VI.

Une conséquence importante des résultats précédemment exposés consiste en ce que toutes les valeurs de $u^8 = \varphi^8(\omega)$ qui font acquérir des racines doubles à l'équation modulaire, représentent également des modules de fonctions elliptiques pour lesquelles a lieu la multiplication complexe. Nous avons vu en effet que la quantité ω dépendait de la relation

$$A\omega^2 + 2B\omega + C = 0,$$

(A, B, C) étant une forme quadratique de déterminant négatif, ce qui est précisément le caractère essentiel de ces modules. Je vais donc présenter à l'égard des équations algébriques qui servent à les déterminer les remarques auxquelles j'ai été naturellement amené par les recherches précédentes, et qui serviront de complément aux théorèmes fondamentaux déjà donnés sur ce sujet par M. Kronecker.

Voici d'abord un choix particulier dont je conviendrai pour les formes destinées à représenter les diverses classes quadratiques qui appartiennent au même déterminant. En désignant ces formes par (A, B, C) et faisant $\Delta = AC - B^2$, je supposerai, ce qui est toujours possible, que C soit pair et A impair, de sorte que dans le groupe proprement primitif (1) on aura, suivant que

$$\Delta \equiv 1 \pmod 4, \qquad B \text{ et } \frac{1}{2}C \text{ impairs};$$
$$\Delta \equiv 2 \pmod 4, \qquad B \text{ pair et } \frac{1}{2}C \text{ impair};$$
$$\Delta \equiv -1 \pmod 4, \qquad B \text{ impair et } C \text{ multiple de } 4.$$

En second lieu, et pour ce qui concerne le groupe improprement primitif, il ne sera posé aucune condition lorsque $\Delta \equiv 3 \pmod 8$; mais, dans le cas de $\Delta \equiv -1 \pmod 8$, nous prendrons C impairement pair. Les formes ainsi choisies, et que nous garderons désormais pour représenter les classes, jouissent de cette propriété de conserver les mêmes caractères dans toutes leurs transformées par des substitutions au déterminant un, $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$, où β est pair, α et δ impairs. Cela posé, si l'on détermine ω en faisant

$$A\omega^2 + 2B\omega + C = 0,$$

(A, B, C) représentant successivement toutes les classes du groupe proprement primitif et de même déterminant $-\Delta$, les diverses quantités $x = \varphi^8(\omega)$ seront racines d'une équation qui sera réciproque, dont le degré sera double du nombre des classes et dont les coefficients seront entiers, en supposant celui de la puissance la plus élevée de x égal à l'unité.

En second lieu, et à l'égard du groupe improprement primitif, on obtiendra comme précédemment une équation réciproque dont le degré sera encore le double du nombre des classes, mais avec une puissance de 2 pour coefficient du premier terme lorsque $\Delta \equiv -1 \pmod 8$. Enfin, si l'on suppose $\Delta \equiv 3 \pmod 8$, le degré sera six fois le nombre des classes, et tous les coefficients entiers, celui du premier terme étant l'unité.

Voici maintenant la méthode par laquelle on peut obtenir ces équations dans tous les cas.

(1) *Comptes rendus*, p. 947 et § I du présent Mémoire.

VII.

Convenons, pour mettre en évidence le déterminant des formes quadratiques dont elles dépendent principalement, de les désigner par

$$F_1(x, \Delta) = 0 \quad \text{lorsque} \quad \Delta \equiv 1 \pmod 4,$$
$$F_2(x, \Delta) = 0 \quad \text{lorsque} \quad \Delta \equiv 2 \pmod 4,$$

le groupe proprement primitif existant seul pour ces deux déterminants. Dans les cas suivants, ce sont les équations qui répondent aux formes du groupe improprement primitif qu'il convient de considérer, et nous les désignerons par

$$\mathcal{F}_1(x, \Delta) = 0 \quad \text{lorsque} \quad \Delta \equiv 3 \pmod 8,$$
$$\mathcal{F}_2(x, \Delta) = 0 \quad \text{lorsque} \quad \Delta \equiv -1 \pmod 8.$$

Cela posé, soit $\Theta(v, u) = 0$ l'équation modulaire pour la transfor-

mation qui se rapporte à un nombre impair n quelconque. En joignant à cette équation celles-ci :

$$1^\circ \qquad u^4 = \frac{\varphi^4 - 1}{\varphi^4 + 1}, \qquad u^8 = x,$$

$$2^\circ \qquad u^4 = -\frac{\varphi^4 - 1}{\varphi^4 + 1}, \qquad u^8 = x,$$

$$3^\circ \qquad u^8 = \frac{1}{1 - \varphi^8}, \qquad u^8 = x,$$

$$4^\circ \qquad u^2 = \frac{1 - \varphi^4}{2\,i\varphi^2}, \qquad u^8 = 1 - x,$$

on en déduira quatre équations en x, dont les premiers membres présenteront cette propriété remarquable d'être le produit de facteurs qui seront respectivement de la forme :

$$\left.\begin{array}{ll} 1^\circ & \mathrm{F}_1(x, \Delta) \\ 2^\circ & \mathrm{F}_2(x, \Delta) \\ 3^\circ & \mathcal{F}_1(x, \Delta) \\ 4^\circ\ x \text{ et } & \mathcal{F}_2(x, \Delta) \end{array}\right\} \Delta \text{ ayant les valeurs } \left\{\begin{array}{l} 2n-1,\ 2n-9,\ 2n-25,\ \ldots, \\ 2n, \qquad 2n-4,\ 2n-16,\ \ldots, \\ 4n-1,\ 4n-9,\ 4n-25,\ \ldots, \\ 8n-1,\ 8n-9,\ 8n-25,\ \ldots. \end{array}\right.$$

Il en résulte que les polynomes $\mathrm{F}_1(x, \Delta)$, $\mathrm{F}_2(x, \Delta)$, $\mathcal{F}_1(x, \Delta)$, $\mathcal{F}_2(x, \Delta)$ s'obtiennent en déterminant le plus grand commun diviseur entre les premiers membres de deux des équations que nous venons de considérer, et répondant à deux valeurs de n, qui seront successivement :

$$1^\circ \qquad \frac{\Delta + \rho^2}{2}, \quad \frac{\Delta + \rho'^2}{2}, \quad \rho \text{ et } \rho' \text{ étant impairs};$$

$$2^\circ \qquad \frac{\Delta + \rho^2}{4}, \quad \frac{\Delta + \rho'^2}{4}, \quad \rho \text{ et } \rho' \text{ étant pairs};$$

$$3^\circ \qquad \frac{\Delta + \rho^2}{4}, \quad \frac{\Delta + \rho'^2}{4}, \quad \rho \text{ et } \rho' \text{ étant impairs};$$

$$4^\circ \qquad \frac{\Delta + \rho^2}{8}, \quad \frac{\Delta + \rho'^2}{8}, \quad \rho \text{ et } \rho' \text{ étant impairs}.$$

Voici ensuite comment, sans changer leur degré, on déduira des deux équations $\mathcal{F}_1(x, \Delta) = 0$, $\mathcal{F}_2(x, \Delta) = 0$, qui se rapportent au groupe improprement primitif, celles qui correspondent au groupe proprement primitif. Dans les deux cas on calculera d'abord la transformée de degré sous-double en $z = \frac{1}{4}\left(x + 2 + \frac{1}{x}\right)$, puis on

y remplacera z par $\left(\frac{x+1}{x-1}\right)^2$, ce qui ramènera au degré primitif (1). Enfin, pour passer des équations relatives au déterminant $-\Delta$ à celles qui concernent le déterminant -4Δ, on fera dans l'équation qui appartient au groupe proprement primitif de formes de déterminant $-\Delta$ la substitution

$$x = \frac{1}{2} + \frac{y+1}{4\sqrt{y}}.$$

Et, si l'on représente les classes de déterminant -4Δ, dont les trois termes ne sont pas pairs en même temps, par des formes $(\mathrm{A}, \mathrm{B}, \mathrm{C})$, où C soit pair, A impair, en posant

$$\mathrm{A}\omega^2 + 2\mathrm{B}\omega + \mathrm{C} = 0,$$

les quantités $\varphi^8(\omega)$ seront précisément les racines de l'équation en y. Elle est d'ailleurs évidemment d'un degré double de l'équation en x, de même que le nombre des classes de déterminant -4Δ, dont il vient d'être question, est double du nombre des classes de déterminant $-\Delta$. L'application plusieurs fois répétée de ce procédé suffirait à donner les équations qui se rapportent aux déterminants multiples d'une puissance de 4. Mais ici il convient de distinguer ceux qui sont le quadruple d'un nombre impair de ceux qui sont multiples de 8. C'est aux premiers que s'applique spécialement la méthode qui vient d'être indiquée; et dorénavant les équations qui leur correspondent seront désignées par $\mathrm{F}_3(x, \Delta) = 0$. En représentant par $\mathrm{F}_4(x, \Delta) = 0$ celles qui concernent les déterminants multiples de 8, on a en effet cette proposition que le premier membre de l'équation en x qui résulte du système

$$\Theta(v, u) = 0, \qquad u^2 = \frac{v^2 - 1}{v^2 + 1}, \qquad u^8 = x,$$

analogue à ceux qui ont été considérés tout à l'heure, est le produit de facteurs de la forme $\mathrm{F}_4(x, \Delta)$, Δ prenant la suite des valeurs $4(n-1)$, $4(n-9)$, $4(n-25)$, etc. Je n'insiste pas en ce moment sur les conséquences à déduire de là, non plus que sur

(1) Ce calcul présente, à l'égard de l'équation $\mathcal{F}_2(x, \Delta) = 0$, la circonstance remarquable que le coefficient de la puissance la plus élevée de x, qui était une puissance de 2, devient dans l'équation transformée égal à l'unité.

beaucoup de questions importantes pour la théorie des formes quadratiques auxquelles conduisent les résultats précédents (1), et je me bornerai à remarquer, que des propositions énoncées sur les réunions d'ordres nommées *groupes proprement* et *improprement primitifs*, on conclut immédiatement les suivantes :

Ayant représenté le système des classes de l'ordre proprement primitif pour un déterminant quelconque par des formes (A, B, C), *où* C *est pair,* A *impair, les quantités* $\varphi^8(\omega)$, *en définissant* ω *par les relations* $A\omega^2 + 2B\omega + C = 0$, *sont racines d'une équation réciproque à coefficients entiers dont le degré est précisément double du nombre des classes.*

Et de même, si l'on représente les classes de l'ordre improprement primitif de déterminant $\Delta \equiv -1 \pmod 8$ *par des formes* (A, B, C), *où* C *est impairement pair, on obtiendra une équation réciproque dont le degré sera encore double du nombre des classes.*

Mais pour l'ordre improprement primitif de déterminant $\equiv 3 \pmod 8$, *le degré est six fois le nombre des classes.*

On peut enfin supposer égal à l'unité le coefficient du premier terme dans ces équations, sauf pour celles qui répondent à l'ordre improprement primitif, où il est une puissance de 2 *lorsque* $\Delta \equiv -1 \pmod 8$.

VIII.

La principale propriété du polynome $\mathcal{F}_1(x, \Delta)$ consiste en ce qu'il se décompose en facteurs du sixième degré de cette forme remarquable

$$(x^2 - x + 1)^3 + \alpha(x^2 - x)^2,$$

de sorte que la substitution $y = \frac{(x^2 - x + 1)^3}{(x^2 - x)^2}$ ramène l'équation $\mathcal{F}_1(x, \Delta) = 0$ à un degré précisément égal au nombre des classes improprement primitives de déterminant $-\Delta$. Cela résulte de ce qu'on peut réunir les racines en groupes, où elles sont représentées

(1) En particulier pour les sommations analogues à celles qui ont été données pour la première fois par M. Kronecker.

par l'expression $\varphi^8\left(\frac{c + d\omega}{a + b\omega}\right)$, a, b, c, d étant des nombres entiers quelconques, tels que $ad - bc = 1$. Or, en faisant $\varphi^8(\omega) = \rho$, cette expression représente les six valeurs distinctes

$$\rho, \quad \frac{1}{\rho}, \quad 1 - \rho, \quad \frac{1}{1 - \rho}, \quad \frac{\rho}{\rho - 1}, \quad \frac{\rho - 1}{\rho},$$

et telles seront les racines de l'équation

$$(x^2 - x + 1)^3 + \alpha(x^2 - x)^2 = 0,$$

car on vérifie immédiatement qu'elle reste la même quand on y remplace x par $\frac{1}{x}$, $1 - x$, et dès lors par les substitutions composées de celles-là, savoir $\frac{1}{1 - x}$, $\frac{x}{x - 1}$, $\frac{x - 1}{x}$. D'ailleurs, ρ étant seul arbitraire, cette équation, qui contient une indéterminée α, aura bien la forme analytique la plus générale. Elle se présente au reste d'elle-même, en recherchant dans les cas les plus simples le polynome $\mathcal{F}_1(x, \Delta)$. Partons, par exemple, des équations modulaires pour $n = 3$ et $n = 5$, auxquelles on doit joindre, d'après ce qui a été dit :

$$u^8 = x = \frac{1}{1 - v^8}.$$

Parmi les diverses formes dont elles sont susceptibles, je choisirai celles que Jacobi obtient en faisant $q = 1 - 2k^2$, $l = 1 - 2\lambda^2$, savoir :

$$(q - l)^4 = 64(1 - q^2)(1 - l^2)(3 + ql),$$
$$(q - l)^6 = 256(1 - q^2)(1 - l^2)[16ql(9 - ql)^2 + 9(45 - ql)(q - l)^2].$$

En effet, ces quantités s'obtiennent immédiatement en x, et en substituant les valeurs

$$q = 1 - 2x, \qquad l = \frac{x + 1}{x - 1},$$

d'où

$$q - l = 2\,\frac{x^2 - x + 1}{1 - x},$$

la première équation donne

$$(x^2 - x + 1)[(x^2 - x + 1)^3 + 2^7(x^2 - x)^2] = 0,$$

et la seconde

$$[(x^2 - x + 1)^3 + 2^7(x^2 - x)^2][(x^2 - x + 1)^3 + 2^7 \cdot 3^3(x^2 - x)^2] = 0.$$

Le facteur commun aux deux cas répond à $\Delta = 11$, et les autres aux déterminants $-3, +19$. Pour $\Delta = 27$, on trouverait

$$(x^2 - x + 1)^3 + 2^7 . 5^3 . 3 (x^2 - x)^2 = 0.$$

En général, lorsque l'ordre improprement primitif de déterminant $-\Delta$ sera formé de la seule classe $\left(2, 1, \frac{\Delta+1}{2}\right)$, α sera un nombre entier qu'on pourra calculer en exprimant que l'équation est vérifiée pour

$$x = \varphi^8(\omega),$$

ou d'après la condition

$$2\omega^2 + 2\omega + \frac{\Delta+1}{2} = 0, \qquad \omega = \frac{-1 + i\sqrt{\Delta}}{2}.$$

Soit donc $q = e^{i\pi\omega}$, on trouvera, en employant l'expression de Jacobi,

$$\sqrt[4]{kk'} = \sqrt{2} . \sqrt[8]{q}\, \frac{\Sigma (-1)^i q^{\lambda i^2 + i}}{\Sigma q^{i^2}},$$

cette valeur où n'entre que q^2 :

$$2^8 \alpha = -\frac{1}{q^2} \frac{(1 + 2^4 . 3 . 5 q^2 + 2^4 . 3^3 . 5 . q^4 + 2^6 . 3 . 5 . 7 . q^6 + \ldots)^3}{(1 - 3 q^2 + 5 q^6 - 6 q^{10} + \ldots)^8},$$

et, par suite, en remarquant que $q^2 = -e^{-\pi\sqrt{\Delta}}$,

$$2^8 . \alpha = e^{\pi\sqrt{\Delta}} - 744 + \frac{196\,880}{e^{\pi\sqrt{\Delta}}} + \ldots.$$

Or, depuis $\Delta = 19$, les termes de la série, à partir du troisième, n'influent plus sur la partie entière, de sorte qu'on a exactement, en désignant par a le nombre entier immédiatement supérieur à $e^{\pi\sqrt{\Delta}}$,

$$\alpha = \frac{a - 744}{2^8}.$$

D'ailleurs ces termes négligés décroissent avec une grande rapidité lorsque Δ augmente; il en résulte que la transcendante numérique $e^{\pi\sqrt{\Delta}}$ approche alors extrêmement d'un nombre entier. Soit, par exemple, $\Delta = 43$, qui donne une seule classe improprement primitive, on trouve

$$e^{\pi\sqrt{43}} = 884\,736\,743{,}999\,777\,5\ldots,$$

et $\alpha = 2^{10} . 3^3 . 5^3$. Les déterminants -67 et -163 sont dans le même cas, de sorte que, dans la quantité $e^{\pi\sqrt{163}}$, la partie décimale commencerait par une suite de douze chiffres égaux à 9.

IX.

L'étude des fonctions $F_1(x, \Delta)$ et $F_2(x, \Delta)$, qui se présentent avec les mêmes propriétés, conduit à des résultats analogues à ceux que nous venons d'indiquer relativement à $\mathcal{F}_1(x, \Delta)$, tandis que $\mathcal{F}_2(x, \Delta)$, qui correspond à l'ordre improprement primitif des classes de déterminant $-\Delta$, dans le cas de $\Delta \equiv -1 \pmod 8$, semble devoir rester entièrement en dehors de cette analogie. Réservant pour un autre moment l'étude de cette fonction, je me bornerai maintenant aux résultats qui concernent les deux premières, et dont voici la principale propriété :

Si l'on excepte les cas de $\Delta = 1$, $\Delta = 2$, l'ensemble de leurs racines peut être décomposé en groupes, qui chacun en comprennent quatre que l'on peut représenter ainsi :

$$\rho, \quad \left(\frac{1 - \sqrt{\rho}}{1 + \sqrt{\rho}}\right)^2, \quad \frac{1}{\rho}, \quad \left(\frac{1 + \sqrt{\rho}}{1 - \sqrt{\rho}}\right)^2.$$

Il s'ensuit qu'elles sont décomposables en facteurs du quatrième degré de cette forme

$$(x + 1)^4 + \alpha x (x - 1)^2,$$

et qu'on peut ramener les deux équations

$$F_1(x, \Delta) = 0, \qquad F_2(x, \Delta) = 0$$

à un degré quatre fois moindre, moitié par conséquent du nombre des classes de déterminant $-\Delta$, par la substitution

$$y = \frac{(x + 1)^4}{x (x - 1)^2}.$$

Les considérations arithmétiques qui conduisent à ce résultat montrent en même temps que le nombre des classes de déterminant $-\Delta$ est toujours pair lorsque $\Delta \equiv 1$ ou $\equiv 2 \pmod 4$, sauf les

exceptions ci-dessus mentionnées de $\Delta = 1$, $\Delta = 2$. S'il se réduit à deux, α sera un nombre entier, qu'on pourra calculer comme il suit :

1°
$$\Delta \equiv 1 \pmod 4.$$

Les deux classes sont alors représentées par les formes réduites

$$(1, 0, \Delta), \qquad \left(2, 1, \frac{\Delta+1}{2}\right),$$

et la première donne l'équation

$$(1, 0, \Delta)_2 = 0,$$

d'où

$$\omega = 1 + i\sqrt{\Delta}.$$

Il suffit donc d'exprimer que

$$(x+1)^3 + \alpha x(x-1)^2 = 0$$

a lieu pour

$$x = \wp^8(\omega),$$

ce qui donne, en faisant $q = e^{i\pi\omega}$,

$$16\alpha = -\left(\frac{1}{q} + 104 + 4\,372q + 96\,256q^2 + \dots\right),$$

et par suite comme, d'après la valeur de ω, $q = -e^{-\pi\sqrt{\Delta}}$,

$$16\alpha = e^{\pi\sqrt{\Delta}} - 104 + \frac{4\,372}{e^{\pi\sqrt{\Delta}}} - \frac{96\,256}{e^{2\pi\sqrt{\Delta}}} + \dots.$$

Or depuis $\Delta = 9$, on peut se borner aux deux premiers termes de cette suite, et, si l'on désigne par a le nombre entier immédiatement supérieur à $e^{\pi\sqrt{\Delta}}$, on aura exactement

$$\alpha = \frac{a - 104}{16}.$$

Les déterminants, qui ne donnent ainsi que deux classes dans l'ordre primitif et auxquels on pourra appliquer cette formule, sont

$$-5, \quad -9, \quad -13, \quad -25, \quad -37, \quad \text{etc.}$$

Par la méthode algébrique indiquée dans un précédent article

(voyez *Comptes rendus*, t. XLVIII, p. 1097 et § VII du présent Mémoire), on obtient les résultats suivants que l'emploi de la formule pourra servir à vérifier, savoir :

$$\begin{aligned}
&(x+1)^3 + 2^6 x \quad (x-1)^2 = 0 \qquad \Delta = 5,\\
&(x+1)^3 + 3.2^8 x \quad (x-1)^2 = 0 \qquad \Delta = 9,\\
&(x+1)^3 + 3^4.2^6 x \quad (x-1)^2 = 0 \qquad \Delta = 13,\\
&(x+1)^3 + 5.3^4.2^7 x(x-1)^2 = 0 \qquad \Delta = 25.
\end{aligned}$$

2°
$$\Delta \equiv 2 \pmod 4.$$

Les deux classes, qu'on suppose seules exister, sont représentées par les formes

$$(1, 0, \Delta), \qquad \left(2, 0, \frac{1}{2}\Delta\right);$$

à la première correspond la valeur

$$\omega = i\sqrt{\Delta},$$

d'où

$$q = e^{-\sqrt{\Delta}},$$

et, tout à fait comme précédemment, on est conduit à l'expression

$$16\alpha = -\left(e^{\pi\sqrt{\Delta}} + 104 + \frac{4\,372}{e^{\pi\sqrt{\Delta}}} + \frac{96\,256}{e^{2\pi\sqrt{\Delta}}} + \dots\right).$$

En désignant encore par a le nombre entier immédiatement supérieur à $e^{\pi\sqrt{\Delta}}$, on aura la formule

$$\alpha = -\frac{a + 104}{16},$$

qui sera applicable à partir de $\Delta = 10$.

Les déterminants qui ne fournissent que deux classes dans l'ordre primitif seront

$$-6, \quad -10, \quad -18, \quad -22, \quad -58, \quad \text{etc.};$$

si on les joint aux précédents, ainsi qu'à ceux dont il a déjà été question à propos du polynome $\mathfrak{F}_1(x, \Delta)$, on aura autant de cas dans lesquels la quantité $e^{\pi\sqrt{\Delta}}$ approche d'autant plus d'un nombre entier que Δ sera plus grand; ainsi, par exemple, dans la quantité $e^{\pi\sqrt{58}}$ la partie décimale commence par neuf chiffres égaux à 9.

Voici les équations auxquelles on parvient, comme on va le voir, par la méthode algébrique générale, savoir :

$$x^2 - 6x + 1 = 0 \qquad \Delta = 2,$$
$$(x+1)^4 - 3^2.2^4.x \quad (x-1)^2 = 0 \qquad \Delta = 6,$$
$$(x+1)^4 - 5^2.2^2.x \quad (x-1)^2 = 0 \qquad \Delta = 10,$$
$$(x+1)^6 - 7^2.2^4.x \quad (x-1)^2 = 0 \qquad \Delta = 18,$$
$$(x+1)^6 - 11^2.3^4.2^4x(x-1)^2 = 0 \qquad \Delta = 22.$$

On remarquera que le coefficient numérique $-\alpha$ est toujours un carré divisible par Δ, sauf le cas du déterminant -18, le seul qui, n'étant pas le double d'un nombre premier, ne renferme cependant que deux classes dans l'ordre primitif. Mais, lorsqu'on a $\Delta \equiv 1 \pmod 4$, c'est la quantité $\alpha + 16$ qui contient Δ en facteur lorsqu'il est un nombre premier, et le quotient $\frac{\alpha+16}{\Delta}$ se présente toujours comme égal à un carré. La même circonstance se remarque dans les équations

$$(x^2 - x + 1)^3 + \alpha(x^2 - x)^2 = 0;$$

à l'égard de la quantité $4\alpha + 27$ (1), qui est également le produit de Δ par un carré, lorsque Δ est un nombre premier.

X.

Le calcul des polynomes $F_1(x, \Delta)$ et $F_2(x, \Delta)$ repose, comme il a été dit, sur la formation de l'équation qui résulte du système

$$\Theta(v, u) = 0, \qquad u^4 = \frac{v^4 - 1}{v^4 + 1},$$

ou

$$\Theta(v, u) = 0, \qquad u^4 = -\frac{v^4 - 1}{v^4 + 1},$$

(1) L'identité

$$4[(x^2 - x + 1)^3 + \alpha(x^2 - x)^2] = (2x^3 - 3x^2 - 3x + 2)^2 + (4\alpha + 27)(x^2 - x)^2$$

en montre l'origine et donne en même temps une résolution facile des équations $\mathcal{F}_1(x, \Delta) = 0$, lorsqu'elles sont du 6e degré.

en faisant $u^8 = x$ (1). Les quantités Δ, qui répondent dans les deux cas aux valeurs de n pour lesquelles on possède l'équation modulaire, sont indiquées dans ce Tableau :

n.	$\Delta \equiv 1 \pmod 4$.	$\Delta \equiv 2 \pmod 4$.
3	5	2, 6
5	1, 9	6, 10
7	5, 13	10, 14
11	13, 21	6, 18, 22
13	1, 17, 25	10, 22, 26
17	9, 25, 33	18, 30, 34
19	13, 27, 39	2, 22, 34, 38

On y remarque que $n = 11$ conduit à trois déterminants $\equiv 2 \pmod 4$, auxquels correspondent seulement deux classes dans l'ordre primitif, le déterminant -18 fournissant en outre une classe dérivée de $(1, 0, 2)$. Ce cas donnera donc les polynomes $F_2(x, \Delta)$ pour les valeurs $\Delta = 2, 6, 18, 22$, et nous le choisirons comme exemple de la marche qu'on peut suivre dans ce genre de calcul.

J'observe à cet effet qu'en disposant dans un ordre convenable les termes de l'équation donnée par M. Sohnke, on peut l'écrire

$$\begin{aligned} &v^{12} - u^{12} + 44u^6v^6(v^4 - u^4) + 165u^4v^4(v^4 - u^4) \\ &\quad + 44u^2v^2(v^4 - u^4) + 32v^{11}v^{11} - 22u^3v^3(v^8 + u^8) + 88u^9v^9 \\ &\quad + 132u^7v^7 - 132u^5v^5 - 88u^3v^3 + 22uv(v^8 + u^8) - 32uv = 0. \end{aligned}$$

ou bien, en mettant en évidence le facteur $v^4 - u^4$,

$$\begin{aligned} &(v^4 - u^4)(v^8 + u^8 + 44u^6v^6 + 166u^4v^4 + 44u^2v^2) \\ &\quad + 32u^{11}v^{11} - 22u^3v^3(v^8 + u^8) + 88u^9v^9 + 132u^7v^7 \\ &\qquad - 132u^5v^5 - 88u^3v^3 + 22uv(v^8 + u^8) - 32uv = 0. \end{aligned}$$

(1) Le système

$$\Theta(v, u) = 0, \qquad v = \frac{e^{\frac{i\pi}{8}}}{u}, \qquad u^8 = x$$

donne aussi une équation en x dont le premier membre est le produit de facteurs qui sont tous de la forme $F_1(x, \Delta)$ ou $F_2(x, \Delta)$. Le premier cas a lieu lorsque le nombre n, qui désigne l'ordre de la transformation à laquelle se rapporte l'équation modulaire, est $\equiv 1 \pmod 4$, et alors

$$\Delta = n - \rho^2,$$

ρ étant impair. Si $n \equiv -1 \pmod 4$, ce sont les facteurs $F_2(x, \Delta)$ qui se présentent, Δ étant encore $n - \rho^2$, mais ρ devant être supposé pair.

Or en faisant $uv = w$, la relation

$$u^4 = -\frac{v^4 - 1}{v^4 + 1},$$

ou

$$u^4 v^4 + u^4 + v^4 - 1 = 0,$$

donne

$$v^4 + u^4 = 1 - w^4,$$
$$v^8 - u^8 = 1 - 4w^4 + w^8,$$
$$v^4 - u^4 = \sqrt{1 - 6w^4 + w^8};$$

de sorte qu'on peut immédiatement déduire de l'équation modulaire une relation contenant seulement w, savoir :

$$\sqrt{1 - 6w^4 + w^8}\,(w^8 + 44w^6 + 162w^4 + 44w^2 + 1) + 10w(w^{10} + 11w^8 + 22w^6 - 22w^4 - 11w^2 - 1) = 0.$$

Or, en faisant disparaître le radical on parvient à une équation réciproque en w^2, ce qui conduit à poser

$$w^2 + \frac{1}{w^2} = z,$$

et l'on trouve ainsi

$$(z^2 - 8)(z^2 + 44z + 160)^2 - 100(z - 2)(z^2 + 12z + 32)^2 = 0$$

ou

$$z(z + 4)^2(z - 20)(z^2 + 192) = 0.$$

Maintenant nous observerons qu'en faisant $u^8 = x$, on a

$$w^4 = \sqrt{x}\,\frac{1 - \sqrt{x}}{1 + \sqrt{x}} \quad \text{et} \quad w^4 + \frac{1}{w^4} - 2 = -\frac{(x + 1)^2}{\sqrt{x}(x - 1)}.$$

Ainsi l'expression $\frac{(x+1)^4}{x(x-1)^2}$ dont il a été déjà parlé comme entrant essentiellement dans la composition des équations que nous voulons obtenir, se présente ici d'elle-même, et, puisque

$$w^4 + \frac{1}{w^4} - 2 = z^2 - 4,$$

la quantité α sera liée à z par cette relation très simple

$$\alpha = -(z^2 - 4)^2.$$

Il en résulte que l'équation en x est le produit des facteurs suivants :

$$(x+1)^4 - 2^4 x(x-1)^2, \qquad [(x+1)^4 - 3^2 \cdot 2^4 x(x-1)^2]^2,$$
$$[(x+1)^4 - 7^4 \cdot 2^4 x(x-1)^2]^2$$

et

$$(x+1)^4 - 11^2 \cdot 3^4 \cdot 2^4 x(x-1)^2,$$

le dernier, qui répond à la valeur la plus élevée de Δ, étant le seul qui n'entre pas au carré, car

$$(x+1)^4 - 2^4 x(x-1)^2 = (x^2 - 6x + 1)^2.$$

Et, comme ils sont écrits en suivant l'ordre des valeurs croissantes de la quantité α, ils correspondent respectivement à $\Delta = 2, 6, 18, 22$, puisque, abstraction faite du signe, α augmente avec Δ d'après la relation

$$16\alpha = -\left(e^{\pi\sqrt{\Delta}} + 104 + \ldots\right).$$

XI.

Le polynome $\mathcal{F}_2(x, \Delta)$, dans le cas le plus simple où l'on a $\Delta = 7$, s'obtient immédiatement par les équations fondamentales

$$u^2 = \frac{1 - v^4}{2v^2}, \qquad u^8 = 1 - x,$$

en supposant $v = u$, et supprimant dans le résultat le facteur x. On trouve ainsi l'équation

$$16x^2 - 31x + 16 = 0.$$

Pour les valeurs suivantes de Δ, le calcul devient plus difficile, et c'est en recourant à des méthodes particulières que le P. Joubert, dans un travail important sur le discriminant des équations en

$$U = \sqrt[4]{kk'} \qquad \text{et} \qquad V = \sqrt[4]{\lambda\lambda'},$$

a réussi à obtenir ces polynomes pour $\Delta = 15, 23, 31$. Je me bornerai à donner l'idée de ces procédés et des méthodes variées qu'on peut suivre dans ces recherches en considérant le cas de $\Delta = 15$.

Alors on a, dans l'ordre improprement primitif, deux formes conduisant aux équations types

$$(2,\ 1,\ 8)_1 = 0, \qquad (4,\ 1,\ 4)_2 = 0;$$

et, si l'on fait pour un instant

$$(4,\ 1,\ 4) = 0 \quad \text{ou} \quad 2\omega^2 + \omega + 2 = 0 \quad \text{et} \quad \xi = \varphi^2(\omega)\psi^2(\omega),$$

on trouvera très aisément l'équation en ξ, en remarquant qu'on peut écrire

$$2\omega + 1 = -\frac{2}{\omega},$$

d'où

$$\psi(2\omega + 1) = \psi\left(-\frac{2}{\omega}\right) = \varphi\left(\frac{2}{\omega}\right),$$

et, par suite, en élevant à la puissance quatrième,

$$\frac{1 + \psi^4(\omega)}{2\psi^2(\omega)} = \frac{2\varphi^2(\omega)}{1 + \varphi^4(\omega)}.$$

Comme on a d'ailleurs

$$[\varphi^4(\omega) + \psi^4(\omega)]^2 = 1 + 2\xi^2,$$

on trouvera

$$1 + \xi^2 + \sqrt{1 + 2\xi^2} = 4\xi,$$

ce qui donne

$$(\xi - 2)(\xi^2 - 6\xi + 4) = 0.$$

Le facteur du second degré convient seul, et l'on en tire l'équation en x, en remarquant qu'on doit supposer

$$x = \varphi^8(\omega + 1) = \frac{\varphi^8(\omega)}{\varphi^8(\omega) - 1},$$

de sorte qu'on aura

$$\xi^4 = -\frac{x}{(x-1)^2},$$

et, par suite,

$$2^8(x-1)^4 + 2^4 \cdot 47x(x-1)^2 + x^2 = 0.$$

Cette équation, conformément à ce qu'on a dit en général, a pour coefficient de x^4 une puissance de 2, et la forme particulière sous laquelle elle se présente permettra d'en déduire très facilement la transformée, qui correspond à l'ordre proprement primitif (1), savoir :

$$(x-1)^4 + 2^8 \cdot 47x(x-1)^2 + 2^{16}x^2 = 0,$$

et de vérifier ainsi que dans cette transformée le coefficient de la puissance de x redevient égal à l'unité.

XII.

Nous possédons maintenant tous les éléments qui figurent dans le discriminant de l'équation modulaire du 12e degré, qui sont les facteurs relatifs à l'ordre improprement primitif de déterminant -7, et à l'ordre primitif de déterminant -24. Le premier, comme on vient de le trouver, est $16x^2 - 31x + 16$. Le second doit être tiré de l'équation

$$(x+1)^4 - 3^2 \cdot 2^4 x(x-1)^2 = 0,$$

qui correspond au déterminant -6, en y remplaçant x par

$$\frac{1}{2} + \frac{x+1}{4\sqrt{x}},$$

et faisant disparaître $\sqrt{x}$ par l'élévation au carré. On trouve ainsi l'expression

$$x^8 - 301\,960x^7 + 3\,550\,492x^6 - 2\,178\,232x^5 - 1\,092\,026x^4 - 2\,178\,232x^3 + 3\,550\,492x^2 - 301\,960x + 1 = 0;$$

ce qui conduit au résultat déjà donné, et qu'il eût été bien difficile, comme on voit, de tirer algébriquement de l'équation modulaire. Il ne me reste plus, pour terminer cette partie de mes recherches, qu'à indiquer un moyen de le vérifier, ce qui sera l'objet d'un prochain article.

XIII.

En désignant par D le produit des carrés des différences des racines de l'équation modulaire $\Theta(v, u) = 0$ de degré $n + 1$, lors-

(1) Voyez *Comptes rendus*, t. XLVIII, p. 1098 et § VII du présent Mémoire.

qu'on suppose n un nombre premier, faisons, pour un instant,

$$\mathfrak{D} = \sqrt{(-1)^{\frac{n-1}{2}} \frac{\mathrm{D}}{n^n}}.$$

Cette expression sera non seulement rationnelle et entière en u, puisque D est un carré parfait, mais les coefficients des diverses puissances de u seront eux-mêmes des nombres entiers. Or, en remplaçant ces puissances par leurs expressions sous forme de séries infinies en fonction de $q = e^{i\pi\omega}$, on parvient à un résultat dont la valeur, par rapport au module premier n, s'obtient comme il suit.

Faisons

$$f(q) = \frac{(1+q^2)(1+q^4)(1+q^6)\dots}{(1-q)(1+q^2)(1+q^5)\dots} = 1 - q + 2q^2 - 3q^3 + 4q^4 - 6q^5 + \dots$$

et, par conséquent,

$$u = \varphi(\omega) = \sqrt{2}\sqrt[8]{q} f(q),$$

on aura cette congruence

$$\mathfrak{D} \equiv 2^{\frac{n^2-1}{4}} (\sqrt{2}\sqrt[8]{q})^{\frac{n+1}{2}} [f(q) + 8q f'(q)]^{\frac{n-1}{2}} \left[f(q) - \left(\frac{2}{n}\right) q^{\frac{n^2-1}{8}} f(q^{n^2}) \right] \bmod n,$$

dans laquelle le coefficient de la puissance la moins élevée de q a été conservé sans addition ni suppression de multiples de n, ce qui permet de déterminer le facteur numérique qui doit être joint aux divers polynomes en u, que maintenant nous connaissons dans les cas de $n = 3, 5, 7, 11$, afin d'obtenir précisément la valeur de $\mathfrak{D}$. Ce facteur, comme on voit, est toujours une puissance de 2; ainsi, dans le cas de $n = 11$, on aura

$$\mathfrak{D} = 2^{26} u^6 (1 - u^8)^5 (16 - 31u^8 + 16u^{16})(1 - 301\,960 u^8 + \dots).$$

On pourrait aussi présenter le second membre de la congruence précédente sous cette autre forme

$$2^{\frac{n^2-1}{4}} \left(\frac{8}{i\pi} \frac{d\varphi}{d\omega}\right)^{\frac{n-1}{2}} \left[\varphi(\omega) - \left(\frac{2}{n}\right) \varphi(n^2\omega) \right];$$

mais c'est la première qu'il convient d'employer pour vérifier,

comme nous l'avons annoncé, le discriminant de l'équation modulaire du douzième degré. Je remarque à cet effet que le polynome

$$1 - 301\,960 u^8 + 3\,556\,492 u^{16} + \dots$$

se réduit suivant le module 11 à cette expression simple

$$1 + u^8 - u^{24} - u^{32} - u^{40} + u^{56} + u^{64}$$

et qu'on trouvera par suite

$$\mathfrak{D} \equiv u^6 (1 + 3u^8 - 3u^{24} - 3u^{32} + u^{40} + \dots) \pmod{11}.$$

Maintenant, si l'on met à la place des diverses puissances de u leurs développements en fonctions de q, il viendra

$$\mathfrak{D} \equiv (\sqrt{2}\sqrt[8]{q})^6 (1 - 2q + 4q^2 + 3q^3 + 4q^4 + 3q^5 + \dots).$$

Or, c'est précisément le résultat auquel conduit la congruence, en faisant les développements indiqués, d'où résulte la vérification que nous désirions obtenir.

XIV.

C'est à ce point que je me suis arrêté jusqu'ici dans l'étude des équations modulaires, et il ne me reste plus, en considérant en particulier celles du sixième, du huitième et du douzième degré, qu'à donner la méthode que j'ai suivie pour en déduire des réduites d'un degré moindre d'une unité. Galois, ainsi que je l'ai déjà dit au commencement de ces recherches, a le premier découvert le fait si remarquable de cette réduction, au double point de vue de la théorie des fonctions elliptiques et de l'Algèbre, et voici, dans ses idées, le théorème qui sert de principe fondamental.

Remarquons préalablement que les racines de l'équation modulaire sont représentées par

$$v = u^n [\sin \operatorname{coam} 2\rho \sin \operatorname{coam} 4\rho \dots \sin \operatorname{coam}(n-1)\rho],$$

en faisant

$$\rho = \frac{m\mathrm{K} + m' i\mathrm{K}'}{n},$$

où m et m' sont deux nombres entiers qu'on peut multiplier par un même facteur sans changer la valeur de ω. Il en résulte que c'est uniquement le rapport $\frac{m'}{m}$ qui définit chaque racine, et, comme les deux termes sont pris suivant le module n, il reçoit d'une part la valeur ∞ pour $m \equiv 0$, et de l'autre la série des n nombres entiers $0, 1, 2, \ldots, n-1$. On est donc conduit naturellement, pour représenter les racines de l'équation modulaire, à la notation ω_k, k désignant $\frac{m'}{m}$ et devant représenter les $n+1$ valeurs ∞, 0, 1, 2, ..., $n-1$. Cela posé, voici la proposition de Galois :

Toute fonction rationnelle non symétrique des racines ω_k qui ne change pas en remplaçant les divers indices k par $\frac{ak+b}{ck+d}$, a, b, c, d étant des nombres entiers pris suivant le module n et le déterminant $ad-cb$ n'étant pas $\equiv 0$ (1), *sera exprimable en fonction rationnelle de u* (2).

J'ajouterai la remarque que ce théorème subsiste en particularisant la substitution $\frac{ak+b}{ck+d}$, de manière que $ad-bc$ soit résidu quadratique de n, pourvu qu'on s'adjoigne le radical

$$\sqrt{(-1)^{\frac{n-1}{2}} n}.$$

Tel est, par exemple, le produit des différences des racines $\Pi(\omega_k - \omega_{k'})$, qui change de signe ou se reproduit exactement, lorsqu'en remplaçant k par $\frac{ak+b}{ck+d}$, $ad-bc$ est non résidu ou résidu quadratique de n, et qui s'exprime, comme on l'a vu au paragraphe XIII, par une fonction rationnelle de u à coefficients entiers, mais affectée du facteur

$$\sqrt{(-1)^{\frac{n-1}{2}} n}.$$

En effet, nommant F et F′ les deux valeurs que peut prendre une

(1) M. Serret a fait des substitutions de cette forme l'objet de ses recherches dans plusieurs articles publiés dans les *Comptes rendus*, t. XLVIII, séances des 10, 17, et 24 janvier 1859.

(2) Une démonstration de ce théorème important a été donnée par le P. Joubert dans un travail que j'ai déjà cité (*Comptes rendus*, t. XLVI, p. 718).

fonction rationnelle des racines invariable par les substitutions où $ad-bc$ est résidu, les deux expressions $F+F'$, $\frac{F-F'}{\Pi(\omega_k - \omega_{k'})}$ resteront invariables pour la totalité des substitutions, et s'exprimeront rationnellement en u, d'après la proposition de Galois; il en résulte que F et F′ s'exprimeront elles-mêmes sous la forme annoncée.

Ce point essentiel établi, la question de l'abaissement des équations modulaires à un degré moindre d'une unité dépend d'une étude plus approfondie des substitutions $\frac{ak+b}{ck+d}$, et dont quelques traces seulement subsistent dans ce qui nous a été conservé des travaux de Galois. C'est en suivant la voie qu'elles indiquent que M. Betti a retrouvé l'importante proposition relative aux équations du sixième, du huitième et du douzième degré, et l'extrait suivant d'une Lettre que m'a fait l'honneur de m'adresser ce savant géomètre montrera comment de cette manière se présentent les résultats auxquels de mon côté je parvenais par une méthode toute différente :

« Pise, 24 mars 1859.

» Dans un Mémoire *Sopra l'abassamento dell' equazioni modulari*, publié en 1853 dans les *Annali di Tortolini*, j'ai fait l'étude des substitutions

$$\frac{ak+b}{ck+d}, \tag{1}$$

pour démontrer la possibilité de l'abaissement des équations modulaires, et j'ai obtenu les résultats que vous me communiquez dans votre Lettre.

» Voici pour le module premier $n = 4p+3$ les expressions que j'ai trouvées alors pour la décomposition en n groupes du groupe dont toutes les substitutions sont données par la forme (1) où $ad-bc$ est résidu de n.

» Si g est une racine primitive de n, jouissant de cette propriété que, $g-1$ étant résidu de n, les puissances impaires $< n-2$ de g vérifient la congruence

$$[g^2x^2 - g(g+1)x + 1][g^2x^2 - (g+1)x + 1] \equiv 0 \pmod{n}$$

(ce qui n'arrive que pour $n = 7, 11$), on aura, si l'on fait

$$\theta(k) = g^{2\delta}\,\frac{k - g^{2\alpha+1}}{k - g^{2\alpha}},\quad g^{2\delta+1}\,\frac{k - g^{2\alpha}}{k - g^{2\alpha+1}},\quad g^{2\delta}k,\quad \frac{g^{2\delta+1}}{k},$$

un groupe $[k, \theta(k)]$ de $\frac{(n+1)(n-1)}{2}$ substitutions de la forme (1) telles, qu'en faisant sur ce groupe les substitutions $(k, k+i)$ on obtient n groupes, dont l'ensemble est le groupe proposé.

» Or si $n = 7$ on a deux racines primitives $g = 3$, $g = 5$; $5 - 1$ est résidu de 7 et les deux puissances impaires de 5 inférieures à 5, c'est-à-dire 5, 5^3 vérifient la congruence

$$(2x^2 + 2x + 1)(4x^2 + x + 1) \equiv 0 \pmod 7.$$

» Donc, lorsque $n = 7$, on a deux systèmes de valeurs pour $\theta(k)$, à savoir :

$$\theta(k) \equiv a\,\frac{k - 3b}{k - b},\quad -a\,\frac{k - b}{k - 3b},\quad ak,\quad \frac{-a}{k}$$

en prenant $g = 3$, et

$$\Im(k) \equiv a\,\frac{k + 2b}{k + b},\quad -a\,\frac{k + b}{k + 2b},\quad ak,\quad \frac{-a}{k},$$

en prenant $g = 5$, a et b désignant des résidus de 7.

» Si $n = 11$, on a quatre racines primitives : $2, 6, 7, 8$; $2 - 1$ est résidu de 11 et les puissances de 2, impaires et inférieures à 9, vérifient la congruence

$$(4x^2 - 6x + 1)(4x^2 - 3x + 1) \equiv 0 \pmod{11}.$$

De même, $6 - 1$ est résidu de 11 et les puissances de 6 impaires et inférieures à 9 vérifient la congruence

$$(3x^2 + 2x + 1)(3x^2 + 4x + 1) \equiv 0 \pmod{11}.$$

» Or, si l'on prend $g = 2$, a et b résidus de 11, on aura

$$\theta(k) \equiv a\,\frac{k - 2b}{k - b},\quad -a\,\frac{k - b}{k - 2b},\quad ak,\quad \frac{-a}{k},$$

et, si l'on prend $g = 6$,

$$\Im(k) \equiv a\,\frac{k - 6k}{k - b},\quad -a\,\frac{k - b}{k - 6b},\quad ak,\quad \frac{-a}{k}.$$

» Les racines primitives 7 et 8 ne jouissent pas de la propriété de rendre $g - 1$ résidu de 11, et la congruence lorsqu'on y fait $g = 7$, 8 n'est pas satisfaite par les puissances de 7 et 8 impaires et inférieures à 9.

» Les substitutions $\theta(k)$, $\Im(k)$ jouissent de la propriété d'être à lettres conjointes, c'est-à-dire qu'en divisant les lettres en systèmes de deux lettres chacune de la manière suivante :

$$v_0 v_\infty,\quad v_{g^0} v_{g^1},\quad v_{g^2} v_{g^3},\quad \ldots,\quad v_{g^{2\alpha}} v_{g^{2\alpha+1}},\quad \ldots,$$

toute substitution $\theta(k)$, $\Im(k)$, ou échange entre elles les lettres d'un système, ou change un système dans un autre.

» Dans le cas de $n = 5$ j'avais obtenu des résultats semblables aux précédents et formé un groupe de douze permutations en considérant les trois substitutions

$$\theta(k) \equiv 4k,\quad \frac{1}{k},\quad 3\,\frac{k+1}{k-1},$$

et celles qu'on en déduit en les composant entre elles.... »

XV.

C'est sous un point de vue bien différent que je vais maintenant traiter les mêmes questions. Ainsi, laissant de côté toute considération relative aux décompositions de groupes, je définis, *a priori*, pour $n = 5, 7, 11$, les racines z des équations réduites du cinquième, du septième et du onzième degré, de cette manière, savoir :

$$\begin{aligned}
n = 5,\quad & z_i = (v_\infty - v_i)(v_{1+i} - v_{4+i})(v_{2+i} - v_{3+i}),\\
n = 7,\quad & z_i = (v_\infty - v_i)(v_{1+i} - v_{5+i})(v_{2+i} - v_{3+i})(v_{4+i} - v_{6+i}),\\
n = 11,\quad & z_i = (v_\infty - v_i)(v_{1+i} - v_{2+i})(v_{4+i} - v_{8+i})(v_{3+i} - v_{6+i})\\
& \qquad\qquad (v_{9+i} - v_{7+i})(v_{5+i} - v_{10+i}),
\end{aligned}$$

les indices i devant être pris respectivement suivant le module n. De la sorte on obtient trois systèmes de n fonctions rationnelles des racines v, et je vérifie que les quantités qu'ils comprennent ne font que s'échanger entre elles lorsqu'on fait respectivement ces

substitutions

$$n = 5 \quad \begin{pmatrix} v_k \\ v_{4k} \end{pmatrix},$$

$$n = 7 \quad \begin{pmatrix} v_k \\ v_{2k} \end{pmatrix},$$

$$n = 11 \quad \begin{pmatrix} v_k \\ v_{4k} \end{pmatrix}.$$

Il en résulte, par des compositions successives, que ces systèmes demeurent invariables pour les substitutions $\begin{pmatrix} v_k \\ v_{ak} \end{pmatrix}$, où a est un résidu quadratique quelconque de n. Maintenant il est visible qu'ils ne changent pas non plus lorsqu'on fait la substitution $\begin{pmatrix} v_k \\ v_{k+1} \end{pmatrix}$; et si l'on vérifie encore qu'il en est de même à l'égard de celle-ci $\begin{pmatrix} v_k \\ v_{-\frac{1}{k}} \end{pmatrix}$, on arrivera à cette conclusion qu'ils demeurent invariables pour toutes les substitutions où l'on met, au lieu de k, $\frac{ak+b}{ck+d}$, $ad - bc$ étant résidu de n. En effet, cette expression, dans toute sa généralité, s'obtient en composant entre elles celles que nous venons de considérer. Le théorème du paragraphe XIV suffit donc pour nous assurer que les équations réduites en z auront pour coefficients des fonctions rationnelles de u, où ne figureront d'irrationnelles, suivant les cas, que les radicaux $\sqrt{5}$, $\sqrt{-7}$, $\sqrt{-11}$.

Si l'on cherche maintenant les substitutions spéciales $\begin{pmatrix} v_k \\ v_{\theta(k)} \end{pmatrix}$ qui laisseront invariable une seule des racines considérée isolément, z_0 par exemple, on trouvera aisément ces résultats, où a et b désignent des résidus quadratiques de n, savoir :

$$n = 5 \quad \theta(k) \equiv ak, \quad \frac{-a}{k}, \quad a\frac{k+b}{k-b}, \quad -a\frac{k-b}{k+b},$$

$$n = 7 \quad \theta(k) \equiv ak, \quad \frac{-a}{k}, \quad a\frac{k+2b}{k+b}, \quad -a\frac{k+b}{k+2b},$$

$$n = 11 \quad \theta(k) \equiv ak, \quad \frac{-a}{k}, \quad a\frac{k-2b}{k-b}, \quad -a\frac{k-b}{k-2b}.$$

Ce sont les expressions auxquelles M. Betti est arrivé par une autre voie, et qui forment en général $\frac{n^2-1}{2}$ substitutions conjuguées, de sorte que toutes les quantités $\frac{ak+b}{ck+d}$, où $ad - bc$ est résidu quadratique de n, peuvent être ainsi représentées :

$$\theta(k+i),$$

i étant un nombre entier pris suivant le module n.

Enfin, si l'on désigne par $z_{\varphi(i)}$ ce que devient z_i lorsqu'on effectue sur les racines v les substitutions que nous avons considérées, on trouvera, pour $n = 5$,

$$\varphi(i) \equiv ai + b \equiv \quad (ai+b)^3 + c,$$

pour $n = 7$,

$$\varphi(i) \equiv ai + b \equiv -(ai+b)^5 - 2(ai+b)^2 + c,$$

pour $n = 11$,

$$\varphi(i) \equiv ai + b \equiv \quad (ai+b)^9 + 3(ai+b)^5 + c,$$

b et c étant des nombres entiers quelconques pris suivant le module n, et a étant résidu quadratique, ce qui représente en général $\frac{n(n^2-1)}{2}$ substitutions distinctes.

Les équations du septième et du onzième degré présentant cette propriété que les fonctions non symétriques de leurs racines invariables par les substitutions ainsi définies ont une valeur rationnelle, constituent un ordre spécial d'irrationalité qui les distingue nettement des équations les plus générales de ces degrés. Ce sont, suivant l'expression de M. Kronecker, des équations douées d'*affections*, et qu'il sera sans doute possible de ramener analytiquement à celles dont la théorie des fonctions analytiques a donné la première notion. Mais, laissant de côté les belles et difficiles questions auxquelles conduit ce sujet, et que M. Kronecker a le premier abordées, je me bornerai à faire voir que $\left\{ \begin{matrix} z_i \\ z_{\varphi i} \end{matrix} \right\}$ représente bien, en attribuant à la fonction φi toutes les valeurs, un système de substitutions conjuguées. Posons en effet, pour un instant,

$$\chi(i) \equiv -i^3 - 2i^2,$$

de sorte qu'on ait, pour $n = 7$,

$$\varphi(i) \equiv ai + b \equiv \chi(ai+b) + c;$$

on vérifie sans peine que

$$\left.\begin{aligned} a\chi(i) &\equiv \chi(a^2 i) \\ \chi[\chi(i)] &\equiv i \\ \chi[a\chi(i)+b] &\equiv 2ab^4\chi\left(i+\frac{2}{a^2 b}\right)+\text{const.} \end{aligned}\right\} \bmod 7,$$

a étant supposé résidu de 7. Et faisant de même, pour $n=11$,

$$\chi(i) \equiv i^9 - 3i,$$

on aura

$$\left.\begin{aligned} a\chi(i) &\equiv \chi(a^4 i) \\ \chi[\chi(i)] &\equiv i \\ \chi[a\chi(i)+b] &\equiv 9ab^8\chi\left(i+\frac{2}{a^2 b}\right)+\text{const.} \end{aligned}\right\} \bmod 11,$$

a étant résidu de 11.

Ainsi les fonctions $\chi(ai+b)$, comme les expressions plus simples $ai+b$, se reproduisent par la composition. De là résulte, pour les nombres premiers $n=7$, 11, l'existence de fonctions de n lettres ayant $\frac{1.2.3\ldots n}{\frac{1}{2}n(n^2-1)}$, c'est-à-dire 30 et 60480 valeurs. Toutes deux ont été rencontrées par M. Kronecker, qui a le premier publié (*Comptes rendus des séances de l'Académie de Berlin*, 22 avril 1858) le cas des fonctions de sept lettres, et fait à l'égard de la représentation analytique des substitutions ici employée [1] une observation pleine de justesse, montrant de quelle manière deux expressions algébriquement différentes peuvent cependant ne représenter que la même substitution, et par là réduisant à un seul et même type deux systèmes que j'avais d'abord considérés comme distincts. (*Voyez* les *Annali di Matematica*, année 1859, nos 1 et 2 et *C. R.*, t. XLVI, p. 879).

---

[1] Les expressions dans le cas des substitutions de cinq lettres, savoir :

$$z_i, \quad z_{ai+b}, \quad z_{(ai+b)^2+c},$$

ont été données avant moi par M. Betti dans le tome II des *Annales de Tortolini*, p. 17. Pour le cas de sept lettres, voyez les *Annali di Matematica*, année 1859, n° 1.

XVI.

Le calcul des équations réduites en z pour les trois valeurs de n que nous avons à considérer repose sur deux remarques : que l'on peut y remplacer d'une part u par εu et z par $\varepsilon^{\frac{n(n+1)}{2}} z$, ε étant une racine huitième de l'unité; et de l'autre, u par $\frac{1}{u}$ et z par

$$\frac{z}{u^{n+1}}(-1)^{\frac{n^2-1}{8}+\frac{n+1}{2}}.$$

La première, jointe à cette observation que le développement des racines en fonctions de q commence par

$$\left(\sqrt{2}\sqrt[8]{\frac{1}{q^n}}\right)^{\frac{n+1}{2}},$$

prouve que les coefficients sont des polynomes en u^8 contenant en facteur une certaine puissance de u; ainsi ces équations sont composées de termes de cette forme

$$z^{n-\nu} u^{\alpha_\nu}(a+bu^8+cu^{16}+\ldots+hu^{8\rho_\nu}),$$

et l'exposant α_ν se détermine en prenant la valeur positive de $\nu\frac{n(n+1)}{2} \pmod 8$, qui est immédiatement supérieure à la quantité $\nu\frac{n+1}{2n}$. La seconde remarque montre que les polynomes

$$a+bu^8+cu^{16}+\ldots$$

sont réciproques, mais à cet égard en distinguant des deux autres le cas de $n=11$, à cause du facteur $(-1)^{\frac{n^2-1}{8}+\frac{n+1}{2}}$, alors égal à -1. De là résulte en effet que les polynomes facteurs des puissances paires de z ont leurs coefficients équidistants des extrêmes égaux et de signes contraires, tandis que ceux qui affectent les puissances impaires ont, comme pour $n=5$, 7, leurs coefficients égaux et de même signe. On en tire d'ailleurs, dans tous les cas, la valeur de ρ_ν sous cette forme

$$\rho_\nu = \frac{(n+1)\nu - 2\alpha_\nu}{8},$$

et si l'on observe enfin, ce qui est très facile à établir, que la quantité $1 - u^8$ entre comme facteur dans le polynome

$$a + bu^8 + cu^{16} + \ldots + hu^{8\rho},$$

avec un exposant (1) dont la limite inférieure est

$$\frac{\nu}{2n}\left[n + \left(\frac{2}{n}\right)\right],$$

on aura réuni tout ce qui est nécessaire pour pouvoir écrire *a priori* et sans calcul les équations réduites sous les formes suivantes, où D représente toujours le discriminant, savoir :

1° $n = 5$.

$$z^5 + z\alpha u^4(1-u^8)^2 - \sqrt{D} = 0.$$

Le terme en z^4 n'existe pas, parce qu'on obtient pour ρ_1 une valeur négative; les termes en z^3 et z^2 disparaissent parce que les coefficients doivent respectivement contenir en facteur $1 - u^8$, $(1-u^8)^2$, ce qui est en contradiction avec les valeurs $\rho_2 = 0$, $\rho_3 = 1$.

2° $n = 7$.

$$z^7 + z^4\alpha u^4(1-u^8)^2 + z^2\alpha' u^4(1-u^8)^4 + z\alpha'' u^8(1-u^8)^4 - \sqrt{D} = 0.$$

On a à remarquer cette circonstance importante que le coefficient α' est nul, et qui tient à ce que dans le développement des racines suivant les puissances de $\sqrt[7]{q} = \mathfrak{q}$, savoir :

$$z = 4\sqrt{-7}\sqrt{\mathfrak{q}}\left(1 + \frac{\sqrt{-7}-1}{2}\mathfrak{q}^2 + \mathfrak{q}^4 + \ldots\right),$$

la quantité entre parenthèses ne contient pas la première puissance de $\mathfrak{q}$. De là sans doute résulte qu'on a ainsi le type analytique le plus simple des équations du septième degré résoluble par les fonctions elliptiques.

3° $n = 11$.

En désignant comme précédemment par $\alpha, \beta, \ldots$, des constantes

(1) Cet exposant est impair lorsque $n = 11$ dans les coefficients des puissances paires de z; mais, ce cas excepté, il est toujours pair.

numériques, on a cette équation

$$\begin{aligned}
&z^{11} + z^{10}\alpha u^2(1-u^8) + z^9\alpha' u^4(1-u^8)^2 + z^8\alpha'' u^6(1-u^8)^3 \\
&\quad + z^7 u^8(1-u^8)^2(\beta + \beta' u^8 + \beta u^{16}) + z^6 u^{10}(1-u^8)^3(\gamma + \gamma' u^8 + \gamma u^{16}) \\
&\quad + z^5 u^4(1-u^8)^4(\delta + \delta' u^8 + \delta'' u^{16} + \delta' u^{24} + \delta u^{32}) \\
&\quad + z^4 u^6(1-u^8)^3(\varepsilon + \varepsilon' u^8 + \varepsilon'' u^{16} + \varepsilon'' u^{24} + \varepsilon' u^{32} + \varepsilon u^{40}) \\
&\quad + z^3 u^8(1-u^8)^4(\eta + \eta' u^8 + \eta'' u^{16} + \eta''' u^{24} + \eta'' u^{32} + \eta' u^{40} + \eta u^{48}) \\
&\quad + z^2 u^{10}(1-u^8)^5(\zeta + \zeta' u^8 + \zeta'' u^{16} + \zeta''' u^{24} + \zeta'' u^{32} + \zeta' u^{40} + \zeta u^{48}) \\
&\quad + z u^4(1-u^8)^6(0 + 0' u^8 + 0'' u^{16} + 0''' u^{24} + 0'' u^{32} + 0' u^{40} + 0 u^{48}) \\
&\qquad - \sqrt{D} = 0.
\end{aligned}$$

Ces constantes pourront être déterminées en développant les coefficients suivant les puissances de q, et substituant pour z le développement correspondant suivant la puissance de $\sqrt[11]{q}$. Le calcul assez long auquel on est conduit n'est nullement impraticable; je n'ai pas cru cependant devoir m'y arrêter, car le principal intérêt qu'on peut attacher au résultat concerne surtout l'étude des équations du onzième degré résolubles par les fonctions elliptiques. J'indique encore une fois, en terminant ici mes recherches, ces belles questions qui offriront une des plus importantes applications de la théorie fondée par Abel et Jacobi. Mais c'est surtout l'œuvre propre de l'immortel auteur des *Fundamenta* d'avoir reconnu ces rapports si remarquables des nouvelles transcendantes avec l'Algèbre et les propriétés des nombres. Entre tant de beaux résultats dus à son génie, et qui ont ouvert des voies fécondes à la Science de nos jours, je ne puis m'empêcher de rappeler dans les Notices des premiers volumes du *Journal de Crelle* les énoncés relatifs aux propriétés des équations entre le multiplicateur M et le module k. C'est là en effet que M. Kronecker a trouvé le principe de la méthode si remarquable pour la résolution de l'équation du cinquième degré qui m'a été communiquée dans une Lettre publiée au tome XLVI, page 1150, des *Comptes rendus*, et l'on pourra voir dans un travail très important de M. Brioschi sur ce sujet (1) comment cette méthode résulte des relations singulières qu'a données Jacobi entre les racines de ces équations dans le cas du sixième

(1) *Sul metodo di Kronecker per la rizoluzione delle equazioni di quinto grado*, dans les *Actes de l'Institut Lombard*, vol. I.

degré. Les travaux de ces deux savants géomètres ont ainsi ouvert une voie plus facile pour arriver à la résolution de l'équation générale du cinquième degré que celle que j'avais suivie en prenant pour point de départ la réduction de Jerrard à la forme

$$x^5 - x - a = 0,$$

et c'est en suivant cette nouvelle direction que j'espère plus tard pouvoir y revenir pour contribuer à en faire l'étude approfondie qu'elle demande.

SUR L'ABAISSEMENT

DE

L'ÉQUATION MODULAIRE DU HUITIÈME DEGRÉ.

Extrait d'une Lettre adressée à M. Brioschi (*Annali di Matematica pura ed applicata*, t. II, 1859, p. 59).

« .... J'ai entrepris le calcul de la réduction de l'équation modulaire du huitième degré au septième, et voici le résultat définitif auquel je viens d'être amené. Soit fait, en introduisant la variable ω (1), $u = \varphi(\omega)$, les huit racines seront

$$\varphi(7\omega) \quad \text{et} \quad \varphi\left(\frac{\omega + 16m}{7}\right),$$

le nombre entier m étant pris suivant le module 7. Or, en prenant, en premier lieu,

$$z = \left[\varphi(7\omega) - \varphi\left(\frac{\omega}{7}\right)\right]\left[\varphi\left(\frac{\omega+16}{7}\right) - \varphi\left(\frac{\omega+16.3}{7}\right)\right] \times \left[\varphi\left(\frac{\omega+16.2}{7}\right) - \varphi\left(\frac{\omega+16.6}{7}\right)\right]\left[\varphi\left(\frac{\omega+16.4}{7}\right) - \varphi\left(\frac{\omega+16.5}{7}\right)\right]$$

et, en second lieu,

$$z' = \left[\varphi(7\omega) - \varphi\left(\frac{\omega}{7}\right)\right]\left[\varphi\left(\frac{\omega+16}{7}\right) - \varphi\left(\frac{\omega+16.5}{7}\right)\right] \times \left[\varphi\left(\frac{\omega+16.2}{7}\right) - \varphi\left(\frac{\omega+16.3}{7}\right)\right]\left[\varphi\left(\frac{\omega+16.4}{7}\right) - \varphi\left(\frac{\omega+16.6}{7}\right)\right],$$

(1) Voir *C. R.*, t. XLVI, p. 510.