432.

THÉORÈME RELATIF À LA THÉORIE DES SUBSTITUTIONS.

Extrait d'une lettre adressée à M. J. A. SERRET.

[From the *Comptes Rendus de l'Académie des Sciences de Paris*, tom. LXVII. (*Juillet—Décembre*, 1868), pp. 784, 785.]

ON peut énoncer par rapport aux substitutions un théorème qui comprend les trois théorèmes III. IV. V., t. II. pp. 260—263 de votre *Cours d'Algèbre Supérieure*.

Pour un nombre quelconque μ on peut former avec les $\phi(\mu)$ nombres inférieurs et premiers à μ plusieurs systèmes de nombres lesquels sont chacun un système conjugué (mod. μ); c'est-à-dire que le produit de deux nombres quelconques d'un tel système est congru suivant le module μ, à un nombre du système. Comme cas extrêmes, l'unité est un tel système, et les $\phi(\mu)$ nombres forment aussi un système conjugué.

Pour μ premier, en dénotant par α une racine primitive de μ et par f un diviseur quelconque de $f-1$, les nombres $\equiv a^{f\alpha}$ (mod. μ), a étant un entier quelconque, forment un système conjugué. Et généralement pour un nombre μ quelconque ce nombre a des racines quasi-primitives α, β, γ, ..., aux exposants A, B, C, ..., tels que $\alpha^A \equiv 1$ (mod. μ), $\beta^B \equiv 1$ (mod. μ), ... et $ABC \ldots = \phi(\mu)$. En choisissant une combinaison quelconque, par exemple α, β de ces racines, soient f, g des diviseurs quelconques de A, B respectivement, les nombres $\equiv a^{f\alpha} b^{g\beta}$ (mod. μ) forment un système conjugué, l'ordre du système ou nombre des termes étant $= \dfrac{AB}{fg}$.

Cela étant, on a ce théorème:

Une substitution T quelconque de l'ordre μ étant formée avec n lettres, l'on forme toutes les substitutions S telles que le produit STS^{-1} se réduise à une puissance de T dont l'exposant soit un nombre quelconque appartenant à un système conjugué (mod. μ), les substitutions S constitueront un système conjugué de l'ordre θM, où θ dénote l'ordre du système conjugué (mod. μ) et M le nombre des substitutions échangeables avec T.

La démonstration est tout à fait la même que celle que vous donnez p. 62 pour votre théorème IV, en y ajoutant seulement que les nombres i, j qui appartiennent au système conjugué (mod. μ) auront leur produit ij congru à un nombre de ce même système conjugué.