

**Zeitschrift:** Commentarii Mathematici Helvetici  
**Herausgeber:** Schweizerische Mathematische Gesellschaft  
**Band:** 4 (1932)  
  
**Artikel:** Sur les systèmes cycliques de triples de Steiner différents pour  $N$  premier de la forme  $6n + 1$ .  
**Autor:** Bays, S.  
**DOI:** <https://doi.org/10.5169/seals-5619>

### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 04.12.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# Sur les systèmes cycliques de triples de Steiner différents pour $N$ premier de la forme $6n + 1$

par S. BAYS, Fribourg

## Les systèmes cycliques de triples différents dans les cas $d = 1$ et $d = 3$

1. Cette étude fait suite directement au mémoire paru sur le même sujet dans les fascicules précédents des Comm. Math. Helv.<sup>1)</sup>. Les références de paragraphes, chiffres et notes, données dans le texte, se rapportent exclusivement au mémoire indiqué<sup>2)</sup>, sauf celles qui de toute évidence se rapportent au texte actuel.

Au chapitre V, nous avons établi, pour chercher à déterminer le nombre et la nature des systèmes cycliques de triples différents, *déterminés* (§ 45, premier alinéa) par un système de caractéristiques  $\Sigma$  qui appartient au diviseur  $d$  de  $3n$ , l'équation suivante (50):

$$2^{n-a-1} = \mu_1' x_1 + \mu_2' x_2 + \dots + \mu_k' x_k, \quad (1)$$

dans laquelle  $\frac{3n}{d} = 2^a n_1$ ,  $n_1$  entier impair  $\equiv 1$ ,  $a$  entier  $\equiv 0$ ;  $\mu_1' = 1$ ,  $\mu_2', \mu_3', \dots, \mu_{k-1}', \mu_k' = n_1$ , sont les diviseurs de  $n_1$ ;  $x_i$  est le nombre des systèmes de triples différents déterminés par  $\Sigma$  qui possèdent (note 44) le diviseur métacyclique  $\{|x, 1+x|, |x, \alpha^{\omega_i} x|\}$ ,  $\omega_i = 2\mu_i' d = 2^{a+1} \cdot \mu_i' d$ .

Dans le cas  $d = 1$ , cette équation est remplacée par une équation plus simple (53):

$$2^{n-a-1} = \mu_1' x_1 + \mu_2' x_2 + \dots + \mu_{k'}' x_{k'}, \quad (2)$$

dans laquelle  $n = 2^a n_1'$ ,  $n_1'$  entier impair  $\equiv 1$ ,  $a$  entier  $\equiv 0$ ;  $\mu_1' = 1$ ,  $\mu_2', \mu_3', \dots, \mu_{k'-1}', \mu_{k'}' = n_1'$ , sont les diviseurs de  $n_1'$ ;  $x_i$  est le nombre

1) Voir Vol. 2, Fasc. IV; Vol. 3, Fasc. I, II et IV.

2) Avec la répartition suivante:

Vol. 2, Fasc. IV: Avant-propos et chap. I,	§ 1 à 16, chiffre 1 à 13, note 1 à 26.
Vol. 3, Fasc. I: Chapitres II et III,	§ 17 à 33, chiffre 14 à 30, note 27 à 40.
Vol. 3, Fasc. II: Chapitres IV et V,	§ 34 à 51, chiffre 31 à 54, note 41 à 46.
Vol. 3, Fasc. IV: Chapitre VI,	§ 52 à 59, chiffre 55 à 69, note 47 à 52.

des systèmes de triples différents, déterminés par le système des caractéristiques principales, qui possèdent (note 44) le diviseur métacyclique  $\{ |x, 1+x|, |x, \alpha^{\omega_i} x| \}$ ;  $\omega_i = 2 \mu_i = 2^{a+1} \cdot \mu_i'$ .

Le cas  $d=3$ , déduit de l'équation (1) donne la même équation (2) que le cas  $d=1$  traité d'une façon particulière (§ 50).

2. Dans cette étude nous établissons pour cette équation (2) commune aux cas  $d=1$  et  $d=3$ , les trois théorèmes suivants :

**Théorème 1.** *La solution  $(x_1, x_2, \dots, x_k)$  de l'équation (2) commune aux deux cas  $d=1$  et  $d=3$ , est la même, pour le système des caractéristiques principales comme pour chaque système de caractéristiques appartenant à  $d=3$ . Elle ne dépend que de  $n$ . En particulier donc, le nombre  $x_1 + x_2 + \dots + x_k$  des systèmes de triples différents déterminés par le système des caractéristiques principales et par chaque système de caractéristiques appartenant à  $d=3$ , est le même.*

**Théorème 2.** *Quel que soit  $n$ , on a dans cette équation (2):  $x_k \equiv 1$ ,  $x_1 \equiv 1$ .*

*Plus explicitement, dans les systèmes de triples déterminés par le système des caractéristiques principales, il en existe au moins un qui ne possède que le diviseur d'ordre minimum  $\{ |x, 1+x|, |x, \alpha^{2^n} x| \}$  et au moins un qui possède le diviseur d'ordre maximum  $\{ |x, 1+x|, |x, \alpha^{\omega} x| \}$ ,  $\omega = 2^{a+1}$ , (§ 49, II).*

*Dans les systèmes de triples déterminés par un système de caractéristiques appartenant à  $d=3$ , il en existe au moins un qui ne possède que le diviseur d'ordre minimum  $\{ |x, 1+x|, |x, \alpha^{6^n} x| \} = \{ |x, 1+x| \}$  et au moins un qui possède le diviseur d'ordre maximum  $\{ |x, 1+x|, |x, \alpha^{\omega} x| \}$ ,  $\omega = 3 \cdot 2^{a+1}$ , (§ 49, I).*

**Théorème 3.** *Pour  $n = 2^a \cdot p$ ,  $p$  premier impair, la solution de l'équation (2), qui dans ce cas n'a que deux termes au second membre,  $2^{n-a-1} = x_1 + p x_2$ , est la suivante :*

$$x_1 = 2^{2^a - a - 1}, \quad x_2 = \frac{2^{n-1} - 2^{2^a - 1}}{n}. \quad (3)$$

Le nombre  $x_1 + x_2$  des systèmes de triples différents déterminés par le système des caractéristiques principales et par chaque système de caractéristiques appartenant à  $d = 3$ , est ainsi, dans ce cas  $n = 2^a \cdot p$ :

$$x_1 + x_2 = \frac{2^{n-1} + 2^{2^a-1} (p - 1)}{n}$$

Nous n'établissons pas ces résultats exactement dans cette disposition, qui a été admise uniquement pour avoir plus de clarté et d'ordre dans les énoncés. Nous démontrons d'abord la première partie du théorème 2,  $x_k \equiv 1$ ; le résultat est tel qu'il contient en somme implicitement le fait du théorème 1. L'établissement de la seconde partie du théorème 2,  $x_1 \equiv 1$ , et du théorème 3 vient ensuite.

Avec ces résultats, la réponse à la question posée au § 51, dernier alinéa, est sans autre:

Pour  $N = 61$ ,  $n = 2^1 \cdot 5$  ;  $x_1 = 2^{2^1-1-1} = 1$  ;

$$x_2 = \frac{2^9 - 2^{2^1-1}}{10} = 51 ; \quad x_1 + x_2 = 52,$$

Pour  $N = 67$ ,  $n = 2^0 \cdot 11$  ;  $x_1 = 2^{2^0-0-1} = 1$  ;

$$x_2 = \frac{2^{10} - 2^{2^0-1}}{11} = 93 ; \quad x_1 + x_2 = 94,$$

Pour  $N = 73$ ,  $n = 2^2 \cdot 3$  ;  $x_1 = 2^{2^2-2-1} = 2$  ;

$$x_2 = \frac{2^{11} - 2^{2^2-1}}{12} = 170 ; \quad x_1 + x_2 = 172,$$

Pour  $N = 79$ ,  $n = 2^0 \cdot 13$  ;  $x_1 = 2^{2^0-0-1} = 1$  ;

$$x_2 = \frac{2^{12} - 2^{2^0-1}}{13} = 315 ; \quad x_1 + x_2 = 316.$$

Ces solutions sont bien celles du *minimum* pour  $x_1 + x_2$  (§ 51 et § 47, 3<sup>o</sup>).

La solution (3) trouvée est en effet celle du *minimum* pour  $x_1 + x_2$  dans les cas  $a = 0$ ,  $a = 1$ ,  $a = 2$ , puisque dans ces cas  $x_1 = 1$ ,  $x_1 = 1$ ,  $x_1 = 2$  ; mais déjà pour  $a = 3$  la solution (3) *n'est plus nécessairement celle du minimum* pour  $x_1 + x_2$ . Il est évident en effet que pour  $a \geq 3$ ,  $x_1 = 2^{2^a-a-1}$  n'est plus nécessairement le plus petit entier<sup>3)</sup>, pour lequel

<sup>3)</sup> Dans l'équation indéterminée  $2^{n-a-1} = x_1 + p x_2$ , le nombre  $x_1 + x_2$  prend sa plus petite valeur pour  $x_1$  minimum.



$\frac{2^{n-a-1} - x_1}{p}$  est entier, ou  $2^{n-a-1} \equiv x_1 \pmod{p}$ . Ainsi pour  $n = 2^3 \cdot 3$ ,  $2^{2^3-3-1} = 2^4 = 16$  et on a déjà  $2^{20} \equiv 1 \pmod{3}$ . Par contre il doit être facile de prouver directement que  $2^{n-a-1} \equiv 2^{2^a-a-1} \pmod{p}$  ou donc que l'expression de  $x_2$  dans (3) est un entier.

3. **Théorème 2, 1<sup>re</sup> partie,  $x_k \equiv 1$ .** Nous ferons la démonstration pour le système [des caractéristiques principales; la démonstration pour un système de caractéristiques appartenant à  $d = 3$  en découle immédiatement.

Soit  $0, 1, 2, \dots, n-1$ , les  $n$  caractéristiques principales (§ 31). La substitution  $\tau = |\underline{x}, \underline{\alpha x}|$  change ce système des caractéristiques principales  $\Sigma_1$  en lui-même en opérant la permutation circulaire (notes 7 et 27) ( $0 \mid 2 \dots \overline{n-1}$ ). Soit  $0$ , l'une des deux colonnes de triples déterminées par  $0$ . La substitution  $t = |x, \alpha x|$  la change en l'une des deux colonnes de triples déterminées par  $1$ ; celle-ci à son tour, en l'une des deux colonnes de triples déterminées par  $2$ , et ainsi de suite. Désignons par  $0, 1, 2, \dots, n-1$ , la série des  $n$  colonnes cycliques de triples ainsi déduites de  $0$  par les substitutions  $t^0, t^1, t^2, \dots, t^{n-1}$ ; elle est un système cyclique de triples déterminée par  $\Sigma_1$  (§ 45).

La série des colonnes cycliques de triples déduites de  $0$  par les puissances successives de la substitution  $t$  se présente donc de la façon suivante, en désignant par  $i'$  la conjuguée de la colonne  $i$ :

$$0, 1, 2, \dots, n-1, 0', 1', 2', \dots, (n-1)', 0, 1, \dots \quad (4)$$

et cela toujours pour les mêmes raisons: d'une part (§ 45, deuxième alinéa), lorsque  $\sigma = |\underline{x}, \underline{\beta x}|$  change une caractéristique en une caractéristique,  $u = |x, \beta x|$  change la paire de colonnes conjuguées déterminée par la première caractéristique en la paire déterminée par la seconde; d'autre part, dans la série des colonnes déduites de l'une d'elles par les puissances successives de la substitution  $t$ , une colonne ne peut se représenter avant sa conjuguée. Par conséquent le système de triples  $S_1$ , constitué des colonnes  $0, 1, 2, \dots, n-1$ , et déterminé par  $\Sigma_1$ , ne possède que le diviseur d'ordre minimum  $\{|x, 1+x|, |x, \alpha^{2^n} x|\}$ , ce qui était à établir.

Un système de caractéristiques  $\Sigma_2$  appartenant à  $d = 3$  est un rectangle (31) de  $n$  caractéristiques (§ 38). Notons aussi momentanément par

0, 1, 2, ...,  $n-1$ , ces  $n$  caractéristiques. Les deux autres systèmes de caractéristiques équivalents à  $\Sigma_2$ , qui se déduisent de  $\Sigma_2$  par les substitutions  $\tau^1$  et  $\tau^2$ , n'ont aucune caractéristique commune avec lui (§ 38).

La substitution  $\tau^3 = |x, \alpha^3 x|$  change le système  $\Sigma_2$  en lui-même, en opérant encore la permutation circulaire (0 1 2 ...  $n-1$ ). Par conséquent, ce qui vient d'être dit de la substitution  $t$  et de ses puissances  $t^0, t^1, t^2, \dots, t^{n-1}, t^n, t^{n+1}, \dots$ , relativement au système  $\Sigma_1$  et aux colonnes de triples qu'il détermine, se répète identiquement de la substitution  $t^3$  et de ses puissances  $t^0, t^3, t^6, \dots, t^{3(n-1)}, t^{3n}, t^{3(n+1)}, \dots$ , relativement au système  $\Sigma_2$  et aux colonnes de triples qu'il détermine. La série des colonnes de triples déduites de la colonne 0 par les puissances successives de  $t^3$  se présente de la même façon (4) et le système de triples  $S_2$ , constitué des colonnes 0, 1, 2, ...,  $n-1$ , et déterminé par  $\Sigma_2$ , ne possède que le groupe cyclique  $\{ |x, 1 + x| \}$ , ce qui était aussi à établir.

4. Une colonne cyclique de  $i$ -uples des éléments 0, 1, 2, ...,  $m-1$ , est l'ensemble des  $m$   $i$ -uples (combinaisons  $i$  à  $i$ ) suivants :

$$a_1 + x, a_2 + x, \dots, a_i + x, \quad 1 \leq i \leq m, \quad (5)$$

où  $a_1, a_2, \dots, a_i$  sont  $i$  entiers différents parmi 0, 1, 2, ...,  $m-1$ ;  $x = 0, 1, 2, \dots, m-1$ ; chaque entier  $> m-1$  est remplacé par son plus petit reste positif ou nul (mod  $m$ ).

Cette colonne est fixée par l'un quelconque de ses  $i$ -uples, que l'on peut appeler sa tête de colonne.

En combien de colonnes cycliques différentes se répartissent les

$$\frac{m(m-1)(m-2) \dots (m-i+1)}{i!}$$

$i$ -uples des  $m$  éléments? Quel est le nombre des  $i$ -uples différents dans chacune de ces colonnes? La réponse à ces deux questions prend une importance de plus en plus grande dans cette recherche des systèmes cycliques de triples différents; elle aurait sans doute la même importance aussi dans l'étude plus générale des fonctions cycliques<sup>4)</sup> différentes d'une forme donnée quelconque.

J'ai cru avoir établi en passant, dans un mémoire précédent<sup>5)</sup>, un théorème qui était une réponse à ces deux questions. J'ai rappelé ce

<sup>4)</sup> Qui possèdent le groupe cyclique  $\{ (0 \ 1 \ 2 \ \dots \ m-1) \}$  de leurs  $m$  variables 0, 1, 2, ...,  $m-1$ .

<sup>5)</sup> Annales de la Faculté des Sciences de Toulouse, 1925, t. XVII, p. 52—53.

théorème dans la note 25 du mémoire actuel auquel je me réfère. Mais mon énoncé contient une erreur; la réponse complète n'est de loin pas aussi simple que je l'avais vue. Heureusement cette erreur n'entache gravement aucune des applications que j'ai faites jusqu'ici du théorème, également dans le mémoire où je l'ai établi<sup>6)</sup>.

L'énoncé incomplet, mais *exact* et suffisant pour corriger le premier et pour l'application qui en sera faite plus loin (§ 8) est le suivant: Soit  $1 < i < m$ <sup>7)</sup>:

I. Si  $i$  est *premier* avec  $m$ , chaque colonne cyclique de  $i$ -uples de  $m$  éléments, contient  $m$   $i$ -uples différents. Le nombre des colonnes cycliques différentes de  $i$ -uples des  $m$  éléments est donc dans ce cas:

$$\frac{(m-1)(m-2)\dots(m-i+1)}{i!}$$

II. Si  $i$  est diviseur **premier** de  $m$ , une colonne n'a que  $\frac{m}{i}$   $i$ -uples différents, celle déterminée par le  $i$ -uple:

$$0, \frac{m}{i}, \frac{2m}{i}, \dots, \frac{(i-1)m}{i}. \quad (6)$$

Les  $i$ -uples des  $m$  éléments se répartissent donc, dans ce cas, en:

$\frac{1}{m} \left\{ \frac{m(m-1)(m-2)\dots(m-i+1)}{i!} - \frac{m}{i} \right\}$  col. cycl. de  $m$   $i$ -uples chacune, et **une** col. cycl. de  $\frac{m}{i}$   $i$ -uples<sup>8)</sup>.

6) C'est en cherchant la démonstration du théorème 3 énoncé plus haut, que j'ai découvert mon erreur. Dans le mémoire actuel des Comm. Math. Helv., au § 41, B, il n'y a qu'à remplacer dans (42) la condition  $i$  non diviseur de  $n$  par  $i$  *premier* avec  $n$  et la condition  $i$  diviseur de  $n$  par  $i$  *diviseur premier* de  $n$ . Avec cela, tout peut subsister à peu près sans aucun changement, parce que dans les deux applications que je fais,  $i=2$  et  $i=3$ ,  $i$  est ou premier avec  $n$ , ou diviseur premier de  $n$ .

7) Le cas  $1=i=m$  est banal. Dans le cas  $i=1 < m$ , il y a **une** colonne de  $m$   $i$ -uples. Dans le cas  $i=m > 1$ , il y a **une** colonne de 1  $i$ -uple.

8) Les expressions:

$$\frac{(m-1)(m-2)\dots(m-i+1)}{i!}, \quad 1 < i < m, \quad i \text{ premier avec } m,$$

et

$$\frac{(m-1)(m-2)\dots(m-i+1)}{i!} - \frac{1}{i}, \quad 1 < i < m, \quad i \text{ diviseur premier de } m,$$

sont donc des *entiers*. Pour la première du moins, le fait est facile à établir directement. Dans les expressions correspondantes (40) et (41), p. 53, du mémoire cité à la note 5), les conditions  $i$  non diviseur de  $n$  et  $i$  diviseur de  $n$  sont à remplacer, comme plus haut (note 6), par  $i$  *premier* avec  $n$  et  $i$  *diviseur premier* de  $n$ .

III. et IV. Si  $i$  est diviseur **composé** de  $m$ , avec la colonne (6), d'autres encore ont moins de  $m$   $i$ -uples. Si  $i$  et  $m$  ont un p. g. c. d.  $\delta > 1$  et  $< i$ , (6) n'est pas un  $i$ -uple, mais certaines colonnes ont encore moins de  $m$   $i$ -uples.

Je reprendrai ailleurs l'étude et si possible l'établissement du théorème sous sa forme complète. La réponse complète aux deux questions posées plus haut paraît en tout cas nécessaire pour résoudre l'équation (2) dans le cas de  $n$  quelconque. Pour ici, le premier point de l'énoncé ci-dessus nous suffit; nous allons l'établir d'une façon simple et cette fois-ci entièrement correcte.

5. Soit la substitution circulaire  $s = (012 \dots \overline{m-1}) = |x, 1+x|$ . Soit une substitution quelconque du groupe  $\{s\}$ . Cette substitution a des cycles égaux, qui contiennent ensemble les  $m$  éléments (note 27), et, par le sens même de la notation cyclique, change les éléments de chacun de ses cycles en eux-mêmes.

Si un  $i$ -uple est constitué de *un* ou *plusieurs* cycles d'une même substitution du groupe  $\{s\}$ , il est changé en lui-même par cette substitution. Inversement, si un  $i$ -uple donné est changé en lui-même par une substitution  $s^a$  du groupe  $\{s\}$ , autre que l'identité, il contient d'un cycle quelconque de  $s^a$  ou *tous les éléments* ou *aucun*. La preuve en est simple. Soit  $\alpha_i$  un élément d'un cycle de  $s^a$ , contenu dans le  $i$ -uple; soit  $\alpha_k$  le premier élément qui suit  $\alpha_i$  dans le cycle et qui ne serait pas contenu dans le  $i$ -uple. L'élément précédent  $\alpha_j$  est contenu dans le  $i$ -uple et par  $s^a$  est changé en l'élément  $\alpha_k$  qui ne s'y trouverait pas; mais cela est impossible avec l'hypothèse que  $s^a$  change le  $i$ -uple en lui-même.

Pour qu'une substitution du groupe  $\{s\}$ , autre que l'identité, change un  $i$ -uple en lui-même, il *faut* donc et il *suffit* que ce  $i$ -uple soit constitué exclusivement des éléments de *un* ou *plusieurs* cycles de cette substitution<sup>9)</sup>. D'autre part, chaque  $i$ -uple est constitué des éléments de un ou plusieurs cycles de l'identité (0) (1) (2) ... ( $m-1$ ); mais l'identité change aussi chaque  $i$ -uple en lui-même.

Le nombre  $k$  des éléments d'un cycle d'une substitution de  $\{s\}$ , autre que l'identité, est un diviseur de  $m$ ,  $> 1$ . Pour qu'une telle substitution change un  $i$ -uple en lui-même, il *faut* donc que  $i$  et  $m$  ait un diviseur commun  $k > 1$ . La colonne cyclique de  $i$ -uples (5) des éléments 0, 1, 2,

<sup>9)</sup> Mon erreur la première fois est venue du fait d'avoir omis de considérer le cas où le  $i$ -uple est constitué de *plusieurs* cycles d'une même substitution du groupe.

...,  $m - 1$ , aura donc  $m$   $i$ -uples différents, tant que  $i$  et  $m$  sont premiers entre eux, c. q. f. d.

6. **Théorème 1.** Appelons de nouveau *éléments* les symboles représentant les colonnes cycliques de triples de la série (4). Les substitutions  $t$ , dans le cas du système de caractéristiques  $\Sigma_1$ ,  $t^3$ , dans le cas du système de caractéristiques  $\Sigma_2$ , appliquées à ces colonnes cycliques de triples, produisent la substitution circulaire  $s = (0\ 1\ 2\ \dots\ \overline{n-1}\ 0'\ 1'\ \dots\ \overline{n-1}')$   $= |x, 1 + x|$  des  $2n$  éléments  $0, 1, 2, \dots, n-1, 0', 1', \dots, (n-1)'$ .

Formons le tableau *cyclique* suivant de ces éléments :

$$\begin{array}{cccccccccccc}
 0, & 1, & 2, & \dots, & n-1, & 0', & 1', & 2', & \dots, & (n-1)', & & \\
 1, & 2, & 3, & \dots, & 0', & 1', & 2', & 3', & \dots, & 0, & & \\
 \dots, & & & & & & & & & & & \\
 \dots, & & & & & & & & & & & \\
 n-1, & 0', & 1', & \dots, & (n-2)', & (n-1)', & 0, & 1, & \dots, & n-2, & & \\
 0', & 1', & 2', & \dots, & (n-1)', & 0, & 1, & 2, & \dots, & n-1, & (7) & \\
 1', & 2', & 3', & \dots, & 0, & 1, & 2, & 3, & \dots, & 0', & & \\
 \dots, & & & & & & & & & & & \\
 \dots, & & & & & & & & & & & \\
 (n-1)', & 0, & 1, & \dots, & n-2, & n-1, & 0', & 1', & \dots, & (n-2)'. & & 
 \end{array}$$

Les systèmes de  $n$  éléments de la première ligne du tableau (ou d'une ligne quelconque du tableau) qui ne contiennent pas deux éléments conjugués entre eux, sont les  $2^n$  systèmes de triples déterminés par  $\Sigma_1$  ou  $\Sigma_2$ . Les colonnes cycliques de  $n$ -uples formées dans ce tableau, qui ne contiennent pas deux rangées verticales conjuguées entre elles, sont les ensembles de systèmes de triples *équivalents*, déterminés par  $\Sigma_2$  dans le second cas, au système de triples représenté par le  $n$ -uple de tête ou l'un quelconque des  $n$ -uples de la colonne. Les systèmes de triples représentés par deux de ces colonnes cycliques de  $n$ -uples différentes, sont donc *différents*.

Les diviseurs métacycliques que peuvent posséder les systèmes de triples déterminés par  $\Sigma_1$ , sont  $\{|x, 1 + x|, |x, \alpha^{\omega_i} x|\}$ ,  $\omega_i = 2^{a+1} \cdot \mu_i'$ , où  $\mu_i'$  est chaque diviseur de  $n_1'$  (§ 1, troisième alinéa). Ceux que peuvent posséder les systèmes de triples déterminés par  $\Sigma_2$ , sont  $\{|x, 1 + x|, |x, \alpha^{\omega_i} x|\}$ ,  $\omega_i = 2^{a+1} \cdot 3 \mu_i'$ , où  $\mu_i'$  est chaque diviseur de  $n_1$  (§ 1, second alinéa). On a  $n = 2^a \cdot n_1'$  et  $\frac{3n}{3} = 2^a \cdot n_1 = n$ ; donc  $n_1' = n_1$ .

Pour simplifier, représentons par  $\Sigma$ , à la fois  $\Sigma_1$  et  $\Sigma_2$ ; posons  $\omega_i = 2^{a+1} \cdot \mu_i'$  et désignons par  $\eta_i$ ,  $\omega_i = 2^{a+1} \cdot \mu_i'$  s'il s'agit de  $\Sigma_1$ ,  $3\omega_i = 2^{a+1} \cdot 3\mu_i'$ , s'il s'agit de  $\Sigma_2$ .

D'après ce qui est dit au premier alinéa des substitutions  $t = |x, \alpha x|$  et  $t^3 = |x, \alpha^3 x|$ , la substitution  $t^{\eta_i}$  appliquée aux colonnes cycliques de triples et la substitution  $s^{\omega_i}$  appliquée aux éléments (7) produisent le même effet. Donc, lorsque les systèmes de triples équivalents déterminés par  $\Sigma$ , possèdent le diviseur  $\{|x, 1+x|, |x, \alpha^{\eta_i} x|\}$ , la colonne cyclique de  $n$ -uples correspondante contient  $\omega_i$   $n$ -uples différents, et inversement. Le nombre  $x_i$  des systèmes de triples différents déterminés par  $\Sigma$ , qui possèdent le diviseur métacyclique  $\{|x, 1+x|, |x, \alpha^{\eta_i} x|\}$  est donc le nombre des colonnes cycliques de  $n$ -uples différentes, dont les  $n$ -uples n'ont pas deux éléments conjugués entre eux, qui contiennent  $\omega_i$   $n$ -uples différents.

Ce nombre  $x_i$ , le même pour  $\Sigma_1$  et  $\Sigma_2$ , dépend donc uniquement de la constitution du tableau (7), c'est-à-dire de  $n$  seul. C'est le contenu du théorème 1, qu'il fallait établir.

**7. Théorème 2. 2<sup>ème</sup> partie,  $x_1 \equiv 1$ .** La plus petite valeur de  $\omega_i$  est  $\omega_1 = 2^{a+1}$ , pour  $\mu_1' = 1$ . Posons, avec  $\omega_1 = 2^{a+1}$ ,  $\omega = 2^a$ . On a  $n = 2^a \cdot n_1' = 2^a (2m+1)$  (§ 1, troisième alinéa)  $= 2^{a+1} \cdot m + 2^a = \omega + m\omega_1$ . Le système d'éléments suivants de la première ligne du tableau (7), est un système de triples, qui se retrouve identique à lui-même à la  $(\omega_1 + 1)^{\text{ème}}$  ligne du tableau:

$$\begin{array}{cccccccc} 0, & \omega_1, & 2\omega_1, & \dots, & m\omega_1, & \omega', & (\omega_1+\omega)', & \dots, (m\omega_1-\omega)', \\ 1, & \omega_1+1, & 2\omega_1+1, & \dots, & m\omega_1+1, & (\omega+1)', & (\omega_1+\omega+1)', & \dots, (m\omega_1-\omega+1)', \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots, \\ \omega-1, & \omega_1+\omega-1, & 2\omega_1+\omega-1, & \dots, & m\omega_1+\omega-1, & (\omega_1-1)', & (2\omega_1-1)', & \dots, (m\omega_1-1)'. \end{array} \quad (8)$$

En effet, d'abord il y a dans cet ensemble de  $\omega = 2^a$  lignes à  $2m+1$  éléments chacune, la moitié des  $2n$  éléments  $0, 1, 2, \dots, n-1, 0', 1', \dots, (n-1)'$ , tantôt l'élément direct et tantôt l'élément conjugué; c'est-à-dire  $n$  éléments qui ne contiennent pas deux éléments conjugués entre eux. Il suffit pour le voir, de lire cet ensemble par rangées verticales, dans l'ordre suivant de ces rangées: 1<sup>ère</sup>,  $(m+2)^{\text{ème}}$ , 2<sup>ème</sup>,  $(m+3)^{\text{ème}}$ , etc.



$$(a_{(i-1)p+1} a_{(i-1)p+2} \dots a_{ip}), \quad i = 1, 2, \dots, \omega. \quad (11)$$

La substitution  $t^{\eta_1}$  appliquée aux colonnes cycliques de triples produit le même effet; appliquée aux colonnes cycliques de triples conjugués, elle produit la permutation circulaire correspondante:

$$(a'_{(i-1)p+1} a'_{(i-1)p+2} \dots a'_{ip}), \quad i = 1, 2, \dots, \omega. \quad (12)$$

On peut en donner deux raisons: une substitution  $|x, \beta x|$  change deux colonnes conjuguées en deux colonnes conjuguées (§45, second alinéa) ou les  $\omega$  lignes (12) ne sont autres que les  $\omega$  derniers cycles de la substitution  $s^{\omega_1}$  (§7).

Les puissances de  $t$  qui peuvent changer en lui-même un système de triples déterminé par  $\Sigma$ , sont  $\omega_i = 2^{a+1} \cdot \mu_i'$  ( $\Sigma = \Sigma_1$ ) ou  $3\omega_i = 2^{a+1} \cdot 3\mu_i'$  ( $\Sigma = \Sigma_2$ ); ce sont donc *des multiples de  $\eta_1$* . Les puissances de  $s$  qui peuvent changer en elle-même la combinaison (10) sont donc *des multiples de  $\omega_1$* .

Par les puissances de  $s^{\omega_1}$ , aucun élément de  $A_i$  ne peut devenir un élément de  $A_k$  ou de  $B'_k$ ,  $k \neq i$ , ou même un élément de  $B'_i$ , à cause des permutations (11) et (12). Donc  $A_i$  ne peut être changé qu'en lui-même, dans une substitution  $s^{\mu\omega_1}$ ,  $\mu$  entier positif, qui change (10) en elle-même.

A cause de (11), les transformés de  $A_i$  par les puissances de  $s^{\omega_1}$  forment une colonne cyclique de  $m_i'$ -uples de  $p$  éléments. Pour  $0 < m_i' < p$ , cette colonne contient  $p$   $m_i'$ -uples différents,  $m_i'$  étant premier à  $p$  (§4, I). On a donc uniquement les deux alternatives:

*1<sup>er</sup> cas.* Un au moins des  $m_i'$  est  $\neq 0$  et  $\neq p$ . Dans ce cas seule la puissance  $s^{p\omega_1}$  change la combinaison (10) en elle-même. Le système de triples représenté par (10) ne possède que le diviseur d'ordre minimum  $\{|x, 1+x|, |x, \alpha^{p\eta_1} x|\}$ , où  $p\eta_1 = p\omega_1 = 2^{a+1} \cdot p = 2n$  pour  $\Sigma = \Sigma_1$  et  $p\eta_1 = p \cdot 3\omega_1 = 6n$  pour  $\Sigma = \Sigma_2$ .

*2<sup>ème</sup> cas.* Tous les  $m_i'$  sont 0 ou  $p$ . Dans ce cas la substitution  $s^{\omega_1}$  change la combinaison (10) en elle-même ((11) et (12)). Le système de triples représenté par (10) possède le diviseur d'ordre maximum  $\{|x, 1+x|, |x, \alpha^{\eta_1} x|\}$ ,  $\eta_1 = \omega_1$  ou  $3\omega_1$  selon qu'il s'agit de  $\Sigma_1$  ou de  $\Sigma_2$ .

Dans cette dernière alternative, chaque  $m_i'$  peut être 0 et  $p$ ;  $i = 1, 2, \dots, \omega$ . Le nombre des systèmes de triples est donc  $2^\omega$ . Lorsque un système de triples du tableau (7) possède le diviseur  $\{|x, 1+x|, |x, \alpha^{\eta_1} x|\}$ , la colonne cyclique de  $n$ -uples correspondante contient  $\omega_1$



$n$ -uples différents (§6, avant-dernier alinéa), c'est-à-dire représente  $\omega_1$  systèmes de triples équivalents. Des  $2^\omega$  systèmes de triples trouvés, il y en a donc  $\frac{2^\omega}{\omega_1}$  qui sont des systèmes de triples *différents*.

On a donc :

$$x_1 = \frac{2^\omega}{\omega_1} = \frac{2^{2^a}}{2^{a+1}} = 2^{2^a - a - 1},$$

et par suite :

$$x_2 = \frac{2^{n-a-1} - x_1}{p} = \frac{2^{n-a-1} - 2^{2^a - a - 1}}{p} = \frac{2^{n-1} - 2^{2^a - 1}}{n},$$

c. q. f. d.

(Reçu le 11 février 1932)