BULLETIN DES SCIENCES
MATHÉMATIQUES ET ASTRONOMIQUES

G. KOENIGS

Sur une généralisation du théorème de Fermat, et ses rapports avec la théorie des substitutions uniformes

Bulletin des sciences mathématiques et astronomiques 2^e série, tome 8, n° 1 (1884), p. 286-288

<http://www.numdam.org/item?id=BSMA_1884_2_8_1_286_0>

© Gauthier-Villars, 1884, tous droits réservés.

L'accès aux archives de la revue « Bulletin des sciences mathématiques et astronomiques » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

MÉLANGES.

SUR UNE GÉNÉRALISATION DU THÉORÈME DE FERMAT, ET SES RAPPORTS AVEC LA THÉORIE DES SUBSTITUTIONS UNIFORMES;

PAR M. G. KOENIGS,
Professeur à la Faculté des Sciences de Besançon.

Dans la séance du 16 avril 1883, M. Picquet a présenté à l'Académie des Sciences une Note qui contient une généralisation du théorème de Fermat, Note qui a été ensuite l'objet de deux Communications de MM. É. Lucas et Pellet. Les recherches sur les substitutions uniformes, dont les premiers résultats ont été publiés dans le *Bulletin* (2e série, t. VII), m'ont conduit à ce même théorème, tout en me donnant une signification très générale de la fonction numérique qui figure dans son énoncé.

Désignant par $\varphi(z)$ une fonction uniforme et représentant par $\varphi_n(z)$ l'opération $\varphi(z)$, n fois répétée, j'envisage les équations E_n de la forme

$$z - \varphi_n(z) = 0.$$

A l'égard de ces équations j'ai démontré les théorèmes suivants :

1° *Si n' divise n, toute racine de $E_{n'}$ vérifie E_n.*

2° *Si d est le plus grand commun diviseur des entiers n et n', l'ensemble des racines communes à $E_{n'}$ et E_n se compose des racines de E_d.*

Il suit de là que les racines de E_n se divisent en deux catégories : les unes vérifient des équations d'indice inférieur à n, les autres ne vérifient aucune équation d'indice inférieur, et de celles-là je dis qu'elles *appartiennent* à l'indice n. Les racines de E_n qui n'appartiennent pas à l'indice n appartiennent à des indices qui divisent n.

Maintenant, si la quantité x appartient à l'indice n, j'ai démontré qu'il en était de même des n quantités

$$x, \varphi(x), \varphi_2(x), \ldots, \varphi_{n-1}(x),$$

que la substitution uniforme $[z, \varphi(z)]$ permute circulairement.

Il en résulte que les racines appartenant à l'indice n se distribuent en groupes circulaires de n racines. Donc, s'il arrive que le nombre des racines appartenant à l'indice n soit fini, *ce nombre doit être divisible par n.*

Ce théorème comprend celui que M. Picquet a démontré.

Prenons, en effet, pour $\varphi(z)$ une fraction rationnelle dont le numérateur et le dénominateur soient des polynômes entiers du degré m. L'équation E_n est du degré $m^n + 1$. Le nombre des racines appartenant à l'indice n, et que je représente par $H(m, n)$, est donc fini; il doit être divisible par n.

Or les $m^n + 1$ racines de E_n se composent de toutes les racines qui appartiennent à l'indice n ou à des indices diviseurs de n : on a donc, en mettant en évidence les facteurs premiers de n,

$$n = a^\alpha b^\beta c^\gamma \dots l^\lambda,$$

$$m^n + 1 = \sum_{\xi=0}^{\xi=\alpha} \sum_{\eta=0}^{\eta=\beta} \sum_{\zeta=0}^{\zeta=\gamma} \dots \sum_{\omega=0}^{\omega=\lambda} H(m, a^\xi b^\eta c^\zeta \dots l^\omega);$$

changeons α en $(\alpha - 1)$, nous aurons, en retranchant l'expression ainsi obtenue de la précédente,

$$m^n - m^{\frac{n}{a}} = \sum_{\eta=0}^{\eta=\beta} \sum_{\zeta=0}^{\zeta=\gamma} \dots \sum_{\omega=0}^{\omega=\lambda} H(m, a^\alpha b^\eta c^\zeta \dots l^\omega);$$

faisons de même en changeant cette fois β en $(\beta - 1)$, il vient

$$m^n - m^{\frac{n}{a}} - m^{\frac{n}{b}} + m^{\frac{n}{ab}} = \sum_{\zeta=0}^{\zeta=\gamma} \dots \sum_{\omega=0}^{\omega=\lambda} H(m, a^\alpha b^\beta c^\zeta \dots l^\omega).$$

On continuerait aisément de la sorte jusqu'à avoir

$$m^n - \Sigma m^{\frac{n}{a}} + \Sigma m^{\frac{n}{ab}} - \Sigma m^{\frac{n}{abc}} \dots = H(m, a^\alpha b^\beta c^\gamma \dots l^\lambda) = H(m, n).$$

Ainsi, la fonction numérique qui figure dans le théorème démontré par M. Picquet exprime le nombre de racines qui appartiennent à l'indice n dans le cas d'une fraction rationnelle du degré m. Le fait que ce nombre est divisible par n résulte immédiatement de la remarque que j'ai faite au début, et le quotient représente le nombre des groupes circulaires de n racines.

On voit que, s'il existe d'autres cas où le nombre des racines appartenant à un *indice donné n* est fini, on obtient un théorème analogue à mon point de vue, mais qui, au point de vue arithmétique, peut être très différent de celui que M. Picquet a démontré. Néanmoins il m'a été impossible jusqu'ici de trouver quelque exemple qui ne conduise pas à un théorème rentrant dans celui de M. Picquet.