NOTE

SUR UN

THÉORÈME RELATIF AUX NOMBRES ENTIERS.

Journal de Mathématiques pures et appliquées, t. XIII, 1re sér.; 1848.

Depuis longtemps j'avais trouvé de mon côté une démonstration élémentaire suivante du théorème relatif aux nombres premiers $4k+1$.

Supposant

$$a^2+1 \equiv 0 \pmod{p},$$

convertissons $\frac{a}{p}$ en fraction continue jusqu'à ce qu'on obtienne deux réduites consécutives $\frac{m}{n}, \frac{m'}{n'}$, telles que n soit $<\sqrt{p}$ et $n'>\sqrt{p}$; on aura, comme on sait,

$$\frac{a}{p} = \frac{m}{n} + \frac{\varepsilon}{nn'},$$

où ε est <1. De là on tire

$$na - mp = \varepsilon \frac{p}{n'};$$

donc

$$(na-mp)^2 < p.$$

Ajoutant membre à membre avec $n^2 < p$, il vient

$$(na-mp)^2 + n^2 < 2p.$$

Or le premier membre de cette inégalité est un multiple entier de p d'après la condition

$$a^2+1 \equiv 0 \pmod{p};$$

il faut donc qu'on ait précisément

$$(na-mp)^2 + n^2 = p.$$

SUR UNE QUESTION RELATIVE

A LA

THÉORIE DES NOMBRES.

Journal de Mathématiques pures et appliquées, t. XIV, 1re sér.; 1849.

Soient $n+1$ nombres entiers

$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \varkappa,\ \lambda,$$

dont le plus grand commun diviseur est l'unité; on propose de trouver tous les systèmes de $n(n+1)$ autres nombres, savoir :

$$\begin{array}{llll}
\alpha', & \alpha'', & \ldots, & \alpha^{(n)}, \\
\beta', & \beta'', & \ldots, & \beta^{(n)}, \\
\gamma', & \gamma'', & \ldots, & \gamma^{(n)}, \\
\vdots & \vdots & & \vdots \\
\varkappa', & \varkappa'', & \ldots, & \varkappa^{(n)}, \\
\lambda', & \lambda'', & \ldots, & \lambda^{(n)},
\end{array}$$

qui rendent le déterminant

$$\begin{array}{lllll}
\alpha, & \alpha', & \ldots, & \alpha^{(i)}, \ldots, & \alpha^{(n)}, \\
\beta, & \beta', & \ldots, & \beta^{(i)}, \ldots, & \beta^{(n)}, \\
\gamma, & \gamma', & \ldots, & \gamma^{(i)}, \ldots, & \gamma^{(n)}, \\
\vdots & \vdots & & \vdots & \vdots \\
\varkappa, & \varkappa', & \ldots, & \varkappa^{(i)}, \ldots, & \varkappa^{(n)}, \\
\lambda, & \lambda', & \ldots, & \lambda^{(i)}, \ldots, & \lambda^{(n)},
\end{array}$$

égal à plus ou moins un.

Solution. — Nommons respectivement

π_1 le plus grand commun diviseur de α et β,
π_2 *idem* π_1 et γ,
π_3 *idem* π_2 et δ,
.....,
π_{n-1} *idem* π_{n-2} et $\varkappa$,
π_n *idem* π_{n-1} et λ;

dans l'hypothèse admise, π_n sera l'unité. Prenons ensuite les nombres entiers

$$\begin{matrix} a, & b, & c, & d, & \ldots, & k, & l, \\ & & c', & d', & \ldots, & k', & l', \end{matrix}$$

d'après les conditions

$$\begin{aligned} a\beta - b\alpha &= \pi_1, \\ c'\gamma - c\pi_1 &= \pi_2, \\ d'\delta - d\pi_2 &= \pi_3, \\ &\cdots\cdots\cdots, \\ k'\varkappa - k\pi_{n-2} &= \pi_{n-1}, \\ l'\lambda - l\pi_{n-1} &= \pi_n = 1. \end{aligned}$$

On satisfera à la question proposée par les valeurs suivantes :

$$\begin{aligned} \alpha^{(i)} &= am_i + \mathrm{M}_i \frac{\alpha}{\pi_1}, \\ \beta^{(i)} &= bm_i + \mathrm{M}_i \frac{\beta}{\pi_1}, \\ \gamma^{(i)} &= cn_i + \mathrm{N}_i \frac{\gamma}{\pi_2}, \\ \delta^{(i)} &= dp_i + \mathrm{P}_i \frac{\delta}{\pi_3}, \\ &\cdots\cdots\cdots, \\ \varkappa^{(i)} &= ks_i + \mathrm{S}_i \frac{\varkappa}{\pi_{n-1}}, \\ \lambda^{(i)} &= lt_i + \mathrm{T}_i \frac{\lambda}{\pi_n}, \end{aligned}$$

les quantités

$$\mathrm{M}_i, \quad \mathrm{N}_i, \quad \mathrm{P}_i, \quad \ldots. \quad \mathrm{S}_i$$

dépendant des nombres entiers

$$m_i, \quad n_i, \quad p_i, \quad \ldots, \quad s_i, \quad t_i$$

par les équations

$$\begin{aligned} \mathrm{M}_i &= c'n_i + \mathrm{N}_i \frac{\pi_1}{\pi_2}, \\ \mathrm{N}_i &= d'p_i + \mathrm{P}_i \frac{\pi_2}{\pi_3}, \\ &\cdots\cdots\cdots, \\ \mathrm{S}_i &= l't_i + \mathrm{T}_i \frac{\pi_{i-1}}{\pi_n}, \end{aligned}$$

et toutes les solutions possibles s'obtiendront en prenant toutes les valeurs des n^2 quantités

$$m_i, \quad n_i, \quad p_i, \quad \ldots, \quad s_i, \quad t_i,$$

pour lesquelles le déterminant

$$\begin{matrix} m_1, & m_2, & \ldots, & m_n, \\ n_1, & n_2, & \ldots, & n_n, \\ p_1, & p_2, & \ldots, & p_n, \\ \vdots & \vdots & & \vdots \\ s_1, & s_2, & \ldots, & s_n, \\ t_1, & t_2, & \ldots, & t_n, \end{matrix}$$

égale plus ou moins un.

Ainsi, par exemple, lorsque $n = 2$, s'il s'agit de rendre égal à l'unité le déterminant

$$\begin{Vmatrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{Vmatrix} = \alpha(\beta'\gamma'' - \gamma'\beta'') + \beta(\gamma'\alpha'' - \alpha'\gamma'') + \gamma(\alpha'\beta'' - \beta'\alpha''),$$

on aura

$$\begin{aligned} \alpha' &= am_1 + \mathrm{M}_1 \frac{\alpha}{\pi_1}, \\ \beta' &= bm_1 + \mathrm{M}_1 \frac{\beta}{\pi_1}, \\ \gamma' &= cn_1 + \mathrm{N}_1 \gamma, \end{aligned}$$

avec

$$\mathrm{M}_1 = c'n_1 + \mathrm{N}_1 \pi_1,$$

ce qui donne

$$\begin{aligned} \alpha' &= am_1 + \frac{\alpha c'}{\pi_1} n_1 + \mathrm{N}_1 \alpha, \\ \beta' &= bm_1 + \frac{\beta c'}{\pi_1} n_1 + \mathrm{N}_1 \beta, \\ \gamma' &= cn_1 \qquad\qquad + \mathrm{N}_1 \gamma; \end{aligned}$$

on trouvera ensuite semblablement

$$\begin{aligned} \alpha'' &= am_2 + \frac{\alpha c'}{\pi_1} n_2 + N_2 \alpha, \\ \beta'' &= bm_2 + \frac{\beta c'}{\pi_1} n_2 + N_2 \beta, \\ \gamma'' &= cn_2 \qquad\qquad + N_2 \gamma, \end{aligned}$$

et l'on devra prendre pour m_1, n_1, m_2, n_2 indéfiniment tous les nombres entiers pour lesquels

$$m_1 n_2 - m_2 n_1 = \pm 1.$$

Si $n = 3$, la solution générale de l'équation

$$\begin{vmatrix} \alpha, & \alpha', & \alpha'', & \alpha''' \\ \beta, & \beta', & \beta'', & \beta''' \\ \gamma, & \gamma', & \gamma'', & \gamma''' \\ \delta, & \delta', & \delta'', & \delta''' \end{vmatrix} = \pm 1$$

sera de même comprise dans les formules

$$\begin{aligned} \alpha' &= am_1 + \frac{\alpha c'}{\pi_1} n_1 + \frac{\alpha d'}{\pi_2} p_1 + P_1 \alpha, \\ \beta' &= bm_1 + \frac{\beta c'}{\pi_1} n_1 + \frac{\beta d'}{\pi_2} p_1 + P_1 \beta, \\ \gamma' &= cm_1 \qquad\qquad + \frac{\gamma d'}{\pi_2} p_1 + P_1 \gamma, \\ \delta' &= dp_1 \qquad\qquad\qquad\qquad + P_1 \delta; \\ \alpha'' &= am_2 + \frac{\alpha c'}{\pi_1} n_2 + \frac{\alpha d'}{\pi_2} p_2 + P_2 \alpha, \\ \beta'' &= bm_2 + \frac{\beta c'}{\pi_1} n_2 + \frac{\beta d'}{\pi_2} p_2 + P_2 \beta, \\ \gamma'' &= cn_2 \qquad\qquad + \frac{\gamma d'}{\pi_2} p_2 + P_2 \gamma, \\ \delta'' &= dp_2 \qquad\qquad\qquad\qquad + P_2 \delta, \\ \alpha''' &= am_3 + \frac{\alpha c'}{\pi_1} n_3 + \frac{\alpha d'}{\pi_2} p_3 + P_3 \alpha, \\ \beta''' &= bm_3 + \frac{\beta c'}{\pi_1} n_3 + \frac{\beta d'}{\pi_2} p_3 + P_3 \beta, \\ \gamma''' &= cn_3 \qquad\qquad + \frac{\gamma d'}{\pi_2} p_3 + P_3 \gamma, \\ \delta''' &= dp_3 \qquad\qquad\qquad\qquad + P_3 \delta. \end{aligned}$$

Voici maintenant l'analyse qui nous a conduit à ces résultats :

Soient, pour abréger, A le déterminant des quantités

$$\text{(A)} \qquad \alpha^{(i)}, \quad \beta^{(i)}, \quad \gamma^{(i)}, \quad \ldots, \quad \delta^{(i)},$$

B celui du système

$$\text{(B)} \qquad \begin{vmatrix} \xi, & \beta, & 0, & 0, & \ldots, & 0 \\ \xi', & -\alpha, & \gamma, & 0, & \ldots, & 0 \\ \xi'', & 0, & -\beta, & \delta, & \ldots, & 0 \\ \xi''', & 0, & 0, & -\gamma, & \ldots, & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \xi^{(n-1)}, & 0, & 0, & 0, & \ldots, & \lambda \\ \xi^{(n)}, & 0, & 0, & 0, & \ldots, & -\varkappa \end{vmatrix},$$

dont la loi est facile à saisir, et où les quantités ξ sont définies par les équations

$$\begin{aligned} &\alpha\xi + \beta\xi' + \gamma\xi'' + \ldots + \lambda\xi^{(n)} = 1, \\ &\alpha'\xi + \beta'\xi' + \gamma'\xi'' + \ldots + \lambda'\xi^{(n)} = 0, \\ &\alpha''\xi + \beta''\xi' + \gamma''\xi'' + \ldots + \lambda''\xi^{(n)} = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &\alpha^{(n)}\xi + \beta^{(n)}\xi' + \gamma^{(n)}\xi'' + \ldots + \lambda^{(n)}\xi^{(n)} = 0. \end{aligned}$$

De la composition des systèmes (A) et (B) résultera le nouveau système

$$\begin{matrix} 1, & 0, & 0, & \ldots, & 0, & \ldots, & 0, \\ 0, & \alpha'\beta - \beta'\alpha, & \alpha''\beta - \beta''\alpha, & \ldots, & \alpha^{(i)}\beta - \beta^{(i)}\alpha, & \ldots, & \alpha^{(n)}\beta - \beta^{(n)}\alpha, \\ 0, & \beta'\gamma - \gamma'\beta, & \beta''\gamma - \gamma''\beta, & \ldots, & \beta^{(i)}\gamma - \gamma^{(i)}\beta, & \ldots, & \beta^{(n)}\gamma - \gamma^{(n)}\beta, \\ 0, & \gamma'\delta - \delta'\gamma, & \gamma''\delta - \delta''\gamma, & \ldots, & \gamma^{(i)}\delta - \delta^{(i)}\gamma, & \ldots, & \gamma^{(n)}\delta - \delta^{(n)}\gamma, \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0, & \varkappa'\lambda - \lambda'\varkappa, & \varkappa''\lambda - \lambda''\varkappa, & \ldots, & \varkappa^{(i)}\lambda - \lambda^{(i)}\varkappa, & \ldots, & \varkappa^{(n)}\lambda - \lambda^{(n)}\varkappa. \end{matrix}$$

En appelant C son déterminant, ou, ce qui revient au même, celui des n^2 quantités

$$\text{(C)} \qquad \alpha^{(i)}\beta - \beta^{(i)}\alpha, \quad \beta^{(i)}\gamma - \gamma^{(i)}\beta, \quad \ldots, \quad \varkappa^{(i)}\lambda - \lambda^{(i)}\varkappa,$$

on aura, par un théorème connu,

$$C = AB.$$

Or on trouve facilement, au signe près,

$$B = \beta\gamma\delta\ldots\varkappa;$$

donc on peut remplacer la condition proposée, savoir

$$A = \pm 1,$$

par la suivante

$$C = \pm\beta\gamma\delta\ldots\varkappa,$$

dont nous allons nous occuper.

Exposons d'abord une transformation des termes du système (C); j'observe, à cet effet, que π_1 désignant le plus grand commun diviseur de α et β, on aura nécessairement

$$\alpha^{(i)}\beta - \beta^{(i)}\alpha = m_i\pi_1,$$

d'où l'on tire

$$\alpha^{(i)} = am_i + M_i\frac{\alpha}{\pi_1},$$

$$\beta^{(i)} = bm_i + M_i\frac{\beta}{\pi_1},$$

les nombres entiers m_i et M_i restant entièrement arbitraires, et a et b étant déterminés par l'équation

$$a\beta - b\alpha = \pi_1.$$

Au moyen de cette valeur de $\beta^{(i)}$, on trouve

$$\beta^{(i)}\gamma - \gamma^{(i)}\beta = b\gamma m_i + \frac{\beta}{\pi_1}(M_i\gamma - \gamma^{(i)}\pi_1).$$

Or, π_2 désignant le plus grand commun diviseur de π_1 et γ, on aura nécessairement

$$M_i\gamma - \gamma^{(i)}\pi_1 = n_i\pi_2,$$

d'où

$$M_i = c'n_i + N_i\frac{\pi_1}{\pi_2},$$

$$\gamma^{(i)} = cn_i + N_i\frac{\gamma}{\pi_2},$$

les nombres entiers n_i et N_i étant quelconques, c et c' dépendant de l'équation

$$c'\gamma - c\pi_1 = \pi_2.$$

La répétition du même calcul nous conduira de l'expression précédente de $\gamma^{(i)}$ à celle de $\delta^{(i)}$; il vient, en effet,

$$\gamma^{(i)}\delta - \delta^{(i)}\gamma = c\delta n_i + \frac{\gamma}{\pi_2}(N_i\delta - \delta^{(i)}\pi_2),$$

et posant encore

$$N_i\delta - \delta^{(i)}\pi_2 = p_i\pi_3,$$

π_3 étant le plus grand commun diviseur de π_2 et δ, on en conclura

$$N_i = d'p_i + P_i\frac{\pi_2}{\pi_3},$$

$$\delta^{(i)} = dp_i + P_i\frac{\delta}{\pi_3},$$

d et d' étant donnés par l'équation

$$d'\delta - d\pi_2 = \pi_3.$$

La loi que suivent ces opérations est maintenant évidente, et l'on en conclura, d'une part,

$$\alpha^{(i)}\beta - \beta^{(i)}\alpha = m_i\pi_1,$$

$$\beta^{(i)}\gamma - \gamma^{(i)}\beta = b\gamma m_i + \frac{\beta\pi_2}{\pi_1}n_i,$$

$$\gamma^{(i)}\delta - \delta^{(i)}\gamma = c\delta n_i + \frac{\gamma\pi_3}{\pi_2}p_i,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\varkappa^{(i)}\lambda - \lambda^{(i)}\varkappa = k\lambda s_i + \frac{\varkappa\pi_n}{\pi_{n-1}}t_i,$$

où il est essentiel d'observer que $m_i, n_i, \ldots, s_i, t_i$ restent jusqu'à présent des entiers entièrement arbitraires.

D'un autre côté, nous obtenons d'ailleurs

$$\alpha^{(i)} = am_i + M_i\frac{\alpha}{\pi_1},$$

$$\beta^{(i)} = bm_i + M_i\frac{\beta}{\pi_1},$$

$$\gamma^{(i)} = cn_i + N_i\frac{\gamma}{\pi_2},$$

$$\delta^{(i)} = dp_i + P_i\frac{\delta}{\pi_3},$$

$$\ldots\ldots\ldots\ldots\ldots,$$

$$\varkappa^{(i)} = ks_i + S_i\frac{\varkappa}{\pi_{n-1}},$$

$$\lambda^{(i)} = lt_i + T_i\frac{\lambda}{\pi_n},$$

et les entiers M_i, N_i, P_i, ... s'expriment de proche en proche, uniquement par m_i, n_i, p_i, ... au moyen de ces autres équations

$$M_i = c' n_i + N_i \frac{\pi_1}{\pi_2},$$

$$N_i = d' p_i + P_i \frac{\pi_2}{\pi_3},$$

$$\dots\dots\dots\dots\dots,$$

$$S_i = l' t_i + T_i \frac{\pi_{n-1}}{\pi_n},$$

lesquelles ne laissent d'indéterminé que T_i.

Ces résultats obtenus, reportons-nous maintenant au système (C), qui a été transformé dans le suivant, savoir :

$$\begin{array}{llll}
m_1\pi_1, & m_2\pi_1, & \dots, & m_i\pi_1, \quad \dots, \quad m_n\pi_1, \\
b\gamma m_1 + \dfrac{\beta\pi_2}{\pi_1} n_1, & b\gamma m_2 + \dfrac{\beta\pi_2}{\pi_1} n_2, & \dots, & b\gamma m_i + \dfrac{\beta\pi_2}{\pi_1} n_i, \quad \dots, \quad b\gamma m_n + \dfrac{\beta\pi_2}{\pi_1} n_n, \\
c\delta n_1 + \dfrac{\gamma\pi_3}{\pi_2} p_1, & c\delta n_2 + \dfrac{\gamma\pi_3}{\pi_2} p_2, & \dots, & c\delta n_i + \dfrac{\gamma\pi_3}{\pi_2} p_i, \quad \dots, \quad c\delta n_n + \dfrac{\gamma\pi_3}{\pi_2} p_n, \\
\dots\dots\dots\dots, & \dots\dots\dots\dots, & & \dots\dots\dots\dots, \quad \dots\dots\dots\dots, \\
k\lambda s_1 + \dfrac{\varkappa\pi_n}{\pi_{n-1}} t_1, & k\lambda s_2 + \dfrac{\varkappa\pi_n}{\pi_{n-1}} t_2, & \dots, & k\lambda s_i + \dfrac{\varkappa\pi_n}{\pi_{n-1}} t_i, \quad \dots, \quad k\lambda s_n + \dfrac{\varkappa\pi_n}{\pi_{n-1}} t_n.
\end{array}$$

On reconnaît bien facilement qu'un pareil système provient de la composition des deux autres, que voici :

(1)
$$\left\{\begin{array}{llll}
m_1, & m_2, & \dots, & m_i, \quad \dots, \quad m_n \\
n_1, & n_2, & \dots, & n_i, \quad \dots, \quad n_n \\
p_1, & p_2, & \dots, & p_i, \quad \dots, \quad p_n \\
\vdots & \vdots & & \vdots \\
s_1, & s_2, & \dots, & s_i, \quad \dots, \quad s_n \\
t_1, & t_2, & \dots, & t_i, \quad \dots, \quad t_n
\end{array}\right\}$$

et

(2)
$$\left\{\begin{array}{llllll}
\pi_1, & b\gamma, & 0, & 0, & \dots, & 0 \\
0, & \dfrac{\beta\pi_2}{\pi_1}, & c\delta, & 0, & \dots, & 0 \\
0, & 0, & \dfrac{\gamma\pi_3}{\pi_2}, & d\varepsilon, & \dots, & 0 \\
0, & 0, & 0, & \dfrac{\delta\pi_4}{\pi_3}, & \dots, & 0 \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
0, & 0, & 0, & 0, & \dots, & k\lambda \\
0, & 0, & 0, & 0, & \dots, & \dfrac{\varkappa\pi_n}{\pi_{n-1}}
\end{array}\right\};$$

donc son déterminant, et par suite celui du système (C), sont le produit des déterminants de ces deux systèmes.

Or le déterminant du système (2) se réduit à son terme principal

$$\beta\gamma\dots\varkappa\pi_n,$$

ou simplement

$$\beta\gamma\dots\varkappa,$$

puisque π_n est l'unité; la condition proposée

$$C = \pm\beta\gamma\dots\varkappa$$

sera donc remplie en prenant égal à l'unité en valeur absolue le déterminant des n^2 nombres entiers du système (1), ce qui est la conclusion que nous avions annoncée, et qu'il s'agissait d'obtenir.

DÉMONSTRATION ÉLÉMENTAIRE

D'UNE

PROPOSITION RELATIVE AUX DIVISEURS

DE $x^2 + Ay^2$.

Journal de Mathématiques pures et appliquées, t. XIV, 1re sér.: 1849.

Je dis que, p désignant un diviseur de la forme $x^2 + Ay^2$, une puissance convenablement déterminée de p pourra toujours être représentée par cette forme, c'est-à-dire qu'on pourra toujours faire

$$p^\mu = X^2 + AY^2.$$

Soit, pour une valeur entière quelconque de μ, α_μ, une valeur de $\sqrt{-A} \pmod{p^\mu}$: l'expression

$$(xp^\mu - y\alpha_\mu)^2 + Ay^2$$

représentera toujours des nombres entiers divisibles par p^μ, et je dis en premier lieu qu'on pourra toujours déterminer x et y de telle manière qu'on ait

$$\frac{(xp^\mu - y\alpha_\mu)^2 + Ay^2}{p^\mu} < 2\sqrt{A}.$$

En effet, il suffira de développer en fraction continue $\frac{\alpha_\mu}{p^\mu}$, jusqu'à ce qu'on arrive à une réduite telle que, son dénominateur étant moindre que $\frac{p^{\frac{1}{2}\mu}}{\sqrt{A}}$, cette limite soit atteinte ou surpassée par le dénominateur de la réduite suivante. Les valeurs de x et y seront respectivement le numérateur et le dénominateur de cette réduite. Cela posé, on voit que, par une infinité de valeurs de μ, on aura la

représentation d'un même multiple de p^μ par la forme $x^2 + Ay^2$. Ainsi, en nommant k le multiplicateur, on trouvera nécessairement deux équations

$$kp^\mu = x^2 + Ay^2,$$
$$kp^{\mu'} = x'^2 + Ay'^2,$$

dans lesquelles $x - x'$ et $y - y'$ seront à la fois divisibles par k. Sous cette condition il vient, en multipliant membre à membre les deux équations précédentes,

$$k^2 p^{\mu+\mu'} = (xx' + Ayy')^2 + A(xy' - yx')^2.$$

Or $xy' - yx'$ est divisible par k, puisqu'on a

$$x \equiv x', \quad y \equiv y' \pmod{k};$$

donc il en est de même de $xx' + Ayy'$, et, finalement, la puissance $\mu + \mu'$ de p se trouve bien représentée par la forme $x^2 + Ay^2$.

Il est facile de voir qu'une démonstration toute semblable s'applique au cas de A négatif; on a, au reste, un théorème plus général et dont voici l'énoncé :

p étant un diviseur de la norme d'un nombre complexe quelconque, formé avec les racines $m^{\text{ièmes}}$ de l'unité, on pourra toujours déterminer une puissance entière de p qui soit représentée précisément par cette norme.

SUR

LES FONCTIONS ALGÉBRIQUES.

Comptes rendus des séances de l'Académie des Sciences, tome XXXII, 1851.

1. Les propositions données par M. Puiseux, sur les racines des équations algébriques considérées comme fonctions d'une variable z, qui entre rationnellement dans leur premier membre, me semblent ouvrir un vaste champ de recherches destinées à jeter un grand jour sur la nature analytique de ce genre de quantités. Je me propose de donner ici le principe de ces recherches, et de faire voir comment elles conduisent à reconnaître si une équation quelconque

$$F(u, z) = 0$$

est résoluble algébriquement, c'est-à-dire si l'inconnue u peut être exprimée par une fonction de la variable z, ne contenant cette variable que sous les signes d'extraction de racines de degré entier. Les théorèmes auxquels nous serons ainsi amenés donneront, et sous un point de vue entièrement nouveau, le beau résultat obtenu par Abel sur la possibilité d'exprimer algébriquement $\sin \operatorname{am}\left(\frac{x}{n}\right)$ par $\sin \operatorname{am}(x)$. Je me borne ici à la question de la résolution par radicaux; plus tard je ferai, au même point de vue, l'étude des équations modulaires, et je montrerai comment les théorèmes de M. Puiseux conduisent à effectuer l'abaissement de ces équations dans les cas annoncés par Galois, dont les principes serviront d'ailleurs de base à tout ce que nous allons dire.

2. Soit

$$\Phi(z) = 0$$

l'équation dont les racines, mises pour z dans l'équation proposée

$$F(u, z) = 0,$$

lui font acquérir des racines multiples; désignons ces diverses valeurs de z par

$$z_0, \quad z_1, \quad \ldots, \quad z_{\mu-1},$$

et, après avoir tracé dans un plan deux axes rectangulaires, représentons-les par autant de points que nous nommerons respectivement

$$Z_0, \quad Z_1, \quad \ldots, \quad Z_{\mu-1}.$$

Soient enfin, pour un point quelconque P du plan,

$$u_0, \quad u_1, \quad \ldots, \quad u_{m-1},$$

toutes les racines de l'équation proposée; M. Puiseux, et c'est là une partie essentielle de ses recherches, a donné le moyen de trouver la substitution qui s'opère entre les valeurs initiales u_0, $u_1, \ldots, u_{m-1}$ des racines de la proposée, quand la variable z décrit un contour fermé partant du point P, et embrassant l'un des points $Z_0, Z_1, \ldots, Z_{\mu-1}$, pour revenir au même point P. Représentons symboliquement par S_i la substitution relative à un contour élémentaire comprenant le seul point Z_i; on aura les théorèmes suivants :

THÉORÈME I. — *Toute fonction des racines u, invariable par les substitutions*

$$S_0, \quad S_1, \quad \ldots, \quad S_{\mu-1},$$

pourra être exprimée rationnellement par la variable z; et aussi la proposition réciproque.

THÉORÈME II. — *Toute fonction des racines u, déterminable rationnellement en z, est invariable par les mêmes substitutions*

$$S_0, \quad S_1, \quad \ldots, \quad S_{\mu-1}.$$

Le groupe des substitutions en question jouera donc précisément le même rôle que le groupe de l'équation irréductible en V de Galois.

Démonstration du théorème I. — Soit U la fonction des racines $u_0, u_1, \ldots, u_{m-1}$, qui vérifie les conditions du théorème I; il est évident qu'on pourra toujours établir entre cette fonction et la variable z une équation rationnelle. En second lieu, si l'on fait décrire au point P un contour fermé quelconque, la fonction reprendra

toujours la même valeur initiale; donc, d'après une remarque qui appartient encore à M. Puiseux, U est une fonction entièrement rationnelle de z.

Démonstration du théorème II. — Toutes les valeurs que pourrait acquérir la fonction U, en appliquant aux racines $u_0, u_1, \ldots, u_{m-1}$, les substitutions $S_0, S_1, \ldots, S_{\mu-1}$, sont autant de valeurs initiales qu'on obtiendrait lorsque le point P, ayant décrit un contour quelconque, serait revenu à sa position primitive; si donc la fonction U remplit les conditions du théorème II, c'est-à-dire si elle est rationnelle, ces valeurs seront toutes les mêmes; donc, etc.

3. Je vais maintenant faire voir, par un exemple très simple, une première application de ce qui précède.

Le degré de l'équation proposée $F(u, z) = 0$ étant un nombre quelconque m, supposons que les divers systèmes circulaires de M. Puiseux soient tous identiques en embrassant toutes les racines, ou bien qu'ils soient réductibles tous aux puissances d'une même substitution circulaire d'ordre m, suivant l'expression employée par M. Cauchy, l'équation proposée sera résoluble par radicaux relativement à z.

En effet, si l'on désigne par α une racine quelconque de l'équation binome $\alpha^m = 1$, la fonction suivante

$$(u_0 + \alpha u_1 + \alpha^2 u_2 + \ldots + \alpha^{m-1} u_{m-1})^m$$

reprendra toujours la même valeur initiale, quel que soit le contour fermé qu'ait décrit le point mobile P en revenant à sa première position; donc cette fonction sera déterminable rationnellement en z; donc, etc.

4. Actuellement supposons que le degré m soit un nombre premier; la condition nécessaire et suffisante de solubilité par radicaux consiste en ce que toute fonction des racines invariable par les substitutions de cette forme spéciale, savoir :

$$\begin{pmatrix} u_k \\ u_{ak+b} \end{pmatrix},$$

a et b étant tous les entiers pris suivant le module m, ainsi que l'indice variable k, soit rationnellement connue.

Donc, d'après le théorème II, la condition nécessaire et suffisante de solubilité revient à ce que :

Les substitutions $S_1, S_2, \ldots, S_{\mu-1}$, données par les principes de M. Puiseux, soient toutes de la forme ci-dessous :

$$\begin{pmatrix} u_k \\ u_{ak+b} \end{pmatrix}.$$

Pour établir de la manière la plus simple la possibilité de la résolution par radicaux, je raisonnerai ainsi :

Posons

$$\varphi(\alpha) = (u_0 + \alpha u_1 + \alpha^2 u_2 + \ldots + \alpha^{m-1} u_{m-1})^m;$$

et désignons par ρ une racine primitive pour le nombre premier m; en employant une racine β de l'équation $\beta^{m-1} = 1$, nous considérerons la nouvelle fonction résolvante

$$T = [\varphi(\alpha) + \beta\varphi(\alpha^\rho) + \beta^2\varphi(\alpha^{\rho^2}) + \ldots + \beta^{n-2}\varphi(\alpha^{\rho^{n-2}})]^{n-1},$$

et je dis que cette fonction est invariable pour toutes les substitutions

$$\begin{pmatrix} u_k \\ u_{ak+b} \end{pmatrix}.$$

Pour cela, il suffit de prouver qu'elle ne varie point pour les deux substitutions

$$\begin{pmatrix} u_k \\ u_{k+1} \end{pmatrix}$$

et

$$\begin{pmatrix} u_k \\ u_{\rho k} \end{pmatrix};$$

car la précédente résulte des produits des puissances de celles-ci.

Or la première

$$\begin{pmatrix} u_k \\ u_{k+1} \end{pmatrix}$$

laisse invariables toutes les quantités

$$\varphi(\alpha), \quad \varphi(\alpha^\rho), \quad \varphi(\alpha^{\rho^2}), \quad \ldots, \quad \varphi(\alpha^{\rho^{m-2}}).$$

Quant à la seconde

$$\begin{pmatrix} u_k \\ u_{\rho k} \end{pmatrix}$$

elle n'a d'autre effet que de remplacer chaque terme de la suite ci-dessus par le précédent, le premier devenant le dernier; or une telle substitution n'altère pas la valeur de T, donc T est bien invariable par toutes les substitutions

$$\begin{pmatrix} u_k \\ u_{ak+b} \end{pmatrix}.$$

Donc enfin T est une fonction rationnelle de z, facilement déterminable par la théorie de M. Puiseux, si les divers systèmes circulaires pour les points $Z_0, Z_1, \ldots, Z_{p-1}$ sont de la forme que nous leur avons assignée.

SUR L'EXTENSION DU THÉORÈME DE M. STURM

A UN

SYSTÈME D'ÉQUATIONS SIMULTANÉES.

Comptes rendus des séances de l'Académie des Sciences, tome XXXV, 1852.

Le théorème de M. Sturm a pour objet de déterminer le nombre des racines réelles d'une équation à une inconnue, qui sont comprises entre deux limites données. Je me suis proposé, dans le Mémoire que j'ai l'honneur de soumettre à l'Académie, une question analogue pour deux équations simultanées, et qu'on peut énoncer ainsi : Considérant l'une des inconnues comme l'abscisse, et l'autre comme l'ordonnée d'un point rapporté à deux axes rectangulaires, déterminer le nombre des points auxquels correspondent des solutions des équations proposées, et qui sont compris dans l'intérieur d'un rectangle donné. Cette question se trouve résolue de la manière suivante. Désignons les sommets du rectangle par les lettres a, b, c, d, et supposons les côtés ab et ad respectivement parallèles aux directions positives des axes des abscisses et des ordonnées. On substituera successivement les valeurs numériques des coordonnées de ces quatre points à la place des lettres x et y, dans une certaine suite de fonctions de ces deux variables; et en désignant par A, B, C, D les nombres de variations que présente cette suite, lorsqu'on prend pour les variables les coordonnées des points a, b, c, d, on aura, pour le nombre cherché, la valeur

$$n = \frac{A - B + C - D}{2}.$$

Ce résultat est, comme on voit, entièrement analogue à celui du théorème de M. Sturm; cette analogie se maintient encore lorsque l'on considère trois équations simultanées au lieu de deux. Désignant alors les inconnues par x, y, z, on les regardera comme les coordonnées d'un point de l'espace rapporté à trois axes rectangulaires, de sorte qu'à chaque solution des équations proposées

ré ponde un point déterminé. Cela posé, considérons un parallélépipède droit, dont les bases parallèles au plan des xy soient les rectangles $abcd$, $a'b'c'd'$. Nous supposerons les côtés ab, ad parallèles aux directions positives des x et des y, et les droites aa', bb', cc', dd' parallèles à la direction positive de l'axe des z. Cela étant, le nombre des points représentant des solutions et compris dans l'intérieur de ce parallélépipède sera déterminé de la manière suivante :

Désignons respectivement par A, B, C, D, A′, B′, C′, D′ les nombres des variations que présente une certaine suite de fonctions de trois variables, lorsqu'on substitue à ces variables les valeurs numériques des coordonnées des points a, b, c, d, a', b', c', d', le nombre cherché sera donné par la formule

$$n = \tfrac{1}{4}[(\mathrm{A}-\mathrm{A}')-(\mathrm{B}-\mathrm{B}')+(\mathrm{C}-\mathrm{C}')-(\mathrm{D}-\mathrm{D}')].$$

Il est remarquable qu'il existe un grand nombre de suites jouissant ainsi de propriétés semblables à celles des fonctions de M. Sturm, dans la théorie des équations simultanées. Voici la plus simple pour le cas de deux équations prises, si l'on veut, sous la forme

$$\mathrm{F}(x) = 0, \qquad y = \Phi(x),$$

$\mathrm{F}(x)$ étant un polynome entier, et $\Phi(x)$ une fonction rationnelle de x.

Nommons $x_1, x_2, \ldots, x_m$ les racines de l'équation $\mathrm{F}(x)=0$, $y_1, y_2, \ldots, y_m$ les valeurs correspondantes de y, S_i la somme symétrique

$$x_1^i + x_2^i + \ldots + x_m^i,$$

et T_i la suivante

$$y_1 x_1^i + y_2 x_2^i + \ldots + y_m x_m^i;$$

le premier terme de la suite sera l'unité, et les autres les déterminants des systèmes

$$\begin{vmatrix} 1 & x \\ \mathrm{T}_0 - \mathrm{S}_0 y & \mathrm{T}_1 - \mathrm{S}_1 y \end{vmatrix}, \qquad \begin{vmatrix} 1 & x & x^2 \\ \mathrm{T}_0 - \mathrm{S}_0 y & \mathrm{T}_1 - \mathrm{S}_1 y & \mathrm{T}_2 - \mathrm{S}_2 y \\ \mathrm{T}_1 - \mathrm{S}_1 y & \mathrm{T}_2 - \mathrm{S}_2 y & \mathrm{T}_3 - \mathrm{S}_3 y \end{vmatrix},$$

$$\begin{vmatrix} 1 & x & x^2 & x^3 \\ \mathrm{T}_0 - \mathrm{S}_0 y & \mathrm{T}_1 - \mathrm{S}_1 y & \mathrm{T}_2 - \mathrm{S}_2 y & \mathrm{T}_3 - \mathrm{S}_3 y \\ \mathrm{T}_1 - \mathrm{S}_1 y & \mathrm{T}_2 - \mathrm{S}_2 y & \mathrm{T}_3 - \mathrm{S}_3 y & \mathrm{T}_4 - \mathrm{S}_4 y \\ \mathrm{T}_2 - \mathrm{S}_2 y & \mathrm{T}_3 - \mathrm{S}_3 y & \mathrm{T}_4 - \mathrm{S}_4 y & \mathrm{T}_5 - \mathrm{S}_5 y \end{vmatrix}, \quad \text{etc.};$$

le dernier terme est le déterminant à $m+1$ colonnes obtenu en continuant la même loi. En général, c'est au moyen de fonctions symétriques des racines des équations proposées que se trouvent immédiatement exprimées les fonctions analogues à celles de M. Sturm, et les propriétés de ces fonctions sont déduites de leur loi même de formation. L'idée d'introduire ainsi explicitement les racines est due à M. Sylvester, qui, le premier, a montré comment elles entraient dans la composition des fonctions de M. Sturm; M. Cayley a fait voir ensuite avec élégance comment les propriétés élémentaires des déterminants permettaient de transformer les premiers termes des formules de M. Sylvester en d'autres qui contiennent seulement les sommes des puissances semblables des racines [1]. Ce sont aussi des expressions analogues à ces sommes, pour le cas de deux équations simultanées, qui figurent dans nos formules et qui les rapprochent de celles du savant géomètre. Mais le fait le plus important qui ressort de mes recherches consiste dans l'existence d'une infinité de fonctions possédant les propriétés de celles de M. Sturm, pour une ou plusieurs équations. Cela ouvre la voie à des recherches importantes, sur lesquelles je pourrai peut-être revenir dans une autre occasion; je me bornerai pour le moment à cette remarque, que les conditions de réalité des racines d'une équation à une inconnue peuvent s'exprimer uniquement à l'aide des fonctions rationnelles des coefficients qu'on nomme *hyperdéterminants* ou *invariants*.

---

[1] Tomes IX et XIII du *Journal de Mathématiques* de M. Liouville.

REMARQUES

SUR

LE THÉORÈME DE M. STURM.

Comptes rendus des séances de l'Académie des Sciences, tome XXXVI; 1853.

En représentant par $V = o$ une équation quelconque de degré m, dont les racines soient $a, b, \ldots, k, l$, et par $V_1, V_2, \ldots, V_m$ la suite des fonctions de M. Sturm, on a, d'après le beau théorème de M. Sylvester, les expressions

$$\frac{V_1}{V} = \sum \frac{1}{x-a},$$
$$\frac{V_2}{V} = \sum \frac{(a-b)^2}{(x-a)(x-b)},$$
$$\frac{V_3}{V} = \sum \frac{(a-b)^2(a-c)^2(b-c)^2}{(x-a)(x-b)(x-c)},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\frac{V_m}{V} = \frac{(a-b)^2(a-c)^2\ldots(k-l)^2}{(x-a)(x-b)\ldots(x-l)}.$$

J'ai remarqué qu'en désignant par A, B, ..., K, L des fonctions rationnelles semblables de $a, b, \ldots, k, l$, de telle sorte que

$$A = \varphi(a), \qquad B = \varphi(b), \qquad \ldots, \qquad L = \varphi(l),$$

les nouvelles fonctions

$$\frac{V_1}{V} = \sum \frac{1}{x-a},$$
$$\frac{\mathfrak{V}_2}{V} = \sum \frac{(A-B)^2}{(x-a)(x-b)},$$
$$\frac{\mathfrak{V}_3}{V} = \sum \frac{(A-B)^2(A-C)^2(B-C)^2}{(x-a)(x-b)(x-c)},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\frac{\mathfrak{V}_m}{V} = \frac{(A-B)^2(A-C)^2\ldots(K-L)^2}{(x-a)(x-b)\ldots(x-l)}$$

ont les mêmes propriétés que celles de M. Sturm. Ainsi l'on a cette proposition : Pour une valeur réelle de x, le nombre des termes positifs de la suite

$$\frac{V_1}{V}, \quad \frac{\mathfrak{V}_2}{V_1}, \quad \frac{\mathfrak{V}_3}{\mathfrak{V}_2}, \quad \ldots, \quad \frac{\mathfrak{V}_m}{\mathfrak{V}_{m-1}}$$

représente le nombre des couples de racines imaginaires de l'équation

$$V = o,$$

augmenté du nombre des racines réelles moindres que x. Le nombre des termes négatifs serait le nombre de couples des racines imaginaires, plus le nombre des racines réelles supérieures à x. De là se tire immédiatement le théorème de M. Sturm, sous la forme que lui a donnée l'illustre géomètre; mais les énoncés précédents sont ceux que fournit d'abord la méthode que j'ai suivie.

En considérant deux équations à deux inconnues dont les solutions simultanées, en nombre m, soient

$$x = a, \quad y = a', \quad x = b, \quad y = b', \quad \ldots, \quad x = k, \quad y = k', \quad x = l, \quad y = l',$$

je désigne d'une manière analogue par A, B, ..., K, L, des fonctions rationnelles semblables de ces solutions, de sorte que

$$A = \varphi(a, a'), \qquad B = \varphi(b, b'), \qquad \ldots, \qquad L = \varphi(l, l').$$

Cela étant, les expressions suivantes, fonctions rationnelles symétriques de ces solutions, savoir :

$$\frac{U_1}{U} = \sum \frac{1}{(x-a)(y-a')},$$
$$\frac{U_2}{U} = \sum \frac{(A-B)^2}{(x-a)(y-a')(x-b)(y-b')},$$
$$\frac{U_3}{U} = \sum \frac{(A-B)^2(A-C)^2\ldots(B-C)^2}{(x-a)(y-a')(x-b)(y-b')(x-c)(y-c')},$$

et, en dernier lieu,

$$\frac{U_m}{U} = \frac{(A-B)^2(A-C)^2\ldots(K-L)^2}{(x-a)(y-a')(x-b)(y-b')\ldots(x-l)(y-l')}$$

donnent lieu à cette proposition :

Pour un système donné de valeurs réelles de x et y, le nombre

des termes positifs de la suite

$$\frac{U_1}{U}, \quad \frac{U_2}{U_1}, \quad \frac{U_3}{U_2}, \quad \ldots, \quad \frac{U_m}{U_{m-1}}$$

représente le nombre des couples de solutions imaginaires, augmenté du nombre des solutions simultanées réelles $x = a$, $y = a'$, pour lesquelles $(x - a)(y - a')$ est positif. Le nombre des termes négatifs serait le nombre des couples de solutions imaginaires augmenté du nombre des solutions réelles, pour lesquelles $(x - a)(y - a')$ est négatif.

D'après cela, si l'on représente par (x, y) le nombre des termes positifs de notre suite, on trouvera très aisément que le nombre des solutions simultanées réelles, pour lesquelles on a à la fois

$$x > x_0, \qquad x < x_1,$$
$$y > y_0, \qquad y < y_1,$$

est donné par la formule

$$\frac{1}{2}[(x_1, y_1) + (x_0, y_0) - (x_1, y_0) - (x_0, y_1)].$$

Ces nouvelles fonctions auxiliaires sont plus simples que celles auxquelles j'étais arrivé dans un précédent Mémoire; elles n'exigent point que l'on connaisse d'avance si, à une valeur de l'une des inconnues, correspond une seule ou plusieurs valeurs de l'autre inconnue. Dans le cas des solutions égales, elles se comportent comme celles de M. Sturm; la dernière fonction U_m s'évanouissant, toutes les autres $U, U_1, U_2, \ldots$ acquièrent un facteur commun, tel que $(x - a)(y - a')$, et, après la suppression de ce facteur, la nouvelle suite présente, avec un terme de moins, exactement la même composition analytique et les mêmes propriétés que l'ancienne. On peut aussi démontrer que trois fonctions consécutives sont liées par une relation de la forme

$$PU_i + QU_{i+1} + RU_{i+2} = 0,$$

où les coefficients extrêmes sont des carrés, de sorte qu'en général, si une fonction s'évanouit, la précédente et la suivante sont de signes contraires. Mais c'est là une conséquence et non le principe de ma méthode, qui repose sur quelques propriétés élémentaires

des formes quadratiques. On s'en rendra compte aisément en remarquant que les fonctions

$$\frac{\mathfrak{V}_2}{V}, \quad \frac{\mathfrak{V}_3}{V}, \quad \ldots, \quad \frac{\mathfrak{V}_m}{V}$$

sont respectivement les invariants des formes quadratiques

$$\sum \frac{1}{x - a}(X_0 + AX_1)^2,$$
$$\sum \frac{1}{x - a}(X_0 + AX_1 + A^2X_2)^2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\sum \frac{1}{x - a}(X_0 + AX_1 + \ldots + A^{m-1}X_{m-1})^2.$$

J'ai ainsi retrouvé, dans une recherche purement algébrique, ce genre spécial de formes quadratiques, que j'ai considérées tant de fois dans mes recherches de théorie des nombres (*Journal de Crelle*, t. 40 et 41). Pour les équations à deux inconnues, les formes analogues sont

$$\sum \frac{1}{(x - a)(y - a')}(X_0 + AX_1)^2,$$
$$\sum \frac{1}{(x - a)(y - a')}(X_0 + AX_1 + A^2X_2)^2,$$

et, en dernier lieu,

$$\sum \frac{1}{(x - a)(y - a')}(X_0 + AX_1 + A^2X_2 + \ldots + A^{m-1}X_{m-1})^2.$$

SUR LA DÉCOMPOSITION D'UN NOMBRE EN QUATRE CARRÉS.

Comptes rendus des séances de l'Académie des Sciences, tome XXXVII; 1853.

Des recherches sur les nombres complexes m'ont conduit à la démonstration suivante du théorème de Fermat sur la décomposition d'un nombre en quatre carrés, que je vais exposer en peu de mots.

Désignant par A un nombre entier impair ou impairement pair, nous commencerons par établir la possibilité de la congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{A}.$$

A cet effet, soit d'abord

$$A \equiv \varepsilon \pmod 4,$$

ε représentant $+1$ ou -1; la progression arithmétique ayant pour terme général

$$4Az + 2\varepsilon A - 1,$$

ne contiendra que des nombres $\equiv 1 \pmod 4$, puisque

$$2\varepsilon A - 1 \equiv 2\varepsilon^2 - 1 \equiv 1 \pmod 4.$$

J'observe ensuite que le premier terme $2\varepsilon A - 1$ et la raison $4A$ sont premiers entre eux, car, de ces deux nombres, l'un est pair, l'autre impair, et la relation

$$4\varepsilon A - 2(2\varepsilon A - 1) = 2$$

montre qu'ils ne pourraient avoir d'autre diviseur commun que 2. Donc, d'après le théorème démontré par M. Dirichlet, cette progression contiendra une infinité de nombres premiers qui seront $\equiv 1 \pmod 4$ et, par suite, décomposables en deux carrés. On pourra

faire ainsi, pour une infinité de valeurs de z,

$$4Az + 2\varepsilon A - 1 = x^2 + y^2;$$

d'où l'on conclura

$$x^2 + y^2 + 1 \equiv 0 \pmod{A}.$$

Soit, en second lieu, $A \equiv 2 \pmod 4$; tout ce qui précède subsistera relativement à la nouvelle progression arithmétique, ayant pour terme général

$$2Az + A - 1.$$

Ainsi la possibilité de la congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{A}$$

se trouve établie pour tout module impair, ou double d'un nombre impair.

Considérons maintenant la forme quadratique définie à quatre indéterminées

$$f = (Ax + \alpha z + \beta u)^2 + (Ay - \beta z + \alpha u)^2 + z^2 + u^2,$$

où les nombres entiers α et β satisfont à la condition

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{A}.$$

L'invariant Δ de cette forme sera en valeur absolue A^4; donc, si l'on cherche son minimum pour des valeurs entières des indéterminées, on trouvera, d'après un théorème que j'ai donné en général, un nombre au-dessous de la limite $\left(\frac{4}{3}\right)^{\frac{3}{2}}\sqrt[4]{\Delta}$, et, par suite, moindre que $2A$. Mais il est aisé de reconnaître que les nombres représentables par f sont nécessairement des multiples de A; donc ce minimum ne peut qu'être A lui-même, qui se trouvera ainsi décomposé en une somme de quatre carrés.

Dans un de mes Mémoires (1) sur la théorie des formes quadratiques, publié dans le *Journal de Crelle*, on pourra voir comment l'analyse précédente conduit à l'expression du nombre de toutes les décompositions possibles, que M. Jacobi a obtenu le premier par la théorie des fonctions elliptiques.

(1) *Voir* p. 259 et suivantes de ce Volume. E. P.

REMARQUES

SUR UN

MÉMOIRE DE M. CAYLEY

RELATIF AUX DÉTERMINANTS GAUCHES.

(*Cambridge and Dublin Mathematical Journal*, IX, 1854.)

M. Cayley a nommé *système gauche symétrique* un système de n^2 quantités, représentées par $\lambda_{r,s}$ en attribuant aux indices toutes les valeurs entières depuis 1 jusqu'à n, lorsqu'on a la condition générale

$$\lambda_{r,s} = -\lambda_{s,r},$$

d'où résulte

$$\lambda_{r,r} = 0.$$

De pareils systèmes jouissent de propriétés importantes qui jouent un grand rôle dans les diverses circonstances analytiques où ils se présentent, et M. Cayley en a fait lui-même un nouvel usage pour la solution de cette question :

Obtenir toutes les transformations d'une forme quadratique en elle-même lorsque cette forme est une somme de carrés.

Je me propose de donner ici des formules analogues à celles de M. Cayley, pour la transformation en elle-même d'une forme quadratique quelconque.

Le problème peut être posé : $f(x_1, x_2, \ldots, x_n)$ désignant la forme quadratique proposée, trouver l'expression la plus générale des quantités $X_1, X_2, \ldots, X_n$, qui donnent

$$f(X_1, X_2, \ldots, X_n) = f(x_1, x_2, \ldots, x_n).$$

Pour cela, j'imagine que les quantités X et x soient exprimées par des indéterminées auxiliaires ξ, de sorte qu'on ait en général

$$X_r + x_r = 2\xi_r,$$

et, sous cette condition, on va voir qu'il est très facile d'obtenir l'expression générale de X et x en ξ. On a, en effet,

$$X_r = 2\xi_r - x_r;$$

donc

$$(1) \qquad f(X_1, X_2, \ldots) = f(2\xi_1 - x_1, 2\xi_2 - x_2, \ldots),$$

ou, en développant le second membre,

$$(2) \quad f(X_1, X_2, \ldots) = 4f(\xi_1, \xi_2, \ldots) - 2\left(x_1\frac{df}{d\xi_1} + x_2\frac{df}{d\xi_2} + \ldots\right) + f(x_1, x_2, \ldots).$$

Donc, par la condition supposée,

$$f(X_1, X_2, \ldots) = f(x_1, x_2, \ldots),$$

cette équation se réduit à

$$(3) \qquad x_1\frac{df}{d\xi_1} + x_2\frac{df}{d\xi_2} + \ldots = 2f.$$

Or, la manière la plus générale de la vérifier en exprimant les quantités x en ξ, sera de faire

$$(4) \qquad x_r = \xi_r + \frac{1}{2}\sum_1^n{}_s \lambda_{r,s}\frac{df}{d\xi_s},$$

les indéterminées λ étant assujetties à la condition

$$\lambda_{r,s} = -\lambda_{s,r}.$$

On en conclut

$$X_r = 2\xi_r - x_r = \xi_r - \frac{1}{2}\sum_1^n{}_s \lambda_{r,s}\frac{df}{d\xi_s},$$

et il est facile de reconnaître *a posteriori* que ces expressions de X et x en ξ donnent bien

$$(5) \qquad f(X_1, X_2, \ldots) = f(x_1, x_2, \ldots).$$

Reprenant en effet l'équation (1) et l'équation (2), on verra par

l'équation (3), équation satisfaite d'elle-même, qu'on retombe précisément sur l'équation (5) qui était à vérifier. Donc enfin, les expressions cherchées de X en x, qui donnent la transformation en elle-même d'une forme quelconque, s'obtiendront en résolvant par rapport aux quantités ξ les équations (4), et substituant les valeurs en x, qu'on aura trouvées de la sorte, dans les formules

$$X_r = 2\xi_r - x_r.$$

Considérons pour l'application les formes binaires

$$f = ax^2 + 2bxy + cy^2,$$

où nous mettons x et y au lieu de x_1 et x_2; nous aurons successivement

$$X + x = 2\xi,$$
$$Y + y = 2\eta,$$

et

$$x = \xi + \lambda(b\xi + c\eta) = \xi(1 + \lambda b) + \lambda c\eta,$$
$$y = \eta - \lambda(a\xi + b\eta) = -\lambda a\xi + (1 - \lambda b)\eta;$$

d'où, en résolvant,

$$\xi = \frac{(1 - \lambda b)x - \lambda cy}{1 - \lambda^2(b^2 - ac)},$$
$$\eta = \frac{\lambda ax + (1 + \lambda b)y}{1 - \lambda^2(b^2 - ac)}.$$

Soit, pour abréger,

$$b^2 - ac = D;$$

on trouvera

$$X = 2\xi - x = \frac{(1 - 2\lambda b + \lambda^2 D)x - 2\lambda cy}{1 - \lambda^2 D},$$
$$Y = 2\eta - y = \frac{2\lambda ax + (1 + 2\lambda b + \lambda^2 D)y}{1 - \lambda^2 D}.$$

Or ces formules, en posant

$$t = \frac{1 + \lambda^2 D}{1 - \lambda^2 D},$$
$$u = \frac{2\lambda}{1 - \lambda^2 D},$$

ce qui donne

$$t^2 - D u^2 = 1,$$

deviendront

$$X = x(t - bu) - cuy,$$
$$Y = xau + (t + bu)y.$$

C'est la forme analytique obtenue par M. Gauss pour la question arithmétique où l'on veut que les coefficients de la substitution soient des nombres entiers.

Enfin, si l'on fait l'application de la même méthode à une forme quadratique d'un nombre quelconque d'indéterminées dans le cas où elle est une somme de carrés, on trouvera immédiatement les résultats que M. Cayley a obtenus dans son beau Mémoire, et je m'empresse de dire que je dois à l'étude de ce Mémoire l'analyse que je viens d'indiquer en peu de mots. J'ajouterai cependant encore les théorèmes suivants, qui servent de lemmes à une recherche arithmétique importante.

I. *Ayant ramené à une somme de carrés de fonctions linéaires une forme quadratique quelconque, de sorte qu'on ait, par exemple,*

$$f = A^2 + B^2 + C^2 + \ldots,$$

si l'on désigne par $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... *ce que deviennent respectivement* A, B, C, ... *lorsqu'on fait dans f une substitution quelconque qui la change en elle-même, on aura évidemment*

$$\mathfrak{A} = \alpha A + \beta B + \gamma C + \ldots,$$
$$\mathfrak{B} = \alpha' A + \beta' B + \gamma' C + \ldots,$$
$$\mathfrak{C} = \alpha'' A + \beta'' B + \gamma'' C + \ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

les quantités α, β, γ, ... *étant des constantes convenablement choisies. Cela posé, à une substitution qui change f en elle-même on pourra toujours faire correspondre une telle représentation de f par la forme*

$$A^2 + B^2 + C^2 + \ldots,$$

que l'expression

$$A\mathfrak{A} + B\mathfrak{B} + C\mathfrak{C} + \ldots$$

ne contienne aucun des rectangles AB, AC, ...

Pour donner une application de ce théorème, nous allons considérer le cas des formules quadratiques ternaires

$$f = A^2 + B^2 + C^2.$$

Alors des constantes α, β, γ, ..., devant être telles que

$$\mathfrak{A}^2 + \mathfrak{B}^2 + \mathfrak{C}^2 = A^2 + B^2 + C^2,$$

auront, d'après M. Cayley, les valeurs suivantes :

$$\begin{aligned} k\alpha &= 1 + \lambda^2 - \mu^2 - \nu^2, & k\alpha' &= 2(\lambda\mu - \nu), & k\alpha'' &= 2(\lambda\nu + \mu), \\ k\beta &= 2(\mu\lambda + \nu), & k\beta' &= 1 - \lambda^2 + \mu^2 - \nu^2, & k\beta'' &= 2(\mu\nu - \lambda), \\ k\gamma &= 2(\nu\lambda - \mu) & k\gamma' &= 2(\nu\mu + \lambda), & k\gamma'' &= 1 - \lambda^2 - \mu^2 + \nu^2, \end{aligned}$$

où

$$k = 1 + \lambda^2 + \mu^2 + \nu^2,$$

et, à toute substitution S qui change f en elle-même, on pourra toujours faire correspondre un système de fonctions linéaires A, B, C, jouissant de la propriété qu'en devenant respectivement $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ lorsqu'on effectue la substitution S, on aura les relations

$$\alpha' + \beta = 0, \qquad \alpha'' + \gamma = 0, \qquad \beta'' + \gamma' = 0.$$

De là se tire la conclusion que deux des quantités λ, μ, ν sont nulles. On peut donc faire, par exemple,

$$\mathfrak{A}^2 = A^2,$$
$$\mathfrak{B}^2 + \mathfrak{C}^2 = B^2 + C^2,$$

ou bien

$$\begin{aligned} \mathfrak{A} &= \pm A, \\ \mathfrak{B} &= B\cos\theta + C\sin\theta, \\ \mathfrak{C} &= -B\sin\theta + C\cos\theta. \end{aligned}$$

De là ces théorèmes :

II. *Soit*

$$\begin{aligned} X &= px + p'y + p''z, \\ Y &= qx + q'y + q''z, \\ Z &= rx + r'y + r''z \end{aligned}$$

une substitution qui change en elle-même une forme ternaire quelconque; l'une des racines λ *de l'équation*

$$\Lambda = \begin{vmatrix} p - \lambda & p' & p \\ q & q' - \lambda & q'' \\ r & r' & r'' - \lambda \end{vmatrix} = 0$$

sera égale à ± 1, *et les deux autres seront réciproques.*

III. *Il existe une infinité de formes ternaires différentes de f que la substitution ci-dessus change en elles-mêmes, ces formes seront toutes données par l'expression*

$$F = kA^2 + l(B^2 + C^2),$$

k et l étant des constantes arbitraires. Cependant le cas des racines égales dans l'équation $\Lambda = 0$ *doit être traité à part et exige une discussion spéciale que nous laisserons faire au lecteur.*