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

Artikel: Sur une manière de différencier les fonctions cycliques d'une forme donnée.
Autor: Lambossy, P.
DOI: https://doi.org/10.5169/seals-4678

Sur une manière de différencier les fonctions cycliques d'une forme donnée

par P. LAMBOSSY, Fribourg.

Introduction

Le présent travail fait directement suite aux théorèmes 4, 5 et 6 du Chapitre II du mémoire de S. Bays qui paraît dans ce même fascicule.

Il s'agissait du théorème suivant, énoncé par S. Bays dans son second mémoire sur les systèmes cycliques de triples de Steiner[1]: *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, p *premier*] *équivalentes, se déduisent l'une de l'autre par une substitution métacyclique.*

Nous avons d'abord démontré le théorème pour le cas $n = p$. Il en résulte que pour décider, dans le cas $n = p$, si deux fonctions cycliques données de n variables, de nature quelconque, sont équivalentes ou non, il suffit d'appliquer à l'une d'elles les substitutions métacycliques, faciles à former, et de voir si l'autre fonction se trouve parmi les fonctions déduites.

Cette démonstration forme le contenu des théorèmes 4, 5, et 6 du mémoire de S. Bays nommés plus haut. On y trouvera également en notes et dans les trois premiers § du même chapitre II[2]) tout ce qu'il serait nécessaire de fixer ou de rappeler pour lire aisément cette étude.

Nous avons cherché ensuite à étendre le théorème au cas où *n est la puissance d'un nombre premier*, et nous avons reconnu qu'il n'est pas vrai dans ce cas, du moins pour des fonctions cycliques de nature quelconque. En d'autres termes, le groupe métacyclique peut toujours servir à découvrir des fonctions cycliques équivalentes à l'une d'entre elles, mais certaines de ces fonctions peuvent nous échapper.

Pour former, dans le cas $n = p^m$, deux fonctions cycliques, équivalentes, qui ne se déduisent pas l'une de l'autre par une substitution métacyclique, nous devons nous appuyer sur des conclusions que nous obtiendrons à la fin du Chapitre II de ce mémoire. Pour $n = p^m$, dès

[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 Math., t. 2, 1923, p. 75.

[2]) Voir aussi les § 1 et 5 de l'Avant-propos pp. 295 et 299 du même mémoire de *S. Bays*, dans le vol. précédent des Commentarii Math. Helv. fasc. 4.

que $n \geqq 8$, le groupe métacyclique contient un ou plusieurs groupes semblables au groupe cyclique H. Désignons par H_1 un tel groupe, et formons une fonction φ qui soit invariable par toutes les substitutions du groupe métacyclique M, et par celles-là seulement.[3]) φ est évidemment cyclique. Soit σ une substitution qui transforme H_1 en H; σ n'est pas métacyclique. En effectuant σ sur φ on obtient la fonction équivalente φ_1, cyclique puisque son groupe $\sigma^{-1} M \sigma$ contient $\sigma^{-1} H_1 \sigma = H$, mais non susceptible d'être déduite de φ par une substitution métacyclique, puisqu'une telle substitution ne change pas φ.

Nous pouvons cependant élargir le théorème cité, en adjoignant aux substitutions métacycliques quelques substitutions construites d'une manière spéciale.

Nous avons désigné ces substitutions spéciales par σ_1^{-1}, σ_2^{-1}, ... et nous avons été conduits à opérer à l'aide du complexe (M désigne le groupe métacyclique):

$$R) \qquad M + \sigma_1^{-1} M + \sigma_2^{-1} M + \ldots$$

qui doit fournir toutes les fonctions cycliques équivalentes à une fonction cyclique donnée φ.

Le complexe R) remplace alors le groupe métacyclique de la méthode de S. Bays. Toutefois son application n'est légitime que sous certaines conditions que doit remplir le groupe de φ. Nous les énoncerons en temps opportun.

L'existence des groupes semblables au groupe cyclique H joue un grand rôle dans ce qui va suivre, et il est utile de savoir former ces groupes. C'est pourquoi, laissant pour le moment les fonctions cycliques, nous allons faire une étude préliminaire sur le groupe métacyclique.

Chapitre premier

1. — *Proposons-nous de rechercher les groupes semblables à H contenus dans le groupe métacyclique.*

Soit n une puissance d'un nombre premier, $n = p^m$, $m > 1$, le nombre premier p pouvant être pair ou impair. Certaines conclusions cependant seront différentes suivant que c'est l'un ou l'autre cas; nous aurons soin de faire la distinction.

---

[3]) On peut toujours former des fonctions qui soient invariables par les seules substitutions d'un groupe donné. Voir *E. Netto,* Substitutionentheorie, p. 27, théor. IV.

$s = (1\ 2\ 3 \ldots n)$ est une substitution circulaire du n^e ordre; le groupe cyclique est constitué par

$$H = [s,\ s^2,\ s^3 \ldots s^n = 1].$$

Parmi ces substitutions, les seules qui soient circulaires du n^e ordre sont celles de la forme s^k, où k est premier à n.

Pour qu'il existe, dans le groupe métacyclique, un groupe semblable à H, il faut et il suffit qu'on y puisse trouver une substitution circulaire du n^e ordre, différente des s^k dont nous venons de parler.

Supposons que $|x,\ \alpha + \beta x|$ soit semblable à s; cherchons à quelles conditions doivent satisfaire α, β, n pour qu'une telle substitution existe. On voit déjà que β doit être premier à n et différent de 1.

Voici le résultat auquel nous arriverons: *Toutes les substitutions circulaires du n^e ordre du groupe métacyclique s'obtiennent en prenant pour α un nombre quelconque premier à n, et pour β un nombre de la forme $\beta = 1 + p\,r$ (r quelconque), si p impair, ou de la forme $\beta = 1 + 4r$, (r quelconque), si $p = 2$.*

On déduit qu'un groupe semblable à H existe dès que $n \geqq 8$.[4])

Pour qu'une substitution $|x, \alpha + \beta x|$ soit formée d'un seul cycle de n éléments, il est *nécessaire* que la suite

$$1)\quad 0,\ \alpha,\ \alpha(1+\beta),\ \alpha(1+\beta+\beta^2),\ \ldots,\ \alpha(1+\beta+\beta^2+\ \ldots\ +\beta^{n-2})$$

constitue un système complet de restes (mod n). Cette condition nécessaire est d'ailleurs *suffisante.*

Cette condition est équivalente aux deux suivantes:

$$2)\qquad (\alpha,\ n) = 1$$

$$2')\qquad 0,\ 1,\ 1+\beta,\ 1+\beta+\beta^2,\ \ldots,\ 1+\beta+\beta^2+\ \ldots\ +\beta^{n-2}$$

forme un système complet de restes mod n.

Tout revient à étudier la condition 2'); elle entraîne les suivantes que nous notons 3), 4), 5), 6) et 7).

$$3)\qquad L = 1+\beta+\beta^2+\ \ldots\ +\beta^{n-1} \equiv 0 \pmod{n}.$$

Sinon, l'un des nombres 2'), autre que le premier, serait congru à 0 (mod n).

---

[4]) Si n est premier, il n'y a pas de groupe semblable à H dans le groupe métacyclique.

4) δ *étant le plus petit exposant tel que* $\beta^{\delta} \equiv 1$ *(mod n),* δ *est diviseur de n.*

Multiplions par β la congruence 3) et ajoutons 1

$$1 + \beta + \beta^2 + \ldots + \beta^{n-1} + \beta^n \equiv 1 \pmod{n}$$

En tenant compte de 3) nous obtenons

4') $$\beta^n \equiv 1 \pmod{n}$$

Dès que β est premier à n (ce que nous supposons), le théorème de Fermat est applicable

$$\beta^{\Phi(n)} \equiv 1 \pmod{n}.$$

Soit δ le plus petit exposant pour lequel on a

$$\beta^{\delta} \equiv 1 \pmod{n}.$$

δ est toujours diviseur de $\Phi(n)$; mais si nous voulons que 4') soit vérifiée, *il faut que* δ *soit également diviseur de n.*

On peut se demander s'il est toujours possible de trouver des nombres β tels que leurs δ soient diviseurs de n.

Si $p = 2$, on a

$$n = 2^m, \quad \Phi(n) = 2^{m-1}$$

δ est toujours diviseur de n. Si p est impair

$$n = p^m, \quad \Phi(n) = p^{m-1}(p - 1)$$

δ doit être une puissance de p. Les seuls δ a priori possibles sont

$$p, p^2, \ldots, p^{m-1}.$$

Un théorème de la Théorie des nombres montre qu'effectivement à chacun de ces nombres correspondent certains β.[5])

5) $$l = 1 + \beta + \beta^2 + \ldots + \beta^{\delta-1} \equiv 0 \pmod{\delta}$$

5) se déduit de 3) en observant que n est multiple de δ. Posons $n = n'\delta$. Puisque $\beta^{\delta} \equiv 1 \pmod{n}$, L peut s'écrire

$$L = (1 + \beta + \ldots + \beta^{\delta-1}) + (1 + \beta + \ldots + \beta^{\delta-1}) + \ldots \equiv 0 \pmod{n}.$$

[5]) *Serret:* Algèbre Supérieure, 2me éd., t. II, p. 85, théor. II.

Chaque parenthèse contient δ termes et il y a n' parenthèses.

$$L = n'(1 + \beta + \ldots + \beta^{\delta-1}) \equiv 0 \pmod{n'\,\delta}$$
$$l = 1 + \beta + \ldots + \beta^{\delta-1} \equiv 0 \pmod{\delta}$$

6) $$l' = \frac{l}{\delta} \text{ est premier avec } n' = \frac{n}{\delta}$$

Pour le voir, observons que

$$1 + \beta + \beta^2 + \ldots + \beta^{r\delta-1} \qquad (1 \leqq r < n')$$

est un terme de la suite 2') autre que 0; on a donc

$$1 + \beta + \beta^2 + \ldots + \beta^{r\delta-1} \not\equiv 0 \pmod{n}$$
$$r\,l \not\equiv 0 \pmod{n} \qquad (1 \leqq r < n')$$
mais $r\,l \equiv 0 \pmod{n}$ pour $r = n'$.

On conclut que $l' = \frac{l}{\delta}$ est premier avec $n' = \frac{n}{\delta}$

7) $$\beta \equiv 1 \pmod{n'}$$

Car on a:

$$\beta^{\delta} - 1 = (\beta - 1)(1 + \beta + \ldots + \beta^{\delta-1}) \equiv 0 \pmod{n}$$
$$(\beta - 1)\,l \equiv 0 \pmod{n}$$
$$(\beta - 1)\,l' \equiv 0 \pmod{n'}$$

et comme $(l', n') = 1$

$$\beta - 1 \equiv 0 \pmod{n'}$$

2. — Ces cinq conséquences 3), 4), 5), 6), 7) sont impliquées dans la condition 2'). *Inversement*, si on a

4) δ étant le plus petit exposant tel que $\beta^{\delta} \equiv 1 \pmod{n}$, δ est diviseur de n.

5) $l = 1 + \beta + \beta^2 + \ldots + \beta^{\delta-1} \equiv 0 \pmod{\delta}$

6) $(l', n') = 1$ avec $l' = \frac{l}{\delta}$, $n' = \frac{n}{\delta}$ la condition 2') se trouve être satisfaite.

En effet, écrivons pour simplifier

$$a = 1 + \beta, \quad b = 1 + \beta + \beta^2, \quad c = 1 + \beta + \beta^2 + \beta^3, \ \ldots,$$
$$l = 1 + \beta + \beta^2 + \ \ldots\ \beta^{\delta-1};$$

tous les nombres 2') peuvent être rangés dans le tableau suivant:

8)
$$\left.\begin{array}{lllll} 1, & a, & b, & c, & \ldots\ l, \\ 1+l, & a+l, & b+l, & c+l, & \ldots\ 2l, \\ 1+2l, & a+2l, & b+2l, & c+2l, & \ldots\ 3l, \\ \ldots\ldots & & & & \\ \ldots\ldots & & & & \\ 1+(n'-1)l, & a+(n'-1)l, & \ldots\ldots & & n'l \end{array}\right\} \begin{array}{l} \delta \text{ colonnes} \\ n' \text{ lignes} \end{array}$$

Pour montrer que les n nombres du tableau sont incongrus entre eux (mod n), prenons-en deux appartenant à la même colonne. S'ils étaient congrus entre eux, nous aurions une congruence telle que

$$r\,l \equiv 0 \pmod{n} \qquad r < n'$$
$$r\,l' \equiv 0 \pmod{n'}$$

Elle n'est pas satisfaite par $r < n'$, puisque $(l', n') = 1$. Prenons ensuite deux nombres appartenant à deux colonnes différentes. Si on avait, p. ex.

$$a + l\,x \equiv c + l\,y \pmod{n}$$

on aurait

$$l\,(x - y) \equiv c - a \pmod{n}$$

Or $(l, n) = \delta$, et deux nombres tels que c et a ont une différence $c - a$ qui n'est pas divisible par δ, comme il est aisé de voir.

$$a = 1 + \beta + \ \vdots\ + \beta^{K-1}$$
$$c = 1 + \beta + \ \ldots\ + \beta^{K-1} + \beta^{K} + \ \ldots\ + \beta^{K+S-1} \qquad (S < \delta)$$

Si on avait

$$c - a = \beta^{K}(1 + \beta + \ \ldots\ + \beta^{S-1}) \equiv 0 \pmod{\delta}$$

on aurait aussi

$$1 + \beta + \ \ldots\ + \beta^{S-1} \equiv 0 \pmod{\delta}.$$

Nous pouvons utiliser 7) c'est-à-dire $\beta - 1 \equiv 0 \pmod{n'}$ puisqu'elle découle des prémisses 4), 5), 6). On déduit:

$$(\beta - 1)\ (1 + \beta + \ \ldots\ + \beta^{S-1}) \equiv 0 \pmod{n'\delta}$$
$$\beta^{S} - 1 \equiv 0 \pmod{n}$$

ce qui n'a pas lieu puisque $S < \delta$.

Il est donc démontré que tous les nombres du tableau, c'est-à-dire tous les nombres 2') forment un système complet de restes (mod n).

3. — Sur la forme de β nous avons un premier renseignement fourni par 7)

$$\beta \equiv 1 \pmod{n'}$$

Si p est impair, $n = p^m$, δ peut prendre les valeurs, p, p^2, ..., p^{m-1}, et par suite $n' = \frac{n}{\delta}$ contient le facteur p. En d'autres termes, β est de la forme

$$\beta = 1 + pr.$$

Si $p = 2$, $n = 2^m$, il n'y a pas de racines primitives (excepté pour $n = 4$),[6]) δ atteint au plus la valeur $\frac{\Phi(n)}{2} = \frac{2^{m-1}}{2} = 2^{m-2}$. Donc $\frac{n}{\delta}$ contient au moins le facteur 4. En d'autres termes, β est de la forme

$$\beta = 1 + 4r.$$

Nous nous proposons de démontrer maintenant que tous les nombres $\beta = 1 + 4r$ ou $\beta = 1 + pr$, selon que le nombre premier p est pair ou impair, r désignant un nombre quelconque, satisfont aux conditions 4), 5), 6).

4. — L'expression

$$l = 1 + \beta + \beta^2 + \ldots \beta^{x-1}$$

lorsque x est la puissance d'un nombre premier, donne lieu au *théorème préliminaire* suivant, qui a une forme double:

A. *Si $x = x_0 p^\alpha$ (x_0 non divisible par p), et $\beta = 1 + pr$ (r quelconque), l est divisible par p^α mais non par une puissance supérieure.*

B. *Si $x = x_0 2^\alpha$ (x_0 impair), et $\beta = 1 + 4r$ (r quelconque), l est divisible par 2^α, mais non par une puissance supérieure.*

Occupons-nous d'abord de la première forme:

A. On a: $$l = 1 + \beta + \ldots + \beta^{x-1} = \frac{\beta^x - 1}{\beta - 1} = \frac{(1+pr)^x - 1}{pr}$$

$$l = x + \frac{x(x-1)}{1.2} pr + \frac{x(x-1)(x-2)}{1.2.3} p^2 r^2 + \ldots + p^{x-1} r^{x-1}.$$

Le premier terme est divisible par p^α et le quotient est x_0. Il faut montrer que tous les autres termes sont divisibles par p^α et que le

[6]) *Serret*, Alg. Sup., t. II, p. 52.

quotient contient le facteur p. Laissons donc le premier terme; la forme générale des autres est:

$$\frac{x(x-1)(x-2)\ \ldots\ (x-s+1)}{1\cdot 2\cdot\ \ldots\ s}\,p^{s-1}\,r^{s-1} \qquad 2 \leqq s \leqq x$$

Puisque l'expression

$$\frac{(x-1)(x-2)\ \ldots\ (x-s+1)}{1\cdot 2\ \ldots\ (s-1)}$$

représente un nombre entier K, le terme général peut s'écrire

9) $$\frac{x\,K}{s}\,p^{s-1}\,r^{s-1}$$

$\frac{x\,K}{s}$ est entier; posons $s = p^{\gamma} q$, où q ne contient plus le facteur p. s est en effet une variable qui peut devenir multiple de p. Si s est premier avec p, alors $\gamma = 0$.

Voyons comment la fraction $\frac{x\,K}{s}$ doit se simplifier. Puisque $x = x_0 p^{\alpha}$, $s = p^{\gamma} q$, q doit être diviseur de $x_0 K$. Posons $\frac{x_0 K}{q} = K'$ (K' entier). L'expression 9) s'écrit

$$\frac{p^{\alpha} K'}{p^{\gamma}}\,p^{s-1}\,r^{s-1} \text{ ou bien } p^{\alpha} K'\,p^{s-1-\gamma}\,r^{s-1}.$$

Nous aurons prouvé que cette expression est divisible par p^{α} et que le quotient contient le facteur p, si nous prouvons que

$$s - 1 - \gamma \geqq 1, \text{ ou bien } s \geqq \gamma + 2.$$

Si $\gamma = 0$, la chose est claire. Supposons donc $\gamma \geqq 1$. Nous aurons certainement

10) $$p^{\gamma} q \geqq \gamma + 2$$

si nous avons $$p^{\gamma} \geqq \gamma + 2$$

ou encore, puisque $p \geqq 3$, si nous avons

$$3^{\gamma} \geqq \gamma + 2.$$

Cette relation effectivement a lieu. Ainsi l se présente sous la forme

$$l = p^{\alpha}\,[x_0 + \text{multiple de } p].$$

Il est donc prouvé que l est divisible par p^{α}, mais non par une puissance supérieure.

B. Pour établir la seconde forme du théorème, remarquons que tout ce qui vient d'être dit dans l'article A jusqu'à la formule 10) est vrai quel que soit le nombre premier p. Imaginons qu'on ait fait $p = 2$ dans toutes les formules. 10) deviendra

$$2^\gamma q \geqq \gamma + 2 \qquad (\gamma \geqq 1).$$

Pour $\gamma = 2$, $q \geqq 1$, et pour $\gamma = 1$, $q > 1$, cette relation est évidemment vérifiée, et pour ces valeurs le terme 9) est divisible par 2.

Il y a doute pour $\gamma = 1$, $q = 1$, c'est-à-dire pour $s = 2$. Reprenons donc la formule 9) en y introduisant $s = 2$, $p = 2$.

$$\frac{x K}{2} 2^1 r^1, \text{ ou bien } x K r.$$

Si l'on retourne à la signification de K, on verra que K est impair. Le terme est donc divisible par 2^α, mais le quotient sera pair seulement si r est pair lui-même. Avec cette supposition, on obtient

$$l = 2^\alpha [x_0 + \text{nombre pair}].$$

Cela veut dire que l est divisible par 2^α, mais non par une puissance supérieure. Si r est impair, l est divisible par une puissance supérieure à 2^α. Enfin les nombres β qu'on obtient en faisant $p = 2$, r pair, dans la formule $\beta = 1 + pr$, sont obtenus avec $\beta = 1 + 4r$ en prenant pour r une valeur quelconque.

5. La démonstration que tout $\beta = 1 + 4r$, pour $n = 2^m$, satisfait aux conditions 4), 5), 6) du n° 2 est maintenant aisée. Premièrement β est premier à n, et son δ, étant diviseur de $\Phi(n) = 2^{m-1}$, est diviseur de n.

Secondement, δ étant une puissance de 2, $\delta = 2^\alpha$, l'expression $1 + \beta + \ldots \beta^{\delta-1}$ est divisible par $\delta = 2^\alpha$, mais non par une puissance supérieure. C'est dire que $l' = \dfrac{1 + \beta + \ldots + \beta^{\delta-1}}{\delta}$ est premier avec $n' = \dfrac{2^m}{2^\alpha} = 2^{m-\alpha}$.

La démonstration analogue pour $\beta = 1 + pr$, $n = p^m$, exige que l'on étudie premièrement le plus petit exposant δ pour lequel on a $\beta^\delta \equiv 1 \pmod{n}$. Il nous faut établir que δ est une puissance de p.

Supposons donc r donné dans $\beta = 1 + pr$ et essayons de trouver la plus petite solution x de la congruence

$$11) \qquad (1 + pr)^x \equiv 1 \pmod{n}.$$

Tout d'abord on doit exclure $x = 1$; cette solution correspond à $r = 0$, $\beta = 1$, valeur écartée. 11) peut s'écrire

$$x \cdot pr + \frac{x(x-1)}{1 \cdot 2} p^2 r^2 + \ldots + p^x r^x \equiv 0 \pmod{p^m}$$

$$r\left[x + \frac{x(x-1)}{1 \cdot 2} pr + \frac{x(x-1)(x-2)}{1 \cdot 2 \cdot 3} p^2 r^2 + \ldots + p^{x-1} r^{x-1}\right] \equiv 0 \pmod{p^{m-1}}.$$

Soit p^a la plus haute puissance de p contenue comme facteur dans r ; on a : $a \leqq m - 2$.

12) $$x + \frac{x(x-1)}{1 \cdot 2} pr + \frac{x(x-1)(x-2)}{1 \cdot 2 \cdot 3} p^2 r^2 + \ldots + p^{x-1} r^{x-1} \equiv 0 \pmod{p^{m-1-a}}.$$

D'après le théorème préliminaire, un nombre quelconque $x = x_0 p^\alpha$ (x_0 non divisible par p) est solution de 12) si $\alpha \geqq m - 1 - a$. La solution la plus petite de la congruence 12), et aussi de la congruence 11), qui lui est équivalente, est évidemment $\delta = p^{m-1-a}$. Cela étant, $l = 1 + \beta + \ldots + \beta^{\delta-1}$ est divisible par $\delta = p^{m-1-a}$, mais non par une puissance supérieure. C'est dire que $l' = \frac{1 + \beta + \ldots + \beta^{\delta-1}}{\delta}$ est premier avec $n' = \frac{n}{\delta} = \frac{p^m}{p^{m-1-a}} = p^{1+a}$.

Il est donc prouvé que tout nombre $\beta = 1 + pr$ vérifie les conditions 4), 5), 6).

6. — *Lorsque $n = p^m$ ou $n = 2^m$, le nombre des groupes semblables à H contenus dans tout diviseur métacyclique est respectivement une puissance de p ou une puissance de 2.*

Pour plus de généralité nous prenons un diviseur métacyclique $\mathcal{F}$; la proposition est aussi vraie pour le groupe métacyclique complet.

Soient H, H_1, H_2, ... les groupes semblables à H contenus dans $\mathcal{F}$, et N leur nombre. Dénombrons les substitutions circulaires du n^e ordre contenues dans $\mathcal{F}$. Dans chaque H il y a $\Phi(n)$ substitutions circulaires d'ordre n. Comme les différents H n'ont entre eux aucune substitution circulaire commune, il y a donc dans $\mathcal{F}$ $N \cdot \Phi(n)$ substitutions circulaires.

Ces substitutions sont de la forme $|x, \alpha + \beta x|$. α peut prendre $\Phi(n)$ valeurs (les nombres premiers à n) et les prend réellement. A une valeur *admissible* pour β (donnant lieu à une substitution circulaire contenue dans $\mathcal{F}$) correspondent $\Phi(n)$ substitutions circulaires qu'on obtient en

donnant à α $\Phi(n)$ valeurs. Donc le nombre des valeurs admissibles pour β est

$$\frac{N \cdot \Phi(n)}{\Phi(n)} = N.$$

Désignons ces valeurs par

13) $$1, \beta_1, \beta_2, \ldots$$

Les substitutions

14) $$1, |x, \beta_1 x|, |x, \beta_2 x|, \ldots$$

sont également dans $\mathcal{F}$. On obtient p. ex. $|x, \beta_1 x|$ à partir de $|x, \alpha + \beta_1 x|$ en multipliant cette dernière par $|x, n - \alpha + x|$. Leur nombre est N. Il est utile de remarquer que $\mathcal{F}$ peut contenir d'autres $|x, \beta x|$, mais alors β n'est pas de la forme $1 + pr$ ou $1 + 4r$.

Nous pouvons montrer que les substitutions 14) forment un groupe, qui par suite est contenu dans $\mathcal{F}$. Formons le produit de deux d'entre elles

$$s = |x, \beta_1 \beta_2 x|$$

s est dans $\mathcal{F}$. Cette substitution multipliée par $|x, 1 + x|$ fournira une substitution de $\mathcal{F}$ qui sera circulaire si $\beta_1 \beta_2$ est de la forme $1 + pr$ ou $1 + 4r$. C'est en effet le cas, parce que le produit de deux nombres de la forme $1 + pr$ est aussi de la forme $1 + pr$. Alors $\beta_1 \beta_2$ figure dans 13), et enfin s est dans 14). Donc les substitutions 14) forment un groupe.

A ce groupe correspond un groupe isomorphe formé par l'ensemble des nombres 13) pris mod n; il a le même ordre. 13) est un sous-groupe du groupe abélien total qu'on obtient en prenant tous les β de la forme $1 + pr$ qui sont au nombre de p^{m-1}, ou tous les β de la forme $1 + 4r$ qui sont au nombre de 2^{m-2}.

Donc N est une puissance de p ou de 2.

7. — *Formation des groupes H.* En utilisant les nombres 13) formons les substitutions circulaires $s, s_1, s_2, \ldots$ et les groupes correspondants $H, H_1, H_2, \ldots$

$$\begin{aligned} s &= |x, 1 + x| & H &= [s, s^2, \ldots] \\ s_1 &= |x, 1 + \beta_1 x| & H_1 &= [s_1, s_1^2, \ldots] \\ s_2 &= |x, 1 + \beta_2 x| & H_2 &= [s_2, s_2^2, \ldots] \\ &\ldots\ldots\ldots\ldots & &\ldots\ldots\ldots\ldots \end{aligned}$$

Nous formons ainsi tous les groupes semblables à H contenus dans le diviseur métacyclique; pour le voir, il suffit de montrer qu'ils sont tous différents.

Deux substitutions quelconques prises parmi s, s_1, s_2, ... sont bien différentes, mais s'il arrivait que l'une fût une puissance de l'autre, que l'on eût p. ex. $s_2 = s_1^{\gamma}$, les groupes H_1 et H_2 seraient identiques. Cela n'a pas lieu, car si l'on forme les puissances successives de s_1, la constante α, qui est égale à 1 dans s_1, deviendra successivement égale à

$$1 + \beta_1, \quad 1 + \beta_1 + \beta_1^2, \quad \ldots$$

et, d'après la propriété de β_1, ne deviendra égale à 1 qu'à la $(n+1)^e$ puissance.

Exemple: Voici pour $n = 3^2 = 9$ les 3 groupes H contenus dans le groupe métacyclique (nous n'écrirons que les substitutions circulaires). De $\beta = 1 + 3r$ on déduit: $\beta = 1$, $\beta_1 = 4$, $\beta_2 = 7$.

H	H_1	H_2
$s = \lvert x, 1+x \rvert$	$s_1 = \lvert x, 1+4x \rvert$	$s_2 = \lvert x, 1+7x \rvert$
$s^2 = \lvert x, 2+x \rvert$	$s_1^2 = \lvert x, 5+7x \rvert$	$s_2^2 = \lvert x, 8+4x \rvert$
$s^4 = \lvert x, 4+x \rvert$	$s_1^4 = \lvert x, 4+4x \rvert$	$s_2^4 = \lvert x, 4+7x \rvert$
$s^5 = \lvert x, 5+x \rvert$	$s_1^5 = \lvert x, 8+7x \rvert$	$s_2^5 = \lvert x, 2+4x \rvert$
$s^7 = \lvert x, 7+x \rvert$	$s_1^7 = \lvert x, 7+4x \rvert$	$s_2^7 = \lvert x, 7+7x \rvert$
$s^8 = \lvert x, 8+x \rvert$	$s_1^8 = \lvert x, 2+7x \rvert$	$s_2^8 = \lvert x, 5+4x \rvert$

Désignons par σ_1 et σ_2 deux substitutions capables de transformer H respectivement en H_1 et H_2; on les obtient comme suit:

$$\sigma_1 = \begin{pmatrix} s \\ s_1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 3 & 4 & 8 & 6 & 7 & 2 & 9 \end{pmatrix} = (258)$$

$$\sigma_2 = \begin{pmatrix} s \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 3 & 4 & 2 & 6 & 7 & 5 & 9 \end{pmatrix} = (285)$$

Les substitutions telles que σ_1 et σ_2 joueront un grand rôle dans la suite.

Chapitre deuxième

8. — Lorsque le nombre des variables est $n = p^m$ ou $n = 2^m$, le problème de la recherche des fonctions cycliques équivalentes à l'une d'entre elles est moins simple que dans le cas $n = p$. Les substitutions métacycliques peuvent toujours être utilisées, mais elles ne peuvent suf-

fire, du moins en général. Toutefois le même groupe métacyclique peut servir à construire d'autres substitutions qui, concuremment avec les précédentes, peuvent servir parfois à découvrir toutes les fonctions cycliques équivalentes. Nous allons former ces substitutions et en même temps chercher des critères qui fixeront des cas où cette méthode est applicable.

Soit G le groupe d'une fonction cyclique φ de n variables ($n = p^m$ ou 2^m); H le groupe cyclique; $\mathfrak{F}$ le groupe formé de toutes les substitutions de G qui sont métacycliques. En général $\mathfrak{F}$ n'est qu'un diviseur du groupe métacyclique complet M. $\mathfrak{F}$ contient, à côté de H, des groupes semblables à H que nous désignerons par H_1, H_2, ...

Soit σ_1 une substitution qui transforme H en H_1

$$\sigma_1^{-1} H \sigma = H_1 .$$

Comme on sait, les substitutions du complexe $M\sigma_1$, et celles-là seulement ont cette propriété.

σ_1^{-1} effectuée sur φ donne une fonction cyclique φ_1. En effet, le groupe de φ_1 est $\sigma_1 G \sigma_1^{-1}$, lequel contient $\sigma_1 H_1 \sigma_1^{-1} = H$. Les substitutions $\sigma_1^{-1} M$ donnent également des fonctions cycliques.

Cela nous amène à examiner les complexes:

$$R) \qquad M,\ \sigma_1^{-1} M,\quad \sigma_2^{-1} M,\ \ldots$$

où M est le groupe métacyclique et σ_i une substitution qui transforme H en H_i de $\mathfrak{F}$. Si nous voulons obtenir toutes les fonctions cycliques équivalentes à φ en utilisant les substitutions R), il nous faut établir le théorème suivant:

Théorème I. La condition nécessaire et suffisante pour que toutes les fonctions cycliques équivalentes à φ puissent se déduire de φ par les substitutions R) est que tous les groupes H de G puissent se déduire de ceux de $\mathfrak{F}$ en transformant ceux-ci par des substitutions de G.

Supposons, *en premier lieu*, que les H_i de G puissent être obtenus en transformant ceux de $\mathfrak{F}$ par des substitutions de G. Pour entrer dans les détails, soit

$$\text{I)} \qquad H,\ H',\ H'',\ \ldots$$

un premier système conjugué obtenu en transformant H par toutes les substitutions de G. Il est possible que dans cette liste figure un ou plusieurs groupes appartenant à $\mathfrak{F}$, autre que H. Soit H_1 un groupe semblable à H contenu dans $\mathfrak{F}$ et qui ne fasse pas partie de la liste I).

Transformons H_1 par toutes les substitutions de G; nous obtenons un second système conjugué

$$\text{II)} \qquad H_1,\ H_1',\ H_1'',\ \ldots$$

Soit H_2 un groupe semblable à H contenu dans $\mathcal{F}$ et qui n'ait paru ni dans I) ni dans II). On obtient de même

$$\text{III)} \qquad H_2,\ H_2',\ H_2'',\ \ldots$$

Ainsi de suite, jusqu'à épuisement des H_i de $\mathcal{F}$. En vertu de notre hypothèse, nous obtiendrons de cette façon tous les groupes semblables à H contenus dans G.

Parmi les substitutions σ_1, σ_2, ... déjà définies, nous ne retenons que celles qui transforment H en H_1, H_2, ... lesquels groupes sont les têtes des listes I), II), III), ... Ces substitutions σ_i ne sont pas contenues dans G. On notera que les substitutions $M\sigma_1$ ont comme σ_1 la propriété de transformer H en H_1, et aucune d'elles n'est contenue dans G parce qu'aucune substitution de G ne transforme H en H_1.

Appliquons maintenant à φ toutes les substitutions métacycliques. On obtient diverses fonctions cycliques

$$\text{I')} \qquad \varphi,\ \varphi',\ \varphi'',\ \ldots$$

Appliquons σ_1^{-1} à φ; nous obtenons une fonction cyclique φ_1; en effectuant sur φ_1 toutes les substitutions métacycliques, nous obtenons une deuxième liste de fonctions cycliques.

$$\text{II')} \qquad \varphi_1,\ \varphi_1',\ \varphi_1'',\ \ldots$$

De même, en appliquant σ_2^{-1} à φ nous obtenons φ_2, puis une 3^e liste

$$\text{III')} \qquad \varphi_2,\ \varphi_2',\ \varphi_2'',\ \ldots.$$

Ainsi de suite;[7]) nous prétendons que toutes les fonctions cycliques équivalentes à φ ont été obtenues.

En effet soit φ_a une fonction cyclique équivalente à φ, d'ailleurs quelconque, et soit τ une substitution qui change φ en φ_a. Le groupe de φ_a est $\tau^{-1} G \tau$. Puisque φ_a est cyclique, son groupe contient H; par suite H est provenu par transformation par τ d'un des groupes semblables à H contenus dans G.

---

[7]) Les substitutions que nous appliquons sont justement les substitutions R).

Si H est provenu de H, alors τ est métacyclique, et φ_a fait partie de la liste I').

Si H est provenu d'un groupe du système conjugué I), autre que H, de H' par exemple, τ n'est pas métacyclique. Mais si s' de G change H en H', la substitution $s'\tau$ qui, exactement comme τ, change φ en φ_a est métacyclique. Cela prouve que, dans ce cas encore, φ_a fait partie de I').

Si H est provenu de H_1, alors τ est de la forme $(m\,\sigma_1)^{-1}$, m désignant une substitution métacyclique déterminée. On peut écrire $\tau = \sigma_1^{-1}\, m^{-1} = \sigma_1^{-1}\, m'$. Mais alors φ_a a été obtenue et figure dans la liste II').

Si H provient d'un groupe du système conjugué II), autre que H_1, de H_1' p. ex., désignons par s_1' une substitution de G qui transforme H_1 en H_1'. Alors $s_1'\tau$ aura sur φ le même effet que τ. Mais $s_1'\tau$ change H_1 en H; comme on vient de le voir, $s_1'\tau$ est de la forme $\sigma_1^{-1}\, m'$, et par conséquent φ_a a été obtenue dans la liste II').

En poursuivant le raisonnement on démontre ainsi qu'il n'y a pas d'autres fonctions cycliques équivalentes à φ que celles des listes I'), II'), ...

Supposons, *en second lieu*, qu'on ne puisse pas déduire tous les H de G en transformant ceux de $\mathcal{F}$ par les substitutions de G.

On peut commencer par effectuer sur φ toutes les substitutions R), et les fonctions cycliques obtenues se rangent en un certain nombre de listes I'), II'), ... comme on l'a vu. Mais il faut montrer que des fonctions cycliques nous échapperont.

Soit H_a un groupe semblable à H contenu dans G, non déductible de ceux de $\mathcal{F}$ par les substitutions de G, et τ une substitution qui transforme H en H_a. Par hypothèse, H_a ne fait donc pas partie des listes I), II), ... On a:

$$\tau^{-1} H \tau = H_a .$$

τ ne fait pas partie de G. Effectuons sur φ la substitution τ^{-1}. Nous obtenons φ_a qui est cyclique parce que son groupe $\tau G \tau^{-1}$ contient $\tau H_a \tau^{-1} = H$. $G\tau^{-1}$ est le complexe de toutes les substitutions qui changent φ en φ_a.

φ_a n'a pas été obtenue à l'aide des substitutions R); car si φ_a figurait parmi les listes I'), II'), ..., nous aurions une égalité telle que

$$\sigma_i^{-1}\, m = g\,\tau^{-1}, \text{ ou bien } m^{-1}\,\sigma_i = \tau\, g^{-1}$$

(g est une certaine substitution de G). Or $m^{-1}\,\sigma_i$ transforme H en H_i; comme τ transforme H en H_a, il s'ensuivrait qu'on pourrait trouver dans

G une substitution g^{-1} transformant H_a en H_i; et aussi une substitution g transformant H_i en H_a. Mais cela est contraire à l'hypothèse.

9. — Par ce théorème général le problème des fonctions cycliques se trouve ramené à un problème de la théorie des groupes, puisque l'application des substitutions R) donnera toutes les fonctions cycliques équivalentes à φ si le groupe de φ remplit certaines conditions.

Malheureusement la détermination pratique du groupe des substitutions qui n'altèrent pas une fonction donnée est laborieuse, et la recherche des propriétés de ce groupe plus difficile encore. C'est pourquoi nous devons supposer que le groupe G de φ n'est pas connu; et nous dirigerons notre étude vers la recherche de *critères*, qui utilisent les données immédiates de la fonction. Parmi ces données immédiates, mentionnons, outre le nombre des variables, le groupe des substitutions métacycliques contenues dans G. Ce groupe, dont l'ordre est relativement petit, est toujours facile à découvrir.

Nous allons donc rechercher des critères fixant des cas assez étendus où les substitutions R) sont suffisantes. Car, contrairement à ce qui a lieu dans le cas $n = p$, ces substitutions R) ne peuvent suffire dans tous les cas possibles.

Nous traiterons séparément les cas $n = p^m$ et $n = 2^m$, et nous commencerons par le cas où le nombre des variables est $n = 2^m$.

10. — *Sur les fonctions de degré $n = 2^m$.* Soit φ une fonction cyclique de degré $n = 2^m$, dont le groupe est G. Comme précédemment, H est le groupe cyclique, et $\mathcal{J}$ le diviseur métacyclique contenu dans G.

L'ordre de $\mathcal{J}$ est une puissance de 2. En effet, l'ordre du groupe métacyclique est $n.\ \Phi(n) = 2^m.\ 2^{m-1} = 2^{2m-1}$, et l'ordre de $\mathcal{J}$ est un diviseur de 2^{2m-1}.

$\mathcal{J}$ contient en général, à côté de H, d'autres groupes semblables à H, et le nombre de ces groupes H est une puissance de 2 (n° 6).

Il se peut qu'il existe dans G, en dehors de $\mathcal{J}$, des substitutions permutables à $\mathcal{J}$. Désignons par $\mathcal{J}'$ le groupe formé par toutes les substitutions de G permutables à $\mathcal{J}$; ce sont donc les substitutions s qui ont la propriété: $s^{-1}\mathcal{J}s = \mathcal{J}$. $\mathcal{J}'$ contient $\mathcal{J}$.

Théorème II. Si dans G on ne trouve en dehors de $\mathcal{J}$ aucune substitution permutable à $\mathcal{J}$, tous les groupes semblables à H contenus dans G peuvent se déduire de ceux de $\mathcal{J}$ par des substitutions de G. Et par suite

toutes les fonctions cycliques équivalentes à φ peuvent se déduire de φ par les substitutions R).

La condition imposée revient à dire $\mathcal{F}' = \mathcal{F}$. Soit ψ_1 une fonction invariable par toutes les substitutions de $\mathcal{F}$ et par celles-là seulement. Quand on effectue sur ψ_1 toutes les substitutions de G, cette fonction acquiert un certain nombre de valeurs

15) $$\psi_1, \psi_2, \psi_3, \ldots, \psi_k.$$

k est égal à l'indice de $\mathcal{F}$ dans G. Nous désignerons par $s_2, s_3, \ldots, s_k$ des substitutions de G qui changent ψ_1 en $\psi_2, \psi_3, \ldots, \psi_k$.

Effectuons sur les fonctions 15) toutes les substitutions de $\mathcal{F}$. Il est clair que ψ_1 ne change pas par cela. On peut se demander si une autre valeur, p. ex. ψ_α, est invariable par toutes les substitutions de $\mathcal{F}$. Supposons qu'il en soit ainsi. Alors le groupe de ψ_α, qui est $s_\alpha^{-1} \mathcal{F} s_\alpha$, est identique à $\mathcal{F}$.

$$s_\alpha^{-1} \mathcal{F} s_\alpha = \mathcal{F}.$$

Cela étant contraire à notre hypothèse, on conclut que ψ_1 est la seule fonction de la liste 15) qui ne change pas par $\mathcal{F}$.

Sous l'action de $\mathcal{F}$, ψ_2 prend un certain nombre de valeurs parmi celles de 15); ces valeurs sont reliées transitivement les unes aux autres, relativement aux substitutions de $\mathcal{F}$, et constituent un système dont le nombre des fonctions est un diviseur de l'ordre de $\mathcal{F}$, c'est-à-dire une puissance de 2. Si ψ_i ne figure pas dans le système précédent, cette fonction donne lieu à un autre système. Ainsi de suite. Puisque, à part ψ_1 qui constitue un système à elle seule, les fonctions de chaque système sont au nombre de $2^a, 2^b, \ldots$; on a

$$k = 1 + 2^a + 2^b + \ldots \qquad (a \neq 0,\ b \neq 0,\ \ldots)$$

ou bien

$$k = 1 + 2h$$

Maintenant soit H' un groupe semblable à H contenu dans G, d'ailleurs quelconque. Effectuons sur la liste 15) les substitutions de H'. Ces $1 + 2h$ fonctions vont de nouveau s'organiser en systèmes, et le nombre de ψ par système et un diviseur de l'ordre de H', donc une puissance de 2. On aura donc une égalité telle que:

$$1 + 2h = 2^a + 2^b + \ldots.$$

Cette égalité ne peut exister que si l'un au moins des exposants $a, b, \ldots$ est nul, autrement dit si un système ne contient qu'une fonction. Appelons ψ_α cette fonction, qui en conséquence est invariable par H'. Le groupe de ψ_α est $s_\alpha^{-1} \mathcal{F} s_\alpha$. On conclut que H' est le transformé par s_α de l'un des groupes H_α de $\mathcal{F}$.

$$s_\alpha^{-1} H_\alpha s_\alpha = H'.$$

Il n'y a donc, en dehors de $\mathcal{F}$, en fait de groupes semblables à H, que ceux qu'on obtient en transformant ceux de $\mathcal{F}$ par les substitutions de G.

11. — *Remarque.* On aurait pu, semble-t-il, donner à l'énoncé de ce critère une plus grande généralité. Si, en effet, au lieu de la condition exigée qui revient à dire $\mathcal{F}' = \mathcal{F}$, on avait seulement supposé sur $\mathcal{F}' > \mathcal{F}$ que l'indice de $\mathcal{F}$ dans $\mathcal{F}'$ fût impair, la démonstration n'aurait été modifiée qu'en ce que, au lieu de $k = 1 + 2h$, on aurait eu $k = i + 2h$, le nombre impair i désignant justement l'indice de $\mathcal{F}$ dans $\mathcal{F}'$. Et alors la conclusion énoncée dans le critère subsisterait.

Toutefois ce cas ne se présente pas, car nous montrerons que *l'ordre de $\mathcal{F}'$ est une puissance de 2, et par suite l'indice de $\mathcal{F}$ dans $\mathcal{F}'$ est toujours pair*, à moins qu'il ne se réduise à l'unité.

D'autre part, si l'on suppose que l'indice en question est pair, la démonstration, reprise suivant la voie que nous avons adoptée, n'aboutit pas. Effectivement, la proposition contenue dans le critère ne peut être étendue à ce cas, du moins si l'on n'introduit pas de condition supplémentaire; car on peut donner des exemples où cette proposition, supposée ainsi généralisée, serait en défaut. Ainsi pour $n = 16$, on peut former un groupe $\mathcal{F}$ pour lequel $\mathcal{F}' > \mathcal{F}$; $\mathcal{F}'$ contient des substitutions circulaires du n^e ordre qui n'appartiennent pas à $\mathcal{F}$. Si maintenant on prend $G = \mathcal{F}'$, il est clair qu'on ne peut obtenir tous les groupes H de G en transformant ceux de $\mathcal{F}$ par des substitutions de G.

Voici comment on montre que *l'ordre de $\mathcal{F}'$ est une puissance de 2.* Si l'ordre de $\mathcal{F}'$ était $2^a p^b q^c \ldots$, où $p, q, \ldots$ sont des nombres premiers différents, nous aurions dans $\mathcal{F}'$, d'après un théorème de Sylow,[8]) un groupe K d'ordre p^b. Ce groupe K est d'ordre impair, et il ne contient, à part l'unité, que des substitutions dont l'ordre est une puissance de p, donc impair.

---

[8]) *L. Sylow,* Théorèmes sur les substitutions, Math. Ann., 1872, Bd. 5, Théor. I, p. 586.

Soient maintenant

$$H,\ H_1,\ H_2,\ \ldots$$

tous les groupes semblables à H contenus dans $\mathcal{F}$; nous savons que leur nombre N est une puissance de 2 (n° 6). Transformons ces groupes par toutes les substitutions de K; les H sont simplement permutés entre eux. Nous affirmons qu'aucun des H ne reste invariant par toutes les substitutions de K.

Premièrement, H doit changer par les substitutions de K; car sinon K serait contenu dans $\mathcal{F}$, comme formé de substitutions métacycliques. Ce n'est pas possible, parce que les sous-groupes de $\mathcal{F}$ sont d'ordre pair.

Un H_α quelconque doit aussi changer, car si s de K avait la propriété

$$s^{-1} H_\alpha\ s = H_\alpha,$$

alors transformons cette équation par une substitution appropriée qui transforme H_α en H. Par cette transformation s devient s', et l'on a

$$s'^{-1} H s' = H$$

s' serait métacyclique. Mais cela n'est pas possible parce que s', qui est semblable à s, est d'ordre impair.

Par les substitutions de K, les groupes H s'organisent en systèmes, et le nombre des H par système est un diviseur de l'ordre de K, donc une puissance de p

$$N = p^\alpha + p^{\alpha'} + p^{\alpha''} + \ldots .$$

$\alpha,\ \alpha',\ \alpha'',\ \ldots$ étant différents de zéro, on déduit que N est un multiple de p. Ce résultat étant en contradiction avec la proposition démontrée selon laquelle N est une puissance de 2, nous devons rejeter l'hypothèse et conclure que l'ordre de $\mathcal{F}'$ ne contient aucun des facteurs impairs $p,\ q,\ \ldots$. L'ordre de $\mathcal{F}'$ est une puissance de 2.

12. — *Procédé pratique.* La démonstration du théorème général au n° 8 donne en même temps la méthode pratique qu'il faut suivre pour déduire de φ toutes les fonctions cycliques équivalentes. Il y a cependant quelques remarques à faire touchant cette méthode elle-même et la manière de reconnaître si la condition exigée par le théorème est remplie.

Les divers H de G peuvent, comme on l'a vu, être répartis en divers systèmes conjugués:

$$\begin{array}{ll} \text{I)} & H,\ H',\ H'',\ \ldots \\ \text{II)} & H_1,\ H_1',\ H_1'',\ \ldots \\ \text{III)} & H_2,\ H_2',\ H_2'',\ \ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

H, H_1, H_2, ... sont les *têtes* des systèmes conjugués, et font partie de $\mathcal{F}$. Comme nous l'avons dit, il est possible que dans chaque système il y ait plusieurs H de $\mathcal{F}$.

Contrairement à la notation du n° 8, nous désignerons par σ_1, σ_2, ... des substitutions qui transforment H respectivement *en tous les* H_i *de* $\mathcal{F}$ *sans exception.* Ces substitutions seront réparties en trois classes, que nous noterons σ_α, σ_β, σ_γ.

σ_α transforme H en H_i, tête d'un système conjugué quelconque (Les σ_1, σ_2, ... du n° 8 sont des σ_α).

σ_β transforme H en H^j appartenant au premier système.

σ_γ transforme H en H_i^j n'appartenant pas au premier système et n'étant pas tête d'un système.

Comme nous l'avons expliqué au n° 7, σ_1, σ_2, ... se forment au moyen des substitutions circulaires $s = |x,\ 1 + x|$, $s_i = |x,\ 1 + \beta_i x|$ qui par leurs puissances engendrent les divers H_i du groupe métacyclique. On obtient les β_i au moyen de la formule $\beta = 1 + 4r$. Pour distinguer les s_i qui appartiennent à $\mathcal{F}$ des autres, on les essaie sur la fonction φ: celles qui ne changent pas φ appartiennent à $\mathcal{F}$.

A l'aide de σ_1, σ_2, ... ainsi formées, on déduit les fonctions cycliques équivalentes à φ selon les principes exposés au n° 8. Le fait que ces substitutions ne correspondent pas uniquement aux H_i qui peuvent être pris comme têtes des systèmes conjugués n'est d'aucune importance; il arrivera simplement que des listes de fonctions cycliques se répèteront; on ne conservera naturellement que celles qui sont différentes. C'est ce que nous allons montrer.

Imaginons qu'on ait pu séparer les σ_α et qu'on ait déduit au moyen d'elles toutes les fonctions cycliques équivalentes à φ. *Etudions maintenant le résultat que donne* σ_β^{-1}.

Ce sera une fonction obtenue dans la première liste, φ' p. ex., et en effectuant sur φ' toutes les substitutions métacycliques, on obtiendra une liste de fonctions coïncidant avec la première, obtenue avec σ_1^{-1}, sauf l'ordre.

En effet, σ_β change H en H^j du premier système conjugué. Soit s une substitution de G qui transforme H en H^j. On peut poser $s = m\sigma_\beta$, où m est une substitution métacyclique déterminée. En formant la liste relative à σ_β, nous sommes appelés à effectuer sur φ la substitution $\sigma^{-1} m^{-1}$, et puisque celle-ci est dans G, nous devons voir apparaître φ dans cette liste qui ne sera autre que I').

Inversement, si en opérant avec σ_k nous voyons apparaître φ, cela prouve qu'une certaine substitution que nous pouvons représenter par $\sigma_k^{-1} m^{-1}$ est dans G. $m\sigma_k$ est aussi dans G et par suite transforme H en un H^j du premier système; cette propriété appartient aussi à σ_k et par suite $\sigma_k = \sigma_\beta$, c'est-à-dire est de la 2e classe.

Etudions enfin le résultat que donne σ_γ^{-1} *sur* φ. Ce sera l'apparition d'une liste de fonctions autre que la première. σ_γ change H en H_i^j et nous supposons que H_i^j fait partie du système dont H_i est la tête. Si s est une substitution de G qui change H_i en H_i^j, on peut poser

$$m\sigma_\gamma = \sigma_\alpha s$$
$$\sigma_\gamma^{-1} m^{-1} = s^{-1} \sigma_\alpha^{-1}.$$

Or $\sigma_\gamma^{-1} m^{-1}$ est une substitution qu'on se propose d'effectuer sur φ; mais s^{-1} ne change pas φ, et s_α^{-1} change φ en φ_α déjà obtenue puisque σ_α est de la première classe. Ainsi φ_α réapparaîtra, de même que la liste entière à laquelle φ_α appartient. Inversement, si par application de σ on voit apparaître une liste déjà obtenue et autre que la première, on a $\sigma = \sigma_\gamma$.

En résumé, le procédé pratique lui-même, en même temps qu'il fournit des fonctions cycliques, fournit l'une des répartitions possibles des σ en trois classes: σ_α, σ_β, σ_γ ce qui sera nécessaire pour nous assurer de la validité du procédé tout entier, comme nous allons le montrer.

13. — Il est nécessaire de s'assurer si la condition exigée par le théorème est bien remplie, c'est-à-dire *si* G *ne contient aucune substitution permutable à* $\mathcal{F}$, sinon on ne serait pas sûr d'avoir trouvé toutes les fonctions cycliques équivalentes à φ.

Une telle substitution, si elle existe, transforme nécessairement H en l'un ou l'autre des groupes semblables à H contenus dans $\mathcal{F}$. Les substitutions σ_i que nous avons formées, ont justement cette propriété. Si σ_1 transforme H en H_1 toutes les substitutions du complexe $M\sigma_1$, où M désigne le groupe métacyclique, font de même, et celles-là seulement.

Par conséquent les substitutions dont nous parlons sont à chercher parmi les trois classes de complexes

$$\text{A)}\ M\sigma_\alpha, \qquad \text{B)}\ M\sigma_\beta, \qquad \text{C)}\ M\sigma_\gamma .$$

Nous pouvons écarter d'emblée les complexes A et C, car ils n'ont aucune substitution commune avec G. En effet, si s était commune à A et G, ou à C et G, on pourrait par une substitution de G passer de H à un H_i non contenu dans le premier système conjugué.

Il reste donc à examiner les complexes B, et si, dans un cas particulier, ces complexes n'existent pas, la discussion est close, et l'on a $\mathcal{F}' = \mathcal{F}$.

Supposons qu'il existe des complexes B; chacun d'eux contient toujours des substitutions qui font partie de G, et nous devons reconnaître si ces dernières transforment $\mathcal{F}$ en lui-même. Cette recherche se simplifie par le fait qu'il suffit d'examiner les σ_β elles-mêmes, car nous allons voir que les complexes $M\sigma_\beta$ se partagent entre ceux dont toutes les substitutions transforment $\mathcal{F}$ en lui-même, et ceux dont aucune substitution n'a cette propriété.

Tout d'abord si σ_0 fait partie d'un complexe $M\sigma_\beta$, ce même complexe peut être représenté par $M\sigma_0$. Pour le voir, remarquons que l'on a: $\sigma_0 = m\,\sigma_\beta$. On peut écrire $M\sigma_\beta = M m^{-1} . m\,\sigma_\beta = M m^{-1} . \sigma_0 = M\sigma_0$.

Ensuite, si σ_0 du complexe $M\sigma_\beta$ transforme $\mathcal{F}$ en lui-même, toutes les substitutions du complexe ont la même propriété. En effet, puisque $M\sigma_\beta = M\sigma_0$, la chose est claire si l'on observe que toute substitution métacyclique transforme en lui-même le diviseur $\mathcal{F}$.

On saura donc si un complexe transforme $\mathcal{F}$ en lui-même en faisant l'essai avec σ_β et voici comment:

On dresse le tableau des substitutions métacycliques fondamentales contenues dans $\mathcal{F}$

$$16) \qquad |x,\ \mu x|, \quad |x,\ \mu' x|, \ \ldots .$$

Une étude plus approfondie des substitutions σ montre que si on a $\sigma_\beta^{-1}\,\mathcal{F}\,\sigma_\beta = \mathcal{F}$, ces substitutions 16), après transformation par σ_β, sont simplement permutées entre elles. Si au contraire, l'une ou l'autre est transformée en une substitution qui ne fait pas partie de 16), alors on n'a pas $\sigma_\beta^{-1}\,\mathcal{F}\,\sigma_\beta = \mathcal{F}$.

14. — Nous nous proposons, pour illustrer cette théorie, de former *deux exemples de fonctions cycliques*, en choisissant le nombre des variables $n = 16$.

L'expression

$$S = x_1^3 x_2^2 x_3 + x_2^3 x_3^2 x_4 + \ldots + x_{16}^3 x_1^2 x_2$$

se compose de 16 termes; nous pouvons, en n'écrivant que les indices, représenter cette somme S symboliquement par la colonne suivante:[9])

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ 5' & 6' & 1 \\ 6' & 1 & 2 \end{array}$$

Dans chaque terme 1 2 3, 2 3 4, ... l'ordre des chiffres ne doit pas être changé. On remarquera que la colonne toute entière s'écrit aisément en partant de la *tête de colonne* 1 2 3, et en effectuant sur 1 2 3 toutes les puissances de la substitution circulaire (1 2 3 ... 6'); de sorte que nous pouvons nous contenter d'écrire le premier terme 1 2 3 qui, par suite, *représentera* toute la colonne. L'expression S peut donc s'écrire d'une manière très concise comme suit:

$$S = 1\ 2\ 3$$

La *première fonction* que nous considérons se compose de 64 termes répartis en quatre colonnes

$$\varphi = 123 + 161' + 103 + 14'1'.$$

C'est une fonction cyclique. Cherchons le diviseur métacyclique qui appartient à φ.

Le groupe métacyclique de 16 éléments est défini par les substitutions fondamentales suivantes:

$$|x,\ 3x|,\quad |x,\ 7x|,\quad |x,\ 11x|,\quad |x,\ 15x|$$
$$m = |x,\ 5x|,\quad m^2 = |x,\ 9x|,\quad m^3 = |x,\ 13x|$$

[9]) Les indices 10, 11, 12, ..., 16 seront notés plus commodément 0, 1', 2', ..., 6'.

Il est facile de voir que, des 7 substitutions écrites, seules les trois dernières: m, m^2, m^3 ne changent pas la valeur de φ, et par suite appartiennent à $\mathcal{J}$. L'ordre de $\mathcal{J}$ est la demi de l'ordre du groupe métacyclique. Il n'est pas nécessaire d'examiner si le groupe de φ contient autre chose que des substitutions métacycliques. En résumé, $\mathcal{J}$ est engendré par

$$s = |x,\ 1+x|, \quad m = |x,\ 5x|.$$

$\mathcal{J}$ contient, indépendamment de H, trois groupes semblables à H, que nous désignerons par H_1, H_2, H_3. En effet, m, m^2, m^3 sont aptes à former des substitutions circulaires du 16e ordre par multiplication par $|x,\ 1+x|$, puisque les constantes 5, 9, 13 sont de la forme $1+4r$. Formons les substitutions s_1, s_2, s_3 qui par leurs puissances donnent H_1, H_2, H_3, et enfin formons σ_1, σ_2, σ_3.

$$\sigma_1^{-1} H \sigma_1 = H_1 \qquad \sigma_1 = (26)\ (35')\ (42')\ (53')\ (71')\ (04') = \sigma_1^{-1}$$
$$\sigma_2^{-1} H \sigma_2 = H_2 \qquad \sigma_2 = (20)\ (31')\ (64')\ (75') = \sigma_2^{-1}$$
$$\sigma_3^{-1} H \sigma_3 = H_3 \qquad \sigma_3 = (24')\ (37)\ (42')\ (53')\ (60)\ (1'5') = \sigma_3^{-1}$$

En nous conformant à la théorie, cherchons toutes les fonctions cycliques équivalentes à φ. Pour cela, on effectue sur φ toutes les substitutions métacycliques. Nous obtenons une nouvelle fonction φ'

$$\varphi' = 147 + 16'5' + 12'7 + 185'$$

et nous avons une première liste

I) $\qquad \varphi, \quad \varphi'.$

Effectuons σ_1^{-1} sur φ; nous obtenons une nouvelle fonction φ_1:

$$\varphi_1 = 165' + 127 + 14'5' + 107.$$

Cette dernière donne lieu, par les substitutions métacycliques, à une 2e liste:

II) $\qquad \varphi_1, \quad \varphi_1'.$

Ainsi de suite. On a le tableau suivant:

I)		$\varphi,\ \varphi'$
II)	par σ_1^{-1}	$\varphi_1,\ \varphi_1'$
III)	par σ_2^{-1}	$\varphi_2,\ \varphi_2'$
IV)	par σ_3^{-1}	$\varphi_3,\ \varphi_3'$.

avec $\varphi = 123 + 161' + 103 + 14'1'$ $\varphi' = 147 + 16'5' + 12'7 + 185'$
$\varphi_1 = 165' + 127 + 14'5' + 107$ $\varphi_1' = 16'1' + 143 + 181' + 12'3$
$\varphi_2 = 101' + 14'3 + 121' + 163$ $\varphi_2' = 12'5' + 187 + 145' + 16'7$
$\varphi_3 = 14'7 + 105' + 167 + 125'$ $\varphi_3' = 183 + 12'1' + 16'3 + 141'$

D'après la théorie, nous pouvons affirmer que toutes les fonctions cycliques équivalentes à φ ont été obtenues, parce que l'application de σ_1^{-1}, σ_2^{-1}, σ_3^{-1} nous a donné chaque fois une liste nouvelle.

La *deuxième fonction* que nous prenons pour exemple est simplement la somme

$$\psi = \varphi + \varphi_1 .$$

Cette fonction cyclique possède le même diviseur métacyclique $\mathcal{F}$ que la fonction φ. En effet, d'une part, m, m^2, m^3 n'altèrent ni φ ni φ_1. D'autre part, une autre substitution métacyclique p. ex. $|x,\ 3x|$, change cette fonction en $\psi' = \varphi' + \varphi_1'$, et l'on peut constater que ψ' n'a aucun terme commun avec ψ.

Essayons, comme précédemment, d'appliquer sur $\varphi + \varphi_1$ les substitutions métacycliques et les substitutions σ_1^{-1}, σ_2^{-1}, σ_3^{-1}. On a le tableau suivant:

I)		$\varphi + \varphi_1,\ \varphi' + \varphi_1'$
II)	par σ_1^{-1}	$\varphi_1 + \varphi,\ \varphi_1' + \varphi'$
III)	par σ_2^{-1}	$\varphi_2 + \varphi_3,\ \varphi_2' + \varphi_3'$
IV)	par σ_3^{-1}	$\varphi_3 + \varphi_2,\ \varphi_3' + \varphi_2'$

Déjà la 2e liste n'est que la répétition de la 1ère. D'après la théorie, puisque ce fait se présente, nous ne pouvons être sûrs d'avoir obtenu toutes les fonctions cycliques équivalentes à $\varphi + \varphi_1$, que si σ_1 ne transforme pas en lui-même le diviseur $\mathcal{F}$. Or c'est le contraire qui a lieu: si on transforme par σ_1 les substitutions m, m^2, m^3, ces dernières sont simplement permutées entre elles, et l'on a $\sigma_1^{-1}\,\mathcal{F}\,\sigma_1 = \mathcal{F}$.

Il est donc possible que des fonctions cycliques équivalentes à $\varphi + \varphi_1$ nous aient échappé. Effectivement, la fonction $\varphi + \varphi_3$ est cyclique et en outre équivalente à $\varphi + \varphi_1$; elle se déduit de cette dernière par la substitution $(35'1'7)\ (42')\ (64')$.

15. — *Sur les fonctions cycliques de degré* $n = p^m$. Nous allons donner un critère analogue à celui du n° 10 lorsque le nombre des variables est $n = p^m$. H, $\mathcal{J}$, M, et G ont la même signification que plus haut, et sont relatifs à une certaine fonction φ.

Considérons les différents *diviseurs métacycliques* contenus dans $\mathcal{J}$, et ayons spécialement en vue ceux qui ont pour ordre une puissance de p. En général il y en a, puisque H et M ont pour ordres respectivement p^m et $p^{2m-1}(p-1)$. *Appelons* $\mathcal{J}^*$ *le diviseur métacyclique dont l'ordre* p^a *est le plus élevé.* S'il s'en trouvait plusieurs qui eussent cet ordre maximum, nous choisirions l'un d'eux ; mais nous montrerons qu'il n'y en a qu'un. L'ordre de toutes les substitutions de $\mathcal{J}^*$, différentes de la substitution unité, est une puissance de p.

$\mathcal{J}$ ne contient, en dehors de $\mathcal{J}^*$, aucune substitution dont l'ordre est une puissance de p. Car s'il y en avait une s, le diviseur métacyclique $\{\mathcal{J}^*, s\}$, puisque s est permutable à $\mathcal{J}^*$, aurait pour ordre l'ordre de $\mathcal{J}^*$ multiplié par l'exposant de la plus petite puissance de s qui figure dans $\mathcal{J}^*$. Cet ordre serait une puissance de p supérieure à p^a, ce qui contredit ce que nous avons supposé sur $\mathcal{J}^*$.

$\mathcal{J}$ ne contient aucun groupe de même ordre p^a que $\mathcal{J}^*$, ou d'ordre $p^{a'}$ supérieur, si ce n'est $\mathcal{J}^*$ lui-même. Car s'il existait un tel groupe différent de $\mathcal{J}^*$, nous aurions, en dehors de $\mathcal{J}^*$, une substitution ayant pour ordre une puissance de p.

Comme ce diviseur $\mathcal{J}^*$ joue ici un certain rôle, il est utile de savoir former les substitutions $|x, \beta x|$ qui le déterminent. Les valeurs de β qui peuvent convenir sont celles qui sont telles que le plus petit exposant δ pour lequel

$$\beta^\delta \equiv 1 \pmod{p^m}$$

est une puissance de p. Tous les β qui répondent à ce caractère satisfont à la congruence

$$\beta \equiv 1 \pmod{p}.$$

En dehors de $\mathcal{F}^*$, mais à l'intérieur de $\mathcal{F}$, on trouve des substitutions $|x, \beta x|$ mais ici β ne peut avoir la forme sus-indiquée, car l'ordre de ces substitutions serait une puissance de p. On reconnaît qu'une substitution particulière $|x, \beta x|$ fait partie de $\mathcal{F}$ ou de $\mathcal{F}^*$ en l'essayant sur la fonction φ: elle la laisse invariante.

A toute substitution $|x, \beta x|$ de $\mathcal{F}^*$ correspond un groupe H_α semblable à H, complètement contenu dans $\mathcal{F}^*$.

Occupons-nous maintenant du théorème; nous en donnerons l'énoncé après la démonstration.

Soit ψ_1 une fonction invariable par les substitutions de $\mathcal{F}$ et par celles-là seulement. Soient

17) $$\psi_1, \psi_2, \ldots, \psi_k$$

toutes les valeurs qu'elle prend quand on lui applique toutes les substitutions de G. k est égal à l'indice de $\mathcal{F}$ dans G.

Effectuons sur les fonctions 17) toutes les substitutions de $\mathcal{F}^*$. ψ_1 demeure évidemment invariable. Cherchons si une autre fonction, p. ex. ψ_α, (qui se déduit de ψ_1 par s_α de G) reste invariable par toutes les substitutions de $\mathcal{F}^*$. S'il en est ainsi, le groupe de ψ_α, qui est $s_\alpha^{-1} \mathcal{F} s_\alpha$, contient $\mathcal{F}^*$. Mais le seul groupe semblable à $\mathcal{F}^*$ contenu dans $\mathcal{F}$ est $\mathcal{F}^*$ lui-même. On aurait donc

$$s_\alpha^{-1} \mathcal{F}^* s_\alpha = \mathcal{F}^*.$$

La question posée conduit donc à celle-ci: Le groupe G contient-il, en dehors de $\mathcal{F}$, des substitutions permutables à $\mathcal{F}^*$?

Désignons par $\mathcal{F}'$ le groupe formé de toutes les substitutions de G permutables à $\mathcal{F}^*$. Donc $\mathcal{F}'^{-1} \mathcal{F}^* \mathcal{F}' = \mathcal{F}^*$. Décomposons $\mathcal{F}'$ suivant $\mathcal{F}$ en ses divers complexes

$$\mathcal{F}' = \mathcal{F} + \mathcal{F}s_2 + \mathcal{F}s_3 + \ldots + \mathcal{F}s_r$$

s_2 transforme H en un certain H_2 de $\mathcal{F}^*$; $s_2^{-1} H s_2 = H_2$. Tout le complexe $\mathcal{F}s_2$ a la même propriété, et aucune autre substitution de G n'a cette propriété.

s_3 et par conséquent $\mathcal{F}s_3$ transforme H en un certain H_3 de $\mathcal{F}^*$. Ainsi de suite. Chaque complexe est caractérisé par le fait qu'il transforme H en un certain H_i de $\mathcal{F}^*$.

Cela dit, G peut être décomposé comme suit:

$$G = \mathcal{J} + \mathcal{J}s_2 + \mathcal{J}s_3 + \ldots + \mathcal{J}s_r + \mathcal{J}s_{r+1} + \ldots + \mathcal{J}s_k$$

et nous pouvons supposer que dans la liste des fonctions 17), $\psi_2, \psi_3, \ldots, \psi_k$ ont été obtenues à partir de ψ_1 précisément au moyen de $s_2, s_3, \ldots, s_k$.

Maintenant il est facile de voir que par l'effet des substitutions de $\mathcal{J}^*$, les fonctions suivantes

$$\psi_1, \psi_2, \ldots \psi_r$$

resteront invariables.

Pour ψ_1, cela est clair. Examinons ψ_2. Le groupe de ψ_2 est $s_2^{-1}\mathcal{J}s_2$; ce groupe contient $s_2^{-1}\mathcal{J}^* s_2 = \mathcal{J}^*$. Il en est de même de toutes les autres fonctions jusqu'à ψ_r; mais ψ_{r+1} n'a plus cette propriété.

On conclut que le nombre des fonctions ψ qui restent invariables par $\mathcal{J}^*$ est r, *et ce nombre r est égal à l'indice de $\mathcal{J}$ dans $\mathcal{J}'$.*

Par les substitutions de $\mathcal{J}^*$ les autres fonctions 17) se groupent en systèmes, et le nombre des fonctions par système est un diviseur de l'ordre de $\mathcal{J}^*$, donc une puissance de p; on a donc

$$k = r + p^\alpha + p^\beta + \ldots$$
$$k = r + hp.$$

Soit maintenant H' un groupe semblable à H contenu dans G, n'importe lequel. Effectuons encore une fois sur les fonctions 17) les substitutions de H'. Ces k fonctions se groupent en de nouveaux systèmes, et le nombre des fonctions par système est une puissance de p. On a done une égalité telle que

$$r + hp = p^a + p^b + \ldots.$$

Si r n'est pas divisible par p, une telle égalité peut subsister seulement si l'un des exposants, p. ex. a est nul; autrement dit seulement si l'une des fonctions 17), p. ex. ψ_α, est invariable par toutes les substitutions de H'. Or le groupe de ψ_a est $s_a^{-1}\mathcal{J}s_a$. On conclut que *tout groupe H' est le transformé par une substitution de G d'un groupe semblable à H contenu dans $\mathcal{J}$.* Cette dernière conclusion, jointe au théorème du n° 8 nous permet de dire:

Théorème. Si l'indice de $\mathcal{J}$ dans $\mathcal{J}'$ n'est pas divisible par p, toutes les fonctions cycliques équivalentes à φ sont obtenues par l'application des substitutions R).

Mais si r est divisible par p, notre conclusion n'est plus légitime; et effectivement on peut former des exemples où les divers H_i de G ne peuvent être tous obtenus en transformant ceux de $\mathcal{J}$ par des substitutions de G, et où par conséquent les substitutions $R)$ ne donnent pas toutes les fonctions cycliques équivalentes à φ.

16. — *Procédé pratique.* Il nous reste à montrer: 1°. — comment on construit et applique les substitutions $R)$; 2°. — comment on s'assure que l'indice de $\mathcal{J}$ dans $\mathcal{J}'$ n'est pas divisible par p.

Nous serons brefs, car les explications et les démonstrations des n^{os} 12 et 13 relatives au cas $n = 2^m$ peuvent être répétées ici presque textuellement.

On part de la fonction étudiée φ et on applique à φ toutes les substitutions métacycliques. On obtient ainsi une première liste de fonctions équivalentes.

$$\text{I')} \qquad \varphi,\ \varphi',\ \varphi'',\ \ldots.$$

La plus simple manière de procéder consiste à chercher une racine primitive β pour le module p^m, puis à appliquer $|x, \beta x|$ et ses puissances à la fonction φ. Toute substitution $|x, \beta x|$ qui laisse φ invariable appartient à $\mathcal{J}$.

Parmi les substitutions $|x, \beta x|$ de $\mathcal{J}$, il s'en trouve de plus remarquables pour lesquelles $\beta \equiv 1 \pmod{p}$. A chacune de ces dernières correspond une autre $|x, 1 + \beta x|$ qui par ses puissances engendre un groupe H_i de $\mathcal{J}$.

Après avoir formé toutes les substitutions circulaires $|x, 1 + \beta x|$, on construit les σ_i qui leur correspondent et qui transforment H en *tous* les groupes semblables à H contenus dans $\mathcal{J}$.

En appliquant σ_1^{-1} à φ on obtient une fonction cyclique φ_1. En effectuant, exactement comme pour φ, toutes les substitutions métacycliques, on obtient une deuxième liste

$$\text{II')} \qquad \varphi_1,\ \varphi_1',\ \varphi_1'',\ \ldots.$$

On procède d'une manière pareille avec σ_2^{-1}, σ_3^{-1}, ... et l'on a pour finir autant de listes qu'il y a de σ_i. C'est en cela que consiste la construction et l'application des substitutions *R)*.

La seconde question posée est relative à l'indice r de $\mathcal{J}$ dans $\mathcal{J}'$. C'est seulement dans le cas où cet indice n'est pas divisible par p que l'on sera sûr d'avoir obtenu toutes les fonctions cycliques équivalentes à φ.

Il peut arriver que certaines listes II'), III'), ... ne soient que la répétition de la première I'), peut-être avec un autre ordre des fonctions $\varphi, \varphi', \varphi'', \ldots$.

Envisageons les σ_i qui ont donné lieu à de telles listes; ce sont, d'après la notation du n° 12, des σ_β. Nous ne retiendrons de ces σ_β que celles qui ont la propriété de transformer $\mathcal{J}^*$ en lui-même.

$$\sigma_\beta^{-1} \mathcal{J}^* \sigma_\beta = \mathcal{J}^*.$$

Cette vérification se fait aisément: on dresse le tableau des $|x, \beta x|$ de $\mathcal{J}^*$; ces substitutions sont alors simplement permutées entre elles, si la propriété signalée a lieu.

Pour finir, après élimination, il nous reste un nombre N de σ_β; *alors* $N+1$ *est l'indice cherché de* $\mathcal{J}$ *dans* $\mathcal{J}'$.

En effet, prenons l'un des σ_β, disons σ_2. Au cas où σ_2 n'appartiendrait pas à G, le complexe $M\sigma_2$ contiendrait certainement une substitution s_2 de G (n° 13); alors $\mathcal{J}s_2$ renferme toutes les substitutions de G qui transforment $\mathcal{J}^*$ en lui-même et H en H_2. On voit aisément qu'à chacune de ces σ_β correspond un complexe $\mathcal{J}s_i$ de la décomposition de $\mathcal{J}'$ suivant $\mathcal{J}$ que nous avons considérée au n° 15; on voit aussi que $r = N+1$.

17. — Pour terminer, nous donnerons un *exemple concret*, afin de prouver surtout que, si nos démonstrations concernant les substitutions *R)* sont longues et délicates, l'application de ces substitutions à un cas pratique est au contraire très facile.

La fonction φ que nous considérons a un nombre de variables égal à $3^3 = 27$. On fera bien de se reporter au n° 14 où un exemple semblable a été donné, et nous emploierons les mêmes notations abrégées qu'alors. Le symbole

$$S = 1\ 2\ 3\ ;$$

représente une somme de 27 termes, et chacun s'obtient à partir du précédent par la substitution cyclique $s = (1234...)$. Nous imaginerons ces termes écrits en colonne, et le terme principal 1 2 3 est la tête de colonne.

Appliquons à la colonne cyclique 123 toutes les substitutions métacycliques qu'on peut former avec 27 éléments. Il suffit évidemment d'appliquer les substitutions $|x, \beta x|$ où β prend les 18 valeurs qui sont les nombres premiers à $n = 27$ et inférieurs à n. Ces substitutions sont toutes les puissances de

$$|x, 2x|.$$

Si l'on fait la somme des 18 colonnes obtenues, on obtient la fonction φ que nous nous proposons d'étudier. [10])

$$\varphi = 123 + 135 + 159 + 197' + 17'6 + 161' + 11'1'' + 11''4' + 14'7'' + 17''6'' + 16''4'' + 14''0' + 10'2' + 12'3'' + 13''8' + 18'8 + 185' + 15'2.$$

Nous allons chercher toutes les fonctions cycliques équivalentes à φ, en employant à cet effet les substitutions *R)*. Tout d'abord les substitutions métacycliques laissent φ invariable, et notre première liste contient l'unique fonction φ.

Formons les σ_i. Les diverses valeurs de β qui sont de la forme $1 + pr$ sont les suivantes:

18) 4, 7, 10, 13, 16, 19, 22, 25.

Avec chacune de ces valeurs on peut construire une substitution circulaire $|x, 1 + \beta x|$. Par exemple

$$s_1 = |x, 1 + 4x| = (151''47'5'72904'33'6''4''6'1'8'9'3''2'2''865''0'7'')$$

et l'on a:

$$\sigma_1 = \begin{pmatrix} s \\ s_1 \end{pmatrix} = (257'1'4'6''0'3''8)\ (31''2')\ (65'4'')$$

---

[10]) Les chiffres accentués représentent les nombres supérieurs à 9: ainsi 9', 0', 1''. 2'' représentent 19, 20, 21, 22. — D'après la théorie, une substitution métacyclique p. ex. $|x, 8x|$ change une fonction cyclique en une fonction cyclique. Le terme 123 deviendra 86'4''; ce terme appartient à la colonne cyclique dont la tête est 197'. Ainsi, sans plus de calcul, nous pouvons dire que la colonne 123 est devenue 197'.

De même σ_2 se construit à l'aide de $s_2 = |x, 1 + 7x|$. Nous n'écrirons pas ces divers σ_i dans le détail; nous les désignerons par

$$\sigma_1, \sigma_2 \cdot \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8$$

et chacun d'eux correspond au nombre du même rang dans 18).

En appliquant σ_1^{-1} à φ nous obtenons une nouvelle fonction cyclique φ_1; [11]) on constante alors que les substitutions métacycliques effectuées sur φ_1 donnent les 6 fonctions cycliques

$$\varphi_1, \varphi_1^{I}, \varphi_1^{II}, \varphi_1^{III}, \varphi_1^{IV}, \varphi_1^{V}.$$

Ce sera notre seconde liste; nous n'entrons pas dans le détail des calculs qui sont aisés. Chaque σ_i^{-1} donne lieu à une liste, et nous obtenons, pour finir, le tableau suivant:

		φ					
par	σ_1^{-1}	φ_1,	φ_1^{I},	φ_1^{II},	φ_1^{III},	φ_1^{IV},	φ_1^{V},
	σ_2^{-1}	φ_1^{III},	φ_1^{IV},	φ_1^{V},	φ_1,	φ_1^{I},	φ_1^{II},
	σ_4^{-1}	φ_1^{IV},	φ_1^{V},	φ_1,	φ_1^{I},	φ_1^{II},	φ_1^{III},
	σ_5^{-1}	φ_1^{V},	φ_1,	φ_1^{I},	φ_1^{II},	φ_1^{III},	φ_1^{IV},
	σ_7^{-1}	φ_1^{II},	φ_1^{III},	φ_1^{IV},	φ_1^{V},	φ_1,	φ_1^{I},
	σ_8^{-1}	φ_1^{I},	φ_1^{II},	φ_1^{III},	φ_1^{IV},	φ_1^{V},	φ_1,
	σ_3^{-1}	φ_2,	φ_2^{I},				
	σ_6^{-1}	φ_2^{I},	φ_2,				

Si, comme nous allons le montrer en effet, toutes les fonctions cycliques équivalentes à φ ont été obtenues, il y en a 9 en tout, qui sont: $\varphi, \varphi_1, \varphi_1^{I}, \varphi_1^{II}, \varphi_1^{III}, \varphi_1^{IV}, \varphi_1^{V}, \varphi_2, \varphi_2^{I}$.

Conformément à la théorie, nous devons voir si la liste à laquelle appartient φ, se trouve répétée. Ce n'est pas le cas; par conséquent $\mathcal{F}' = \mathcal{F}$, et toutes les fonctions cycliques équivalentes à φ ont été obtenues.

Pour illustrer davantage la théorie, nous pouvons, sans changer d'exemple, observer l'une quelconque des 9 fonctions qui sont équivalentes entre elles, p. ex. φ_1, et traiter φ_1 à l'aide des substitutions *R)*.

---

[11]) Il est important de remarquer qu'uue substitution σ, qui correspond à $|x, 1 + \beta x|$, ne donnera une fonction *cyclique* que si $|x, \beta x|$ fait partie du groupe de φ (n'altère pas φ). — Par σ_1^{-1} le terme 123 devient 182'; mais la colonne 123, après substitution, n'est plus cyclique. Ce n'est qu'après avoir rétabli l'ordre dans le résultat de la substitution qu'on verra la fonction φ_1 sous la forme cyclique, et l'on verra apparaître toute la colonne cyclique 182'.

φ_1 est invariable par les substitutions $|x, 10x|$ et $|x, 9x|$; son groupe $\mathcal{J}^*$ contient donc deux groupes semblables à H, et nous devons appliquer à φ_1 les substitutions σ_3^{-1} et σ_6^{-1} à l'exclusion des autres. Nous obtenons le tableau suivant:

	$\varphi,$	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$
par σ_3^{-1}	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$
par σ_6^{-1}	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$

Chose remarquable, il est impossible, à l'aide des substitutions *R)* de déduire de φ_1 toutes les fonctions cycliques qui lui sont équivalentes; nous n'obtenons pas φ_2 et φ_2^{I}. On vérifie aisément qu'on a

$$\sigma_3^{-1}\,\mathcal{J}^*\,\sigma_3 = \mathcal{J}^*, \qquad \sigma_6^{-1}\,\mathcal{J}^*\,\sigma_6 = \mathcal{J}^*$$
$$r = N + 1 = 2 + 1 = 3$$

r est divisible par 3. Conformément à la théorie, des fonctions ont pu nous échapper, et c'est le cas en effet.

Enfin partons de φ_2, dont le groupe possède les substitutions

$$|x, \beta x| \text{ où } \beta = 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22,\ 25.$$

Tous les σ_i peuvent être appliqués à φ_2; aucun n'est à exclure.

On trouve:

	$\varphi_2,$	$\varphi_2^{\mathrm{I}},$				
par σ_3^{-1}	$\varphi_2^{\mathrm{I}},$	$\varphi_2,$				
σ_1^{-1}	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	φ_1^{III}
σ_2^{-1}	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$	φ_1^{IV}
σ_4^{-1}	$\varphi_1^{\mathrm{II}};$	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	φ_1^{I}
σ_5^{-1}	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	φ_1
σ_7^{-1}	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$	$\varphi_1^{\mathrm{II}},$	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	φ_1^{V}
σ_8^{-1}	$\varphi_1^{\mathrm{III}},$	$\varphi_1^{\mathrm{IV}},$	$\varphi_1^{\mathrm{V}},$	$\varphi_1,$	$\varphi_1^{\mathrm{I}},$	φ_1^{II}
σ_6^{-1}	φ					

La liste à laquelle appartient φ_2 ne se trouve répétée qu'une fois, le σ_3 correspondant à la propriété:

$$\sigma_3^{-1}\,\mathcal{J}^*\,\sigma_3 = \mathcal{J}^*.$$

L'indice de $\mathcal{J}$ dans $\mathcal{J}'$ est cette fois

$$r = N + 1 = 1 + 1 = 2.$$

Cet indice n'est pas divisible par $p = 3$. Conformément à la théorie, nous devons cette fois obtenir toutes les fonctions cycliques équivalentes à φ_2. Ce résultat est bien, en effet, en concordance avec le premier.

(Reçu le 12 mars 1931)