IV*(2) ont les deux éléments différents dans leurs caractéristiques de tête, 1 et 5, appartenant à la même caractéristique imprimitive. Cette propriété, et celle que cette paire de colonnes III et IV est encore unique de son espèce, nous ont fait plus de difficultés. Elles ont d'ailleurs une certaine connexion avec le fait de la colonne II. Nous établirons les propriétés de ces colonnes II, III et IV dans le *second* chapitre.

L'unicité de ces colonnes *singulières*, la colonne II et la paire de colonnes III et IV, étant établie, nous sommes en état d'obtenir une catégorie importante de systèmes de caractéristiques différents, les systèmes de caractéristiques différents constitués de *carrés entiers de caractéristiques*, complétés éventuellement par *des caractéristiques imprimitives*. Pour les formules *approchées* du nombre de ces systèmes de caractéristiques différents que nous établissons ou que nous donnons le moyen d'établir dans le *troisième* chapitre, les $n - 4$ autres colonnes de caractéristiques ne peuvent plus présenter de particularité. Pour le nombre *exact* de ces systèmes de caractéristiques différents, elles peuvent, par contre, être encore de deux constitutions différentes. Mais nous n'entrerons pas plus avant ici dans cette question; nous espérons parvenir à ce nombre exact dans un autre Mémoire.

---

(1) Autrement dit, que les seules substitutions transformant chaque caractéristique en une caractéristique, sont celles du groupe σ.

(2) Pour $N = 31$, exceptionnellement la colonne I est en même temps la colonne IV. Les colonnes III et IV ne sont jamais la colonne II; par contre il n'est pas exclu que pour $N > 31$, le fait $I = IV$ ou $I = III$ puisse se représenter. Les résultats du chapitre II permettraient probablement de résoudre la question.

CHAPITRE PREMIER

La colonne I; le groupe de substitutions qui appartient à l'ensemble des caractéristiques.

[**5**] Remarquons d'abord dans (4), que les couples d'éléments $1, 2$ et $1, 3n$ entrent chacun dans une seule caractéristique. Par contre chaque autre couple d'éléments $1, a$, $(a = 3, 4, \ldots, 3n-1)$, entre dans deux caractéristiques différentes. Le groupe qui appartient à l'ensemble des caractéristiques est donc au plus *simplement transitif*. D'autre part il est transitif, possédant le sous-groupe transitif σ.

Remarquons ensuite que la colonne de caractéristiques (2), déduite de la caractéristique initiale $\alpha^a, \alpha^b, \alpha^c$ par les substitutions $|x, \alpha^\nu x|$, est aussi l'ensemble des $3n$ triples $\alpha^a x, \alpha^b x, \alpha^c x$, $x = 1, 2, \ldots, 3n$, puisque $\alpha^0, \alpha^1, \ldots, \alpha^{3n-1}$, sont, à l'ordre près, les entiers $1, 2, \ldots, 3n$ (voir § 2, 3° et 4°). Si donc nous rangeons verticalement et des deux manières ces caractéristiques de la colonne (2), dans l'ordre où elles se déduisent de la caractéristique de tête :

$$\begin{array}{lll} \alpha^a, & \alpha^b, & \alpha^c \\ \alpha^{a+1}, & \alpha^{b+1}, & \alpha^{c+1} \\ \alpha^{a+2}, & \alpha^{b+2}, & \alpha^{c+2} \\ \ldots\ldots\ldots\ldots & & \\ \alpha^{a+3n-1}, & \alpha^{b+3n-1}, & \alpha^{c+3n-1} \end{array} \qquad \begin{array}{lll} \alpha^a, & \alpha^b, & \alpha^c \\ \alpha^a.2, & \alpha^b.2, & \alpha^c.2 \\ \alpha^a.3, & \alpha^b.3, & \alpha^c.3 \\ \ldots\ldots\ldots\ldots & & \\ \alpha^a.3n, & \alpha^b.3n, & \alpha^c.3n, \end{array} \tag{6}$$

les deux rangées ne diffèrent que par l'ordre de succession des caractéristiques, et dans chaque rangée, les couples d'éléments disposés verticalement sont toujours les transformés de l'un d'eux par les substitutions $|x, \alpha^\nu x|$.

[**6**] Soit maintenant la colonne déterminée par la caractéristique 123. Rangée de la seconde manière, en écrivant de nouveau horizontalement ce qui est disposé verticalement dans (6), elle sera nécessairement, puisque $4n = 2n + 1$ et $6n = 1$ (1) :

$$1, 2, 3; \quad 2, 4, 6; \quad 3, 6, 9; \ \ldots; \ 2n, 2n+1, 1; \ \ldots; \ 3n, 1, 3n-1. \tag{7}$$

---

(1) Les trois caractéristiques de cette colonne qui contiennent l'élément 1, ne sont identiques que pour $n = 1$. Autrement dit, la caractéristique 123 détermine toujours une *colonne* de caractérisques, excepté pour $n = 1$. Pour $n = 1$, $N = 7$, elle est, à *elle seule*, le système des caractéristiques imprimitives et l'ensemble des caractéristiques.

Les $3n$ couples d'éléments :

$$1,2;\quad 2,4;\quad 3,6;\ \ldots;\ 3n,1, \tag{8}$$

qui sont les transformés de $1,2$ (ou de $1,3n$) par les substitutions du groupe σ, ne se retrouvent dans aucune des $n-2$ autres colonnes de caractéristiques et non plus dans le système des caractéristiques imprimitives, puisque le couple $1,2$ $(1,3n)$ n'appartient qu'à la caractéristique 123 $(1,3n-1,3n)$.

Par contre, les couples transformés par les substitutions $|\underline{x},\ \underline{\alpha^{\nu}x}|$ de chacun des couples suivants :

$$1,3;\quad 1,4;\quad 1,5;\ \ldots;\ 1,3n-1, \tag{9}$$

entrent chacun *exactement dans deux caractéristiques de l'ensemble.* En effet, d'une part la transformation des caractéristiques, $1,a-1,a$ et $1,a,a+1$ $(a=3,4,\ldots,3n-1)$ par une même puissance de $|\underline{x},\ \underline{\alpha x}|$, ne peut donner que deux caractéristiques différentes. D'autre part un couple donné a,b $(a<b)$ ne peut entrer au plus que dans deux caractéristiques différentes. Car si $a+b\leqq 3n$, seules $a,b,a+b$ et $a,b,b-a$ sont des caractéristiques; si $a+b>3n$, seules $a,b,\mathrm{N}-(a+b)$ et $a,b,b-a$ peuvent être des caractéristiques. Les $n(3n-2)$ caractéristiques de l'ensemble contiennent $3n(3n-2)$ couples d'éléments. Elles contiennent une seule fois chacun des $3n$ couples (8). Il reste dans ces caractéristiques $3n(3n-2)-3n = 3n(3n-3)$ couples qui, comme transformés des couples (9) par les substitutions $|\underline{x},\ \underline{\alpha^{\nu}x}|$ (§ 2, 6° et § 3), se trouvent chacun dans deux caraetéristiques différentes. Le nombre des couples *différents* entrant dans les $n(3n-2)$ caractéristiques est donc $3n+\dfrac{3n(3n-3)}{2}=\dfrac{3n(3n-1)}{2}$; c'est précisément le nombre des couples possibles avec les $3n$ éléments $1,2,\ldots,3n$.

Ainsi tous les couples des éléments $1,2,\ldots 3n$ *entrent dans la formation des caractéristiques; les* $3n$ *couples* (8) *n'appartiennent qu'aux caractéristiques de la colonne I; chaque autre couple des éléments* $1,2,\ldots 3n$ *se présente dans deux caractéristiques de l'ensemble.*

[7] Théorème. — *Le groupe de substitutions qui appartient à l'ensemble des caractéristiques pour* $\mathrm{N}=6n+1$ *premier (ou puissance de nombre premier) est le groupe* $\sigma=\{|\underline{x},\ \underline{\alpha x}|\}$.

En effet, une substitution transformant en lui-même cet ensemble, ne peut que transformer entre eux les $3n$ couples (8) et ainsi entre elles les caractéristiques de la colonne I. Écrivons à nouveau les caractéristiques de cette colonne I contenant l'élément 1 (en séparant les 3 couples qui se transforment entre eux), et à droite les autres caractéristiques contenant l'élément 1 :

1, 2	3		
$3n$, 1	$3n-1$	1, 3, 4; 1, 4, 5; ...; 1, $3n-3$, $3n-2$;	1, $3n-2$, $3n-1$.
$2n$, $2n+1$	1		

Fixons l'élément 1. — Ces caractéristiques, dans le groupe de gauche et dans le groupe de droite, ne peuvent alors que se transformer entre elles, et celles de gauche de la manière qui vient d'être dite. Il y a deux cas possibles :

1er cas. 2 *et* $3n$ *ne changent pas.* — De cette manière, se trouvent fixés successivement : les caractéristiques 1, 2, 3 et $3n$, 1, $3n-1$, donc les éléments 3 et $3n-1$; les caractéristiques 1, 3, 4 et 1, $3n-2$, $3n-1$, donc les éléments 4 et $3n-2$; les caractéristiques 1, 4, 5 et 1, $3n-3$, $3n-2$, donc les éléments 5 et $3n-3$; et ainsi de suite.

2e cas. *On a la transposition* $(2, 3n)$. — Elle exige la transposition $(3, 3n-1)$, par suite les transpositions successives $(4, 3n-2)$, $(5, 3n-3)$, ..., $(n+1, 2n+1)$, $(n+2, 2n)$, ... Si n est impair, la dernière est $\left(\frac{3n+1}{2}, \frac{3n+3}{2}\right)$; si n est pair, la dernière est $\left(\frac{3n}{2}, \frac{3n}{2}+2\right)$ et l'élément $\frac{3n}{2}+1$ reste en place. Or la caractéristique restante à gauche exige la transposition $(2n, 2n+1)$ ou que les éléments $2n$ et $2n+1$ restent en place. Ce qui est incompatible avec les transpositions précédentes.

Il n'y a ainsi que la substitution-identité qui transforme l'ensemble des caractéristiques en lui-même et laisse en place l'élément 1. L'ordre d'un groupe simplement transitif est égal à son degré multiplié par le nombre de ses substitutions qui laissent en place un élément donné. Par suite, l'ordre du groupe qui appartient à l'ensemble des caractéristiques est $3n \times 1$; il n'y a donc pas d'autres substitutions transformant l'ensemble des caractéristiques en lui-même que celles du groupe σ (c. q. f. d.).

CHAPITRE II

La colonne II et les colonnes III et IV.

[8] 1° Nous notons dorénavant les caractéristiques imprimitives contenant respectivement $\underline{\alpha^0}, \underline{\alpha^1}, \underline{\alpha^2}, \ldots, \underline{\alpha^{n-1}}$ par les symboles $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1}$.

2° Nous notons par $\boldsymbol{a}$ le *plus petit reste positif ou nul* de l'entier positif ou négatif a (mod. n). D'une façon plus précise, chaque fois que nous écrirons dans la suite une expression *quelconque* d'un entier en caractères gras, elle signifie le plus petit reste positif ou nul de cet entier (mod. n).

3° Avec cette notation, l'élément $\underline{\alpha^\nu}$ appartient à la caractéristique imprimitive $\mathbf{\nu}$(*). En effet, l'élément $\underline{\alpha^\nu}$ appartient à la caractéristique imprimitive $\underline{\alpha^\nu}, \underline{\alpha^{n+\nu}}, \underline{\alpha^{2n+\nu}}$. Supposons les trois exposants $\nu, n+\nu, 2n+\nu$ remplacés par leurs plus petits restes positifs ou nuls (mod. $3n$); l'un de ces restes sera compris dans les entiers $0, 1, \ldots, n-1$ et sera le plus petit reste positif ou nul de ν (mod. n), soit l'entier $\mathbf{\nu}$. La caractéristique $\underline{\alpha^\nu}, \underline{\alpha^{n+\nu}}, \underline{\alpha^{2n+\nu}}$ est donc celle dont le symbole est $\mathbf{\nu}$.

4° Dans chacun des carrés de la colonne (3), trois éléments disposés verticalement forment une caractéristique imprimitive. En représentant ces caractéristiques imprimitives par leurs symboles respectifs, les carrés successifs de (3) deviennent les triples suivants :

$$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}; \quad \boldsymbol{a+1}, \boldsymbol{b+1}, \boldsymbol{c+1}; \quad \ldots; \quad \boldsymbol{a+n-1}, \boldsymbol{b+n-1}, \boldsymbol{c+n-1}. \tag{10}$$

Nous les appellerons simplement des triples *réduits*, et la série cyclique qu'ils constituent(1), une *colonne réduite*. Le groupe cyclique $\{(\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1})\}$, qui laisse invariante cette colonne réduite, est isomorphe au groupe des permutations des carrés (3) entre eux par les substitutions du groupe σ; il est triplement isomorphe au groupe σ lui-même.

Les colonnes réduites pour $N = 31$ sont, correspondantes aux colonnes de caractéristiques du tableau (5) :

I = IV			II			III		
0	**4**	**1**	**0**	**1**	**3**	**0**	**3**	**0**	**0**	**4**	**1**
1	**0**	**2**	**1**	**2**	**4**	**1**	**4**	**1**	**1**	**0**	**2**
2	**1**	**3**	**2**	**3**	**0**	**2**	**0**	**2**	**2**	**1**	**3**
3	**2**	**4**	**3**	**4**	**1**	**3**	**1**	**3**	**3**	**2**	**4**
4	**3**	**0**	**4**	**0**	**2**	**4**	**2**	**4**	**4**	**3**	**0**

(*) Remplace un ν en caractère gras.

(1) Se rappeler ce qui est dit plus haut, sous 2°.

[**9**] Il est également utile de fixer encore une fois dans ce qui est établi jusqu'ici, quels sont les concepts *indépendants* de la racine primitive choisie α.

En premier lieu, les substitutions du groupe σ, celles du sous-groupe $\{|\underline{x}, \underline{\alpha^n x}|\}$ et le système des caractéristiques imprimitives sont, à l'ordre près, indépendants de α (voir J., § 3, 4 et 5). Avec une autre racine primitive β, telle que $\alpha \equiv \beta^\nu$ et donc $\underline{\alpha} = \underline{\beta^\nu}$ (mod. N), où ν est premier avec $6n$, les caractéristiques imprimitives contenant respectivement les éléments $\underline{\alpha^0}, \underline{\alpha^1}, \ldots, \underline{\alpha^{n-1}}$ et notées de ce fait d'abord par les symboles, $\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}$, deviennent celles qui contiennent les éléments $\underline{\beta^0}, \underline{\beta^\nu}, \ldots, \underline{\beta^{(n-1)\nu}}$, et portent donc respectivement les nouveaux symboles $\mathbf{0}, \mathbf{v}, \mathbf{2v}, \ldots, (\boldsymbol{n-1})\mathbf{v}$. Autrement dit, le remplacement de la racine α par la racine β effectue sur les symboles des caractéristiques imprimitives la substitution $|\boldsymbol{x}, \mathbf{v}\boldsymbol{x}|$ (1) des éléments $\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}$. $\mathbf{v}$, qui est congru à ν (mod. n), est, comme ν, premier avec n, ce qui est la condition pour que la notation $|\boldsymbol{x}, \mathbf{v}\boldsymbol{x}|$ soit une substitution.

En second lieu, les colonnes de caractéristiques et dans chaque colonne, leurs carrés de caractéristiques, sont, à l'ordre près des caractéristiques ou des carrés dans la colonne, indépendants de la racine α. En effet, les caractéristiques d'une colonne sont les transformées d'une caractéristique donnée par les substitutions de σ, et celles d'un carré sont les transformées d'une caractéristique donnée par celles de son sous-groupe $\{|\underline{x}, \underline{\alpha^n x}|\}$. Le remplacement de la racine α par la racine β effectue sur la colonne réduite (10) la substitution $|\boldsymbol{x}, \mathbf{v}\boldsymbol{x}|$; elle devient la colonne :

$$\boldsymbol{a}\mathbf{v}, \boldsymbol{b}\mathbf{v}, \boldsymbol{c}\mathbf{v}; (\boldsymbol{a}+\mathbf{1})\mathbf{v}, (\boldsymbol{b}+\mathbf{1})\mathbf{v}, (\boldsymbol{c}+\mathbf{1})\mathbf{v}; \ldots; (\boldsymbol{a}+\boldsymbol{n}-\mathbf{1})\mathbf{v}, (\boldsymbol{b}+\boldsymbol{n}-\mathbf{1})\mathbf{v}, (\boldsymbol{c}+\boldsymbol{n}-\mathbf{1})\mathbf{v};$$

ou encore :

$$\boldsymbol{a}\mathbf{v}, \boldsymbol{b}\mathbf{v}, \boldsymbol{c}\mathbf{v}; \boldsymbol{a}\mathbf{v}+\mathbf{v}, \boldsymbol{b}\mathbf{v}+\mathbf{v}, \boldsymbol{c}\mathbf{v}+\mathbf{v}; \ldots; \boldsymbol{a}\mathbf{v}+(\boldsymbol{n}-\mathbf{1})\mathbf{v}, \boldsymbol{b}\mathbf{v}+(\boldsymbol{n}-\mathbf{1})\mathbf{v}, \boldsymbol{c}\mathbf{v}+(\boldsymbol{n}-\mathbf{1})\mathbf{v}.$$

Cette seconde forme montre que la colonne reste cyclique; ce qui est bien conforme d'abord au fait que nos raisonnements jusqu'ici auraient conduit à une colonne réduite (10) cyclique aussi bien avec la racine β qu'avec la racine α arbitrairement choisie, et secondement au fait qu'une substitution métacyclique $|x, a + bx|$, et $|\boldsymbol{x}, \mathbf{v}\boldsymbol{x}|$ est de cette forme, change une série cyclique en une série cyclique (A., p. 68).

Cette pointe, que nous poussons ici, n'a pas grande nécessité pour la suite. Elle est par contre le point de départ de considérations qui conduisent à de nouvelles propriétés invariantes des colonnes de caractéristiques, et avec lesquelles nous espérons obtenir le nombre exact des systèmes de caractéristiques différents que nous cherchons (§ 4).

---

(1) Conformément à la notation admise (§ 8, 2°), nous entendons par $\mathbf{v}\boldsymbol{x}$, ici et quelques lignes plus haut, le plus petit reste positif ou nul du produit $\nu . x$ (mod. n), mais c'est aussi le plus petit reste positif ou nul du produit $\mathbf{v} . \boldsymbol{x}$ (mod. n). De même plus bas, nous aurons $(\boldsymbol{a}+\mathbf{1})\mathbf{v} = \boldsymbol{a}\mathbf{v}+\mathbf{v}$, etc., car $(\boldsymbol{a}+\mathbf{1})\mathbf{v}$ est soit le plus petit reste positif ou nul du produit $(a+1)\nu = a\nu + \nu$, soit le plus petit reste positif ou nul du produit $(\boldsymbol{a}+\mathbf{1})\mathbf{v} = \boldsymbol{a}\mathbf{v}+\mathbf{v}$.

[10] 1° La caractéristique imprimitive qui contient l'élément 1 est $\underline{\alpha^0}$, $\underline{\alpha^n}$, $\underline{\alpha^{2n}}$, indépendamment de la racine primitive choisie α. Par conséquent, pour toutes les racines primitives de N, $\underline{\alpha^n}$ et $\underline{\alpha^{2n}}$ sont les mêmes deux entiers consécutifs.

2° On a simultanément (mod. N) :

$$\text{ou} \quad \underline{\alpha^n} \equiv \alpha^n, \qquad \underline{\alpha^{2n}} \equiv \alpha^{2n}, \tag{11}$$

$$\text{ou} \quad \underline{\alpha^n} \equiv -\alpha^n, \qquad \underline{\alpha^{2n}} \equiv -\alpha^{2n}. \tag{12}$$

En effet, désignons par $\overline{\alpha^n}$ et $\overline{\alpha^{2n}}$ les plus petits restes *positifs* de α^n et α^{2n} (mod. N). $\overline{\alpha^n}$ et $\overline{\alpha^{2n}}$ sont deux des entiers $1, 2, \ldots, 6n$. On a la congruence connue(1) :

$$\alpha^n - 1 \equiv \alpha^{2n} \qquad \text{mod. N.}, \tag{13}$$

et donc aussi la congruence :

$$\overline{\alpha^n} - 1 \equiv \overline{\alpha^{2n}} \quad \text{ou l'égalité} \quad \overline{\alpha^n} - 1 = \overline{\alpha^{2n}}.$$

Ainsi $\overline{\alpha^n}$ et $\overline{\alpha^{2n}}$ sont deux entiers consécutifs; $\overline{\alpha^n}$ est le plus grand et ils sont simultanément ou $\leqq 3n$ ou $> 3n$. Il suffit, en effet, d'exclure le cas $\overline{\alpha^{2n}} = 3n$, $\overline{\alpha^n} = 3n + 1$, qui ne peut se présenter, puisque de :

$$\alpha^{2n} \equiv 3n, \qquad \alpha^n \equiv 3n + 1, \quad \text{on aurait} \quad \alpha^{2n} + \alpha^n \equiv \alpha^n(\alpha^n + 1) \equiv 0,$$

et on n'a ni $\alpha^n \equiv 0$, ni $\alpha^n + 1 \equiv 0$, mod. N.

On a donc simultanément,

$$\text{ou :} \quad \begin{matrix} \overline{\alpha^n} \leqq 3n \\ \overline{\alpha^{2n}} \leqq 3n \end{matrix} \quad \text{et donc} \quad \begin{matrix} \underline{\alpha^n} = \overline{\alpha^n} \equiv \alpha^n, \\ \underline{\alpha^{2n}} = \overline{\alpha^{2n}} \equiv \alpha^{2n}, \end{matrix}$$

et alors $\underline{\alpha^n}$ est le plus grand des deux entiers consécutifs $\underline{\alpha^n}$ et $\underline{\alpha^{2n}}$,

$$\text{ou :} \quad \begin{matrix} \overline{\alpha^{2n}} > 3n \\ \overline{\alpha^n} > 3n \end{matrix} \quad \text{et donc} \quad \begin{matrix} \underline{\alpha^n} = \mathrm{N} - \overline{\alpha^n} \equiv -\alpha^n \\ \underline{\alpha^{2n}} = \mathrm{N} - \overline{\alpha^{2n}} \equiv -\alpha^{2n} \end{matrix}$$

et alors $\underline{\alpha^{2n}}$ est le plus grand des deux entiers consécutifs $\underline{\alpha^n}$ et $\underline{\alpha^{2n}}$.

3° Si une racine primitive α satisfait aux congruences (11), la racine primitive $\beta \equiv \alpha^{N-2}$ (N − 2 est premier avec N − 1) satisfait aux congruences (12), et inversement.

---

(1) On a $\alpha^{3^n} \equiv -1$, et donc $\alpha^{3n} + 1 \equiv (\alpha^n + 1)(\alpha^{2n} - \alpha^n + 1) \equiv 0$ mod. N. Des deux facteurs dans les parenthèses, le second seul peut être congru à 0.

En effet, on a successivement :

$$\alpha^N \equiv \alpha, \qquad \alpha^{Nn} \equiv \alpha^n \equiv \alpha^{7n}, \qquad \alpha^{(N-2)n} \equiv \alpha^{5n} \equiv -\alpha^{2n},$$

et donc, si α satisfait aux congruences (11) :

$$\beta'' \equiv -\alpha^{2n} \equiv -\underline{\alpha^{2n}}, \qquad \text{mod. N}. \tag{14}$$

Puisque $\underline{\alpha^{2n}}$ est un des entiers $1, 2, \ldots, 3n$, ce résultat signifie :

$$\underline{\beta''} = \underline{\alpha^{2n}} \quad \text{ou} \quad \underline{\beta''} \equiv -\beta'', \quad \text{par suite} \quad \underline{\beta^{2n}} \equiv -\beta^{2n}.$$

Pour l'inverse, il suffit d'écrire dans (14) : $-\alpha^{2n} \equiv \underline{\alpha^{2n}}$, au lieu de $-\alpha^{2n} \equiv -\underline{\alpha^{2n}}$.

Nous opérerons constamment dans la suite avec une racine primitive α qui satisfait aux congruences (11), *et ainsi pour laquelle* $\underline{\alpha''} = \underline{\alpha^{2n}} + 1$. Dans ce cas, α'' (α^{2n}) sera toujours congru au *même* entier positif $\overline{\alpha''} = \underline{\alpha''}$ ($\overline{\alpha^{2n}} = \underline{\alpha^{2n}}$), *le plus grand* (*le plus petit*) des deux entiers consécutifs, $\underline{\alpha^{2n}}$ et $\underline{\alpha''}$, *indépendants* de α.

Ainsi, dès maintenant, $\underline{\alpha''}$ et $\underline{\alpha^{2n}}$ sont des éléments déterminés sans ambiguité, *indépendants* de α, et les congruences où interviennent dans la suite α'' et α^{2n} ont également un sens entièrement indépendant de la racine α (satisfaisant aux congruences (11)) que nous adopterons.

La colonne II.

[**11**] Une colonne qui a dans sa caractéristique de tête, et par suite dans chacune de ses caractéristiques, deux éléments appartenant à la même caractéristique imprimitive, contient nécessairement les trois caractéristiques suivantes, qui sont d'ailleurs un *carré* de caractéristiques :

$$\begin{array}{l} \underline{\alpha^0}, \ \underline{\alpha''}, \ \underline{\alpha''+1} \\ \underline{\alpha^0}, \ \underline{\alpha^{2n}}, \ \underline{\alpha^{2n}-1} \\ \underline{\alpha''}, \ \underline{\alpha^{2n}}, \ \underline{\underline{\alpha''+\alpha^{2n}}}. \end{array} \tag{15}$$

En effet, la raison des deux premiers éléments de chacune est immédiate. Le troisième élément de la première ne peut être que $\underline{\alpha''}+1$, puisque $\underline{\alpha''}-1$ serait $\underline{\alpha^{2n}}$ (§ 3, (4)); le troisième élément de la seconde ne peut être que $\underline{\alpha^{2n}}-1$, puisque $\underline{\alpha^{2n}}+1$ serait $\underline{\alpha''}$. Le troisième élément de la troisième ne peut être $\underline{\alpha^0}$. $\underline{\alpha''}$ et $\underline{\alpha^{2n}}$ sont deux entiers consécutifs; si cette troisième caractéristique a la somme de deux de

ses éléments égale au troisième, ce troisième élément ne peut être que $\underline{\alpha''} + \underline{\alpha^{2n}}$. Si elle a la somme de ses trois éléments égale à N, le troisième élément est :

$$N - (\underline{\alpha''} + \underline{\alpha^{2n}}), \quad \text{c'est-à-dire} \quad \underline{\underline{\alpha''} + \underline{\alpha^{2n}}}.$$

Dans les deux cas, son troisième élément peut s'écrire $\underline{\underline{\alpha''} + \underline{\alpha^{2n}}}$.

Ainsi cette colonne II, avec deux éléments de la même caractéristique imprimitive dans ses caractéristiques, est *unique*. Chacune des caractéristiques (15) la détermine également, et sa colonne réduite est formée de triples à *deux éléments égaux*.

Cette colonne II *existe*, à moins que $\underline{\alpha''} = 3n$. Dans ce dernier cas, on aura :

$$\alpha'' \equiv 3n, \quad 2\alpha'' \equiv 6n \equiv -1 \equiv \alpha^{3n}$$

d'où

$$\alpha^{2n} \equiv 2, \quad \alpha^{6n} \equiv 8 \equiv 1 \qquad \text{mod. N}$$

d'où enfin $N = 7$. Il suffit donc de nouveau d'exclure le cas $N = 7$, $n = 1$ (note du § 6).

[**12**] Il est utile que nous reprenions ici, pour être plus concis dans la suite, la notation que nous avons déja employée dans J., p. 78(1).

La relation congruentielle :

$$x \Xi b \qquad \text{mod. N} \tag{16}$$

équivaut à l'égalité $\underline{x} = \underline{b}$ (mod. N), et par suite aux deux congruences $x \equiv \pm b$ (mod. N); autrement dit, elle est satisfaite par tous les entiers x qui ont *la valeur absolue* de leur *plus petit reste positif ou négatif* (mod. N) égale à $\underline{b}$, ce qui revient à tous les entiers x congrus à $+b$ ou à $-b$ (mod. N). Nous considérerons cet ensemble d'entiers comme une *seule* racine de la relation (16), racine que nous représenterons par l'un de ces entiers, $\underline{b}$, par exemple.

La relation congruentielle :

$$ax \Xi b, \qquad \text{mod. N}, \quad a \text{ premier avec N}, \tag{17}$$

est équivalente aux deux congruences :

$$ax \equiv \pm b, \quad \text{qui s'écrivent aussi :} \quad ax \pm b \equiv 0 \quad \text{mod. N}; \tag{18}$$

x_1 et $-x_1$ sont les racines de ces deux congruences, si x_1 est la racine de l'une d'elles. Par suite la relation (17) a encore une *seule* racine, que nous représenterons par $\underline{x_1}$ et qui est déterminée sans autre par l'une des deux congruences (18).

---

(1) Sauf que nous changeons un peu le symbole de la notation employé dans J., pour faciliter le travail du typographe.

Remarquons enfin que la relation congruentielle introduite a en partie les propriétés de la congruence ordinaire (mod. N) (J., p. 78). De :

$$a \equiv b \text{ et } b \equiv c, \text{ il suit } a \equiv c \qquad \text{(mod. N)},$$

et vis-à-vis de la multiplication :

$$\text{si } a \equiv b \text{ et } c \equiv d, \text{ il suit } ac \equiv bd \qquad \text{(mod. N)}.$$

En particulier nous aurons :

$$ax \equiv \underline{a}x \equiv \underline{\underline{a}}x \equiv \underline{a}x \equiv \underline{\underline{a}}x \qquad \text{(mod. N)},$$

et les relations congruentielles :

$$ax \equiv b, \quad \underline{a}x \equiv b, \quad \underline{a}x \equiv \underline{b}, \text{ etc.}, \qquad \text{(mod. N)}$$

sont entièrement équivalentes.

[**13**] L'élément $\underline{\underline{\alpha^n + \alpha^{2n}}}$ de la troisième caractéristique (15), différent de $\underline{\alpha^0}$, peut également s'écrire $\underline{\alpha^n + \alpha^{2n}}$ (§ 10, 3°). La relation congruentielle :

$$x(\alpha^n + \alpha^{2n}) \equiv 1 \qquad \text{(mod. N)} \qquad (19)$$

a une *seule* racine $x \equiv \underline{\alpha^{\eta}}$, α^{η} étant la puissance de α *déterminée* par l'une des deux congruences(1) :

$$\alpha^y(\alpha^n + \alpha^{2n}) \equiv \pm 1 \qquad \text{(mod. N)}. \qquad (19\ bis)$$

Écrivons l'élément $\underline{\alpha^n + \alpha^{2n}}$ plus simplement encore $\underline{\alpha^{\varepsilon}}$, où ε est un des entiers $1, 2, \ldots, 3n-1$. Nous aurons(2) :

$$\underline{\alpha^{\eta_1}} \cdot \underline{\alpha^{\varepsilon}} \equiv \underline{\alpha^{\eta_1}} \cdot \underline{\alpha^{\varepsilon}} \equiv \underline{\alpha^{\eta_1 + \varepsilon}} \equiv \underline{\alpha^0} \qquad \text{(mod. N)}.$$

---

(1) L'exposant y qui satisfait à l'une ou à l'autre de ces deux congruences, n'est déterminé qu'au module $6n$ près. Si la racine de l'une est α^{y_1}, la racine de l'autre est $-\alpha^{y_1} \equiv \alpha^{y_1} \pm 3n$. Ainsi les exposants y qui satisfont à l'une *et* à l'autre des deux congruences, sont congrus entre eux (mod. $3n$). Cela est bien conforme au sens de $\underline{\alpha^{\eta_1}}$, où η_1 est déterminé au module $3n$ près.

(2) Il est évident d'ailleurs que, ayant l'élément $\underline{\alpha^{\varepsilon}}$, où ε est un des entiers $1, 2, \ldots, 3n-1$, il y a un seul entier η_1 pris également dans $1, 2, \ldots, 3n-1$, tel que $\underline{\alpha^{\eta_1 + \varepsilon}} \equiv \underline{\alpha^0}$. Ce qui est encore la preuve, sous une seconde forme, que la relation congruentielle (19) n'a qu'une seule racine.

La troisième caractéristique de la colonne II qui contient l'élément $\underline{\alpha^0}$, est ainsi la caractéristique suivante :

$$\underline{\alpha^{n+\eta_1}}, \underline{\alpha^{2n+\eta_1}}, \underline{\alpha^0}.$$

Ses deux premiers éléments sont consécutifs; par suite la caractéristique *imprimitive* $\underline{\alpha^{\eta_1}}, \underline{\alpha^{n+\eta_1}}, \underline{\alpha^{2n+\eta_1}}$ contient deux entiers consécutifs, comme la première caractéristique imprimitive $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$.

Nous pouvons prouver que ce sont là *les deux seules* caractéristiques imprimitives avec deux éléments consécutifs. Admettons, en effet, une troisième caractéristique imprimitive avec deux éléments consécutifs. Nous pouvons toujours noter ces deux éléments consécutifs $\underline{\alpha^\nu}, \underline{\alpha^{n+\nu}}$. Nous aurons dans ce cas :

$$\underline{\alpha^{n+\nu}} = \underline{\alpha^\nu} \pm 1, \quad \text{ou en congruences (§ 12)}; \quad \alpha^{n+\nu} \equiv \pm\alpha^\nu \pm 1$$

c'est-à-dire
$$\begin{array}{ll} \text{ou} & \alpha^\nu(\alpha^n - 1) \equiv \pm 1 \\ \text{ou} & \alpha^\nu(\alpha^n + 1) \equiv \pm 1 \end{array} \qquad \text{(mod. N)}.$$

Les deux premières congruences donnent (13) $\alpha^{2n+\nu} \equiv \pm 1$, c'est-à-dire $\underline{\alpha^{2n+\nu}} = \underline{\alpha^0}$; les deux dernières que l'on peut écrire encore :

$$\alpha^\nu(\alpha^{2n} + \alpha^n) \equiv \pm\alpha^n \qquad \text{(mod. N)},$$

sont satisfaites par $\pm\alpha^{n+\eta_1}$ et donnent $\underline{\alpha^0} = \underline{\alpha^{n+\eta_1}}$. Ainsi les deux seules caractéristiques imprimitives avec deux éléments consécutifs sont les caractéristiques $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$ et $\underline{\alpha^{\eta_1}}, \underline{\alpha^{n+\eta_1}}, \underline{\alpha^{2n+\eta_1}}$.

Les colonnes III et IV.

[**14**] Il a déjà été dit, dans l'Introduction, que l'étude du *fait* des colonnes III et IV présente beaucoup plus de difficultés. Nous procéderons par étapes.

Soit une caractéristique contenant l'élément 1, autre que $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$:

$$\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}. \tag{20}$$

THÉORÈME. — *Les triples* $\underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^{b+2n}}$ *et* $\underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^{b+n}}$ *ne peuvent être une caractéristique que si* $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ *appartient à la colonne II, et dans ce cas, un seul d'entre eux est une caractéristique et elle appartient à la colonne II.*

Preuve. — Admettons que $\underline{x^0}, \underline{x^{a+n}}, \underline{x^{b+2n}}$ est une caractéristique(1). On a alors :

$$\underline{x^b} = \underline{x^a} \pm 1, \qquad \underline{x^{b+2n}} = \underline{x^{a+n}} \pm 1,$$

ce qui, en congruences, donne(2) :

$$x^b \equiv \pm x^a \pm 1, \tag{21}$$

$$x^{b+2n} \equiv \pm x^{a+n} \pm 1. \tag{22}$$

Toutes les combinaisons de signes sont admissibles et différentes et celles de (22) *indépendantes* de celles de (21). En multipliant (21) par x^{2n} et comparant avec (22), il résulte :

$$\pm x^{a+2n} \pm x^{2n} \equiv \pm x^{a+n} \pm 1,$$

ou

$$x^a(\pm x^{2n} \mp x^n) + (\pm x^n \mp 1) \equiv 0.$$

Il est immédiat que des 16 combinaisons de signes, huit seulement donnent des congruences différentes. Ce sont les congruences :

$$x^a(x^{2n} - x^n) \pm (x^{2n} - 1) \equiv 0,$$
$$x^a(x^{2n} - x^n) \pm (x^{2n} + 1) \equiv 0,$$
$$x^a(x^{2n} + x^n) \pm (x^{2n} - 1) \equiv 0,$$
$$x^a(x^{2n} + x^n) \pm (x^{2n} + 1) \equiv 0.$$

Les quatre relations congruentielles équivalentes ont leurs racines $\underline{x^a}$ déterminées, par exemple, par les quatre congruences respectives :

$$x^a(x^{2n} - x^n) + (x^{2n} - 1) \equiv 0,$$
$$x^a(x^{2n} - x^n) + (x^{2n} + 1) \equiv 0,$$
$$x^a(x^{2n} + x^n) - (x^{2n} - 1) \equiv 0,$$
$$x^a(x^{2n} + x^n) - (x^{2n} + 1) \equiv 0.$$

---

(1) Il est évident que la démonstration est valable aussi pour la seconde hypothèse : $\underline{x^0}, \underline{x^{a+2n}}, \underline{x^{b-n}}$ est une caractéristique. Il suffit d'appeler a dans (20) l'exposant auquel on ajoute n et b celui auquel on ajoute $2n$.

(2) Nous négligerons dorénavant d'écrire mod. N, quand cela ne peut prêter à aucune confusion.

qui se réduisent aux suivantes, en se rappelant $x^n - 1 \equiv x^{2n}$:

$$x^a \equiv x^{2n} - 1, \qquad 1)$$

$$x^a \equiv x^n, \qquad 2)$$

$$x^a(x^{2n} + x^n) \equiv x^{2n} - 1, \qquad 3)$$

$$x^a(x^{2n} + x^n) \equiv x^n. \qquad 4)$$

Les congruences 2) et 3) ont la même racine $x^a \equiv x^n$, qui donne $\underline{x^a} = \underline{x^n}$.

La congruence 1) a lieu dans le cas où, dans les congruences initiales (21) et (22), les quatre signes sont positifs ou les quatre signes sont négatifs. On aura alors :

$$x^b \equiv x^a + 1 \equiv x^{2n} \quad \text{ou} \quad x^b \equiv -x^a - 1 \equiv -x^{2n}$$

qui donnent $\underline{x^b} = \underline{x^{2n}}$.

Enfin la congruence 4) a lieu dans le cas où, dans les congruences initiales (21) et (22), les combinaisons de signes sont les suivantes :

$$x^b \equiv x^a - 1, \qquad x^{b+2n} \equiv -x^{a+n} + 1,$$

ou

$$x^b \equiv -x^a + 1, \quad x^{b+2n} \equiv x^{a+n} - 1.$$

On aura alors, en vertu de 4) :

$$\pm(x^a - 1)(x^{2n} + x^n) \equiv \pm(x^n - x^{2n} - x^n) \equiv \pm x^{2n},$$

et en tenant compte de (19 *bis*) :

$$x^a \equiv \pm x^{n+r_1}, \quad x^b \equiv \pm x^{2n+r_1},$$

qui donnent :

$$\underline{x^a} = \underline{x^{n+r_1}}, \qquad \underline{x^b} = \underline{x^{2n+r_1}}.$$

Ainsi, en admettant que $\underline{x^0}, \underline{x^{a+n}}, \underline{x^{b+2n}}$ est une caractéristique, la caractéristique $\underline{x^0}, \underline{x^a}, \underline{x^b}$ ne peut être que l'une des trois suivantes :

$$\underline{x^0}, \underline{x^n}, \underline{x^n + 1}; \quad \underline{x^0}, \underline{x^{2n}}, \underline{x^{2n}} - 1; \quad \underline{x^0}, \underline{x^{n+r_1}}, \underline{x^{2n+r_1}}; \qquad (23)$$

qui sont les caractéristiques de la colonne II contenant $\underline{x^0}$.

Les deux premières des caractéristiques (23) appartiennent au même carré (15); la troisième à un carré différent. Or $\underline{x^0}, \underline{x^{a+n}}, \underline{x^{b+2n}}$ et $\underline{x^0}, \underline{x^{a+2n}}, \underline{x^{b+n}}$ ne peuvent être que des caractéristiques appartenant à un carré de même triple réduit que celui de

la caractéristique $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$. Mais d'une part la colonne II est unique de son espèce. D'autre part $\underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^{b+2n}}$ ne peut être *le même* triple que $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ que si $\underline{\alpha^b} = \underline{\alpha^{a+n}}$. La caractéristique $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ est alors $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{a+n}}$, c'est-à-dire contient deux éléments, $\underline{\alpha^a}$ et $\underline{\alpha^{a+n}}$, consécutifs et appartenant à la même caractéristique imprimitive, autre que $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$. Elle ne peut être que la caractéristique $\underline{\alpha^0}, \underline{\alpha^{n+r_1}}, \underline{\alpha^{2n+r_1}}$ (§ 13).

Par conséquent, la caractéristique $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ appartenant à la colonne II, un seul des deux triples différents $\underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^{b+2n}}$; $\underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^{b+n}}$ est une caractéristique. Si $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ est l'une des deux premières caractéristiques (23), il sera l'autre de ces deux caractéristiques; si $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ est la troisième caractéristique (23), il sera cette même caractéristique.

[**15**] *Remarque.* — Soient les deux congruences (mod. N) :

$$\begin{aligned} Ax + B &\equiv 0, \\ Bx + A &\equiv 0, \end{aligned} \qquad \text{(A et B premiers avec N.)}$$

Si α^a est la racine de la première, α^{-a} est la racine de la seconde et inversement. La preuve est immédiate, et le théorème est vrai d'ailleurs pour la congruence générale de degré μ : $Ax^\mu + Bx^{\mu-1} + \ldots + K \equiv 0$ (mod. N).

Les racines α^a et α^{-a} sont dites *associées*, parce que $\alpha^a . \alpha^{-a} \equiv 1$ (mod. N). L'entier associé à un entier donné A, premier avec N, est univoquement déterminé par la congruence $Ax \equiv 1$ (mod. N).

Soient maintenant les deux congruences, *indépendantes* de α (§ 10, 3°) :

$$\begin{aligned} x(\alpha^n - 1) + (\alpha^n + 1) &\equiv 0, \\ x(\alpha^n + 1) + (\alpha^n - 1) &\equiv 0. \end{aligned} \qquad \text{(mod. N.)} \qquad (24)$$

Elles ont les racines $\alpha^{a'}$ et $\alpha^{-a'}$. Les deux éléments $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$, ainsi déterminés, donnent les triples suivants qui sont, dans le cas général, deux paires de caractéristiques :

$$\begin{aligned} &\underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} - 1}. \\ &\underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} - 1}. \end{aligned} \qquad (25)$$

[**16**] Nous considérerons d'abord des cas particuliers.

Les racines des congruences (24) ne peuvent être ± 1, qui sont associées à elles-mêmes; la vérification est immédiate.

Elles ne peuvent être non plus $+\alpha^n$ pour la première et $-\alpha^n$ pour la seconde, associées respectivement à $-\alpha^{2n}$ et $+\alpha^{2n}$. La vérification est encore immédiate.

Par contre, elles peuvent être $-\alpha^n$ pour la première et $+\alpha^n$ pour la seconde,

et ± 2, associées respectivement à $\mp 3n$, pour les deux congruences, mais *seulement* pour les modules $N = 7$ et 13.

On aura en effet (mod. N) :

1° $\quad -\alpha^n(\alpha^n - 1) + (\alpha^n + 1) \equiv -\alpha^{3n} + \alpha^n + 1 \equiv 2 + \alpha^n \equiv 0$

d'où $\quad \alpha^n \equiv -2, \quad \alpha^{3n} \equiv -8 \equiv -1, \quad N = 7.$

2° $\quad \alpha^n(\alpha^n + 1) + (\alpha^n - 1) \equiv \alpha^{2n} + \alpha^n + \alpha^{2n} \equiv \alpha^n(2\alpha^n + 1) \equiv 0$

d'où $\quad 2\alpha^n \equiv -1, \quad 8\alpha^{3n} \equiv -1 \equiv -8, \quad N = 7.$

3° $\quad 2(\alpha^n - 1) + (\alpha^n + 1) \equiv 0, \quad 3\alpha^n \equiv 1, \quad 27\alpha^{3n} \equiv 1$

d'où $\quad 28 \equiv 0, \quad N = 7.$

4° $\quad -2(\alpha^n - 1) + (\alpha^n + 1) \equiv 0, \quad \alpha^n \equiv 3, \quad \alpha^{3n} \equiv 27$

d'où $\quad 28 \equiv 0, \quad N = 7.$

5° $\quad 2(\alpha^n + 1) + (\alpha^n - 1) \equiv 0, \quad 3\alpha^n \equiv -1, \quad 27\alpha^{3n} \equiv -1$

d'où $\quad 26 \equiv 0, \quad N = 13.$

6° $\quad -2(\alpha^n + 1) + (\alpha^n - 1) \equiv 0, \quad \alpha^n \equiv -3, \quad \alpha^{3n} \equiv -27$

d'où $\quad 26 \equiv 0, \quad N = 13.$

Ainsi les éléments $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$ peuvent être $\underline{\alpha^n}$ et $\underline{\alpha^{2n}}$, pour le module $N = 7$; ils peuvent être 2 et $3n$ pour les modules $N = 7$ et 13.

Pour $N = 7$, comme nous l'avons déjà remarqué, il n'existe que la caractéristique imprimitive 123, qui est $\underline{\alpha^0}, \underline{\alpha^{2n}}, \underline{\alpha^n}$ avec la racine α avec laquelle nous opérons (§ 10, 3°). Les congruences (24) ont pour racines 5 et 3; $\underline{5}$ et $\underline{3}$ sont bien $\underline{\alpha^{2n}}$ et $\underline{\alpha^n}$, et deux seuls des triples (25) sont des caractéristiques, et la même caractéristique 123.

Si $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$ sont 2 et $3n$, deux seuls également des triples (25) sont des caractéristiques, et ces deux caractéristiques sont 123 et $1, 3n, 3n - 1$. Elles appartiennent donc à la colonne I, voir (7). Pour $N = 7$, $n = 1$, ces deux caractéristiques sont encore 123; pour $N = 13$, $n = 2$, avec les caractéristiques imprimitives 134, 256, il n'existe qu'une colonne de caractéristiques, la colonne I, qui est, rangée dans l'ordre (7) :

$$123, \quad 246, \quad 364, \quad 451, \quad 532, \quad 615.$$

Elle est en même temps la colonne II; ses caractéristiques (15) $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^n + 1}$ et $\underline{\alpha^0}, \underline{\alpha^{2n}}, \underline{\alpha^{2n} - 1}$ étant 145 et 132. Les congruences (24) ont pour racines 2 et $-3n$.

[17] Pour tout autre module N, les triples (25) sont *quatre* caractéristiques.

On ne peut avoir $\underline{\alpha^{a'}} = \underline{\alpha^{-a'}}$, c'est-à-dire $\alpha^a \equiv \pm \alpha^{-a'}$.

En effet, pour que les deux congruences (24) aient des racines égales, $\alpha^{a'} \equiv \alpha^{-a'}$, il faudrait que (1) :

$$(\alpha^n + 1)^2 \equiv (\alpha^n - 1)^2, \quad \text{c'est-à-dire} \quad 4\alpha^n \equiv 0 \qquad (\text{mod. N}),$$

ce qui est impossible.

Pour qu'elles aient des racines égales et de signes contraires, $\alpha^{a'} \equiv \alpha^{-a'}$, il faudrait que :

$$(\alpha^n + 1)^2 \equiv -(\alpha^n - 1)^2, \quad \text{c'est-à-dire} \quad \alpha^{2n} \equiv -1 \qquad (\text{mod. N}),$$

ce qui est également impossible.

Si $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$ *diffèrent de* 1, ces quatre caractéristiques (25) se réduisent à *trois*, de la forme suivante, si nous désignons par a le plus petit des deux entiers $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$, indépendants de α :

$$\begin{array}{lll} 1, & a-1, & a \\ 1, & a, & a+1 \\ 1, & a+1, & a+2. \end{array} \qquad (\bigstar)$$

On a dans ce cas :

$$\underline{\alpha^{-a'}} = \underline{\alpha^{a'}} \pm 1 \quad \text{ou en congruences} \quad \alpha^{-a'} \equiv \pm \alpha^{a'} \pm 1,$$

et en développant :

$$\begin{aligned} \alpha^{-a'} &\equiv \alpha^{a'} + 1, \\ \alpha^{-a'} &\equiv -\alpha^{a'} + 1, \\ \alpha^{-a'} &\equiv \alpha^{a'} - 1, \\ \alpha^{-a'} &\equiv -\alpha^{a'} - 1. \end{aligned} \qquad (26)$$

$\alpha^{a'}$ et $\alpha^{-a'}$ sont respectivement les racines de la première et de la seconde congruence (24). D'une part :

$$\alpha^{a'+n} - \alpha^{a'} + \alpha^n + 1 \equiv 0 \qquad (\text{mod. N}). \qquad (27)$$

D'autre part, correspondant aux quatre congruences (26) :

$$\begin{aligned} (\alpha^{a'} + 1)(\alpha^n + 1) + (\alpha^n - 1) &\equiv 0, \\ (-\alpha^{a'} + 1)(\alpha^n + 1) + (\alpha^n - 1) &\equiv 0, \\ (\alpha^{a'} - 1)(\alpha^n + 1) + (\alpha^n - 1) &\equiv 0, \\ (-\alpha^{a'} - 1)(\alpha^n + 1) + (\alpha^n - 1) &\equiv 0. \end{aligned}$$

---

(1) Si l'on a (mod. N) :
$$\begin{aligned} ax_1 + b &\equiv 0, \\ a'x_1 + b' &\equiv 0, \end{aligned}$$
(a et a' premiers avec N), on aura : $a'b - ab' \equiv 0$.
Si les deux racines sont x_1 et $-x_1$, on aura : $a'b + ab' \equiv 0$.

En faisant les multiplications, et soustrayant ou additionnant chaque fois avec la congruence (27), on trouve d'abord les congruences de gauche suivantes, et ensuite, en multipliant ces congruences obtenues par α^{2n} et se servant toujours de $\alpha^n - 1 \equiv \alpha^{3n}$, les congruences de droite :

$$\begin{aligned} 2\alpha^{a'} + \alpha^n - 1 &\equiv 0, & 2\alpha^{a'+2n} &\equiv \alpha^n, \\ 2\alpha^{a'} - 3\alpha^n - 1 &\equiv 0, & 2\alpha^{a'+2n} &\equiv \alpha^n - 4, \\ 2\alpha^{a'} - \alpha^n - 3 &\equiv 0, & 2\alpha^{a'+2n} &\equiv 3\alpha^n - 4, \\ 2\alpha^{a'} - \alpha^n + 1 &\equiv 0, & 2\alpha^{a'+2n} &\equiv -\alpha^n. \end{aligned}$$

En comparant ces dernières congruences (de droite) avec la congruence (27) qui peut aussi s'écrire :

$$2\alpha^{a'}(\alpha^n - 1) + 2(\alpha^n + 1) \equiv 0 \quad \text{ou} \quad 2\alpha^{a'+2n} \equiv -2\alpha^n - 2,$$

on obtient enfin :

$$\begin{aligned} \alpha^n &\equiv -2\alpha^n - 2, & \text{c'est-à-dire} \quad 3\alpha^n &\equiv -2, \\ \alpha^n - 4 &\equiv -2\alpha^n - 2, & \text{»} \quad \text{»} \quad 3\alpha^n &\equiv 2, \\ 3\alpha^n - 4 &\equiv -2\alpha^n - 2, & \text{»} \quad \text{»} \quad 5\alpha^n &\equiv 2, \\ -\alpha^n &\equiv -2\alpha^n - 2, & \text{»} \quad \text{»} \quad \alpha^n &\equiv -2. \end{aligned}$$

Ces congruences ne *peuvent* exister que relativement à certains modules N que nous cherchons. Elles donnent successivement en les élevant au cube et remplaçant α^{3n} par -1 :

$$\begin{aligned} -27 \equiv -8 \quad \text{ou} \quad 19 \equiv 0 \quad (\text{mod. N}), \quad \text{d'où} \quad N = 19, \\ -27 \equiv 8 \quad \text{ou} \quad 35 \equiv 0 \quad (\text{mod. N}), \quad \text{»} \quad N = 7, \\ -125 \equiv 8 \quad \text{ou} \quad 133 \equiv 0 \quad (\text{mod. N}), \quad \text{»} \quad N = 7 \text{ et } 19, \\ -1 \equiv -8 \quad \text{ou} \quad 7 \equiv 0 \quad (\text{mod. N}), \quad \text{»} \quad N = 7. \end{aligned}$$

Pour $N = 7$, nous savons ce qu'il en est; le cas est déjà écarté. Pour $N = 19$, avec les trois caractéristiques imprimitives 178, 235, 469, il n'existe que deux colonnes de caractéristiques; l'une est la colonne I qui est en même temps la colonne II, l'autre contient les trois caractéristiques de la forme (★) : 134, 145, 156, où 4 et 5 sont effectivement les deux éléments $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$ déterminés par les congruences (24).

Nous écartons définitivement ces cas $N = 7$, 13 et 19. Ainsi, dès maintenant, $\underline{\alpha^{a'}}$ et $\underline{\alpha^{-a'}}$ sont deux des entiers $3, 4, \ldots, 3n-1$, exceptés $\underline{\alpha^n}$ et $\underline{\alpha^{2n}}$; *ils sont différents de 2 ou plus* et les quatre caractéristiques (25), *differentes* et contenant $\underline{\alpha^0}$, font partie au moins de *deux* colonnes de caractéristiques différentes.

[**18**] Les deux congruences (24), qui sont après substitution des racines $\alpha^{a'}$ et $\alpha^{-a'}$:

$$\alpha^{a'+n} - \alpha^{a'} + \alpha^n + 1 \equiv 0,$$
$$\alpha^{-a'+n} + \alpha^{-a'} + \alpha^n - 1 \equiv 0,$$

donnent aussi :

$$\alpha^n(\alpha^{a'} + 1) \equiv \alpha^{a'} - 1,$$
$$\alpha^n(\alpha^{-a'} + 1) \equiv -(\alpha^{-a'} - 1).$$

Posons

$$\alpha^{b'} \equiv \alpha^{a'} + 1, \quad \text{d'où} \quad \alpha^{b'-a'} \equiv 1 + \alpha^{-a'}. \tag{28}$$

Les deux congruences précédentes deviennent :

$$\alpha^{b'+n} \equiv \alpha^{a'} - 1,$$
$$\alpha^{b'-a'+n} \equiv -(\alpha^{-a'} - 1).$$

Avec la première et la première congruence (28), et tenant compte que $\underline{\alpha^{a'}}$ ne peut être 1, 2 et $3n$, on a :

$$\text{si} \quad \alpha^{a'} \equiv \underline{\alpha^{a'}}, \qquad \underline{\alpha^{b'}} = \underline{\alpha^{a'}} + 1, \quad \underline{\alpha^{b'+n}} = \underline{\alpha^{a'}} - 1,$$
$$\text{si} \quad \alpha^{a'} \equiv \underline{-\alpha^{a'}}, \quad \underline{\alpha^{b'+n}} = \underline{\alpha^{a'}} + 1, \qquad \underline{\alpha^{b'}} = \underline{\alpha^{a'}} - 1.$$

Avec la seconde et la seconde congruence (28), et tenant compte que $\underline{\alpha^{-a'}}$ ne peut être 1, 2 et $3n$, on a :

$$\text{si} \quad \alpha^{-a'} \equiv \underline{\alpha^{-a'}}, \qquad \underline{\alpha^{b'-a'}} = \underline{\alpha^{-a'}} + 1, \quad \underline{\alpha^{b'-a'+n}} = \underline{\alpha^{-a'}} - 1,$$
$$\text{si} \quad \alpha^{-a'} \equiv \underline{-\alpha^{-a'}}, \quad \underline{\alpha^{b'-a'+n}} = \underline{\alpha^{-a'}} + 1, \qquad \underline{\alpha^{b'-a'}} = \underline{\alpha^{-a'}} - 1.$$

Ainsi dans la première paire des caractéristiques (25), que nous écrirons à nouveau :

$$\begin{aligned} &\underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} - 1}, \\ &\underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} - 1}, \end{aligned} \tag{25}$$

les deux derniers éléments sont de la forme $\underline{\alpha^{b'}}$ et $\underline{\alpha^{b'+n}}$, et dans la seconde paire, les deux derniers éléments sont de la forme $\underline{\alpha^{b'-a'}}$ et $\underline{\alpha^{b'-a'+n}}$.

Or les trois caractéristiques qui contiennent $\underline{\alpha^0}$, dans les colonnes déterminées par les caractéristiques $\underline{\alpha^0}, \underline{\alpha^{a'}}, \underline{\alpha^{b'}}$ et $\underline{\alpha^0}, \underline{\alpha^{a'}}, \underline{\alpha^{b'+n}}$, sont respectivement :

$$\begin{aligned} &1) \quad \underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{b'}}; \qquad 1') \quad \underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{b'+n}}; \\ &2) \quad \underline{\alpha^{-a'}}, \ \underline{\alpha^0}, \ \underline{\alpha^{b'-a'}}; \qquad 2') \quad \underline{\alpha^{-a'}}, \ \underline{\alpha^0}, \ \underline{\alpha^{b'-a'+n}}; \\ &3) \quad \underline{\alpha^{-b'}}, \ \underline{\alpha^{a'-b'}}, \ \underline{\alpha^0}; \qquad 3') \quad \underline{\alpha^{-b'+2n}}, \ \underline{\alpha^{a'-b'+2n}}, \ \underline{\alpha^0}. \end{aligned} \tag{29}$$

Les caractéristiques des deux premières lignes sont les quatre caractéristiques (25). En vertu de ce qui est dit à la fin du paragraphe précédent, les deux colonnes de caractéristiques (29) sont donc différentes. D'autre part, les carrés de tête de ces deux colonnes ont le même triple réduit (§ 8) $\mathbf{0}, a', b'$, et les colonnes réduites correspondantes sont identiques.

Nous avons donc le résultat :

Pour $N > 19$, *les deux colonnes* (29) *différentes, déterminées par l'une ou l'autre des paires de caractéristiques* (25), *ont les mêmes colonnes réduites. Nous les appellerons les colonnes III et IV.*

[**19**] Nous avons ainsi *l'existence* des colonnes III et IV; mais le point essentiel que toute cette étude arrivera à établir est *l'unicité* de cette paire de colonnes III et IV, ou plutôt un résultat *plus complet*, que nous formulerons seulement à la fin de notre exposé (§ 22), parce que, alors seulement, nous pourrons lui donner une forme simple et claire.

Pour poursuivre, les remarques suivantes sont encore nécessaires.

1° Dans toute colonne de caractéristiques, *autre que la colonne II*, les trois caractéristiques qui contiennent l'élément $\underline{\alpha^0}$ appartiennent à trois carrés différents. En effet, si deux d'entre elles appartenaient au même carré, le triple réduit de ce carré contiendrait deux fois l'élément $\mathbf{0}$, et cela n'a lieu que pour un triple réduit de la colonne II.

2° Aucune des colonnes III et IV, pour $N > 19$, ne peut être en même temps la colonne II, sinon, les colonnes III et IV ayant les mêmes colonnes réduites, il y aurait, pour N, deux colonnes réduites du type de celle de la colonne II, ce qui n'est pas. Par suite, les six caractéristiques (29) appartiennent *chacune à un carré différent.*

3° Les carrés d'une même colonne ont des triples réduits *différents*, puisque ces triples réduits forment une série cyclique (§ 8). Par contre, dans (29), les carrés des caractéristiques 1) et 1'), 2) et 2'), 3) et 3') ont respectivement le même triple réduit.

Notons par $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ l'une *quelconque* des six caractéristiques (29). Formons sur cette caractéristique les six triples suivants :

$$\begin{array}{lll} a) \quad \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{b+n}}; & b) \quad \underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^b}; & c) \quad \underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^{b+n}}; \\ a') \quad \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{b+2n}}; & b') \quad \underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^b}; & c') \quad \underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^{b+2n}}. \end{array} \tag{30}$$

Chacun est différent de la caractéristique $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$. La chose est évidente pour les triples *a*), *b*), *a'*) et *b'*); pour que le triple *c*) soit le même que $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$, il faudrait que $\underline{\alpha^a} = \underline{\alpha^{b+n}}$ et $\underline{\alpha^b} = \underline{\alpha^{a+n}}$. Il s'ensuivrait $\underline{\alpha^a} = \underline{\alpha^{a+2n}}$, ce qui n'est pas. La même démonstration est valable pour le triple *c'*).

Si l'un de ces triples est une caractéristique, elle appartient à un carré de même triple réduit que la caractéristique $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$. Puisque, en vertu des remarques faites plus haut, dans (29) seule la caractéristique de la même ligne que $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$, appartient à un carré de même triple réduit que celui de $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$, *au plus un seul* des triples (30) est une caractéristique *contenue dans les caractéristiques* (29), celui qui est éventuellement cette seconde caractéristique de la même ligne que $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$. Mais, d'autre part, cette seconde caractéristique de la même ligne que $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ est toujours, relativement à cette dernière, de la forme de l'un des triples (30), comme on le voit immédiatement.

Par conséquent, $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ *étant, l'une après l'autre, chacune des six caractéristiques* (29), *chaque fois un et un seul des triples* (30) *est une caractéristique contenue dans les cinq autres caractéristiques* (29).

[**20**] Soit maintenant une caractéristique *quelconque*, $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$, autre que la caractéristique imprimitive $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$, et n'appartenant pas à la colonne II.

Formons encore les six triples suivants :

$$\begin{array}{lll} \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{b+n}}; & \underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^b}; & \underline{\alpha^0}, \underline{\alpha^{a+n}}, \underline{\alpha^{b+n}}; \\ \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{b+2n}}; & \underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^b}; & \underline{\alpha^0}, \underline{\alpha^{a+2n}}, \underline{\alpha^{b+2n}}. \end{array} \tag{31}$$

Si l'un de ces triples, $\underline{\alpha^0}, \underline{\alpha^{a+\varepsilon n}}, \underline{\alpha^{b+\varepsilon' n}}$, $\varepsilon, \varepsilon'$ étant l'une des six combinaisons des valeurs 0, 1, 2 correspondantes à (31), est une caractéristique, les deux caractéristiques :

$$\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b} \quad \text{et} \quad \underline{\alpha^0}, \underline{\alpha^{a+\varepsilon n}}, \underline{\alpha^{b+\varepsilon' n}} \tag{32}$$

déterminent deux colonnes, qui ne peuvent être que *différentes* et autres que la colonne II, puisque les deux caractéristiques (32) appartiennent à deux carrés de même triple réduit, qui ne sauraient donc appartenir à la même colonne, ou à la colonne II.

Dans les six caractéristiques de ces deux colonnes qui contiennent $\underline{\alpha^0}$:

$$\begin{array}{llll} 1) & \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}; & 1') & \underline{\alpha^0}, \underline{\alpha^{a+\varepsilon n}}, \underline{\alpha^{b+\varepsilon' n}}; \\ 2) & \underline{\alpha^{-a}}, \underline{\alpha^0}, \underline{\alpha^{b-a}}; & 2') & \underline{\alpha^{-a-\varepsilon n}}, \underline{\alpha^0}, \underline{\alpha^{b-a+(\varepsilon'-\varepsilon)n}}; \\ 3) & \underline{\alpha^{-b}}, \underline{\alpha^{a-b}}, \underline{\alpha^0}; & 3') & \underline{\alpha^{-b-\varepsilon' n}}, \underline{\alpha^{a-b+(\varepsilon-\varepsilon')n}}, \underline{\alpha^0}; \end{array}$$

il y en a toujours *au moins une paire* (exactement deux) de la forme suivante :

$$\underline{\alpha^0}, \underline{\alpha^{a'}}, \underline{\alpha^{b'}} \quad \text{et} \quad \underline{\alpha^0}, \underline{\alpha^{a'}}, \underline{\alpha^{b'+n}},$$

l'une des caractéristiques étant dans l'une des colonnes, et l'autre dans la seconde. La vérification est immédiate :

si $\varepsilon, \varepsilon'$ est 0, 1 ou 1, 0, nous prenons 1) et 1'),
si $\varepsilon, \varepsilon'$ est 1, 1, nous prenons 2') et 2),
si $\varepsilon, \varepsilon'$ est 0, 2 ou 2, 0, nous prenons 1') et 1),
si $\varepsilon, \varepsilon'$ est 2, 2, nous prenons 2) et 2'),

[**21**] Nous arrivons maintenant au point essentiel et terme de cette étude du *fait* des colonnes III et IV.

Si les deux triples suivants *quelconques* :

$$\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}; \quad \underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^{b+n}} \tag{33}$$

sont deux caractéristiques, autres que $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$ et n'appartenant pas à la colonne II, déterminant ainsi deux colonnes différentes et autres que la colonne II (paragraphe précédent), *ces deux colonnes sont les colonnes III et IV obtenues au* § 18, déterminées par les deux paires de caractéristiques (25).

En effet, on n'aura pour les éléments $\underline{\alpha^b}$ et $\underline{\alpha^{b+n}}$ que les deux alternatives :

$$\underline{\alpha^b} = \underline{\alpha^a} \pm 1,$$
$$\underline{\alpha^{b+n}} = \underline{\alpha^a} \mp 1,$$

où les deux signes supérieurs vont ensemble et les deux signes inférieurs également. Ces égalités sont équivalentes aux congruences :

$$\pm\alpha^b \equiv \pm\alpha^a \pm 1 \quad \text{ou encore} \quad \pm\alpha^{b+n} \equiv \pm\alpha^{a+n} \pm \alpha^n,$$
$$\pm\alpha^{b+n} \equiv \pm\alpha^a \mp 1 \quad \text{»} \quad \text{»} \quad \pm\alpha^{b+n} \equiv \pm\alpha^a \mp 1.$$

Avec chacune des quatre congruences différentes que fournit la première ligne, sont possibles deux congruences de la seconde ligne, celles qui ont aux seconds membres la combinaison de signes correspondants (semblablement placés) et aux premiers membres une fois $+\alpha^{b+n}$ et une fois $-\alpha^{b+n}$. Ainsi, par exemple, avec $\alpha^{b+n} \equiv \alpha^{a+n} + \alpha^n$, sont possibles :

$$\alpha^{b+n} \equiv \alpha^a - 1 \quad \text{ou aussi} \quad \alpha^{b+n} \equiv \alpha^a - 1,$$
$$-\alpha^{b+n} \equiv \alpha^a - 1 \quad \text{»} \quad \text{»} \quad \alpha^{b+n} \equiv -\alpha^a + 1.$$

Ces huit paires de congruences admissibles donnent, par l'intermédiaire des premiers membres, les seules quatre congruences possibles suivantes :

$$\alpha^{a+n} + \alpha^n \equiv \pm(\alpha^a - 1),$$
$$\alpha^{a+n} - \alpha^n \equiv \pm(\alpha^a + 1), \tag{34}$$

car les quatre autres, on le voit immédiatement, sont celles-ci changées de signes. Ces quatre congruences (34) s'écrivent également :

$$\begin{aligned} &\alpha^a(\alpha^n - 1) \pm (\alpha^n + 1) \equiv 0, \\ &\alpha^a(\alpha^n + 1) \pm (\alpha^n - 1) \equiv 0. \end{aligned} \tag{35}$$

Les deux premières (la première de chaque ligne) sont les congruences (24); les quatre ont les racines $\pm\alpha^{a'}$ et $\pm\alpha^{-a'}$ du § 15, et les deux caractéristiques (33) sont *l'une* ou *l'autre* des paires de caractéristiques (25) :

$$\begin{aligned} &\underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{a'}}, \ \underline{\alpha^{a'} - 1}, \\ &\underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} + 1} \quad \text{et} \quad \underline{\alpha^0}, \ \underline{\alpha^{-a'}}, \ \underline{\alpha^{-a'} - 1}, \end{aligned}$$

déterminant les colonnes III et IV obtenues au § 18.

[**22**] En reprenant maintenant ce qui est établi dans les trois derniers paragraphes, et également au § 14 et suivants, nous sommes en état de formuler, sous sa forme complète, le résultat suivant.

Soit $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ une caractéristique *quelconque*, autre que $\underline{\alpha^0}, \underline{\alpha^n}, \underline{\alpha^{2n}}$. Soient les huit triples suivants :

$$\begin{aligned} &\underline{\alpha^0}, \ \underline{\alpha^{a+n}}, \ \underline{\alpha^b}; \quad \underline{\alpha^0}, \ \underline{\alpha^a}, \ \underline{\alpha^{b+n}}; \quad \underline{\alpha^0}, \ \underline{\alpha^{a+n}}, \ \underline{\alpha^{b+n}}; \quad \underline{\alpha^0}, \ \underline{\alpha^{a+n}}, \ \underline{\alpha^{b+2n}}; \\ &\underline{\alpha^0}, \ \underline{\alpha^{a+2n}}, \ \underline{\alpha^b}; \quad \underline{\alpha^0}, \ \underline{\alpha^a}, \ \underline{\alpha^{b+2n}}; \quad \underline{\alpha^0}, \ \underline{\alpha^{a+2n}}, \ \underline{\alpha^{b+2n}}; \quad \underline{\alpha^0}, \ \underline{\alpha^{a+2n}}, \ \underline{\alpha^{b+n}}. \end{aligned} \tag{36}$$

UN et UN SEUL *de ces triples est une caractéristique, et* SEULEMENT *dans le cas où la caractéristique* $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ *appartient à la colonne II, ou à l'une des colonnes, toujours différentes de II, que nous avons désignées par III et IV, déterminées par les racines des congruences* (24).

Si le triple (36) qui est une caractéristique, est l'un ou l'autre des deux derniers (le dernier de chaque ligne), $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ appartient à la colonne II (§ 14); s'il est l'un des six premiers (et chacun d'eux peut être une caractéristique), $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ est l'une des six caractéristiques (29) contenant $\underline{\alpha^0}$ dans les colonnes III et IV.

D'autre part, si deux colonnes *différentes* ont la même colonne réduite déterminée par le triple $\mathbf{0}, \boldsymbol{a}, \boldsymbol{b}$, $\underline{\alpha^0}, \underline{\alpha^a}, \underline{\alpha^b}$ étant la caractéristique de tête de l'une d'elles, le carré de tête de l'autre doit nécessairement contenir l'un des triples (36) comme caractéristique. *Il n'y a donc que la paire de colonnes différentes III et IV qui aient la même colonne réduite.*

CHAPITRE III

Formules *approchées* du nombre des systèmes de caractéristiques *différents* appartenant à n ou à un diviseur de n.

[**23**] Nous appelons (J., § 12, p. 86) systèmes de caractéristiques *différents*, ceux qui ne sont pas déductibles l'un de l'autre par les substitutions du groupe

$$\sigma = \{ |\underline{x}, \underline{\alpha x}| \}(^1).$$

En conséquence, les systèmes de caractéristiques déductibles l'un de l'autre par une substitution de σ seront les seuls que nous dirons *équivalents*(²).

Tout système de caractéristiques est transformé en lui-même par la substitution-identité $|\underline{x}, \underline{\alpha^{3n} x}|$.

Si aucune autre substitution du groupe σ ne le transforme en lui-même, nous dirons que ce système ne *possède*(³) que l'identité, ou *appartient au diviseur de* $3n : d = 3n$. Il y a alors $3n$ systèmes de caractéristiques qui lui sont équivalents (en le comptant lui-même) et il peut être remplacé par l'un quelconque d'entre eux.

Si la première puissance de $|\underline{x}, \underline{\alpha x}|$, qui le transforme en lui-même, est $|\underline{x}, \underline{\alpha^d x}|$, $d < 3n$, d est un diviseur de $3n$, et nous dirons que ce système *possède* le sous-groupe $\{ |\underline{x}, \underline{\alpha^d x}| \}$, ou *appartient au diviseur de* $3n : d < 3n$. Il y a alors d systèmes de caractéristiques qui lui sont équivalents (en le comptant lui-même), et il peut être remplacé par l'un quelconque d'entre eux.

Aucun système de caractéristiques, *autre* que le système des caractéristiques imprimitives, ne possède le groupe entier $\{ |\underline{x}, \underline{\alpha x}| \}$. La preuve est immédiate, puisque une caractéristique d'une colonne est transformée par les substitutions de σ en $3n$ caractéristiques différentes.

(¹) En admettant le théorème que les systèmes cycliques de triples de Steiner équivalents (par une substitution quelconque du groupe symétrique des N éléments) sont déductibles l'un de l'autre par une substitution métacyclique, c'est-à-dire une substitution du groupe $\{ |x, 1 + x|, |x, \alpha x| \}$, nous savons (J., § 14, p. 90) que ces systèmes de caractéristiques *différents* sont *les seuls nécessaires* pour l'obtention des systèmes cycliques de triples de Steiner *différents* (relativement au groupe symétrique des N éléments, c'est-à-dire déductibles l'un de l'autre par aucune substitution des N éléments).

(²) Sans nous occuper ici de savoir, si deux tels systèmes de caractéristiques *différents* ne pourraient pas être éventuellement *équivalents* par une substitution des élements $1, 2 \ldots, 3n$, *autre* que celles du groupe σ, quoique cela ne nous paraisse pas probable.

(³) Encore une fois, sans nous occuper de savoir s'il n'est pas en dehors du groupe σ, éventuellement une substitution *autre* que l'identité qui transforme ce système en lui-même.

Une caractéristique imprimitive et un carré de caractéristiques sont transformés en eux-mêmes par les substitutions du sous-groupe de τ : $\{|\underline{x}, \underline{\alpha''x}|\}$ (§ 2, 6°). Par suite, tout système de caractéristiques constitué de carrés entiers de caractéristiques, complété éventuellement par des caractéristiques imprimitives, possède le sous-groupe $\{|\underline{x}, \underline{\alpha''x}|\}$ ou un sous-groupe plus étendu de σ, dont $\{|\underline{x}, \underline{\alpha''x}|\}$ est lui-même un sous-groupe. Autrement dit, le système *appartient au diviseur* n de $3n$, ou *à un diviseur de* n.

Inversement un système, qui appartient au diviseur n ou à un diviseur de n, possède le sous-groupe $\{|\underline{x}, \underline{\alpha''x}|\}$; s'il contient une caractéristique d'une colonne, il contient le carré de cette caractéristique. Par suite, il est constitué de *carrés entiers* de caractéristiques et complété éventuellement par des caractéristiques imprimitives.

Comme il a déjà été dit, nous espérons obtenir, en partant des considérations du § 9 qui conduisent à de nouvelles propriétés invariantes des colonnes réduites, le nombre exact des systèmes de caractéristiques différents appartenant au diviseur n ou à un diviseur de n. Dans ce Mémoire, nous donnerons seulement une borne *inférieure* et une borne *supérieure* de ce nombre (ou le moyen d'établir ces deux bornes) déterminant ainsi son *ordre de grandeur*, et en faisant remarquer de plus que notre procédé nous met en état également de donner ces systèmes avec la plus grande facilité.

[**24**] Nous appellerons $1, 2, \ldots, 3n$ les éléments β),
et $\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}$ les éléments γ).

Un triple *réduit* représente d'une part les trois caractéristiques de son carré, et d'autre part les éléments β) de trois caractéristiques imprimitives. Si le triple réduit a ses trois éléments γ) *différents*, ces trois caractéristiques imprimitives sont différentes et leurs éléments β) sont neuf des éléments $1, 2, \ldots, 3n$.

Les triples réduits de la colonne II sont les *seuls* (§ 11) à ne pas remplir cette dernière condition; les trois caractéristiques de chacun des carrés de la colonne II ont deux à deux un élément β) commun (voir (15)). Il ne peut pas entrer un carré entier de la colonne II dans un système de caractéristiques.

Nous excluons dès maintenant la colonne II et ses triples réduits des considérations qui suivent.

Un système de m triples réduits, dont les $3m$ éléments γ) sont tous différents, représente $9m$ des éléments $1, 2, \ldots, 3n$, qui sont les éléments de $3m$ caractéristiques imprimitives. Si nous complétons ce système d'éléments γ) par les $(n-3m)$ éléments γ) restants, pris isolément, et qui sont les symboles des $(n-3m)$ caractéristiques imprimitives restantes, nous aurons un *système d'éléments* γ), *constitué de triples et d'éléments isolés*, représentant d'*un système de caractéristiques constitué de carrés entiers, complété par des caractéristiques imprimitives.*

Inversement un système de caractéristiques constitué de carrés entiers, complété éventuellement par des caractéristiques imprimitives, est représenté par le système d'éléments γ) constitué des triples réduits de ses carrés et des éléments γ) restants, symboles de ses caractéristiques imprimitives.

Nous appellerons encore, uniquement pour abréger :

1° Un tel système d'éléments γ), sans élément répété, formé de triples réduits et d'éléments isolés, un *système réduit*.

2° Un système de caractéristiques constitué de carrés entiers, complété ou non par des caractéristiques imprimitives, un *système entier*.

[**25**] Nous appellerons systèmes réduits *différents*, ceux qui ne sont pas déductibles l'un de l'autre par une substitution du groupe

$$\{(\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1})\} = \{|\boldsymbol{x}, \mathbf{1}+\boldsymbol{x}|\},$$

et en conséquence, systèmes réduits *équivalents* ceux du cas contraire.

Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ est triplement isomorphe au groupe $\{|\boldsymbol{x}, \mathbf{1}+\mathbf{x}|\}$; les trois substitutions :

$$|\underline{x}, \underline{\alpha x}|^{a}, \quad |\underline{x}, \underline{\alpha x}|^{a+n}, \quad |\underline{x}, \underline{\alpha x}|^{a+2n}, \quad (a = 0, 1, 2, \ldots, n-1) \tag{37}$$

du premier, correspondent à la substitution $|\boldsymbol{x}, \boldsymbol{a}+\boldsymbol{x}|$ du second. Lorsque l'une des substitutions (37), et par suite les trois, transforment le système entier S_1 en un système S_2, la substitution $|\boldsymbol{x}, \boldsymbol{a}+\boldsymbol{x}|$ transforme le système réduit de S_1 dans le système réduit de S_2 et inversement.

Ainsi les systèmes réduits sont *différents* ou *équivalents*, selon que les systèmes entiers correspondants sont *différents* ou *équivalents*, et le problème de la recherche des systèmes de caractéristiques *différents* appartenant à n ou à un diviseur de n, est ramené à la recherche des systèmes réduits *différents*.

[**26**] Mais pour passer à cette recherche, les définitions suivantes nous sont encore nécessaires et en particulier le théorème plus bas.

Soient les n éléments $0, 1, 2, \ldots, n-1$, n entier positif quelconque, et le groupe cyclique de ces éléments :

$$s = \{(0, 1, 2, \ldots, n-1)\} = \{|x, 1+x|\}.$$

Soit une combinaison quelconque de ces éléments :

$$a_1, a_2, \ldots, a_i; \qquad i = 1, 2, \ldots, n, \tag{38}$$

et toutes les combinaisons qui s'en déduisent par les substitutions du groupe s. Nous appelons l'ensemble de ces combinaisons une *série cyclique* de combinaisons i à i ou simplement *de* C^i.

On a immédiatement les remarques :

1° Une série cyclique de C^i est déterminée par l'une quelconque de ses combinaisons.

2° Une série cyclique de C^i a i et i seules de ses combinaisons contenant l'un quelconque fixé des n éléments(1).

3° Deux séries cycliques de C^i différentes n'ont aucune combinaison commune.

THÉORÈME. — *Chaque série cyclique de* C^i *contient* n *combinaisons, excepté une seule, dans le cas où* n *est multiple de* i, *et qui est celle contenant la combinaison :*

$$0, \frac{n}{i}, 2\frac{n}{i}, \ldots, (i-1)\frac{n}{i}.$$

Ce théorème résulte entièrement du fait suivant (de la théorie des groupes de substitutions) :

Le groupe cyclique $\{|x, 1+x|\}$ est *régulier transitif*, c'est-à-dire : son ordre est égal à son degré, chacune de ses substitutions (autre que la substitution-identité) 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.

Un groupe régulier transitif est de plus *imprimitif*, et chacune de ses substitutions donne une répartition des n éléments en systèmes imprimitifs, constitués directement par les éléments de chaque cycle. Cela signifie que par les substitutions du groupe, les éléments $0, 1, \ldots n$ ne peuvent se transformer les uns dans les autres *autrement que*, les éléments de chaque cycle d'une substitution en eux-mêmes ou entièrement en ceux d'un autre cycle de la même substitution.

Ainsi la combinaison quelconque (38) : $a_1, a_2, \ldots a_i$, ne peut être transformée en elle-même par une substitution du groupe $s = \{|x, 1+x|\}$, autre que l'identité, que si cette substitution contient le cycle $(a_1 a_2 \ldots a_i)$ ou l'une de ses puissances. Mais le cycle $(a_1 a_2 \ldots a_i)$ ou ses puissances ne peuvent appartenir à une substitution de s que lorsque i est diviseur de n, et dans ce cas les seules substitutions de s, ayant des cycles de i éléments ou d'un nombre d'éléments diviseur de i, sont la substitution :

$$|x, 1+x|^{\frac{n}{i}} = \left(0, \frac{n}{i}, \frac{2n}{i}, \ldots, \frac{(i-1)n}{i}\right)\left(1, \frac{n}{i}+1, \frac{2n}{i}+1, \ldots, \frac{(i-1)n}{i}+1\right)\ldots\ldots$$

(1) Il y a une *seule* exception, dans le cas où i est diviseur de n, celle du théorème plus bas.

et ses i premières puissances. Autrement dit, i *étant diviseur de* n, la série cyclique de C^i :

$$\begin{aligned} &0, \quad \frac{n}{i}, \quad \frac{2n}{i}, \ \ldots, \ \frac{(i-1)n}{i}, \\ &1, \quad \frac{n}{i}+1, \ \frac{2n}{i}+1, \ \ldots, \ \frac{(i-1)n}{i}+1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\frac{n}{i}-1, \ \frac{2n}{i}-1, \ \frac{3n}{i}-1, \ \ldots, \ n-1, \end{aligned} \tag{39}$$

est la *seule* dont les combinaisons admettent pour les transformer en elles-mêmes d'autres substitutions de s que l'identité, soit les substitutions du sous-groupe de s : $\{|x, 1+x|^{\frac{n}{i}}\}$. La série cyclique (39) ne contient que $\frac{n}{i}$ combinaisons; la $\left(\frac{n}{i}+1\right)^{\text{ième}}$ reproduit déjà la première, tandis que pour chaque autre série cyclique de combinaisons i à i, ce n'est que la $(n+1)^{\text{ième}}$ qui reproduit la première.

Le nombre des combinaisons i à i est $\frac{n(n-1)\ldots(n-i+1)}{i!}$.

Le nombre des séries cycliques de C^i est donc :

1° Pour i non diviseur de n :

$$\frac{(n-1)(n-2)\ldots(n-i+1)}{i!}; \tag{40}$$

2° Pour i diviseur de n :

$$\frac{1}{n}\left\{\frac{n(n-1)(n-2)\ldots(n-i+1)}{i!}-\frac{n}{i}\right\}+1=\frac{(n-1)(n-2)\ldots(n-i+1)}{i!}+\frac{i-1}{i} \tag{41}$$

Ainsi les deux quotients (40) et (41) sont des nombres *entiers*. Il est possible que l'intégrité de ces quotients soit connue ou ait été remarquée déjà; il est cependant intéressant de la signaler en passant.

Systèmes réduits différents provenant d'une seule colonne réduite.

[**27**] Tout ce qui vient d'être dit au § 26 s'applique aux n éléments γ) $\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}$ et au groupe $\{|\boldsymbol{x}, \mathbf{1}+\boldsymbol{x}|\}$, que nous écrirons dès maintenant, pour simplifier, en caractères courants $0, 1, \ldots, n-1$ et $s=\{|x, 1+x|\}$.

Soit une colonne réduite quelconque, autre que la colonne II; elle peut toujours être rangée de cette manière :

$$0,\ a,\ b;\quad 1,\ a+1,\ b+1;\quad \ldots;\quad n-1,\ a+n-1,\ b+n-1. \qquad (A)$$

Par les substitutions de s, les triples réduits de (A) *se transforment entre eux comme leurs premiers éléments*. Nous les représentons respectivement par ces *premiers* éléments.

Conformément au § 25, ayant deux systèmes quelconques (combinaisons ou systèmes de combinaisons) des éléments $0, 1, \ldots, n-1$, nous continuons à les appeler *équivalents* ou *différents* selon qu'ils sont déductibles l'un de l'autre ou non par les substitutions du groupe s.

Avec cela, ayant la combinaison quelconque de triples réduits de (A) :

$$\alpha,\ a+\alpha,\ b+\alpha;\quad \beta,\ a+\beta,\ b+\beta;\quad \gamma,\ a+\gamma,\ b+\gamma;\quad \ldots,$$

nous la représentons par $\alpha, \beta, \gamma, \ldots$, et pour savoir si une autre combinaison :

$$\alpha',\ a+\alpha',\ b+\alpha';\quad \beta',\ a+\beta',\ b+\beta';\quad \gamma',\ a+\gamma',\ b+\gamma';\quad \ldots,$$

lui est *équivalente* ou en est *différente*, il suffit de savoir si la combinaison $\alpha', \beta', \gamma', \ldots$ est *équivalente* à $\alpha, \beta, \gamma, \ldots$ où en est *différente*, c'est-à-dire si ces deux combinaisons appartiennent ou non à *la même série cyclique*.

Soit l'un des triples de la colonne réduite (A), le triple 0 par exemple. Les éléments $0, a$ et b se retrouvent chacun dans *deux* autres triples de la colonne. Il y a donc *au moins* $n-7$ triples de la colonne (A) dont les éléments diffèrent entièrement de ceux du triple 0. Il en est de même pour chacun des triples $1, 2, \ldots, n-1$. Cela nous donne *au moins* $n(n-7)$ couples des éléments $0, 1, \ldots, n-1$, *représentants* de couples de triples réduits de (A) sans élément répété. Dans ces $n(n-7)$ couples, le même se retrouve *au plus*(1) deux fois; il en reste *au moins* $\frac{n(n-7)}{2}$ différents, au sens habituel du mot. De ces $\frac{n(n-7)}{2}$ couples, il y en a *au plus* n par série cyclique; ils sont donc répartis en *au moins* $\frac{n-7}{2}$ séries cycliques différentes. Nous entendrons sans autre, ici et plus loin, par l'écriture d'un quotient, le plus grand entier *inférieur* ou *égal* à ce quotient, et notre résultat est :

Il y a AU MOINS $\frac{n-7}{2}$ *systèmes réduits différents constitués de deux triples de la colonne* (A) *et des* $n-6$ *caractéristiques imprimitives restantes.*

(1) Il peut se faire que pour le couple a, b, par exemple, le couple b, a soit dans ceux que je néglige en prenant seulement $n(n-7)$ de ces couples de triples sans élément répété.

[**28**] Soit maintenant l'un de ces couples de triples de la colonne (A) sans élément répété. Ses six éléments se retrouvent *chacun* dans *deux* autres triples de la colonne (A). Il y a donc *au moins* $n-14$ triples de la colonne (A) dont les éléments diffèrent entièrement de ces six éléments. Cela nous donne *au moins* $\frac{n(n-7)}{2}(n-14)$ triples des éléments $0, 1, \ldots, n-1$, *représentants* de triples des triples réduits de (A) sans élément répété. Dans ces $\frac{n(n-7)(n-14)}{2}$ triples, le même se retrouve *au plus* trois fois(1); il en reste *au moins* $\frac{n(n-7)(n-14)}{2.3}$ différents, au sens habituel du mot. De ces $\frac{n(n-7)(n-14)}{1.2.3}$ triples, il y en a *au plus* n par série cyclique; ils sont donc répartis en *au moins* $\frac{(n-7)(n-14)}{3!}$ séries cycliques différentes. Notre résultat est :

Il y a AU MOINS $\frac{(n-7)(n-14)}{3!}$ *systèmes réduits différents constitués de trois triples de la colonne* (A) *et des* $n-9$ *caractéristiques imprimitives restantes.*

En continuant de la même manière pour la constitution des quadruples, des quintuples, etc., de triples de la colonne (A) sans élément répété, en tenant compte encore du système réduit constitué de *un* triple de la colonne (A) et des $n-3$ caractéristiques imprimitives restantes, et enfin que notre opération s'applique aux $n-2$ colonnes réduites autres que la colonne II, nous obtenons le nombre *minimum* de systèmes de caractéristiques *différents*, formés avec des carrés entiers pris dans *une seule* colonne de caractéristiques, exprimé par la formule suivante(2) :

$$(n-2)\left\{1+\frac{n-7}{2}+\frac{(n-7)(n-14)}{2.3}+\frac{(n-7)(n-14)(n-21)}{2.3.4}+\ldots\right\} \quad (42)$$

dans laquelle les termes sont à poursuivre tant que les facteurs aux numérateurs restent *positifs*.

[**29**] Il est d'autre part immédiat que le nombre de ces systèmes de caractéristiques *différents*, formés avec des carrés entiers pris dans *une seule* colonne de caractéristiques, *ne dépassera pas* le nombre des séries cycliques des combinaisons i à i,

---

(1) Le triple a, b, c peut se trouver en associant le couple a, b à l'élément c, le couple b, c à l'élément a, et le couple c, a à l'élément b.

(2) Dans notre Note aux Comptes Rendus (voir note du § 1), nous avons donné une formule un peu différente. Celle-ci, que nous avons établie depuis, très simplement comme on l'a vu, est bien meilleure.

pour $i = 1, 2, 3, \ldots, n$, des éléments $0, 1, \ldots, n-1$, multiplié par le nombre $(n-2)$ des colonnes réduites, soit l'expression suivante :

$$(n-2)\left\{1 + \frac{n-1}{2} + \frac{(n-1)(n-2)}{2.3} + \frac{(n-1)(n-2)(n-3)}{2.3.4} + \ldots\right\}. \quad (43)$$

Nous négligeons l'unité qu'il faudrait ajouter aux termes pour lesquels i est diviseur de n, d'après l'expression (41); il est évident que même ainsi ce nombre est encore trop grand et n'est pas atteint par le nombre *exact* de ces systèmes de caractéristiques différents formés de carrés pris dans une seule colonne de caractéristiques.

Pour un n très grand, nous avons ainsi pour ce nombre exact les deux bornes *inférieure* et *supérieure* du *même ordre* de grandeur, (42) et (43).

Systèmes réduits différents provenant de deux colonnes réduites.

[**30**] Soit, avec la colonne (A), une autre colonne réduite quelconque, autre que la colonne II, et rangée encore de la même manière :

$$0, a', b'; \quad 1, a'+1, b'+1; \quad \ldots; \quad n-1, a'+n-1, b'+n-1. \quad (B)$$

Nous continuons à représenter ses triples par leur *premier* élément.

Soit un triple quelconque de la colonne (A). Ses éléments se retrouvent chacun dans *trois* triples de la colonne (B); il y a donc *au moins* $n-9$ triples de la colonne (B) dont les éléments diffèrent entièrement de ceux d'un triple fixé de la colonne (A). Pour un couple de triples de la colonne (A), sans élément répété, il y aura *au moins* $n-18$ triples de la colonne (B), dont les éléments différeront entièrement des six éléments du couple; pour un triple de triples de la colonne (A), *au moins* $n-27$ triples de la colonne (B) dans les mêmes conditions, et ainsi de suite.

Nous notons par la lettre a les éléments représentants des triples (A) et par la lettre b les éléments représentants des triples (B), soit leurs *premiers* éléments. Sans que nous y refassions allusion, il n'est question dans ce qui suit que de combinaisons de triples des colonnes (A) et (B) propres à constituer des systèmes réduits, c'est-à-dire *où les triples sont sans élément commun*.

1° Soit

$$a_1, a_2, \ldots, a_i, \qquad i = 1, 2, 3, \ldots, n, \quad (44)$$

une combinaison quelconque de triples (A), telle que l'identité est la seule substi-

tution de s qui la transforme en elle-même. Les deux combinaisons suivantes :

$$\begin{aligned} &a_1, a_2, \ldots, a_i; \quad b_1, b_2, \ldots, b_k, \qquad k = 1, 2, 3, \ldots, n, \\ &a_1, a_2, \ldots, a_i; \quad b'_1, b'_2, \ldots, b'_{k'}, \qquad k' = 1, 2, 3, \ldots, n, \end{aligned} \tag{45}$$

sont *différentes*, dès que la combinaison $b'_1, b'_2, \ldots, b'_{k'}$ n'est pas *la même* que la combinaison $b_1, b_2, \ldots, b_k$. En effet la partie $a_1, a_2, \ldots, a_i$ ne peut se transformer en elle-même que par l'identité de s; mais pour cette substitution, la partie $b_1, b_2, \ldots, b_k$ se transforme en elle-même et non en $b'_1, b'_2, \ldots, b'_{k'}$.

2° Soit

$$a'_1, a'_2, \ldots, a'_i,$$

une combinaison *équivalente* à la combinaison (44). Toute combinaison :

$$a'_1, a'_2, \ldots, a'_i; \quad b''_1, b''_2, \ldots, b''_{k''}, \qquad k'' = 1, 2, \ldots, n, \tag{46}$$

est équivalente à une combinaison du type (45), puisqu'il y a une substitution de s qui la transforme en une combinaison du type (45).

3° Soit

$$a''_1, a''_2, \ldots, a''_k, \qquad k = 1, 2, \ldots, n,$$

une combinaison *différente* de la combinaison (44). Aucune combinaison :

$$a''_1, a''_2, \ldots, a''_k; \quad b''_1, b''_2, \ldots, b''_{k''} \tag{47}$$

ne peut être équivalente à une combinaison du type (45), car il n'y a aucune substitution de s qui la transforme en une combinaison du type (45).

4° Chaque combinaison de la forme :

$$a_1, a_2, \ldots, a_i; \quad b_1, b_2, \ldots, b_i, \qquad i = 1, 2, \ldots, n, \tag{48}$$

est en même temps une combinaison de i triples de la colonne (A) complétée par i triples de la colonne (B), et une combinaison de i triples de la colonne (B) complétée par i triples de la colonne (A). S'il existe p combinaisons *différentes* formées de i triples de (A) complétés avec i triples de (B), ces combinaisons sont aussi celles que l'on obtiendra en formant les combinaisons différentes de i triples de (B) complétés par i triples de (A).

5° Deux combinaisons sont *différentes* dès que le nombre de leurs triples dans l'une des colonnes n'est pas le même, puisque les triples qui auraient à se transformer les uns dans les autres ne sont pas en nombre égal.

[**31**] Nous sommes maintenant en état d'écrire le nombre *minimum* des systèmes réduits différents formés avec des triples pris dans les deux colonnes (A) et (B).

Nous écartons, comme nous l'avons déjà fait dans 1° et 2° (§ 30), les combinaisons de triples $a_1, a_2, \ldots, a_i$ ou $b_1, b_2, \ldots, b_k$ qui appartiendraient à la série cyclique singulière (39), dans le cas de i ou k diviseur de n, et admettant pour les transformer en elles-mêmes, avec l'identité d'autres substitutions de s.

D'après 1°, et en tenant compte de ce qui est établi aux § 27 et 28 pour le nombre des combinaisons de triples d'une même colonne, le nombre minimum des systèmes réduits différents, formés avec la combinaison (44) de la colonne (A), est, en posant $n - 9i = \mu$:

$$\mu + \frac{\mu(\mu-7)}{2} + \frac{\mu(\mu-7)(\mu-14)}{2.3} + \ldots .$$

D'après 2° et 3°, et en tenant compte de ce qui est établi aux § 27 et 28 pour le nombre des séries cycliques auxquelles peuvent appartenir les combinaisons de triples d'une même colonne, le nombre minimum des systèmes réduits différents du type :

$$a_1, a_2, \ldots, a_i; \quad b_1, b_2, \ldots, b_k, \qquad i = 1, 2, \ldots, n, \qquad k \gtreqless i,$$

$a_1, a_2, \ldots, a_i$ étant une combinaison quelconque des n triples de la colonne (A) et $b_1, b_2, \ldots, b_k$ une combinaison quelconque d'un nombre de triples égal ou supérieur pris dans les $n - 9i$ triples de la colonne (B) admissibles avec $a_1, a_2, \ldots, a_i$ est :

$$\begin{aligned}
&1\left\{n - 9 + \frac{(n-9)(n-16)}{2} + \frac{(n-9)(n-16)(n-23)}{2.3} + \ldots\right\}\\
&+\frac{n-7}{2}\left\{\frac{(n-18)(n-25)}{2} + \frac{(n-18)(n-25)(n-32)}{2.3} + \ldots\right\}\\
&+\frac{(n-7)(n-14)}{2.3}\left\{\frac{(n-27)(n-34)(n-41)}{2.3} + \frac{(n-27)(n-34)(n-41)(n-48)}{2.3.4} + \ldots\right\}\\
&+ \ldots\ldots
\end{aligned} \tag{49}$$

Les termes dans les grandes parenthèses et les termes facteurs de celles-ci sont à poursuivre tant que les facteurs aux numérateurs restent positifs. Les termes facteurs des grandes parenthèses sont à diminuer de 1 pour les i diviseurs de n, excepté $i = 1$, car il pourrait se faire que la série cyclique singulière (39), dans le cas de i diviseur de n, soit comprise dans les $\frac{(n-7)(n-14)\ldots[n-(i-1)7]}{i!}$ séries cycliques du cas général obtenues aux § 27 et 28, et nous avons écarté les combinaisons $a_1, a_2, \ldots, a_i$ qui appartiendraient à cette série singulière (§ 30, 1°).

En opérant maintenant avec la colonne (B) comme nous venons de le faire avec la colonne (A), le nombre minimum des systèmes réduits différents du type :

$$b_1, b_2, \ldots, b_i; \quad a_1, a_2, \ldots, a_k, \qquad i = 1, 2, \ldots, n, \qquad k \gtreqless i,$$

$b_1, b_2, \ldots, b_i$ étant une combinaison quelconque des n triples de la colonne (B) et $a_1, a_2, \ldots, a_k$ une combinaison quelconque d'un nombre de triples égal ou supérieur pris dans les $n-9i$ triples de la colonne (A) admissibles avec $b_1, b_2, \ldots, b_i$, est la même expression (49). D'après 4°, § 30, nous savons que les systèmes réduits différents dans lesquels $i=k$, sont les mêmes dans les deux opérations faites. Par contre, d'après 5°, ceux de la seconde opération dans lesquels $i<k$, c'est-à-dire où il y a plus de triples de (A) que de (B), ne peuvent être que tous différents des systèmes réduits de la première opération avec $i<k$, dans lesquels il y a plus de triples de (B) que de (A).

Ainsi le résultat des deux opérations sera, en les appliquant à chaque paire des $n-2$ colonnes réduites autres que la colonne II, et en complétant constamment, comme il est sous-entendu déjà, les systèmes de carrés par les caractéristiques imprimitives manquantes, le nombre *minimum* suivant de systèmes de caractéristiques différents formés avec des carrés pris dans *deux* colonnes de caractéristiques :

$$\begin{aligned}
&\frac{(n-2)(n-3)}{2}\Bigg[1\Big\{n-9+2\frac{(n-9)(n-16)}{2!}+2\frac{(n-9)(n-16)(n-23)}{3!}+\ldots\Big\}\\
&\qquad+\frac{n-7}{2!}\Big\{\frac{(n-18)(n-25)}{2!}+2\frac{(n-18)(n-25)(n-32)}{3!}+\ldots\Big\}\\
&+\frac{(n-7)(n-14)}{3!}\Big\{\frac{(n-27)(n-34)(n-41)}{3!}+2\frac{(n-27)(n-34)(n-41)(n-48)}{4!}+\ldots\Big\}\\
&+\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\Bigg].
\end{aligned}\tag{50}$$

[**32**] D'autre part il est facile de donner une borne *supérieure* pour ce nombre des systèmes de caractéristiques différents formés de carrés pris dans deux colonnes de caractéristiques, ou de systèmes réduits différents formés de triples pris dans deux colonnes réduites.

Une combinaison de triples des deux colonnes (A) et (B) ne peut être constituée que de *l'une des façons suivantes* :

un triple de A (de B) avec un, deux, trois, etc., triples de B (de A),

deux triples de A (de B) avec deux, trois, quatre, etc., triples de B (de A),

trois triples de A (de B) avec trois, quatre, cinq, etc., triples de B (de A),

. . . . . .

C'est *conformément à cette marche* que nous avons établi les expressions (49) et (50). *D'après les points* 1° *à* 5° *du* § 30, *nous sommes assurés, en suivant la même*

marche, d'écrire un nombre *supérieur* au nombre exact de ces systèmes réduits différents, en écrivant l'expression :

$$\begin{aligned}\frac{(n-2)(n-3)}{2}\Bigg[&1\left\{n-3+2\frac{(n-3)(n-7)}{2!}+2\frac{(n-3)(n-7)(n-11)}{3!}+\dots\right\}\\&+\frac{n-1}{2}\left\{\frac{(n-6)(n-10)}{2!}+2\frac{(n-6)(n-10)(n-14)}{3!}+\dots\right\}\\&+\frac{(n-1)(n-2)}{3!}\left\{\frac{(n-9)(n-13)(n-17)}{3!}+2\frac{(n-9)(n-13)(n-17)(n-21)}{4!}+\dots\right\}\\&+\dots\dots\dots\Bigg].\end{aligned} \tag{51}$$

En effet, nous prenons comme facteurs des parenthèses $\{\dots\}$ le nombre même des séries cycliques de combinaisons i à i; pour i diviseur de n, excepté $i=1$, ce facteur écrit dans (51) est à augmenter de 1 (voir (41)), car la série cyclique singulière (39), que nous écartons dans 1°, § 30, peut également fournir des combinaisons du type (45), mais qui peuvent être équivalentes entre elles sans que $b'_1, b'_2, \dots, b'_{k'}$ soit identique à $b_1, b_2, \dots, b_k$. Pour les facteurs binômes dans les parenthèses $\{\dots\}$, nous partons de $n-3$, $n-6$, etc., car les trois éléments d'un triple d'une colonne se retrouvent *au moins* dans *trois* triples de l'autre colonne(¹), les six éléments d'un couple de triples d'une colonne, *au moins* dans *six* triples de l'autre colonne, etc.; et nous retranchons 4 pour les facteurs successifs qui s'en déduisent, parce que les trois éléments d'un triple d'une colonne se retrouvent *au moins* dans *trois autres* triples de cette colonne(²), etc.

[33] Nous pourrions maintenant poursuivre et appliquer le procédé établi à trois colonnes réduites, autres que la colonne II, puis à quatre colonnes réduites, etc. Nous donnerions ainsi une borne inférieure et une borne supérieure du nombre des systèmes de caractéristiques différents formés de carrés pris dans *trois*, puis dans *quatre*, etc., colonnes de caractéristiques. Il serait en tout cas facile de donner ici encore des expressions du *même ordre de grandeur* que ces bornes pour trois, pour quatre colonnes de caractéristiques, etc. Mais nous ne pouvons étendre davantage cet exposé, déjà suffisamment long, et la complication des résultats les rend moins intéressants. Il sera temps d'ailleurs d'aborder ces expressions, lorsque nous vou-

(¹) Chacun des trois éléments d'un triple a, b, c de la colonne (A) doit se retrouver dans *trois* triples de la colonne (B); il faut donc *au moins trois* triples de la colonne (B) pour contenir ces 9 éléments $a, a, a,\ b, b, b,\ c, c, c$.

(²) Chacun des trois éléments d'un triple a, b, c, de la colonne (A) doit se retrouver dans *deux autres* triples de la colonne (A); il faut donc *au moins trois autres* triples de (A) pour contenir les 6 éléments $a, a,\ b, b,\ c, c$, qui ne peuvent, en aucun cas, se retrouver trois ensemble dans un triple de (A).

drons parvenir au nombre exact de ces systèmes de caractéristiques différents, appartenant à n ou à un diviseur de n, à moins que nous ne puissions trouver une voie plus courte, qui évite l'établissement de ce nombre successivement pour une, pour deux, pour trois, etc., colonnes de caractéristiques.

Un système de caractéristiques, appartenant à n ou à un diviseur de n, possède le sous-groupe $\{|x, \alpha^n x|\}$; autrement dit la substitution $|x, \alpha x|^n$ le transforme en lui-même. D'après J., § 14, p. 90, les transformés d'un système cyclique de triples de Steiner déterminé par un tel système de caractéristiques, par les puissances $0, n, 2n, 3n, 4n, 5n$ de la substitution $|x, \alpha x|$ et par ces seules puissances de cette substitution, sont des systèmes cycliques de triples du même système de caractéristiques.

En admettant le théorème(1) *que les systèmes cycliques de triples de Steiner équivalents sont déductibles l'un de l'autre par une substitution métacyclique* (note 1 du § 23), *tous* les systèmes cycliques de triples *équivalents* à un système donné sont ses transformés par les substitutions $|x, \alpha x|^\nu$, $\nu = 0, 1, \ldots, 6n-1$. Par suite, CHACUN *des systèmes de caractéristiques, appartenant à n ou à un diviseur de n, obtenus précédemment, détermine au moins* $\frac{2^n}{6} = \frac{2^{n-1}}{3}$ (2) *systèmes cycliques de triples de Steiner* DIFFÉRENTS (§ 2, 2°). Ainsi, en admettant le théorème indiqué, le résultat *pour les systèmes cycliques de triples de Steiner* est important; mais même indépendamment de ce théorème, non démontré encore et sur lequel nous nous sommes exprimés dans J., p. 75 et 98, les résultats obtenus *pour les seuls systèmes de caractéristiques*, c'est-à-dire pour la solution du problème de Heffter (voir A., p. 58), ont déjà leur intérêt.

---

(1) *Le théorème est actuellement démontré* et ainsi les résultats que nous énonçons plus bas, *établis d'une façon définitive*. (Voir Actes de la Soc. helvétique des Sciences naturelles, Lucerne 1924. II[e] partie, p. 104-105.)

(2) En entendant sans autre, comme jusqu'ici, par ce quotient le plus grand entier qui lui est *inférieur* ou *égal*.