

## Des substitutions de la forme

$$\Theta(r) \equiv \varepsilon \left( r^{n-2} + ar^{\frac{n-3}{2}} \right)$$

pour un nombre  $n$  premier de lettres.

Par FRANC. BRIOSCHI à MILAN.

1°. La congruence:

$$(1) \quad \Theta \equiv \varepsilon (r^{2\mu-1} + ar^{\mu-1}) \pmod{n}$$

où  $\mu = \frac{n-1}{2}$ , donne pour la puissance  $m^{ième}$  de  $\Theta$ :

$$(2) \quad \Theta^m \equiv \varepsilon^m [L_m r^{2\mu-m} + a M_m r^{\mu-m}]$$

étant:

$$(3) \quad 2L_m \equiv (1+a)^m + (1-a)^m; \quad 2aM_m \equiv (1+a)^m - (1-a)^m.$$

Si l'on fait  $m = \mu$ , la relation (2), à cause de  $\Sigma \Theta^\mu \equiv 0$  donne:

$$(4) \quad M_\mu \equiv 0$$

et par conséquent:

$$(5) \quad (1+a)^\mu \equiv (1-a)^\mu \equiv L_\mu; \quad \Theta^\mu \equiv \varepsilon^\mu L_\mu r^\mu.$$

Cela posé, des relations (3) on déduit:

$$(6) \quad L_{\mu+m} \equiv L_\mu L_m; \quad M_{\mu+m} \equiv L_\mu M_m$$

et:

$$(7) \quad (1-a^2)^m L_{\mu-m} \equiv L_\mu L_m; \quad (1-a^2)^m M_{\mu-m} \equiv -L_\mu M_m$$

lesquelles, en observant que  $L_1 = M_1 = 1$ , nous donnent:

$$(8) \quad L_{\mu-1} + M_{\mu-1} \equiv 0 \quad (1-a^2) L_{\mu-1} \equiv L_\mu.$$

2°. L'expression:

$$\Theta(\Theta) \equiv \varepsilon \left( \Theta^{n-2} + a \Theta^{\frac{n-3}{2}} \right)$$

au moyen des relations (2), (6), (8) se réduit à:

$$\Theta(\Theta) \equiv L_{\mu-1} [(L_\mu - \varepsilon^\mu a^2) r + a (\varepsilon^\mu - L_\mu) r^{\mu+1}]$$

ou en supposant:

$$(9) \quad L_\mu \equiv \varepsilon^\mu$$

on aura:

$$\Theta(\Theta) \equiv r \quad \text{et} \quad \Theta^\mu \equiv r^\mu.$$

Donc les substitutions de la forme (1), dans lesquelles on suppose pour les nombres  $a$ ,  $\varepsilon$  des valeurs satisfaisantes les congruences (4), (9), sont douées des propriétés suivantes:

I°. En faisant sur la substitution  $\Theta$  la même substitution on obtient la fonction primitive.

II°. Les valeurs de  $r$  et de  $\Theta$  sont ensemble des résidus ou des non résidus quadratiques.

3<sup>me</sup>. En posant:

$$h_m \equiv \frac{1 \cdot 3 \cdot 5 \cdots (2m-1)}{2 \cdot 4 \cdot 6 \cdots 2(m-1)}$$

on démontre très-facilement que:

$$\Theta(\alpha\Theta + \beta) \equiv \varepsilon \sum_{n=1}^{m-\mu} (-1)^{m-1} \left[ m\alpha^\mu \Theta^\mu + (-1)^\mu (m+\mu) \beta^\mu + ah_m \right] \Theta^{\mu-m} \alpha^{\mu-m} \beta^{\mu-1}$$

ou en substituant les valeurs de  $\Theta^\mu$ ,  $\Theta^{\mu-m}$  données par les relations (2), (10) on obtient:

$$(10) \Theta(\alpha\Theta + \beta) \equiv \varepsilon^{\mu+1} \sum_{m=1}^{m-\mu} (-1)^{m-1} \varepsilon^m \left[ P_m + Q_m r^\mu \right] r^m \alpha^{\mu-m} \beta^{m-1}$$

étant:

$$P_m \equiv m\alpha^\mu L_{\mu-m} + a [(-1)^\mu (m+\mu) \beta^\mu + ah_m] M_{\mu-m}$$

$$Q_m \equiv m\alpha^\mu a M_{\mu-m} + [(-1)^\mu (m+\mu) \beta^\mu + ah_m] L_{\mu-m}.$$

Mais si dans la fonction  $\Theta$  l'on pose  $r+p$  au lieu de  $r$ ,  $p$  étant une indéterminée, on arrive après quelques transformations à:

$$(11) \quad \Theta(r+p) \equiv (-1)^\mu \varepsilon \sum_{m=0}^{m-\mu-1} (-1)^{m-1} [(\mu-m)r^\mu - (-1)^\mu (m+1) p^\mu + ah_{\mu-m}] r^m p^{\mu-m-1}$$

par conséquent la congruence:

$$(12) \quad \Theta(\alpha\Theta + \beta) \equiv A\Theta(r+p) + C$$

sera vérifiée lorsque:

$$I^\circ. \varepsilon(P_\mu r^\mu + Q_\mu) \beta^{\mu-1} \equiv \varepsilon A (\mu r^\mu - (-1)^\mu p^\mu + ah_\mu) p^{\mu-1} - (-1)^\mu C.$$

$$II^\circ. \varepsilon^{\mu+m} (P_m + Q_m r^\mu) \alpha^{\mu-m} \beta^{m-1} \equiv$$

$$(-1)^\mu A [(\mu-m) r^\mu - (-1)^\mu (m+1) p^\mu + ah_{\mu-m}] p^{\mu-m-1}$$

pour  $m=1, 2, \dots, \mu-1$ . Chacune de ces conditions se décompose en deux en comparant les coefficients de  $r^\mu$  et de  $r^0$ . La première donne les deux suivantes:

$$\mu A p^{\mu-1} \equiv P_\mu \beta^{\mu-1}; \quad \varepsilon A (ah_\mu - (-1)^\mu p^\mu) p^{\mu-1} - (-1)^\mu C \equiv \varepsilon Q_\mu \beta^{\mu-1};$$

mais évidemment:

$$P_\mu \equiv \mu \alpha^\mu; \quad h_\mu \equiv (-1)^{\mu-1}; \quad Q_\mu \equiv (-1)^{\mu-1} (\alpha + \beta^\mu);$$

on aura donc :

$$(13) \quad A p^{\mu-1} \equiv \alpha^\mu \beta^{\mu-1} ; \quad C \equiv \varepsilon [\beta^\mu - \alpha^\mu p^\mu - a (\alpha^\mu - 1)] \beta^{\mu-1}.$$

Analoguement de la deuxième on déduira :

$$(14) \quad \begin{aligned} \varepsilon^{\mu+m} Q_m p^m &\equiv (-1)^\mu (\mu - m) \alpha^m \beta^{\mu-m} \\ \varepsilon^{\mu+m} P_m p^m &\equiv -[a h_{m+1} + (m+1) p^\mu] \alpha^m \beta^{\mu-m} \end{aligned}$$

et pour  $m = \mu - 1$ , à cause de la première des (13), on obtiendra :

$$(15) \quad A \equiv (-1)^\mu \varepsilon Q_{\mu-1} \alpha \beta^{\mu-2} ; \quad p \equiv -3 \varepsilon (1 - \alpha^2) \alpha \beta^{\mu-2}.$$

En substituant la valeur trouvée de  $p$  dans la première des (14) on a :

$$(-1)^\mu (\mu - m) \beta^\mu \equiv (-1)^m \cdot 3^m \cdot \varepsilon^{\mu+2m} (1 - \alpha^2)^m Q_m ;$$

mais en se rappelant les relations (7) on démontre que :

$$(1 - \alpha^2)^m Q_m \equiv \varepsilon^\mu [-m \alpha^\mu a M_m + ((-1)^\mu (m + \mu) \beta^\mu + a h_m) L_m],$$

par conséquent :

$$\begin{aligned} &(-1)^\mu (\mu - m) \beta^\mu \equiv \\ &(-1)^m \cdot 3^m \varepsilon^{2m} \{ -m \alpha^\mu a M_m + [(-1)^\mu (m + \mu) \beta^\mu + a h_m) L_m \}. \end{aligned}$$

Cette condition se décompose évidemment à son tour dans les deux suivantes :

$$\begin{aligned} (-1)^m 3^m \varepsilon^{2m} (2m - 1) L_m + (2m + 1) &\equiv 0 \\ h_m L_m - m \alpha^\mu M_m &\equiv 0. \end{aligned}$$

Pour  $m = 1$  ces relations se réduisant à :

$$\varepsilon^2 \equiv 1 ; \quad \alpha^\mu \equiv 1 ;$$

on aura  $\varepsilon \equiv \pm 1$  et  $\alpha$  résidu quadratique (mod.  $n$ ) ; de plus :

$$(16) \quad \begin{aligned} (-1)^m 3^m (2m - 1) L_m + (2m + 1) &\equiv 0 \\ (-1)^m 3^m (2m - 1) M_m + 2 h_{m+1} &\equiv 0. \end{aligned}$$

La seconde des congruences (14) nous donnera analoguement les deux :

$$(17) \quad \begin{aligned} (-1)^m 3^m (2m - 1) M_m - (-1)^\mu 2 h_{m+1} &\equiv 0 \\ (-1)^m 3^m [m L_m - \alpha^2 h_m M_m] + (-1)^\mu 3^\mu \varepsilon^\mu (m + 1) &\equiv 0 \end{aligned}$$

la première desquelles comparée avec la seconde des (16) donne la condition  $\mu - 1 = \frac{n-3}{2}$  pair.

Les conditions à vérifier pour la subsistance de la relation (12) sont donc les deux (16) et la :

$$(18) \quad (-1)^m 3^m (m L_m - \alpha^2 h_m M_m) - 3^\mu \varepsilon^\mu (m + 1) \equiv 0$$

pour  $m = 1, 2 \dots \mu - 1$ . Or en posant dans la seconde des (16)  $m = 2$  on a :

$$27 M_2 + 2 h_3 \equiv 0 , \quad \text{mais } M_2 \equiv 2 , \quad h_3 \equiv \frac{1 \cdot 3 \cdot 5}{2 \cdot 4}$$

en conséquence on aura :

$$2 \cdot 3 \cdot 7 \cdot 11 \equiv 0 \pmod{n}$$

c'est-à-dire la seconde des conditions ne peut être satisfaite que dans les deux cas de  $n = 7$ ,  $n = 11$ .

Mais en faisant  $m = 2$  dans la première des (16) et  $m = 1$  en (18) on obtient:

$$\alpha^2 \equiv 4, \varepsilon \equiv -1 \pmod{7}; \quad \alpha^2 \equiv 9, \varepsilon \equiv 1 \pmod{11}$$

on aura donc, pour  $n = 7$

$$A \equiv 2\alpha\beta^1; \quad p \equiv -2\frac{\alpha}{\beta}; \quad C \equiv -2\beta^5 \pmod{7}$$

et pour  $n = 11$

$$A \equiv -2\alpha\beta^4; \quad p \equiv 2\frac{\alpha}{\beta}; \quad C \equiv 2\beta^9 \pmod{11}.$$

On arrive de cette manière au théorème suivant:

Les substitutions de la forme (1) ne peuvent satisfaire aux relations (10), (12), c'est-à-dire ne peuvent être des substitutions conjuguées, que dans les deux cas de  $n = 7$ ,  $n = 11$ .

Pour  $n = 7$  en posant:

$$\Theta(r) \equiv -(r^5 \pm 2r^2)$$

on a:

$$\Theta(\Theta) \equiv r, \quad \Theta(\alpha\Theta + \beta) \equiv 2\alpha\beta^4\Theta\left(r - 2\frac{\alpha}{\beta}\right) - 2\beta^5 \pmod{7};$$

et pour  $n = 11$ , si

$$\Theta(r) \equiv r^9 \pm 3r^4$$

on trouve que:

$$\Theta(\Theta) \equiv r, \quad \Theta(\alpha\Theta + \beta) \equiv -2\alpha\beta^8\Theta\left(r + 2\frac{\alpha}{\beta}\right) + 2\beta^9 \pmod{11};$$

$\alpha$  étant résidu quadratique dans les deux cas.

On aura donc pour  $n = 7$  un système de 4 . 6 . 7 substitutions conjuguées\*), et les fonctions invariables par ce système ne pourront avoir que trente valeurs\*\*), et pour  $n = 11$  un système de 6 . 10 . 11 substitutions conjuguées, et une fonction de onze lettres invariables par le même système ne pourra avoir que 60480 valeurs.

\*) Hermite. Sur les fonctions de sept lettres. Comptes Rendus de l'Académie des Sciences. Novembre 1863.

\*\*) Kronecker. Notiz über Gleichungen des siebenten Grades. Monatsbericht der Akademie zu Berlin. 1858.