Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 3 (1931)

Artikel: Sur les sytèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme 6n + 1(suite).
Autor: Bays, S.
DOI: https://doi.org/10.5169/seals-4676

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

Par S. BAYS, Fribourg

Chapitre II

Effet du groupe $\{|\, x,\ a+\alpha x \,|\}$ sur les colonnes cycliques de triples

17. Soit l'entier *quelconque* $N=6n+1$. Nous entendrons toujours par un entier $>6n$ son plus petit reste positif ou nul (mod. N).

L'ensemble des N substitutions:

$$r=|\, x,\ a+x \,|, \quad a=0, 1, 2, \ldots, 6n,$$

constitue un groupe *cyclique*[27]), engendré par la substitution *circulaire:*

$$s=|\, x,\ 1+x \,|.$$

---

[27]) La manière la plus claire pour noter une substitution est $\begin{pmatrix} a, & b, & c, & \ldots, & k \\ a_1, & b_1, & c_1, & \ldots, & k_1 \end{pmatrix}$, a_1 étant l'élément qui remplace a; b_1, l'élément qui remplace b, etc. La notation par *cycles* est celle-ci: chaque élément est remplacé par celui qui suit dans le cycle. Exemple: $\begin{pmatrix} 1&2&3&4&5&6&7 \\ 4&3&2&6&7&1&5 \end{pmatrix}$ se note (146) (23) (57). Si un élément n'est pas changé par la substitution, son cycle n'a que cet élément; on peut omettre ce cycle. La notation *analytique* $|\, x, f(x) \,|$ est la plus courte; x parcourt les éléments de la substitution et $f(x)$ signifie l'élément qui remplace x. C'est celle que nous employons ici.

Une substitution est dite *cyclique* ou *circulaire* (nous emploierons le second terme), lorsqu'elle ne contient qu'un seul cycle. Elle est dite *régulière,* lorsqu'elle est formée de cycles égaux. Toutes les puissances s^1, s^2, ... s^{N-1} sont des substitutions régulières; seules celles d'exposant premier à N sont circulaires. Un groupe de substitutions est dit *cyclique,* lorsqu'il est constitué uniquement des puissances d'une substitution. Un groupe de substitutions est dit *régulier,* lorsque son ordre (nombre des substitutions) est égal à son degré (nombre des éléments). Chacune de ses substitutions, autre que l'identité, est alors régulière et déplace tous les éléments. Le groupe cyclique $\{s\}$ est aussi régulier.

Lorsque N est premier, ce groupe n'a pas de diviseur propre; lorsque N est composé, il a les diviseurs $\{s^a\}$, où a est chaque diviseur de N.

Théorème 1. Les substitutions de ce groupe transforment chaque colonne cyclique de triples en elle-même.

18. L'ensemble des $\varphi(N)$ substitutions[28]:

$$u = |x, \beta x|, \quad \beta = \text{les } \varphi(N) \text{ entiers premiers à } N,$$

constitue un groupe. Lorsqu'il existe une *racine primitive* α (mod. N), c'est-à-dire un entier α dont la plus petite puissance congrue à 1 (mod. N) est $\varphi(N)$[29]), le groupe est cyclique et il est engendré par la substitution:

$$t = |x, \alpha x|.$$

Dans ce cas les diviseurs propres du groupe sont engendrés par les substitutions:

$$v = |x, \alpha^{\omega} x|$$

où ω est un diviseur propre quelconque de $\varphi(N)$. L'ordre du diviseur $\{|x, \alpha^{\omega} x|\}$ est naturellement $\frac{\varphi(N)}{\omega}$.

Théorème 2. Les substitutions du groupe $\{|x, \alpha x|\}$ transforment une colonne cyclique de triples en une colonne cyclique de triples.

---

[28]) La substitution $|x, N-x|$ du § 13 qui transforme deux colonnes conjuguées l'une dans l'autre est la dernière de cet ensemble:

$$|x, N-x| = |x, -x| = |x, (N-1)x| = |x, 6n x|.$$

[29]) Soit $a^{\delta} \equiv 1$ (mod. N). Si δ est le plus petit exposant positif pour lequel cette congruence a lieu, on dit que *a appartient* à l'exposant δ (mod. N).

Soit $N = p_1^{a_1} \cdot p_2^{a_2} \ldots$; on a $\varphi(N) = \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \ldots$. Soit $\psi(N)$ le p. p. c. m. des facteurs $\varphi(p_1^{a_1})$, $\varphi(p_2^{a_2})$, ...; $\psi(N)$ est l'exposant le plus élevé auquel appartiennent des nombres (mod. N). On a $\psi(N) = \varphi(N)$ dans les deux cas seulement: $N = p^{\lambda}$, $\lambda \geqq 1$, p premier, et $N = 2p^{\lambda}$, $\lambda \geqq 1$, p premier impair; la chose est aisée à montrer. Si a appartient à l'exposant $\varphi(N)$ (mod. N), il est dit une racine *primitive* mod. N.

En effet par la substitution $t = |x, \alpha x|$, les deux triples de la même colonne cyclique:

$$m, n, p \text{ et } m+q, n+q, p+q$$

deviennent $m\alpha, n\alpha, p\alpha$ et $m\alpha+q\alpha, n\alpha+q\alpha, p\alpha+q\alpha,$

qui sont encore deux triples de la même colonne cyclique.

19. L'ensemble des $N.\varphi(N)$ substitutions:

$$w = |x,\ a+bx|,\ a = 0, 1, 2, \ldots, 6n,$$

$$b = \text{les } \varphi(N) \text{ entiers premiers à } N,$$

constitue le groupe que nous appellerons ici le groupe *métacyclique*[30]). Lorsque α est une racine primitive (mod. N), le groupe est engendré par les deux substitutions déjà vues:

$$s = |x, 1+x| \quad \text{et} \quad t = |x, \alpha x|.$$

Dans ce cas ses diviseurs non cycliques (nous les appellerons diviseurs *métacycliques*) sont engendrés par les deux substitutions:

$$s = |x, 1+x| \quad \text{et} \quad v = |x, \alpha^{\omega} x|$$

et l'ordre du diviseur $\{s, v\}$ est ainsi $N.\frac{\varphi(N)}{\omega}$.

Théorème 3. Les substitutions du groupe métacyclique transforment une colonne cyclique en une colonne cyclique, et par suite un système cyclique de triples en un système cyclique de triples.

---

[30]) La substitution w sera appelée aussi, pour simplifier, une substitution métacyclique. Cette appellation de groupe métacyclique pour désigner le groupe des substitutions w, lorsque N est *premier,* est due à Kronecker (*Netto,* Gruppen und Substitutionentheorie, Sam. Schubert LV., p. 133). *Weber,* Lehrbuch der Algebra, Bd. 1, p. 647' appelle métacycliques, les groupes dits *résolubles* par Frobenius et Hölder, c'est-à-dire les groupes correspondants aux équations *résolubles* par radicaux, et dont la série des indices de composition est constituée uniquement de nombres premiers. C'est là aussi une extension, mais dans un autre sens, du mot de Kronecker, puisque, lorsque le degré est premier, les équations les plus générales, résolubles par radicaux, sont celles dont le groupe est métacyclique au sens de Kronecker.

20. *Théorème 4. Le groupe des substitutions permutables au groupe cyclique* $\{ s \}$ *est le groupe métacyclique*[31]).

Nous en ferons la preuve en deux parties:

1) La substitution métacyclique w est permutable au groupe $\{ s \}$; en effet:

$$| x, a_1 + x | . | x, a + bx | = | x, a + ba_1 + bx |$$

$$| x, a + bx | . | x, a_2 + x | = | x, a_2 + a + bx |$$

---

31) Cette note rappelle et fixe les données utiles pour lire aisément ce § et les § suivants.

La substitution $t^{-1} . s . t = s_1$ est dite la ***transformée*** de la substitution s par la substitution t; elle est le résultat que donnent le ou les cycles de s quand on fait sur leurs éléments la substitution t; elle est donc ***semblable*** à s, c'est-à-dire constituée du même nombre de cycles égaux respectivement à ceux de s. Autrement dit s_1 ne diffère de s que par la notation des éléments. Inversement $s = t . s_1 . t^{-1}$; s est la transformée de s_1 par la substitution t^{-1} .

Si on a $st = ts$, (1), on a $t^{-1} st = s$ et $s^{-1} ts = t$ et inversement de chacune des deux dernières égalités on a les deux autres. A cause de (1), on dit alors que les substitutions s et t sont ***permutables*** entre elles; chacune transforme l'autre en elle-même.

Le groupe $t^{-1} . G . t = G_1$ est dit le ***transformé*** du groupe G par la substitution t; il est le groupe que donnent les substitutions de G, quand on les transforme chacune par la substitution t; il est donc constitué de substitutions respectivement semblables à celles de G et il est évidemment isomorphe au groupe G. D'ailleurs de $s_\alpha \; s_\beta = s_\gamma$ suit $(t^{-1} s_\alpha t) . (t^{-1} s_\beta t) = t^{-1} s_\gamma t$ et inversement. Réciproquement $G = t . G_1 . t^{-1}$; G est le transformé de G_1 par la substitution t^{-1} . Nous appellerons encore ***semblables*** deux groupes qui, comme G et G_1, sont les transformés l'un de l'autre par une substitution t ou t^{-1} . Autrement dit, deux groupes semblables ne diffèrent entre eux que par la notation des éléments.

Si on a $Gt = tG$, c'est-à-dire $s_\alpha t = ts_\beta$ où s_α et s_β parcourent chacun les substitutions de G, on a $t^{-1} Gt = G$ et inversement. On dit alors que la substitution t est ***permutable*** au ***groupe*** G; autrement dit, ***la substitution t transforme le groupe G en lui-même.*** L'ensemble des substitutions permutables à G forme un groupe; en effet de $s_\alpha t_1 = t_1 s_\beta$ et $s_\alpha \; t_2 = t_2 \, s_\gamma$ suit $s_\alpha (t_1 \, t_2) = t_1 (s_\beta \, t_2) = (t_1 \, t_2) \, s_\delta$, où s_γ et s_δ sont encore des substitutions de G.

Soit une fonction φ, G le groupe de substitutions qui lui appartient et S le groupe symétrique ou un diviseur du groupe symétrique contenant G. Les substitutions de S changent φ en un certain nombre de fonctions équivalentes à φ:

$$\varphi = \varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_r . \tag{2}$$

Soit $s_1 = 1, s_2, s_3, \ldots, s_r$ des substitutions de S qui changent respectivement φ en φ_1, $\varphi_2, \ldots, \varphi_r$. Les complexes de substitutions qui changent φ en $\varphi_1, \varphi_2, \ldots, \varphi_r$ sont $Gs_1 = G$, $Gs_2, \ldots, Gs_r$ et on a:

$$S = Gs_1 + Gs_2 + \ldots + Gs_r \tag{3}$$

Le système (2) est dit un système de fonctions équivalentes ***conjuguées*** relativement à S. Les groupes

$$s_1^{-1} \, Gs_1 = G, \; s_2^{-1} \, Gs_2, \; s_3^{-1} \, Gs_3, \; \ldots, \; s_r^{-1} \, Gs_r, \tag{4}$$

contenus dans S, sont les groupes de substitutions qui appartiennent aux fonctions (2) respectives; cela ressort immédiatement de ce qui a été dit. Ils sont tous les transformés de G que l'on peut obtenir au moyen des substitutions de S; en effet, g étant une substitution quelconque de G, on a: $(gs_i)^{-1} \, G \, (gs_i) = s_i^{-1} \, (g^{-1} \, Gg) \; s_i = s_i^{-1} \, Gs_i$; donc toutes les substitutions du complexe Gs_i transforment G dans le même groupe $s_i^{-1} \, G \, s_i$. Le système (4) est également dit un système de diviseurs ***conjugués*** dans S.

et la congruence $ba_1 \equiv a_2 \pmod{N}$ a toujours une solution, b étant premier à N.

2) Inversement si $\sigma = |\, x, f(x)\,|$ est une substitution permutable au groupe $\{\, s \,\}$, elle est métacyclique. En effet:

a) On a dans ce cas $s\sigma = \sigma s^\beta$ où β est premier à N, car $\sigma^{-1} s \sigma$, qui est une substitution de $\{\, s \,\}$ et semblable à s, est circulaire et donc égale à une puissance s^β, où β est premier à N. De $\sigma^{-1} s \sigma = s^\beta$, suit $s\sigma = \sigma s^\beta$.

b) Il résulte de là:

$$s\sigma = |\, x, 1 + x \,|\, .\, |\, x, f(x)\,| = |\, x, f(1 + x)\,|,$$

$$\sigma s^\beta = |\, x, f(x)\,|\, .\, |\, x, \beta + x\,| = |\, x, \beta + f(x)\,|\, .$$

On doit avoir pour chaque x: $f(1 + x) \equiv \beta + f(x) \pmod{N}$, soit:

$$\begin{aligned} f(1) &\equiv \beta + f(0), \\ f(2) &\equiv \beta + f(1), \\ &\cdots\cdots\cdots\cdots\cdots, \\ f(x) &\equiv \beta + f(x-1). \end{aligned}$$

En additionnant, il reste $f(x) \equiv \beta x + f(0)$; autrement dit σ est bien de la forme $|\, x, a + b\,x\,|$, avec b premier à N[32]).

21. Soit φ une fonction des éléments 0, 1, 2, ... $6n$, G le groupe de substitutions qui appartient à φ et H un diviseur de G. Soit P le groupe des substitutions permutables à H; une substitution quelconque p de P change φ en une fonction φ_1 dont le groupe G_1 contient en tout cas le diviseur $p^{-1} H p = H$.

---

[32]) Entendons par chaque entier son plus petit reste positif ou nul (mod. p), *p premier.* Le groupe ***arithmétique*** de Cauchy est le suivant, d'ordre et de degré p^k. Les p^k éléments étant $x_{i_1, i_2, \ldots, i_k}$; $i_1, i_2, \ldots, i_k = 0, 1, 2, \ldots, p-1$; il est l'ensemble des p^k substitutions où nous n'écrirons que les indices, $|\, (i_1, i_2, \ldots, i_k), (i_1 + c_1, i_2 + c_2, \ldots, i_k + c_k)\,|$; $c_1, c_2, \ldots, c_k = 0, 1, 2, \ldots, p-1$. Pour $k = 1$ et N premier, il se réduit à notre groupe cyclique $\{\, s \,\}$, mais de toute évidence, seulement dans ce cas.

L'ensemble des substitutions permutables au groupe arithmétique est le groupe ***linéaire***. Il est l'ensemble des substitutions $|\, (i_1, i_2, \ldots, i_k), (\Sigma c_{1\beta}\, i_\beta + d_1, \Sigma c_{2\beta}\, i_\beta + d_2, \ldots\ldots, \Sigma c_{k\beta}\, i_\beta + d_k)\,|$, $\beta = 1, 2, \ldots, k$; $d_1, d_2, \ldots, d_k = 0, 1, 2, \ldots, p-1$ et le déterminant des coefficients $c_{\alpha\beta}$, entiers pris dans 0, 1, 2, ..., $p-1$, remplit la condition: $\Delta = |\, c_{\alpha\beta}\,| \not\equiv 0 \pmod{p}$. Pour $k = 1$ et N premier, le groupe ***linéaire*** se réduit à notre groupe métacyclique des substitutions w.

Théorème 5. La condition nécessaire et suffisante pour que toutes les fonctions possédant[33]) *le groupe H équivalentes à φ, puissent se déduire de φ par les substitutions de P, est que tous les groupes* **semblables** *à H contenus dans G puissent être obtenus en transformant H par des substitutions de G.*

La condition est suffisante. Nous supposons donc qu'il n'existe dans G, en fait de groupes semblables à H, que le système des groupes *conjugués:*

$$s^{-1} H s = H;\ s'^{-1} H s' = H';\ s''^{-1} H s'' = H'';\ \ldots\ldots \qquad (14)$$

obtenus en transformant H par toutes les substitutions de G.

Soit φ' une fonction équivalente à φ, possédant le groupe H et τ une substitution qui change φ en φ'. Le groupe de φ', $G' = \tau^{-1} G \tau$, contient les transformés, semblables à H:

$$\tau^{-1} H \tau,\ \tau^{-1} H' \tau,\ \tau^{-1} H'' \tau,\ \ldots\ldots \qquad (15)$$

et ne contient point d'autre groupe semblable à H; en effet s'il en contenait un autre, H_1, $\tau H_1 \tau^{-1}$ serait dans G et autre que H, H', H'', ..., puisque de $\tau H_1 \tau^{-1} = H^{(i)}$ suivrait $H_1 = \tau^{-1} H^{(i)} \tau$. Par hypothèse, le groupe G' contient H. Donc H est l'un des groupes (15). S'il est le premier, τ est une substitution du groupe P. S'il est un autre d'entre eux, soit par exemple le second, $s' \tau$ sera une substitution de P puisque:

$$\tau^{-1} H' \tau = \tau^{-1} (s'^{-1} H s') \tau = (s' \tau)^{-1} H (s' \tau) = H$$

et qui change φ en φ', puisque s' laisse φ inchangée et τ change φ en φ'.

La condition est nécessaire. Si elle n'est pas remplie, G contient en plus du système conjugué (14), d'autres groupes semblables à H:

$$H_1,\ H_2,\ H_3,\ \ldots\ldots$$

Il y a une substitution t, extérieure à G, qui transforme H en H_1. La substitution t^{-1} changera φ en une fonction équivalente φ' qui possédera le groupe H, puisque son groupe $G' = t G t^{-1}$ contient $t H_1 t^{-1} = H$.

---

[33]) J'entends par là que le groupe qui appartient à chacune de ces fonctions *contient* le diviseur H.

L'ensemble des substitutions changeant φ en φ' sera Gt^{-1}; soit gt^{-1} l'une quelconque d'entre elles. gt^{-1} n'appartient pas au groupe P, sinon $(gt^{-1})^{-1} = tg^{-1}$ lui appartiendrait aussi et transformerait H en lui-même. Or t transforme H en H_1; par suite g^{-1} devrait transformer H_1 en H et g devrait transformer H en H_1, ce qui n'est pas.

Ainsi aucune des substitutions changeant φ en φ' n'appartient au groupe P; il existe donc des fonctions comme φ', possédant le groupe H, équivalentes à φ et qui ne peuvent se déduire de φ par une substitution de P.

22. *Théorème 6.*[34]) *Lorsque N est premier, deux systèmes cycliques de triples de Steiner équivalents se déduisent l'un de l'autre par une substitution métacyclique.*

Pour le prouver, il suffit maintenant de s'appuyer sur le théorème suivant de Sylow, concernant les groupes d'ordre p^m contenus dans un groupe G d'ordre $r = p^m\varrho$, p premier et ϱ premier à p[35]): *Tous les diviseurs H d'ordre p^m contenus dans G forment un seul système conjugué; autrement dit tous ces diviseurs sont les transformés de l'un quelconque d'entre eux par les substitutions de G.*

Le groupe cyclique $\{s\}$ est d'ordre N. Si $N = p$ (premier), l'ordre r du groupe symétrique G, $r = p!$, est de la forme $r = p\varrho$, ϱ premier à p. Donc les diviseurs d'ordre p contenus dans G forment un seul système conjugué; en vertu des théorèmes 5 et 4, toutes les fonctions possédant le groupe $\{s\}$, équivalentes à l'une d'elles, peuvent se déduire de celle-ci par une substitution métacyclique. On a ainsi ce qu'il fallait démontrer.

Mais le théorème de Sylow ne nous donne rien, déjà dans le cas où $N = p^m$ (puissance d'un nombre premier); le groupe cyclique $\{s\}$ est d'ordre p^m et p^m n'est plus en général la plus haute puissance de p

[34]) Les théorèmes 4, 5 et 6 sont de P. Lambossy (§ 1 et 5, note 23). J'ai raccourci seulement sa démonstration du théorème 4; d'ailleurs pour N premier, le fait découle de ce qui est dit dans ma note 32) et pour N quelconque le théorème n'est sans doute pas nouveau. Le théorème 5 est démontré par P. Lambossy directement pour le cas du groupe cyclique $\{s\}$ et du groupe des substitutions permutables à $\{s\}$, le groupe métacyclique. Mais sa démonstration vaut, sans y changer un mot, pour le cas général d'un groupe H ***quelconque*** et du groupe P des substitutions permutables à H. C'est le seul changement que j'y ai apporté.

[35]) C'est le second des trois théorèmes de Sylow sur les groupes d'ordre p^m contenus dans un groupe G d'ordre r, m étant la plus haute puissance de p contenue dans r. Voir, si l'on veut la référence originale, *L. Sylow,* Théorèmes sur les substitutions, Mathem. Annalen, 1872, Bd. 5, p. 586, ou par exemple, *Netto,* Gruppen und Substitutionentheorie, Sam. Schubert LV, p. 103.

contenue dans p^m !. Il y a plus; P. Lambossy a montré que le théorème sous la forme générale que je lui avais donnée (J., p. 75): *deux fonctions cycliques de n variables* $x_1, x_2, \ldots, x_n$ [possédant le groupe cyclique $\{(x_1 x_2 \ldots x_n)\}$, $n = p$ ou p^m] *équivalentes, se déduisent l'une de l'autre par une substitution métacyclique*, n'est plus vrai pour $n = p^m$. Il a construit pour ce cas des fonctions cycliques équivalentes, qui ne peuvent pas se déduire l'une de l'autre par une substitution métacyclique. Mais cela n'empêche nullement que le théorème reste exact pour le cas des systèmes cycliques de triples; il n'est plus exact dans le cas général de fonctions cycliques de constitution *quelconque*, mais les systèmes cycliques de triples sont des fonctions cycliques de nature très particulière et il est parfaitement possible que pour eux le théorème soit valable pour $N = p^m$ et même pour N quelconque (voir § 5 et note 24).

23. Lorsqu'il existe une racine primitive α (mod. N), le groupe métacyclique est engendré par les deux substitutions

$$s = |x, 1 + x|, \quad t = |x, \alpha x|.$$

C'est le cas lorsque $N = p$ ou $N = p^m$ (note 29). La substitution s change chaque système cyclique de triples en lui-même. Représentons par S un système cyclique de triples donné pour $N = 6n + 1$ des formes p ou p^m. La puissance $\varphi(N)$ de la substitution t, $t^{\varphi(N)} = |x, \alpha^{\varphi(N)} x| = |x, x|$ changera le système S en lui-même.

Théorème 7. Si ω est la plus petite puissance positive de t qui change le système S en lui-même, ω est diviseur de $\varphi(N)$, le système S possède le diviseur métacyclique d'ordre $N \cdot \frac{\varphi(N)}{\omega}$, $\{s, t^\omega\}$ et la série des systèmes déduits de S par les puissances de la substitution t se présente de la façon suivante:

$$S = S_0, S_1, S_2, \ldots, S_{\frac{\omega}{2}-1}, S_0', S_1', S_2', \ldots, S'_{\frac{\omega}{2}-1}, S_0, S_1, \ldots, \quad (16)$$

le système S_i' désignant le conjugué de S_i.

Les deux premiers points sont immédiats. Pour le troisième nous remarquerons d'abord que si la substitution $|x, \beta x|$, β quelconque, premier à N, change S en son conjugué S', elle change à son tour S' en S. Cela résulte du fait que $|x, \beta x| . |x, -x| = |x, -\beta x| = |x, -x| . |x, \beta x|$; si $|x, \beta x|$ change S en S', $|x, -\beta x|$ change S

en lui-même d'après le premier membre; $|x, \beta x|$ doit donc changer S' en S d'après le dernier membre. Alors d'une part le conjugué de chacun des systèmes entrant dans la série (16) doit s'y trouver également, puisque $|x, -x|$ est une des puissances de t. D'autre part le conjugué d'un système S_i ne peut se présenter avant le $\frac{\omega}{2}$ ième système qui le suit dans la série, sinon une puissance de t inférieure à ω transformerait S_i en lui-même, ce qui est impossible.

Il résulte encore de là et des théorèmes démontrés que:

1° ω est un entier *pair*. En particulier on ne peut avoir $\omega = 1$; autrement dit S peut posséder *au plus* le *demi-groupe* métacyclique $\{|x, 1+x|, |x, \alpha^2 x|\}$ d'ordre $N \cdot \frac{\varphi(N)}{2}$.

2° $\frac{\varphi(N)}{\omega}$ est un entier *impair*. En effet ω est diviseur de $\varphi(N)$, mais non de $\frac{\varphi(N)}{2}$, car la substitution $t^{\frac{\varphi(N)}{2}} = |x, \alpha^{\frac{\varphi(N)}{2}} x| = |x, -x|$ change S en S', tandis qu'elle changerait S en S si $\frac{\varphi(N)}{2}$ était multiple de ω. Par suite ω doit contenir tous les facteurs 2 contenus dans $\varphi(N)$. $N \cdot \frac{\varphi(N)}{\omega}$ est donc impair; autrement dit S ne peut posséder un diviseur métacyclique d'ordre *pair*.

3° Tous les systèmes de la série (16) possèdent *le même diviseur métacyclique* $\{|x, 1+x|, |x, \alpha^\omega x|\}$; autrement dit, pour chacun d'eux ce sont les mêmes substitutions métacycliques qui les changent en eux-mêmes.

4° Enfin il n'est peut-être pas inutile de faire observer ici que les diviseurs $\{|x, \alpha^\omega x|\}$ et $\{|x, 1+x|, |x, \alpha^\omega x|\}$ sont *indépendants* de la racine primitive α que l'on a choisie. En effet les puissances α^ω, $\alpha^{2\omega}$, ..., $\alpha^{\frac{\varphi(N)}{\omega}\omega}$ donnent, pour toutes les racines primitives α de N, le même système de restes (mod. N), car si β est une seconde racine primitive de N, on a $\beta \equiv \alpha^\nu$ (mod. N), $\nu \not\equiv 1$ et premier à $\varphi(N)$, et les exposants $\nu\omega$, $2\nu\omega$, ..., $\frac{\varphi(N)}{\omega}\nu\omega$ sont mod. $\varphi(N)$ incongrus entre eux et ont les mêmes restes: ω, 2ω, ..., $\frac{\varphi(N)}{\omega}\omega$, seulement dans un autre ordre.

D'ailleurs la série (16) des systèmes qui se déduisent de S par les puissances de la substitution t, est évidemment indépendante de α, puisque le groupe $\{t\}$ est indépendant de α. Cela suffit aussi pour établir l'indépendance du diviseur $\{|x, \alpha^{\omega} x|\}$; la série S, S_1, S_2, ..., $S_{\frac{\omega}{2}-1}$, avec une autre racine primitive, se présentera seulement dans un autre ordre.

Chapitre III

Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ et les colonnes cycliques de caractéristiques

24. Les entiers $-3n, \ldots, -1, 0, 1, \ldots, 3n$ forment un système *complet* de restes (mod. N). Nous l'appelons le système des plus petits restes positifs ou négatifs (mod. N). Soit b l'un de ces restes; l'ensemble des entiers qui ont ce reste (mod. N) est donné par $b \pm m N$, $m = 0, 1, 2, \ldots$. D'une façon plus générale, soit b un entier quelconque; l'ensemble des entiers qui ont le même reste que b, (mod. N), est donné par $b \pm m N$, $m = 0, 1, 2 \ldots$.

Nous appellerons *la valeur absolue* du plus petit reste positif ou négatif de l'entier a (mod. N), le reste *absolu* de l'entier a (mod. N). Les restes absolus (mod. N) sont ainsi $0, 1, 2, \ldots, 3n$. Soit b l'un de ces restes; l'ensemble des entiers qui ont ce reste absolu (mod. N) est donné par $\pm b \pm m N$, $m = 0, 1, 2 \ldots$. D'une façon plus générale, soit b un entier quelconque; l'ensemble des entiers qui ont le même reste absolu que b, (mod. N), est donné par $\pm b \pm m N$, $m = 0, 1, 2 \ldots$.

Pour simplifier, nous appellerons congruence *absolue* la relation qui lie deux entiers ayant le même reste absolu (mod. N) et nous la noterons par le signe $\cong$. La congruence absolue aura en partie les propriétés de la congruence ordinaire (mod. N):

$$\text{Si } a \cong b \text{ et } b \cong c, \text{ on a } \quad a \cong c \ (\text{mod. } N); \tag{17}$$

$$\text{Si } a \cong b \text{ et } c \cong d, \text{ on a } \quad ac \cong bd \ (\text{mod. } N). \tag{18}$$

La première congruence est immédiate. Pour la seconde il suffit de remarquer que:

$$\begin{aligned} a \cong b \quad & \text{équivaut à} \quad a \equiv \pm b \pmod{N}, \\ c \cong d \quad & \text{,,} \quad \text{à} \quad c \equiv \pm d \pmod{N}, \\ \text{et } ac \cong bd \quad & \text{,,} \quad \text{à} \quad ac \equiv \pm bd \pmod{N}. \end{aligned}$$

De la congruence (18) on a en particulier:

$$\text{Si } a \cong b, \text{ puisque } m \cong m, \text{ on a } \quad ma \cong mb. \tag{19}$$

Mais vis-à-vis de l'addition, la congruence absolue n'a plus la propriété de la congruence ordinaire (mod. N):

De $a \cong b$ et $c \cong d$, ne suit pas nécessairement $a + c \cong b + d$, car de

$$a \equiv \pm b \text{ et } c \equiv \pm d, \quad \text{suit } a + c \equiv \pm b \pm d,$$

et le second membre $\pm b \pm d$ a deux valeurs absolues différentes.

Nous désignerons par $\underline{a}$ le reste absolu de l'entier a (mod. N). Tant qu'il ne s'agit *que de multiplications seules*, en vertu de (18) et (19), la congruence absolue a vis-à-vis d'elles exactement les propriétés de la congruence ordinaire; par conséquent les mêmes règles de calcul pour la multiplication sont valables dans l'un comme dans l'autre cas.

25. La substitution $u = |x, \beta x|$, β premier à N, des N éléments 0, 1, 2, ..., $6n$, (§ 18), ou ce qui revient au même, puisque l'élément 0 reste inchangé, des $6n$ éléments 1, 2, ..., $6n$, se réduit, en y remplaçant chaque élément par son reste absolu (mod. N), à la substitution $\sigma = |\underline{x}, \underline{\beta x}|$ des $3n$ éléments 1, 2, ..., $3n$. On peut l'admettre immédiatement; mais on le voit très bien et très simplement avec la notation complète (note 27):

$$\begin{pmatrix} 1, & 2, & 3, & \ldots, & 3n, & 3n+1, & 3n+2, & \ldots, & 6n \\ \beta, & 2\beta, & 3\beta, & \ldots, & 3n\beta, & (3n+1)\beta, & (3n+2)\beta, & \ldots, & 6n\beta \end{pmatrix}.$$

Comme nous le savons, β étant premier à N, les nombres de la seconde ligne donnent un système complet de restes positifs (mod. N)

et reproduisent les nombres de la première ligne. Remplaçons dans les deux lignes chaque élément par son reste absolu (mod. N), autrement dit chaque élément $a > 3n$ par son complément $N - a \leqq 3n$; nous obtenons:

$$\left(\begin{array}{cccc|ccc} 1, & 2, & 3, & \ldots\ldots, & 3n, & 3n-1, & \ldots\ldots, & 1 \\ \underline{\beta}, & \underline{2\beta}, & \underline{3\beta}, & \ldots\ldots, & \underline{3n\beta}, & \underline{(3n-1)\beta}, & \ldots\ldots, & \underline{\beta} \end{array}\right) \qquad (20)$$

Comme $(3n - \nu)\,\beta \equiv -(3n + \nu + 1)\,\beta$ (mod. N), $\nu = 0, 1, 2, \ldots, 3n-1$, il est évident que les $3n$ premiers éléments de la seconde ligne sont tous les entiers $1, 2, \ldots, 3n$. Ainsi la substitution (20) est partagée par le trait vertical en deux parties symétriques, qui sont chacune la même substitution; elle se réduit donc à la substitution des $3n$ éléments $1, 2, \ldots, 3n$:

$$\left(\begin{array}{cccc} 1, & 2, & 3, & \ldots\ldots, & 3n \\ \underline{\beta}, & \underline{2\beta}, & \underline{3\beta}, & \ldots\ldots, & \underline{3n\beta} \end{array}\right) = |\,\underline{x}, \underline{\beta x}\,|\,^{36)}.$$

Faisons encore remarquer que, de même que $\beta, 2\beta, 3\beta, \ldots, 6n\beta$ donnent un système complet de restes positifs (mod. N), soit les entiers $1, 2, 3, \ldots, 6n$, $\underline{\beta}$, $\underline{2\beta}$, $\underline{3\beta}$, $\ldots$, $\underline{3n\beta}$ est un système complet de restes absolus (mod. N), soit les entiers $1, 2, \ldots, 3n$; $\underline{(3n+1)\beta}$, $\underline{(3n+2)\beta}$, $\ldots$, $\underline{6n\beta}$ reproduisent ces mêmes entiers dans l'ordre inverse; $\underline{(6n+2)\beta}$, $\underline{(6n+3)\beta}$, $\ldots\ldots$ reproduisent indéfiniment la série entière dans le même ordre.

26. La substitution $\sigma = |\,\underline{x}, \underline{\beta x}\,|$, β premier à N, change *une caractéristique* en *une caractéristique*.

En effet la substitution correspondante $u = |\,x, \beta x\,|$ change une colonne cyclique de triples en une colonne cyclique de triples et les trois triples contenant l'élément 0 de la première en les trois triples contenant l'élément 0 de la seconde. Par conséquent la substitution σ changera la caractéristique de la première colonne dans la caractéristique de la seconde.

---

36) Les éléments de la substitution étant maintenant $1, 2, \ldots, 3n$, on pourrait écrire simplement $|\,x, \underline{\beta x}\,|$; nous préférons garder l'écriture symétrique $|\,\underline{x}, \underline{\beta x}\,|$.

27. L'ensemble des $\frac{\varphi(N)}{2}$ substitutions :

$$\sigma = |\underline{x}, \underline{\beta x}|, \beta = \text{les } \frac{\varphi(N)}{2} \text{ entiers premiers à } N, \leqq 3n,$$

constitue un groupe, au même titre que les $\varphi(N)$ substitutions $|x, \beta x|$ en constitue un. Il résulte d'ailleurs de ce dernier groupe, en remplaçant dans la moitié de ses substitutions les éléments $a > 3n$ par leurs compléments $N - a \leqq 3n$. En effet si β est premier à N, $N - \beta$ l'est aussi et les deux substitutions :

$$|x, \beta x| \text{ et } |x, (N-\beta)x| = |x, -\beta x|, \beta \text{ premier à } N, \leqq 3n,$$

réduites à la manière du § précédent, donnent chacune la même substitution $|\underline{x}, \underline{\beta x}|$. Les $\frac{\varphi(N)}{2}$ substitutions $|x, \beta x|$ où β, premier à N, est $> 3n$, donnent donc en les réduisant le même résultat que les $\frac{\varphi(N)}{2}$ substitutions $|x, \beta x|$, où β, premier à N, est $\leqq 3n$.

28. Si α appartient à l'exposant $\varphi(N)$ (mod. N), les restes des puissances $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{\varphi(N)-1}$ forment, comme nous l'avons déjà admis implicitement au § 18, un système complet de restes positifs (mod. N), *premiers* à N. $\alpha^{\varphi(N)}, \alpha^{\varphi(N)+1}, \alpha^{\varphi(N)+2}, \ldots\ldots$ redonnent indéfiniment la même série de restes (mod. N) dans le même ordre. Puisque :

$$\alpha^{\frac{\varphi(N)}{2}+\nu} \equiv -\alpha^\nu \text{ (mod. } N), \ \nu = 0, 1, 2, \ldots\ldots, \frac{\varphi(N)}{2} - 1,$$

$\underline{\alpha^0}, \underline{\alpha^1}, \underline{\alpha^2}, \ldots, \underline{\alpha^{\frac{\varphi(N)}{2}-1}}$ sont un système complet de restes absolus (mod. N), *premiers* à N ; ils sont dans un certain ordre les $\frac{\varphi(N)}{2}$ entiers premiers à N compris dans $1, 2, \ldots, 3n$. $\underline{\alpha^{\frac{\varphi(N)}{2}}}, \underline{\alpha^{\frac{\varphi(N)}{2}+1}}, \underline{\alpha^{\frac{\varphi(N)}{2}+2}}, \ldots\ldots$ reproduisent indéfiniment la même série d'entiers dans le même ordre.

Le groupe cyclique des substitutions $u = |x, \beta x|$ est constitué des puissances de la substitution $|x, \alpha x|$. Le groupe des substitutions $\sigma = |\underline{x}, \underline{\beta x}|$, d'après ce qui vient d'être dit, est cyclique aussi et constitué des puissances de la substitution $\tau = |\underline{x}, \underline{\alpha x}|$.

29. Dès maintenant nous nous limitons au cas $N = 6n + 1$ *premier*. Alors $\varphi(N) = 6n$; tous les entiers $1, 2, \ldots 6n$ sont premiers à N ; α^0,

$\alpha^1, \ldots, \alpha^{6n-1}$ donnent un système *complet* de restes positifs (mod. N), c'est-à-dire les entiers 1, 2, ..., $6n$ dans un certain ordre; $\underline{\alpha^0}, \underline{\alpha^1}, \ldots, \underline{\alpha^{3n-1}}$ sont un système *complet* de restes absolus (mod. N), soit les entiers 1, 2, ..., $3n$, dans un certain ordre.

La substitution $t = |x, \alpha x|$ est circulaire, n'ayant que le cycle:

$$t = (\alpha^0 \alpha^1 \alpha^2 \ldots \alpha^{6n-1}). \tag{21}$$

Le groupe $\{|x, \alpha x|\}$ est régulier (note 27); toutes les puissances $|x, \alpha x|^\nu = |x, \alpha^\nu x|$, $\nu = 0, 1, 2 \ldots$, autre que l'identité, sont des substitutions formées de cycles égaux et déplacent tous les éléments. Celles dont l'exposant > 1 est premier avec $6n$ sont circulaires; elles correspondent aux autres racines primitives de N. On sait d'ailleurs que les puissances α^ν, dont l'exposant $\nu > 1$ est premier avec $6n$, sont congrues aux autres racines primitives de N. Plus généralement, soit ω un diviseur quelconque de $6n$. La puissance $t^\omega = |x, \alpha^\omega x|$ est:

$$(\alpha^0 \alpha^\omega \alpha^{2\omega} \ldots \alpha^{6n-\omega})(\alpha^1 \alpha^{\omega+1} \alpha^{2\omega+1} \ldots \alpha^{6n-\omega+1}) \ldots\ldots (\alpha^{\omega-1} \alpha^{2\omega-1} \ldots \alpha^{6n-1}); \tag{22}$$

elle a donc ω cycles de $\frac{6n}{\omega}$ éléments chacun. Les substitutions du diviseur $\{|x, \alpha^\omega x|\}$ sont les puissances $t^0, t^\omega, t^{2\omega}, \ldots, t^{\left(\frac{6n}{\omega}-1\right)\omega}$; celles de ces puissances pour lesquelles dans l'exposant $\mu\omega$, μ est premier avec $\frac{6n}{\omega}$, auront comme (22) des cycles de $\frac{6n}{\omega}$ éléments; elles seront évidemment les substitutions du groupe $\{t\}$ ayant des cycles de $\frac{6n}{\omega}$ éléments.

La substitution $\tau = |\underline{x}, \underline{\alpha x}|$ est le cycle:

$$\tau = (\underline{\alpha^0}\ \underline{\alpha^1}\ \underline{\alpha^2} \ldots \underline{\alpha^{3n-1}}). \tag{23}$$

Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ est donc régulier; toutes les puissances $|\underline{x}, \underline{\alpha x}|^\nu = |\underline{x}, \underline{\alpha^\nu x}|$, $\nu = 0, 1, 2, \ldots$, autre que l'identité, sont formées de cycles égaux et déplacent tous les éléments. Du § 25, nous savons que la substitution $|\underline{x}, \underline{\alpha^\nu x}|$ vient de la substitution $|x, \alpha^\nu x|$ en y remplaçant chaque élément $a > 3n$ par son complément $N - a \leqq 3n$; du § 27 nous savons que les $3n$ substitutions $|x, \alpha^\nu x|$ dans lesquelles α^ν a un reste

positif (mod. N) $\leqq 3n$ donnent le groupe entier $\{|\underline{x}, \underline{\alpha x}|\}$. D'autre part $\alpha^{3n+\nu} \equiv -\alpha^{\nu}$ (mod. N), $\nu = 0, 1, 2, \ldots, 3n-1$, et les deux puissances $|x, \alpha^{3n+\nu} x|$ et $|x, \alpha^{\nu} x|$ donneront la même substitution réduite $|\underline{x}, \underline{\alpha^{\nu} x}|$. Il suffit donc pour passer des substitutions du groupe $\{|x, \alpha x|\}$ à celles du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, de réduire dans le sens indiqué, ou bien les $3n$ premières puissances de $|x, \alpha x|$, ou bien les $3n$ puissances $|x, \alpha^{\nu} x|$ dans lesquelles α^{ν} (mod. N) est un élément $\leqq 3n$.

Chaque substitution circulaire du groupe $\{|x, \alpha x|\}$ peut prendre la forme (21) en se servant de la racine primitive appropriée; elle donne donc en la réduisant, une substitution *circulaire* du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, puisqu'elle prend alors la forme (23). Si $\varphi(3n) = \varphi(6n)$, ($N$ est alors de la forme $4n - 1$), les deux groupes $\{|\underline{x}, \underline{\alpha x}|\}$ et $\{|x, \alpha x|\}$ ont le même nombre de substitutions circulaires; dans le premier groupe sont circulaires celles pour lesquelles α^{ν} est, ou une racine primitive $\beta \leqq 3n$, ou le complément $N - \beta$ d'une racine primitive $\beta > 3n$. Si $\varphi(3n) = \frac{1}{2}\varphi(6n)$, ($N$ est alors de la forme $4n + 1$), le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ n'a qu'une substitution circulaire pour deux du groupe $\{|x, \alpha x|\}$; dans ce cas, si $\alpha \leqq 3n$ est une racine primitive de N, $N - \alpha > 3n$ *en est une aussi* et les deux substitutions $|x, \alpha x|$ et $|x, (N - \alpha) x|$ donnent la même substitution réduite $|\underline{x}, \underline{\alpha x}|$.

Soit d un diviseur quelconque de $3n$. La puissance $\tau^d = |\underline{x}, \underline{\alpha^d x}|$ est:

$$(\underline{\alpha^0\ \alpha^d\ \alpha^{2d} \ldots \alpha^{3n-d}})\ (\underline{\alpha^1\ \alpha^{d+1}\ \alpha^{2d+1} \ldots \alpha^{3n-d+1}}) \ldots\ldots (\underline{\alpha^{d-1}\ \alpha^{2d-1} \ldots \alpha^{3n-1}});\ (24)$$

elle a donc d cycles de $\frac{3n}{d}$ éléments chacun. Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ a le diviseur $\{|\underline{x}, \underline{\alpha^d x}|\}$ dont les substitutions sont les puissances $\tau^0, \tau^d, \tau^{2d}, \ldots, \tau^{\left(\frac{3n}{d}-1\right)d}$; celles de ces puissances pour lesquelles dans l'exposant μd, μ est premier avec $\frac{3n}{d}$, auront comme (24) des cycles de $\frac{3n}{d}$ éléments; elles seront évidemment les substitutions du groupe $\{\tau\}$ ayant des cycles de $\frac{3n}{d}$ éléments.

Les deux groupes $\{t\}$ et $\{\tau\}$ sont évidemment *transitifs*: par leurs substitutions chaque élément se trouve successivement changé en tous

les autres. On sait qu'un groupe régulier transitif est *imprimitif;* chacune de ses substitutions donne une répartition des éléments en systèmes imprimitifs, constitués directement par les éléments de chaque cycle [37]).

30. *Le triple* $\underline{\alpha^0}\ \underline{\alpha^n}\ \underline{\alpha^{2n}}$ *est une caractéristique.*

Preuve: Les 6 éléments α^0, α^n, α^{2n}, α^{3n}, α^{4n}, α^{5n} appartiennent aux trois triples contenant l'élément o dans la colonne cyclique qui a pour tête le triple o, α^0, α^n. En effet les trois triples contenant l'élément o dans cette colonne sont:

$$\text{o},\ \alpha^0,\ \alpha^n;\ -\alpha^0,\ \text{o},\ -\alpha^0+\alpha^n;\ -\alpha^n,\ \alpha^0-\alpha^n,\ \text{o}. \tag{25}$$

On a la congruence:

$$\alpha^{3n}\equiv -1 \pmod{N}, \tag{26}$$

de laquelle il résulte, puisque $(\alpha^{3n}+1)=(\alpha^n+1)\ (\alpha^{2n}-\alpha^n+1)\equiv \text{o}$ aussi celle-ci:

$$\alpha^{2n}\equiv \alpha^n-\alpha^0. \tag{27}$$

Avec ces congruences (26) et (27), les triples (25) s'écrivent immédiatement, comme nous devions l'établir:

$$\text{o},\ \alpha^0,\ \alpha^n;\quad \alpha^{3n},\ \text{o},\ \alpha^{2n};\quad \alpha^{4n},\ \alpha^{5n},\ \text{o}.\ ^{38})$$

---

[37]) Un groupe de substitutions est ***simplement transitif*** lorsque, α et α' étant deux éléments quelconques, il y a dans le groupe une substitution qui change α en α'; ***doublement transitif*** lorsque, (α, β) et (α', β') étant deux couples quelconques des éléments, il y a dans le groupe une substitution qui change le couple (α, β) en (α', β'); etc.

Un groupe de substitutions transitif est ***imprimitif,*** lorsque ses éléments se répartissent en systèmes dits ***imprimitifs*** tels que par les substitutions du groupe, les éléments de chaque système sont toujours changés, ou entièrement en eux-mêmes, ou entièrement en ceux d'un autre système. Si aucune répartition de ce genre n'est possible, le groupe transitif est dit ***primitif.*** Il résulte immédiatement de la première définition donnée que seul un groupe ***simplement*** transitif peut être imprimitif. Il résulte aussi immédiatement de la seconde définition que tous les systèmes d'une répartition imprimitive ont le même nombre d'éléments.

[38]) Cette propriété des 6 éléments α^0 à α^{5n} et la preuve donnée sont de Netto. C'est au moyen de cette propriété, ou plutôt de la suivante plus générale, qui s'établit immédiatement de la même manière: les 6 éléments α^a à α^{5n+a}, $a=\text{o}, 1, 2, \ldots, n-1$, sont toujours associés à l'élément o dans la même colonne cyclique, qu'il a construit un système de triples de Steiner cyclique pour $N=6n+1$ premier (§ 4). Voir A., p. 57 ou *Netto,* Combinatorik, p. 220.

D'autre part, encore comme suite de la congruence (26), les restes absolus des 6 éléments en question sont $\underline{\alpha^0}$, $\underline{\alpha^n}$, $\underline{\alpha^{2n}}$. Le triple $\underline{\alpha^0}\ \underline{\alpha^n}\ \underline{\alpha^{2n}}$ est donc bien une caractéristique.

31. En vertu du § précédent et du § 26, les n triples suivants, déduits du premier d'entre eux par les n premières puissances de la substitution $|\underline{x}, \underline{\alpha x}|$:

$$\begin{array}{lll} \underline{\alpha^0} & \underline{\alpha^n} & \underline{\alpha^{2n}}, \\ \underline{\alpha^1} & \underline{\alpha^{n+1}} & \underline{\alpha^{2n+1}}, \\ \cdots\cdots\cdots\cdots\cdots & & \\ \underline{\alpha^{n-1}} & \underline{\alpha^{2n-1}} & \underline{\alpha^{3n-1}}. \end{array} \tag{28}$$

sont n caractéristiques. Elles contiennent exactement les $3n$ éléments $1, 2, \ldots, 3n$. Elles forment donc un système de n caractéristiques, dans lequel les n caractéristiques sont sans élément commun (§ 16), nous dirons désormais tout court un *système de caractéristiques*. Nous appellerons celui-ci, pour des raisons qui apparaîtront encore, le système des caractéristiques *principales* [39]).

Les puissances suivantes, égale ou supérieures à n, de la substitution $|\underline{x}, \underline{\alpha x}|$ reproduisent indéfiniment et dans le même ordre la suite de caractéristiques (28). Nous l'appellerons pour cela, aussi, une *colonne cyclique* de caractéristiques. Cette colonne est *fixée* par l'une quelconque de ses caractéristiques. Le triple $\underline{\alpha^a}\ \underline{\alpha^{n+a}}\ \underline{\alpha^{2n+a}}$ où $a \leqq n$ est donc toujours une caractéristique principale; il est la caractéristique $\underline{\alpha^{a'}}\ \underline{\alpha^{n+a'}}\ \underline{\alpha^{2n+a'}}$, si a' est le plus petit reste positif ou nul de l'entier a (mod. n).

La caractéristique principale $\underline{\alpha^a}\ \underline{\alpha^{n+a}}\ \underline{\alpha^{2n+a}}$, $a = 0, 1, 2, \ldots, n-1$, est *fixée* par son élément $\underline{\alpha^a}$ et plus simplement par l'exposant a. Nous pouvons donc représenter les n caractéristiques principales (28) par les *nouveaux éléments:*

$$\mathbf{0, 1, 2, \ldots\ldots, n-1.}$$

---

[39]) Je l'ai appelé dans *J.* et *T.* (*J.*, § 5) le système des caractéristiques ***imprimitives.*** Il forme en effet les cycles de la substitution $|\underline{x}, \underline{\alpha^n x}| = (\underline{\alpha^0}\ \underline{\alpha^n}\ \underline{\alpha^{2n}})\ (\underline{\alpha^1}\ \underline{\alpha^{n+1}}\ \underline{\alpha^{2n+1}})$ $\ldots\ldots$ $(\underline{\alpha^{n-1}}\ \underline{\alpha^{2n-1}}\ \underline{\alpha^{3n-1}})$ et le sens de cette appellation est claire d'après la fin du § 29 et la note jointe. Elle ne tient cependant qu'à une propriété de ces caractéristiques, si importante qu'elle soit pour elles, et j'ai préféré ici le terme plus simple de caractéristiques principales.

La caractéristique principale $\underline{\alpha^a\ \alpha^{n+a}\ \alpha^{2n+a}}$, où a est entier naturel quelconque, sera ainsi représentée par l'élément $\boldsymbol{a}$, $\boldsymbol{a}$ étant le plus petit reste positif ou nul de l'entier a (mod. n).

Les résultats de ce § peuvent alors se résumer ainsi: Une caractéristique principale est changée en elle-même par la substitution $|\underline{x, \alpha^n x}|$; le système des caractéristiques principales est changé en lui-même par la substitution $|\underline{x, \alpha x}|$; dit autrement, le système des caractéristiques principales possède le groupe entier $\{|\underline{x, \alpha x}|\}$. Le groupe des permutations des caractéristiques principales entre elles par les substitutions du groupe cyclique $\{|\underline{x, \alpha x}|\}$ est isomorphe au groupe cyclique $\{(\mathbf{0\,1\,2} \ldots \overline{\boldsymbol{n-1}})\}$; le groupe $\{|\underline{x, \alpha x}|\}$ lui-même est triplement isomorphe à ces deux derniers groupes [40]).

32. Soit maintenant une caractéristique quelconque autre que les caractéristiques (28). Nous pouvons l'écrire:

$$\underline{\alpha^a\ \alpha^b\ \alpha^c}\text{, où } a, b, c, \text{ sont trois entiers différents}$$

parmi 0, 1, 2, ..., $3n-1$, et pour lesquels on n'a pas $a \equiv b \equiv c$ (mod. n).

Aucune puissance de la substitution $|\underline{x, \alpha x}|$, autre que l'identité, ne peut changer cette caractéristique en elle-même. En effet, si une puissance de $|\underline{x, \alpha x}|$, autre que l'identité et déplaçant donc tous les éléments, changeait cette caractéristique en elle-même, elle contiendrait le cycle $(\underline{\alpha^a\ \alpha^b\ \alpha^c})$ ou son inverse $(\underline{\alpha^a\ \alpha^c\ \alpha^b})$. Or les seules puissances de la substitution $|\underline{x, \alpha x}|$ formées de cycles de trois éléments sont (§ 29):

$$|\underline{x, \alpha^n x}| = (\underline{\alpha^0\ \alpha^n\ \alpha^{2n}})\ (\underline{\alpha^1\ \alpha^{n+1}\ \alpha^{2n+1}})\ \ldots\ldots\ (\underline{\alpha^{n-1}\ \alpha^{2n-1}\ \alpha^{3n-1}}),$$

$$|\underline{x, \alpha^{2n} x}| = (\underline{\alpha^0\ \alpha^{2n}\ \alpha^n})\ (\underline{\alpha^1\ \alpha^{2n+1}\ \alpha^{n+1}})\ \ldots\ldots\ (\underline{\alpha^{n-1}\ \alpha^{3n-1}\ \alpha^{2n-1}}).$$

Leurs cycles sont les caractéristiques principales (28) et $\underline{\alpha^a\ \alpha^b\ \alpha^c}$ devrait être l'une d'entre elles, ce qui n'est pas.

[40]) Deux groupes sont *simplement isomorphes* lorsque, en tant que groupes abstraits, ils sont identiques. Un groupe G est *triplement isomorphe* à un groupe Γ, si à chaque opérateur de Γ: $\alpha, \beta, \gamma, \ldots$, correspond un triple d'opérateurs de G: (a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3), ... de façon telle que, si $\alpha\beta = \gamma$, $a_i b_k = c_l$; $i, k, l = 1, 2, 3$ et inversement.

Les $3n$ premières puissances de la substitution $|\underline{x}, \underline{\alpha x}|$ changent la caractéristique $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$ en $3n$ caractéristiques *différentes* qui sont:

$$\begin{array}{lll} \underline{\alpha^a} & \underline{\alpha^b} & \underline{\alpha^c}, \\ \underline{\alpha^{a+1}} & \underline{\alpha^{b+1}} & \underline{\alpha^{c+1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & \\ \underline{\alpha^{a+3n-1}} & \underline{\alpha^{b+3n-1}} & \underline{\alpha^{c+3n-1}}. \end{array} \qquad (29)$$

En effet chacun de ces $3n$ triples est une caractéristique d'après le § 26. Deux d'entre eux ne sauraient être la même caractéristique, sinon, $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$ étant la première de deux caractéristiques (29) identiques, une puissance de $|\underline{x}, \underline{\alpha x}|$ autre que l'identité changerait $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$ en elle-même, ce qui n'a pas lieu.

Les puissances suivantes, égale ou supérieures à $3n$, de la substitution $|\underline{x}, \underline{\alpha x}|$ reproduisent indéfiniment et dans le même ordre la suite de caractéristiques (29). Nous l'appellerons encore une *colonne cyclique* de caractéristiques. Cette colonne est *fixée* par l'une quelconque de ses caractéristiques que l'on peut appeler sa *tête* de colonne. $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$ étant l'une quelconque des caractéristiques (29), elle s'écrit plus simplement $\underline{\alpha^{a'}}\ \underline{\alpha^{b'}}\ \underline{\alpha^{c'}}$, a', b', c' étant respectivement les plus petits restes positifs ou nuls des exposants a, b, c (mod. $3n$).

Les résultats obtenus peuvent encore s'énoncer: Une caractéristique qui n'est pas principale n'est changée en elle-même que par la substitution-identité du groupe $\{|\underline{x}, \underline{\alpha x}|\}$. Chaque colonne cyclique de caractéristiques est changée en elle-même par la substitution $|\underline{x}, \underline{\alpha x}|$; autrement dit, elle possède le groupe entier $\{|\underline{x}, \underline{\alpha x}|\}$. Le groupe des permutations des caractéristiques (29) entre elles par les substitutions du groupe cyclique $\{|\underline{x}, \underline{\alpha x}|\}$ est isomorphe au groupe cyclique $\{(0\ 1\ 2\ \ldots\ \overline{3n-1})\}$.

33. Il y a $n(3n-2)$ caractéristiques (§ 15). Il y a n caractéristiques principales. Les $n(3n-2) - n = 3n(n-1)$ caractéristiques restantes se répartissent donc en $n-1$ colonnes cycliques de $3n$ caractéristiques chacune.

Cette répartition peut se vérifier encore aisément de la manière suivante. Les caractéristiques contenant l'élément $\underline{\alpha^0} = 1$ sont:

$$1, 2, 3; \quad 1, 3, 4; \quad 1, 4, 5; \ldots\ldots, 1, 3n-1, 3n. \tag{30}$$

En effet, rappelons que dans une caractéristique, ou la somme de deux éléments est égale au troisième, ou la somme des trois éléments est égale à N. Une caractéristique contenant l'élément 1 ne peut avoir la somme de ses trois éléments égale à N, car les deux plus grands éléments qui peuvent être associés à 1 dans une caractéristique sont $3n-1$ et $3n$ et $1 + (3n-1) + 3n < N$. Il ne peut donc exister une caractéristique contenant l'élément 1, autre que les $3n-2$ caractéristiques (30).

Chaque colonne cyclique de $3n$ caractéristiques a trois et trois seules de ses caractéristiques contenant l'élément $\underline{\alpha^0} = 1$ et une des caractéristiques principales contient l'élément 1. Il y aura donc $\frac{3n-2-1}{3} = n-1$ colonnes cycliques de $3n$ caractéristiques.

(Reçu le 19 février 1931)