JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

SYLOW

Sur la multiplication complexe des fonctions elliptiques

Journal de mathématiques pures et appliquées 4^e série, tome 3 (1887), p. 109-254.
<http://www.numdam.org/item?id=JMPA_1887_4_3__109_0>

Sur la multiplication complexe des fonctions elliptiques;

PAR M. SYLOW.

Le but de ce Mémoire est de traiter les principales questions d'Algèbre qui se rattachent aux fonctions elliptiques douées d'une multiplication complexe, en exceptant toutefois la question de l'irréductibilité des équations. Les propriétés les plus importantes de ces fonctions furent en partie trouvées, en partie entrevues par Abel; mais, outre la théorie de la division de la lemniscate et quelques exemples de multiplication complexe, il n'a fait qu'énoncer ses résultats. Plus tard, la multiplication complexe a été l'objet de travaux célèbres de M. Hermite et surtout de M. Kronecker, qui ont confirmé les résultats et les prévisions d'Abel et enrichi la Science de beaucoup de choses nouvelles et extrêmement remarquables. Quoique MM. Kronecker et Hermite aient en partie indiqué les méthodes qui les ont conduits à leurs découvertes, le manque d'une exposition suivie s'est fait sentir; c'est pourquoi, sur l'invitation de l'éminent directeur de ce Journal, j'ai entrepris de rédiger mes recherches sur cette théorie. En attendant, M. G. Pick (*Mathematische Annalen*, t. XXV et XXVI) et M. H. Weber (*Acta mathematica*, t. VI) ont publié des travaux remarquables sur la même matière.

Voici, en peu de mots, l'enchaînement des idées qui m'ont guidé dans la partie la plus essentielle de ces recherches. A l'occasion de la nouvelle édition des *Œuvres d'Abel*, j'eus à me rendre compte de l'exactitude de certaines propositions de ce grand géomètre, énoncées

sans démonstration; par là mon attention fut appelée sur ce fait que, pour les modules de la multiplication complexe, les modules *singuliers* d'après l'expression de M. Kronecker, l'équation de la division des périodes est, dans certains cas, réductible; il s'ensuit presque immédiatement que, dans les mêmes cas, l'équation modulaire a une ou deux racines rationnelles, pourvu qu'on lui adjoigne la racine carrée du *déterminant*. Les modules transformés étant eux-mêmes singuliers, cette question s'impose : Quel rapport ont ces racines rationnelles de l'équation modulaire avec le module primitif? La réponse est facile à trouver : elles satisfont à la même équation algébrique. On est ainsi conduit à étudier la résolution de l'équation des modules, et la route à suivre est toute tracée; on établit sans difficulté que chaque racine s'exprime en fonction rationnelle de chaque autre, et que les symboles de ces fonctions sont échangeables.

Par l'expression *multiplication complexe*, j'entends une formule qui exprime $\lambda[(a+bi\sqrt{n})z+\alpha]$ en fonction rationnelle de $\lambda(z)$, α étant une constante. J'ai conservé la classification des modules singuliers, à laquelle on est conduit par cette définition; elle ne coïncide pas avec celle de M. Kronecker, mais le passage de l'une de ces classifications à l'autre est très simple; je l'indiquerai à la fin du Mémoire. Mon objet étant les questions algébriques, je ne parle qu'occasionnellement des nombreuses relations que possède la théorie des modules singuliers avec l'Arithmétique; je fais exception seulement pour les formules de M. Kronecker relatives aux nombres des classes, dont je déduis celles que j'ai rencontrées en cherchant les équations des modules singuliers.

I. — Propositions fondamentales.

1. *Notations.* — Nous désignerons, avec MM. Briot et Bouquet, les trois fonctions elliptiques par les symboles λ, μ, ν, de sorte que, en posant

$$\int_0^x \frac{dx}{\sqrt{1-x^2}\sqrt{1-k^2x^2}} = z,$$

on a

$$x=\lambda(z), \qquad \sqrt{1-x^2}=\mu(z), \qquad \sqrt{1-k^2x^2}=\nu(z).$$

En représentant par 2ω, ω' un système de périodes elliptiques de la fonction λ, les valeurs du module et de son complément sont définies sans ambiguïté par les formules

$$\lambda\left(\frac{\omega+\omega'}{2}\right)=\frac{1}{k}, \qquad \nu\left(\frac{\omega}{2}\right)=k'.$$

Quand nous aurons à parler de la racine carrée du module, nous la supposerons définie, quant au signe, par l'une des équations

$$\lambda\left(\frac{\omega}{2}+\frac{\omega'}{4}\right)=\frac{1}{\sqrt{k}}, \qquad \lambda\left(\frac{\omega'}{4}\right)=\frac{i}{\sqrt{k}}.$$

Enfin nous désignerons le rapport des périodes par la lettre ζ, en posant

$$\zeta=\frac{\omega'}{2\omega}.$$

2. Si l'on fait

$$\lambda(\varepsilon z+\alpha, k_1)=f[\lambda(z, k)], \tag{1}$$

f dénotant une fonction rationnelle, ε et α étant des constantes, et qu'on désigne par $2\omega_1$, ω'_1 un système de périodes elliptiques relatives au module k_1, cette équation entraîne deux relations de la forme

$$\begin{cases} \varepsilon.2\omega=p.2\omega_1+q.\omega'_1, \\ \varepsilon.\ \omega'=p'.2\omega_1+q'.\omega'_1, \end{cases} \tag{2}$$

où p, q, p', q' sont des nombres entiers dont le déterminant $pq'-p'q$, que nous désignerons par n, est nécessairement positif. Réciproquement, si les relations (2) sont satisfaites, il est toujours possible de satisfaire à l'équation (1), et le degré de la fonction rationnelle f sera égal à n. Or, si l'on veut avoir $k_1^2=k^2$, en d'autres termes si l'on veut que l'équation (1) donne lieu à une formule de multiplication, on n'a qu'à faire $\omega_1=\omega$, $\omega'_1=\omega'$; on aura donc, dans ce cas,

$$\begin{cases} \varepsilon.2\omega=p.2\omega+q\omega', \\ \varepsilon.\ \omega'=p'.2\omega+q'\omega'. \end{cases} \tag{3}$$

Il est facile de voir qu'on obtient, de cette manière, toutes les multiplications possibles; en effet, si les périodes $2\omega_1$, ω'_1 appartiennent au module k, on a

$$2\omega_1 = r.2\omega + s\omega'$$
$$\omega'_1 = r'.2\omega + s'\omega',$$

où $rs' - r's = 1$; donc, en substituant ces valeurs dans l'équation (2), on a un système d'équations analogue au système (3). Les relations (3), bien connues depuis Abel, expriment donc la condition nécessaire et suffisante pour que la multiplication soit possible. On en tire

$$q\omega'^2 + (p - q')\omega'.2\omega - p'(2\omega)^2 = 0, \tag{4}$$

$$\varepsilon^2 - (p + q')\varepsilon + pq' - p'q = 0; \tag{5}$$

d'où

$$\begin{cases} \zeta = \dfrac{\omega'}{2\omega} = \dfrac{-p + q' + i\sqrt{4n - (p+q')^2}}{2q}, \\ \varepsilon = p + q\zeta = \frac{1}{2}\left[p + q' + i\sqrt{4n - (p+q')^2}\right]. \end{cases} \tag{6}$$

Les équations (6) ne sont sujettes qu'à une seule exception; quand on a

$$p' = q = 0, \qquad p = q' = \varepsilon,$$

ζ est indéterminé; c'est le cas de la multiplication ordinaire.

Dans tout autre cas, on a une *multiplication complexe*, car, ζ étant toujours imaginaire, le nombre $4n - (p+q')^2$ est positif. Puisque dans l'expression de ζ le coefficient de i est essentiellement positif, le radical $\sqrt{4n - (p+q')^2}$ doit être positif ou négatif en même temps que q. Or, en changeant au besoin le signe de ε dans les équations (3), nous pouvons supposer q et $\sqrt{4n - (p+q')^2}$ positifs; cela étant, l'égalité

$$4n - (p+q')^2 = -4p'q - (p - q')^2$$

fait voir que p' est négatif.

3. A chaque module répondent évidemment une infinité de valeurs du multiplicateur ε; cherchons donc la valeur de ε, pour laquelle le degré n de la fonction f est le moindre possible. D'après le numéro précédent, les périodes elliptiques satisfont à une relation de la forme

$$A\omega'^2 + B\omega'.2\omega + C.(2\omega)^2 = 0,$$

où A et C sont positifs, et où il est permis de supposer que A, B et C n'aient pas de diviseur commun. En la comparant à l'équation (4) et désignant par m le plus grand diviseur commun des nombres q, $p-q'$, $-p'$, on a

$$q = mA, \qquad p - q' = mB, \qquad -p' = mC.$$

Faisant

$$p = \tfrac{1}{2}mB + r, \qquad q' = -\tfrac{1}{2}mB + r,$$

on en tire

$$n = pq' - p'q = r^2 + m^2(AC - \tfrac{1}{4}B^2),$$

ce qui fait voir qu'on a la plus petite valeur de n en faisant $m = 1$, $r = 0$ si B est un nombre pair, mais $m = 1$, $r^2 = \frac{1}{4}$ si B est impair. On a ainsi deux cas :

Premier cas. — Le rapport des périodes satisfait à l'équation

$$a\zeta^2 + 2b\zeta + c = 0,$$

d'où

$$n = ac - b^2, \qquad \zeta = \frac{-b + i\sqrt{n}}{a};$$

on a la plus simple multiplication complexe en posant

$$(7) \qquad \begin{cases} \varepsilon.2\omega = \quad b.2\omega + a\omega', \\ \varepsilon.\ \omega' = -c.2\omega - b\omega', \\ \varepsilon = i\sqrt{n}; \end{cases}$$

une multiplication quelconque est définie par les équations

$$(8) \qquad \begin{cases} (x + yi\sqrt{n})\,2\omega = (x + yb).2\omega + ya\omega', \\ (x + yi\sqrt{n})\ \ \omega' = -yc.2\omega + (x - yb)\omega', \end{cases}$$

x et y étant des entiers, et son degré est égal à $x^2 + y^2 n$.

Second cas. — Le rapport ζ satisfait à l'équation

$$a\zeta^2+(2b+1)\zeta+c=0,$$

d'où

$$n=ac-b(b+1), \qquad \zeta=\frac{-(2b+1)+i\sqrt{4n-1}}{2a};$$

on a les multiplications complexes du plus petit degré possible, en adoptant l'un ou l'autre des deux systèmes de formules

$$(9)\quad \begin{cases} \varepsilon.2\omega=(b+1)2\omega+a\omega', & \varepsilon.2\omega=b.2\omega+a\omega', \\ \varepsilon.\ \omega'=-c.2\omega-b\omega', & \varepsilon.\ \omega'=-c.2\omega-(b+1)\omega', \\ \varepsilon=\dfrac{1+i\sqrt{4n-1}}{2}, & \varepsilon=\dfrac{-1+i\sqrt{4n-1}}{2}. \end{cases}$$

Une multiplication quelconque est définie par les équations suivantes :

$$(10)\quad \begin{cases} \dfrac{x+yi\sqrt{4n-1}}{2}\cdot 2\omega=\left(\dfrac{x+y}{2}+yb\right)2\omega+ya\omega', \\ \dfrac{x+yi\sqrt{4n-1}}{2}\quad \omega'=-yc.2\omega+\left(\dfrac{x-y}{2}-yb\right)\omega'; \end{cases}$$

son degré est égal à $\frac{1}{4}[x^2+y^2(4n-1)]$; x et y sont des nombres entiers de la même parité. On voit que, si x et y sont pairs, les équations (10) rentrent dans les équations (8).

Dans les deux cas, les trois coefficients de l'équation en ζ n'ont pas de diviseur commun; a et c sont positifs; de même, $\sqrt{n}$ et $\sqrt{4n-1}$ désignent des quantités positives. Le nombre n sera appelé le degré du module, et nous dirons qu'un module singulier appartient à la première ou à la seconde espèce, suivant qu'il rentre dans le premier ou dans le second des cas dont nous venons de parler. On verra en effet, au numéro suivant, qu'un module ne peut appartenir qu'à un seul de ces cas.

4. On a vu que le rapport des périodes elliptiques satisfait à une équation de la forme

$$(11)\qquad A\zeta^2+B\zeta+C=0.$$

Réciproquement, toute équation de second degré à coefficients entiers définit un module singulier, pourvu que ses racines ne soient pas réelles. En effet, le module et la période 2ω se déterminent par les formules

$$(12)\qquad \begin{cases} \sqrt{k} = 2\sqrt[4]{q}\prod_1^\infty \left(\frac{1+q^{2m}}{1+q^{2m-1}}\right)^2, \\ \omega = \pi\prod_1^\infty \left(\frac{1-q^{2m}}{1-q^{2m-1}}\cdot\frac{1+q^{2m-1}}{1+q^{2m}}\right)^2, \\ \text{où} \\ q = e^{2\pi i\zeta}, \qquad \sqrt[4]{q} = e^{\frac{\pi}{2}i\zeta}. \end{cases}$$

Or, en faisant $\omega' = 2\omega\zeta$, la fonction $\lambda(z, k)$ admet les périodes elliptiques 2ω et ω', et l'on a, pour la plus simple multiplication complexe, les formules du numéro précédent. Des formules (12), on peut aussi conclure que, si les équations (3) du n° **2** sont satisfaites, on a non seulement $k_1^2 = k^2$, mais aussi $\sqrt{k_1} = \sqrt{k}$.

Supposons maintenant qu'une autre équation du second degré

$$(13)\qquad A_1\zeta_1^2 + B_1\zeta_1 + C_1 = 0$$

donne la même valeur de k^2 que l'équation (11), et soient $2\omega_1$, ω_1' les périodes qu'on obtient par les formules (12), en y remplaçant ζ par ζ_1. La fonction $\lambda(z, k)$ admet des périodes élémentaires $2\omega_1$ et ω_1', quoiqu'elles ne soient pas nécessairement des périodes elliptiques du module k; donc on a

$$2\omega = r\cdot 2\omega_1 + s\omega_1',$$

$$\omega' = r'\cdot 2\omega_1 + s'\omega_1',$$

d'où

$$\zeta = \frac{r' + s'\zeta_1}{r + s\zeta_1},$$

et l'on a

$$rs' - r's = \pm 1;$$

mais, comme le coefficient de i dans l'expression de ζ_1 doit être positif, on a

$$rs' - r's = 1.$$

En faisant cette substitution, il faut que l'équation (11) se change en (13); en d'autres termes, il faut que les formes quadratiques

$$Ax^2 + Bxy + Cy^2 \quad \text{et} \quad A_1x^2 + B_1xy + C_1y^2$$

soient proprement équivalentes.

A chaque équation du second degré définissant une valeur de ζ, nous ferons correspondre une forme quadratique à déterminant négatif. Dans le premier des cas dont il est parlé au numéro précédent, où l'équation est

$$a\zeta^2 + 2b\zeta + c = 0,$$

la forme correspondante sera (a, b, c); dans le second cas, au contraire, où l'on a

$$a\zeta^2 + (2b + 1)\zeta + c = 0,$$

nous prendrons pour forme correspondante $(2a, 2b + 1, 2c)$. Une première condition à remplir pour que deux valeurs de ζ donnent la même valeur de k^2 est donc que les formes quadratiques correspondantes appartiennent à la même classe. Ainsi, tout module singulier de la première espèce du degré n appartient à une classe proprement primitive du déterminant $-n$, tout module de la seconde espèce à une classe improprement primitive du déterminant $-(4n-1)$, d'où l'on voit que les deux espèces sont réellement distinctes. Nous appellerons $-n$ ou $-(4n-1)$ le *déterminant du module singulier*.

A chaque classe de formes répondent plusieurs valeurs de k^2. Pour en déterminer le nombre et pour trouver les relations qui les font dépendre les unes des autres, nous ferons usage des transformations linéaires de la fonction $\lambda(z)$.

II. — Les transformations linéaires. Les plus simples modules singuliers.

5. Pour avoir tous les modules qui répondent à la même classe de formes quadratiques que le module k, il faut substituer à ζ l'expression

$$\frac{r' + s'\zeta_1}{r + s\zeta_1},$$

r, s, r', s' étant des entiers satisfaisant à l'équation

$$rs' - r's = 1,$$

ce qui équivaut à effectuer la transformation linéaire $\begin{pmatrix} r & s \\ r' & s' \end{pmatrix}$ définie par les équations

$$\varepsilon' . 2\omega = r . 2\omega_1 + s\omega_1',$$
$$\varepsilon' . \omega' = r' . 2\omega_1 + s'\omega_1'.$$

On sait que le carré k_1^2 du module transformé a l'une des six valeurs suivantes :

$$(14) \quad k^2, \quad \frac{1}{k^2}, \quad \left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^4, \quad \left(\frac{1+\sqrt{k}}{1-\sqrt{k}}\right)^4, \quad \left(\frac{1+i\sqrt{k}}{1-i\sqrt{k}}\right)^4, \quad \left(\frac{1-i\sqrt{k}}{1+i\sqrt{k}}\right)^4,$$

et l'on vérifie sans difficulté que ces valeurs répondent respectivement aux six suppositions suivantes :

$$s \equiv 0, \qquad s \equiv 2, \qquad s' \equiv 0,$$
$$s' \equiv 2, \qquad s \equiv s' \equiv \pm 1, \qquad s \equiv -s' \equiv \pm 1 \qquad (\mathrm{mod}\ 4).$$

En employant les transformations linéaires, il faut supposer connu $\sqrt{k}$; souvent il nous faudra aussi pousser la distinction jusqu'à la détermination complète de $\sqrt{k_1}$. Voici le Tableau complet des formules de transformations, où l'on a écrit $\lambda_1(0)$ au lieu de $\lambda(0, k_1)$.

A, $s \equiv 0 \pmod 4$:

$$\sqrt{k_1} = i^{-r's'}\sqrt{k}, \qquad \varepsilon' = (-1)^{\frac{r-1}{2}}, \qquad \lambda_1(\varepsilon' 0) = \varepsilon' \lambda(0).$$

B, $s \equiv 2 \pmod 4$:

$$\sqrt{k_1} = \frac{i^{-r's'}}{\sqrt{k}}, \qquad \varepsilon' = (-1)^{\frac{r-1}{2}+r'} k, \qquad \lambda_1(\varepsilon' 0) = \varepsilon' \lambda(0).$$

C, $r \equiv s' \equiv 0 \pmod 2$:

$$\alpha = \frac{\omega_1}{2} + \frac{\omega_1'}{4}, \qquad \sqrt{k_1} = (-1)^{\frac{r}{2}} \frac{1-(-1)^{\frac{s'}{2}}\sqrt{k}}{1+(-1)^{\frac{s'}{2}}\sqrt{k}};$$

$$\varepsilon' = \frac{i^s}{2}\left[1+(-1)^{\frac{s'}{2}}\sqrt{k}\right]^2, \qquad \lambda_1(\varepsilon' 0 + \alpha) = \frac{1}{\sqrt{k_1}} \frac{1+(-1)^{\frac{s+s'-1}{2}}\sqrt{k}\,\lambda(0)}{1-(-1)^{\frac{s+s'-1}{2}}\sqrt{k}\,\lambda(0)}.$$

D, $r \equiv 0$, $s \equiv r' \equiv s' \equiv 1 \pmod 2$:

$$\alpha = \frac{\omega_1}{2} + \frac{\omega_1'}{4}, \qquad \sqrt{k_1} = (-1)^{\frac{r}{2}} \frac{1 + i^{ss'}\sqrt{k}}{1 - i^{ss'}\sqrt{k}},$$

$$\varepsilon' = \frac{i^s}{2}(1 - i^{ss'}\sqrt{k})^2, \qquad \lambda_1(\varepsilon' 0 + \alpha) = \frac{1}{\sqrt{k_1}} \frac{1 - i^{s'}\sqrt{k}\lambda(0)}{1 + i^{s'}\sqrt{k}\lambda 0}.$$

E, $s' \equiv 0$, $r \equiv r' \equiv s \equiv 1 \pmod 2$:

$$\alpha = \frac{\omega_1'}{4}, \qquad \sqrt{k_1} = i^{-rs} \frac{1 - (-1)^{\frac{s'}{2}}\sqrt{k}}{1 + (-1)^{\frac{s'}{2}}\sqrt{k}},$$

$$\varepsilon' = \frac{i^s}{2}\left[1 + (-1)^{\frac{s'}{2}}\sqrt{k}\right]^2, \qquad \lambda_1(\varepsilon' 0 + \alpha) = \frac{i}{\sqrt{k_1}} \frac{1 + (-1)^{\frac{s+s'-1}{2}}\sqrt{k}\lambda(0)}{1 - (-1)^{\frac{s+s'-1}{2}}\sqrt{k}\lambda(0)}.$$

F, $r' \equiv 0$, $r \equiv s \equiv s' \equiv 1 \pmod 2$:

$$\alpha = \frac{\omega_1'}{4}, \qquad \sqrt{k_1} = i^{-rs} \frac{1 - i^{-ss'}\sqrt{k}}{1 + i^{-ss'}\sqrt{k}},$$

$$\varepsilon' = \frac{i^s}{2}(1 + i^{-ss'}\sqrt{k})^2, \qquad \lambda_1(\varepsilon' 0 + \alpha) = \frac{i}{\sqrt{k_1}} \frac{1 - i^{s'}\sqrt{k}\lambda(0)}{1 + i^{s'}\sqrt{k}\lambda(0)}.$$

Remarquons que les formules qui donnent les valeurs de $\sqrt{k_1}$ et ε' dans le cas F embrassent celles des cas C, D, E.

Dans les cas C, D, E, F, la dernière formule peut être remplacée par la suivante :

$$\lambda_1(\varepsilon' 0) = \frac{2\varepsilon'\lambda(0)}{1 + \mu(0)\nu(0) - (-1)^{\frac{s}{2}} k\lambda^2 0}.$$

Supposons maintenant $\sqrt{k}$ défini par l'équation

$$A\zeta^2 + B\zeta + C = 0, \tag{15}$$

laquelle, en faisant

$$\zeta = \frac{r' + s'\zeta_1}{r + s\zeta_1},$$

se change en

$$A_1\zeta_1^2 + B_1\zeta_1 + C_1 = 0, \tag{16}$$

où, par conséquent,

$$A_1 = As'^2 + Bs's + Cs^2; \tag{17}$$

le carré k_1^2 du module transformé a l'une des six valeurs (14). Il y a donc généralement six valeurs du carré du module pour chaque classe de formes quadratiques; cette règle ne souffre d'exceptions que dans les cas où quelques-unes des valeurs (14) coïncident, c'est-à-dire pour les modules qu'on trouve en faisant $\sqrt{k_1} = \sqrt{k}$, et que nous appellerons, dans la suite, *modules singuliers linéaires*.

D'après ce qu'on a vu dans le paragraphe précédent, on peut classifier les modules singuliers d'après les déterminants des formes correspondantes; ainsi un module de la première espèce du déterminant $-D$ est du degré D, et son plus simple multiplicateur est $i\sqrt{D}$; au contraire, un module de la seconde espèce est du degré $\frac{1}{4}(D+1)$, ses plus simples multiplicateurs sont $\frac{1}{2}(\pm 1 + i\sqrt{D})$. Nous nous servirons aussi d'une autre classification : les modules pour lesquels le coefficient A est un nombre pair seront appelés *modules de la première catégorie*, les autres *modules de la seconde catégorie*. En effet, on verra plus tard que les équations algébriques qui déterminent les modules singuliers diffèrent, et suivant l'espèce et suivant la catégorie.

Supposons que le module primitif k soit de la première espèce et de la première catégorie; A et B sont pairs, C impair, et par suite A_1 est pair ou impair en même temps que s. Donc, les deux premières des valeurs (14) appartiennent à la première catégorie, les quatre dernières à la seconde.

Si k est de la seconde espèce, le déterminant $4AC - B^2$ est égal à $4n - 1$, n désignant le degré du module. Si maintenant n est impair, et par conséquent $4AC - B^2 = 8h + 3$, A est nécessairement impair; donc, dans ce cas, la seconde catégorie existant seule, toutes les six valeurs (14) lui appartiennent. Au contraire, si n est pair, le déterminant est de la forme $8h - 1$, donc AC est pair. En supposant que k appartienne à la première catégorie, la congruence

$$A_1 = As'^2 + Bss' + Cs^2 \equiv s(Bs' + Cs) \pmod 2$$

fait voir que $\frac{1}{k^2}$ y appartient aussi. Au reste, il y a deux cas à consi-

dérer : si C est pair, A_1 devient pair si s est impair, s' pair; mais il est impair si s et s' sont impairs : donc les valeurs $\left(\frac{1\pm\sqrt{k}}{1\mp\sqrt{k}}\right)^4$ appartiennent à la première catégorie, $\left(\frac{1\pm i\sqrt{k}}{1\mp i\sqrt{k}}\right)^4$ à la seconde; si C est impair, l'inverse a lieu. Donc, parmi les six valeurs (14), quatre appartiennent à la première catégorie, deux seulement à la seconde.

Dans tous les cas, k^2 et $\frac{1}{k^2}$ sont de la même catégorie.

Voici encore une application des transformations linéaires qui nous sera utile dans la suite. En posant $\zeta = x + yi$ et faisant croître indéfiniment y, on a

$$q = 0,$$

et, par suite,

$$\sqrt{k} = 0;$$

en même temps, ζ_1 devient égal à $-\frac{r}{s}$, $\sqrt{k_1}$ prend l'une des valeurs 0, ∞, ± 1, $\pm i$. A la vérité, on ne peut pas dire que réciproquement $\sqrt{k_1}$ prend l'une de ces valeurs quand ζ_1 converge vers $-\frac{r}{s}$, puisque l'équation $\zeta_1 = -\frac{r}{s}$ n'entraîne pas $y = \infty$, mais seulement $\zeta = \infty$. Cependant, la remarque suivante nous suffira. On sait que, si l'affixe de ζ_1 se meut sur un cercle dont le centre est situé sur l'axe réel, l'affixe de ζ se meut également sur un cercle dont le centre se trouve sur le même axe. Or, si le premier cercle passe par le point de l'axe réel dont l'abscisse est $-\frac{r}{s}$, le second cercle, ayant un point à l'infini, devient une droite perpendiculaire à l'axe; donc, dans ce cas, on a bien $y = \infty$ pour $\zeta_1 = -\frac{r}{s}$. En déterminant la valeur de $\sqrt{k_1}$ au moyen du tableau, on a ainsi le résultat suivant. Quand ζ_1 converge vers l'une des valeurs

$$\frac{2\rho+1}{4\sigma},\quad \frac{2\rho+1}{4\sigma+2},\quad \frac{4\rho}{2\sigma+1},\quad \frac{4\rho+2}{2\sigma+1},\quad \frac{4\rho\pm 1}{4\sigma\pm 1},\quad \frac{4\rho\pm 1}{4\sigma\mp 1},$$

son affixe décrivant un arc de cercle dont le centre est situé sur l'axe

réel, $\sqrt{k_1}$ convergera respectivement vers les valeurs

$$0, \quad \infty, \quad 1, \quad -1, \quad i, \quad -i.$$

6. Les modules singuliers linéaires se trouvent presque sans calcul, au moyen du tableau. Pour avoir ceux de la première espèce, il faut employer les cas où r et s' sont de la même parité, les cas B, C, F.

Dans le cas B, il faut prendre r' impair, par exemple

$$\varepsilon.2\omega = -2\omega + 2\omega',$$
$$\varepsilon.\ \omega' = -2\omega + \omega';$$

d'où

$$2\zeta^2 - 2\zeta + 1 = 0, \qquad \zeta = \frac{1+i}{2}, \qquad \varepsilon = i,$$
$$k = i, \qquad k^2 = -1, \qquad \lambda(i0) = i\lambda(0).$$

Du cas C, on tire

$$\sqrt{k} = \pm\sqrt{2} - 1, \qquad k = 3 \mp 2\sqrt{2}, \qquad k^2 = 17 \mp 12\sqrt{2};$$

on peut faire, par exemple,

$$\varepsilon.2\omega = \omega', \qquad \varepsilon\omega' = -2\omega,$$

d'où

$$\zeta = \varepsilon = i, \qquad \lambda\left(i0 + \frac{\omega}{2} + \frac{\omega'}{4}\right) = \frac{1}{\sqrt{k}}\,\frac{1-\sqrt{k}\,\lambda(0)}{1+\sqrt{k}\,\lambda(0)}$$

ou bien

$$\lambda(i0) = \frac{2i\lambda(0)}{1+\mu(0)\nu(0)-k\lambda^2(0)}.$$

Il est facile de prévoir qu'on n'aura pas d'autres valeurs de k^2. A l'unique classe du déterminant -1 répondent donc, au lieu de six, seulement trois valeurs de k^2, dont l'une de la première catégorie, deux de la seconde.

Les cas D et E donnent les modules de la seconde espèce répondant à l'unique classe improprement primitive du déterminant -3. On

trouve, en faisant $r \equiv 0$, $s \equiv s' \pmod 4$,

$$\sqrt{k} = \frac{1+i}{2}(-1 \pm \sqrt{3}), \qquad k = i(2 \mp \sqrt{3}), \qquad k^2 = -(7 \mp 4\sqrt{3}).$$

On peut faire

$$\zeta^2 - \zeta + 1 = 0, \qquad \zeta = \varepsilon = \frac{1+i\sqrt{3}}{2},$$

$$\lambda\left(\varepsilon\theta + \frac{\omega}{2} + \frac{\omega'}{4}\right) = \frac{1}{\sqrt{k}} \frac{1 + i\sqrt{k}\,\lambda(\theta)}{1 - i\sqrt{k}\,\lambda(\theta)}$$

ou bien

$$\lambda(\varepsilon\theta) = \frac{2\varepsilon\lambda(\theta)}{1 + \mu(\theta)\nu(\theta) + k\lambda^2(\theta)}.$$

On ne trouve pas d'autres valeurs de k^2; ici l'on a donc seulement deux valeurs de k^2 au lieu de six.

7. On a vu que les carrés des modules singuliers linéaires sont tous réels, ceux de la seconde catégorie de la première espèce positifs, les autres négatifs. Recherchons dans quels cas le carré d'un module non linéaire k est réel. Soit (a, b, c) une des formes quadratiques qui lui correspondent; le rapport des périodes satisfait à l'équation

$$a\zeta^2 + 2b\zeta + c = 0.$$

En remarquant que dans les formules (12) on a

$$q = e^{2\pi i\zeta} = e^{-\frac{\pi 2\sqrt{D}}{a}}\left(\cos\frac{2\pi b}{a} - i\sin\frac{2\pi b}{a}\right),$$

on voit que, si k^2 est réel, il est identique au carré du module défini par l'équation

$$a\zeta^2 - 2b\zeta + c = 0,$$

d'où il suit que les formes (a, b, c) et $(a, -b, c)$ sont proprement équivalentes. Les valeurs réelles de k^2 appartiennent donc toujours aux classes ambiguës. Si k^2 est positif, nous pouvons supposer que la valeur de $\sqrt{k}$ définie par l'équation en ζ soit réelle; alors $\frac{1}{k^2}$, $\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^4$,

$\left(\frac{1+\sqrt{k}}{1-\sqrt{k}}\right)^4$ sont aussi réels et positifs. Au contraire, $\left(\frac{1+i\sqrt{k}}{1-i\sqrt{k}}\right)^4$, $\left(\frac{1-i\sqrt{k}}{1+i\sqrt{k}}\right)^4$ sont généralement imaginaires; les modules linéaires seuls font exception; car, si l'une de ces deux quantités est réelle, elle se confond avec l'autre, ce qui n'arrive que pour les modules linéaires. Si k^2 est réel et négatif, nous pouvons supposer $\sqrt{k}$ égal à $(1+i)\alpha$, α étant réel; d'où

$$\left(\frac{1\mp\sqrt{k}}{1\pm\sqrt{k}}\right)^4=\left[\frac{1\mp(1+i)\alpha}{1\pm(1+i)\alpha}\right]^4,\quad \left(\frac{1\pm i\sqrt{k}}{1\mp i\sqrt{k}}\right)^4=\left[\frac{1\mp(1-i)\alpha}{1\pm(1-i)\alpha}\right]^4;$$

alors $\frac{1}{k^2}$ sera réel et négatif; mais les carrés des autres modules qui appartiennent à la même classe que k^2 seront généralement imaginaires, et évidemment il n'y a d'exceptions que pour les modules linéaires. Or on sait (Gauss, *Disquis. arithm.*, art. 257, 258) que chaque classe ambiguë contient une forme de l'un des deux types $\left(a, 0, \frac{D}{a}\right)$, $\left(a, \frac{1}{2}a, \frac{a^2+4D}{4a}\right)$, où dans la seconde a est pair. Dans le cas du premier type la classe donne évidemment quatre valeurs de k^2 réelles et positives. Dans le cas du second type on a l'équation

$$a\zeta^2+a\zeta+\frac{a^2+4D}{4a}=0;$$

en y faisant $\zeta=\zeta_1-1$, et désignant la nouvelle valeur de $\sqrt{k}$ par $\sqrt{k_1}$, on a

$$a\zeta_1^2-a\zeta_1+\frac{a^2+4D}{4a}=0,\qquad \sqrt{k_1}=i\sqrt{k};$$

donc, en posant $\sqrt{k}=u+vi$, u et v étant réels, on a

$$i\sqrt{k}=u-vi,$$

d'où

$$k^2=-(u^2+v^2)^2;$$

par conséquent la classe donne deux valeurs de k^2 réelles et négatives.

Cela posé, considérons les divers cas, en désignant par μ le nombre des diviseurs premiers impairs de D.

Si $D = 4h + 1$, il y a $2^{\mu-1}$ classes appartenant à chacun des deux types. Celles du premier type donnent $2^{\mu+1}$ valeurs réelles et positives de k^2, et, puisque a et $\frac{D}{a}$ sont impairs, il est facile de voir qu'elles appartiennent toutes à la seconde catégorie. Les autres donnent 2^{μ} valeurs réelles et négatives de k^2 appartenant à la première catégorie.

Si $D = 4h - 1$, il y a $2^{\mu-1}$ classes proprement primitives du premier type; donc la première espèce contient $2^{\mu+1}$ modules dont les carrés sont réels et positifs, tous appartenant à la seconde catégorie. De plus, il est facile de voir qu'il existe $2^{\mu-1}$ classes improprement primitives du second type, qui donnent 2^{μ} modules de la seconde espèce dont les carrés sont réels et négatifs; ces modules sont tous de la seconde catégorie.

Si D est pair mais non divisible par 8, on a 2^{μ} classes, toutes du premier type. En prenant a pair et par conséquent $\frac{D}{a}$ impair, on voit qu'il y a $2^{\mu+1}$ modules réels de chaque catégorie.

Enfin, si D est divisible par 8, il y a 2^{μ} classes de chaque type. Celles du premier type donnent $2^{\mu+1}$ modules réels de chaque catégorie; celles du second type donnent $2^{\mu+1}$ modules de la première catégorie dont les carrés sont réels et négatifs.

III. — Formation des équations algébriques dont dépendent les modules singuliers, et des formules de multiplication complexe.

8. Pour trouver les formules de la multiplication complexe la plus simple que comporte un module singulier défini par le rapport des périodes, et pour déterminer algébriquement ce module, il suffit de trouver les formules de transformation qui répondent aux équations (7) et (9). Rappelons d'abord quelques points de la théorie de la transformation

Considérons les équations

$$(18)\qquad \begin{cases} \varepsilon.2\omega = r.2\omega_1 + s\,\omega_1', \\ \varepsilon.\ \omega' = r'.2\omega_1 + s'\omega_1', \end{cases} \qquad rs' - r's = n,$$

et la formule de transformation correspondante

$$\lambda(\varepsilon\theta + \alpha, k_1) = f[\lambda(\theta)].$$

Au moyen de la relation $\lambda(\omega - \theta) = \lambda(\theta)$, on trouve pour la constante α l'expression suivante

$$\alpha = (2p + 1 - r)\frac{\omega_1}{2} + (2q - s)\frac{\omega_1'}{4},$$

où, en changeant convenablement la fonction rationnelle f, on peut choisir arbitrairement les nombres p et q. Il en résulte qu'on peut faire

$\alpha = 0$, si s est pair, r impair,

$\alpha = \frac{\omega_1}{2}$, si s et r sont pairs,

$\alpha = \frac{\omega_1}{2} + \frac{\omega_1'}{4}$, si s est impair, r pair,

$\alpha = \frac{\omega_1'}{4}$, si s et r sont impairs.

Des équations (18) on tire

$$2\omega_1 = \varepsilon\,\frac{s'.2\omega - s\omega'}{n}, \qquad \omega_1' = \varepsilon\,\frac{-r'.2\omega + r\omega'}{n},$$

d'où l'on voit que les n valeurs différentes de $\lambda(\theta)$ qui répondent à une même valeur de $\lambda(\varepsilon\theta + \alpha, k_1)$ sont contenues dans l'expression

$$(19)\qquad \lambda\left(\theta + m\,\frac{s'.2\omega - s\omega'}{n} + \mu\,\frac{-r'.2\omega + r\omega'}{n}\right).$$

Dans la suite nous aurons à considérer les cas où les quatre nombres r, s, r', s' n'ont pas de diviseur commun; en désignant par δ le

plus grand commun diviseur de r et de s, posons

$$(20)\quad r=\rho\delta,\qquad s=\sigma\delta,\qquad \text{et par suite}\qquad n=\delta(\rho s'-r'\sigma)=\delta n'.$$

Or, en faisant

$$(21)\quad \begin{cases} \mu\rho-m\sigma=1,\\ -\mu r'+ms'=t, \end{cases}$$

l'expression (19) devient

$$\lambda\left(\theta+\frac{t.2\omega+\delta\omega'}{\delta n'}\right).$$

Dans cette expression on peut rendre t premier à δ; car premièrement le plus grand commun diviseur de t et de n' est premier à δ; on tire, en effet, des équations (21)

$$\mu(\rho s'-r'\sigma)=\mu n'=\sigma t+s',$$
$$m(\rho s'-r'\sigma)=mn'=\rho t+r';$$

donc un diviseur commun à t et à n' divise r' et s', et par conséquent il est premier à δ. Secondement, si t et δ admettent un diviseur commun, on peut remplacer μ et m respectivement par $\mu+h\sigma$ et $m+h\rho$, ce qui revient à remplacer t par $t+hn'$; or, puisque t et n' n'ont pas un même diviseur commun avec δ, on peut choisir h de manière à rendre $t+hn'$ premier à δ.

En faisant, pour abréger,

$$\Omega=t.2\omega+\delta\omega',$$

on voit que les n valeurs de l'expression (19) peuvent être représentées par

$$(22)\qquad \lambda\left(\theta+\frac{p\Omega}{n}\right),\qquad \text{où}\qquad p=0,\ 1,\ 2,\ \ldots.(n-1).$$

Si l'on pose

$$n=q_1^{\beta_1}q_2^{\beta_2}q_3^{\beta_3}\ldots.,$$

$q_1, q_2, q_3, \ldots$ étant les diviseurs premiers de n, le nombre N des périodes Ω qui donnent des transformations différentes est déterminé par l'équation

$$(23) \qquad N = q_1^{\beta_1-1}(q_1+1)\,q_2^{\beta_2-1}(q_2+1)\,q_3^{\beta_3-1}(q_3+1)\ldots.$$

A chacune de ces N valeurs de Ω répondent plusieurs transformations ; on en peut choisir une, qui donne les formules les plus simples, et que nous appellerons la *transformation principale*. Ces transformations seront choisies de telle manière que les modules correspondants satisfassent à une même équation algébrique, dépourvue de racines étrangères à la question, et qui d'ailleurs, pour les degrés pairs, se décompose en deux ou en plusieurs facteurs. On sait que, la transformation principale étant connue, les autres transformations répondant à la même valeur de Ω s'en déduisent au moyen des transformations linéaires. Soient

$$\begin{aligned} \varepsilon_0 . 2\omega &= r_0 . 2\omega_0 + s_0\omega_0', \\ \varepsilon_0 .\ \omega' &= r_0' . 2\omega_0 + s_0'\omega_0' \end{aligned}$$

les équations qui définissent la transformation principale, et

$$Y = \lambda(\varepsilon_0 0 + \alpha_0, k_0)$$

la fonction transformée; soient de plus

$$\begin{aligned} \varepsilon' . 2\omega_0 &= r_1 . 2\omega_1 + s_1\omega_1', \\ \varepsilon' .\ \omega_0' &= r_1' . 2\omega_1 + s_1'\omega_1' \end{aligned}$$

les équations de la transformation linéaire qu'il faut employer pour avoir la transformation (18), on a

$$(24) \qquad \begin{cases} \varepsilon = \varepsilon_0\varepsilon', & r = r_0 r_1 + s_0 r_1', \quad s = r_0 s_1 + s_0 s_1', \\ & r' = r_0' r_1 + s_0' r_1', \quad s' = r_0' s_1 + s_0' s_1'. \end{cases}$$

Ayant déterminé au moyen de ces équations les nombres r_1, s_1, r_1', s_1', ou seulement leurs valeurs (mod 4), le tableau des transformations

linéaires donne $\lambda(\varepsilon\theta + \alpha, k_1)$ en fonction linéaire de Y, et, par suite, en fonction rationnelle de $\lambda(\theta)$. De plus on a $\sqrt{k_0}$ exprimé en fonction linéaire de $\sqrt{k_1}$; en substituant cette expression dans l'équation modulaire principale, on trouve l'équation modulaire répondant au genre de transformations en question.

Cela posé, si l'on veut avoir la multiplication complexe définie par un système d'équations de la forme (7) ou (9), on n'a qu'à identifier les équations en question avec les équations (18) en faisant

$$\omega_1 = \omega, \qquad \omega'_1 = \omega', \qquad \sqrt{k_1} = \sqrt{k}.$$

On a ainsi $\lambda(\varepsilon\theta + \alpha, k)$ en fonction rationnelle de $\lambda(\theta)$, ou bien, si l'on veut, $\lambda(\varepsilon\theta)$ en fonction rationnelle de $\lambda(\theta)$ et de $\mu(\theta)\nu(\theta)$; de plus on obtient une équation algébrique satisfaite par le module k. Les équations qu'on obtient de cette manière ne sont pas libres de racines étrangères à la question; elles peuvent avoir les racines $k = 0$, $k = \pm 1$, et elles sont généralement satisfaites par des modules singuliers d'un degré moindre que n. Il faut maintenant trouver les racines étrangères et déterminer la multiplicité de chaque racine.

Les relations modulaires s'expriment par des équations en $\sqrt{k_1}$, en k_1, ou en k_1^2. Pour embrasser ces trois cas dans une même expression, dénotons l'équation modulaire dont il s'agit par $F(\xi, \eta_1) = 0$, ξ et η_1 désignant respectivement ou $\sqrt{k}$ et $\sqrt{k_1}$, ou k et k_1, ou enfin k^2 et k_1^2. Ainsi l'équation dont il faut chercher les racines est

$$F(\xi, \xi) = 0, \tag{25}$$

Soit, en *premier lieu*, l un module de la première espèce, déterminé par la racine $\xi = \xi_0$ de l'équation (25); désignons par n_1 son degré, par 2ϖ, ϖ' un couple de périodes elliptiques, par ζ_1 leur rapport, et soit

$$a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0, \qquad a_1c_1 - b_1^2 = n_1. \tag{26}$$

Par hypothèse il existe une multiplication complexe du degré n, qui

d'après le n° **3** est définie par les équations

$$(27)\qquad \begin{cases} (x+yi\sqrt{n_1})\,2\varpi = (x+yb_1)\,2\varpi + ya_1\varpi', \\ (x+yi\sqrt{n_1})\;\varpi' = -yc_1.2\varpi + (x-yb_1)\varpi', \\ x^2+y^2n_1 = n. \end{cases}$$

On voit que les quantités $\lambda\left(\theta+\frac{p\Omega}{n}\right)$ et, par suite, la transformation principale sont complètement déterminées par ces équations, de sorte que pour chaque couple de valeurs de x et de y il n'y a qu'une seule racine de l'équation modulaire principale. Donc, si les racines de cette équation et de l'équation $F(\xi, \eta) = 0$ se correspondent une à une, on peut conclure que chaque valeur de $x+yi\sqrt{n_1}$ ne peut répondre qu'à une seule racine de la dernière équation. Le contraire ne se rencontre que dans le cas des modules de la seconde catégorie d'un degré pair, où, comme on le verra plus tard, on doit faire $l_0 = \left(\frac{1-i^m\eta_1}{1+i^m\eta_1}\right)^2$ ou même $l_0^2 = \left(\frac{1-i^m\eta_1}{1+i^m\eta_1}\right)^4$, l_0 désignant le module obtenu par la transformation principale; mais il est facile de voir que seulement une des valeurs de η_1 qui correspondent à une même valeur de l_0 ou de l_0^2 peut être égale à ξ, puisque autrement on aurait $l_0 = 0$, supposition impossible; donc aussi dans ce cas chaque valeur de $x+yi\sqrt{n_1}$ répond à une seule racine de l'équation

$$F(\xi, \eta) = 0.$$

Réciproquement, si $x^2+y^2n_1 = n$, les équations (27) définissent une multiplication, généralement complexe, du degré n.

Ainsi chaque module singulier de la première espèce et du degré n_1 admet un nombre de multiplications égal au nombre des solutions de l'équation $x^2+y^2n_1 = n$; le nombre de transformations qu'il faut compter n'en est que la moitié, puisque chaque valeur du module transformé, de son carré ou de sa racine carrée, s'obtient avec deux multiplicateurs qui ne se distinguent que par les signes (*voir* le Tableau des transformations linéaires A).

En considérant en *second lieu* les modules de la seconde espèce, les

équations (26), (27) sont remplacées par les suivantes :

$$(28)\quad \begin{cases} a_1\zeta_1^2+(2b_1+1)\zeta_1+c_1=0, \qquad a_1c_1-b_1(b_1+1)=n_1, \\ \dfrac{x+y\,i\sqrt{4n_1-1}}{2}\,2\varpi=\left(\dfrac{x+y}{2}+yb_1\right)2\varpi+ya_1\varpi', \\ \dfrac{x+y\,i\sqrt{4n_1-1}}{2}\,\varpi'=-yc_1.2\varpi+\left(\dfrac{x-y}{2}-yb_1\right)\varpi', \\ x^2+y^2(4n_1-1)=4n, \end{cases}$$

x et y étant de la même parité. Au reste, les conclusions sont les mêmes.

Les transformations définies par les équations (27), (28) ne sont pas toutes de l'espèce que nous avons à considérer; il faut d'abord écarter celles où x et y ont un diviseur commun, s'il s'agit d'un module de la première espèce; pour les modules de la seconde espèce, il faut omettre celles où x et y ont un diviseur commun autre que 2; par là les cas des multiplications ordinaires sont exclus. Enfin il faut que la valeur $\xi=\xi_0$, déterminée par les équations (27) ou (28), satisfasse à l'équation spéciale $F(\xi,\xi)=0$ dont il est question. Supposons d'abord qu'on ait fait $\sqrt{k}=\xi$. En désignant par $f(\xi,\eta_1)=0$ l'équation modulaire principale, on a

$$F(\xi,\eta_1)=f(\xi,i^{r_1s_1}\eta), \qquad \text{si } s_1\equiv 0 \pmod 4,$$

$$F(\xi,\eta_1)=f\left(\xi,\frac{i^{r_1s_1}}{\eta_1}\right), \qquad \text{si } s_1\equiv 2 \pmod 4,$$

$$F(\xi,\eta)=f\left(\xi,i^{s_1s_1}\frac{1-i^{r_1s_1}\eta_1}{1+i^{r_1s_1}\eta_1}\right), \quad \text{si } s_1 \text{ est impair.}$$

Soit de plus $\begin{pmatrix} R_1 & S_1 \\ R_1' & S_1' \end{pmatrix}$ la transformation linéaire qu'il faut combiner avec la transformation principale pour avoir la multiplication complexe (27) ou (28), et qui se détermine par un système d'équations analogue au système (24). Or il faut que la racine carrée du module l_0 déduite de $\sqrt{l}$, c'est-à-dire de ξ, par la transformation principale, se change en η par chacune des transformations linéaires $\begin{pmatrix} r_1 & s_1 \\ r_1' & s_1' \end{pmatrix}$ et

$\begin{pmatrix} R_1 & S_1 \\ R'_1 & S'_1 \end{pmatrix}$; donc on doit avoir

$$\begin{pmatrix} r_1 & s_1 \\ r'_1 & s'_1 \end{pmatrix} = \begin{pmatrix} R_1 & S_1 \\ R'_1 & S'_1 \end{pmatrix} \begin{pmatrix} r_2 & s_2 \\ r'_2 & s'_2 \end{pmatrix},$$

où $r_2 s'_2 - r'_2 s_2 = 1$, et où, au moins s'il ne s'agit pas d'un module linéaire, $r'_2 \equiv s_2 \equiv 0$ et, par suite, $r_2 s'_2 \equiv 1 \pmod 4$. Mais effectivement les modules linéaires ne font pas exception; en effet, si l_0 est linéaire, il admet une multiplication complexe linéaire

$$\varepsilon' \cdot 2\varpi_0 = r_3 \cdot 2\varpi_0 + s_3 \varpi'_0,$$
$$\varepsilon' \cdot \varpi_0 = r'_3 \cdot 2\varpi_0 + s'_3 \varpi'_0,$$

et, par conséquent, on peut remplacer la transformation $\begin{pmatrix} R_1 & S_1 \\ R'_1 & S'_1 \end{pmatrix}$ par $\begin{pmatrix} R_1 & S_1 \\ R'_1 & S'_1 \end{pmatrix} \begin{pmatrix} r_3 & s_3 \\ r'_3 & s'_3 \end{pmatrix} = \begin{pmatrix} R_2 & S_2 \\ R'_2 & S'_2 \end{pmatrix}$, ce qui donne

$$\begin{pmatrix} r_1 & s_1 \\ r'_1 & s'_1 \end{pmatrix} = \begin{pmatrix} R_2 & S_2 \\ R'_2 & S'_2 \end{pmatrix} \begin{pmatrix} s'_3 & -s_3 \\ -r'_3 & r_3 \end{pmatrix} \begin{pmatrix} r_2 & s_2 \\ r'_2 & s'_2 \end{pmatrix}.$$

Or, si l'on n'a pas $r'_2 \equiv s_2 \equiv 0 \pmod 4$, les deux transformations linéaires $\begin{pmatrix} r_2 & s_2 \\ r'_2 & s'_2 \end{pmatrix}$ et $\begin{pmatrix} r_3 & s_3 \\ r'_3 & s'_3 \end{pmatrix}$ donnent nécessairement un résultat identique, quand on les applique à un module quelconque, car autrement $\sqrt{l_0}$ serait déterminé par deux équations incompatibles; donc la transformation $\begin{pmatrix} s'_3 & -s_3 \\ -r'_3 & r_3 \end{pmatrix} \begin{pmatrix} r_2 & s_2 \\ r'_2 & s'_2 \end{pmatrix} = \begin{pmatrix} r_4 & s_4 \\ r'_4 & s'_4 \end{pmatrix}$ n'altère pas la racine carrée d'un module quelconque, c'est-à-dire qu'on a

$$r'_4 \equiv s_4 \equiv 0 \pmod 4.$$

Cela posé, ayant

$$r_4 = R_1 r_2 + S_1 r'_2, \qquad s_4 = R_1 s_2 + S_1 s'_2,$$
$$r'_4 = R'_1 r_2 + S'_1 r'_2, \qquad s'_4 = R'_1 s_2 + S'_1 s'_2,$$

on conclut

$$r_4 \equiv R_1 r_2, \qquad s_4 \equiv S_1 s'_2, \qquad r'_4 \equiv R'_1 r_2, \qquad s'_4 \equiv S'_1 s'_2 \pmod 4;$$

d'où

$$r_1 s_1 \equiv R_1 S_1, \qquad r'_1 s'_1 \equiv R'_1 S'_1, \qquad s_1 s'_1 \equiv S_1 S'_1 \pmod 4.$$

Donc si $s_1 \equiv 0$, on a

$$S_1 \equiv 0, \qquad r'_1 s_1 \equiv R'_1 S'_1 \pmod 4;$$

si $s_1 \equiv 2$,

$$S_1 \equiv 2, \qquad r'_1 s'_1 \equiv R'_1 S'_1:$$

et si $s_1 \equiv \pm 1$,

$$S_1 \equiv \pm 1, \qquad r_1 s_1 \equiv R_1 S_1, \qquad s_1 s'_1 \equiv S_1 S'_1.$$

En substituant les valeurs r_1, s_1, r'_1, s'_1; R_1, S_1, R'_1, S'_1, on a dans chacun des trois cas un système de congruences en x et y, qui expriment que la valeur $\xi = \xi_0$ satisfait à l'équation $F(\xi, \xi) = 0$.

Dans les cas où l'on a $\xi = k$ les congruences $r'_1 s'_1 \equiv R'_1 S'_1$, $r_1 s_1 \equiv R_1 S_1$ doivent évidemment être prises suivant le module 2; si $\xi = k^2$, elles doivent être omises.

Le nombre des transformations des formes (27) et (28) qui satisfont à ces conditions est égal à la multiplicité de la racine $\eta_1 = \xi_0$ de l'équation $F(\xi_0, \eta) = 0$, pourvu qu'on ne compte que pour une seule transformation deux multiplications complexes qui se déduisent l'une de l'autre en changeant simultanément les signes de x et y.

Ce nombre est en même temps la multiplicité de la racine ξ_0 de l'équation $F(\xi, \xi) = 0$. Pour le démontrer, il suffit de faire voir qu'en considérant l'équation $F(\xi, \eta) = 0$ comme l'expression analytique d'une courbe, aucune des droites $\eta = \xi$, $\xi = \xi_0$ ne coïncide avec une tangente de la courbe au point $\xi = \eta = \xi_0$. Dans le cas où l'on a fait $\xi = k$, on a, d'après une formule de Jacobi,

$$\frac{d\eta_1}{d\xi} = \frac{\eta_1(1-\eta_1^2)}{\xi(1-\xi^2)} \frac{\varepsilon^2}{n},$$

ce qui pour $\xi = \eta$ donne

$$\frac{d\eta_1}{d\xi} = \frac{\varepsilon^2}{n},$$

détermination qui est encore valable pour $\xi = k^2$ et pour $\xi = \sqrt{k}$,

comme on le voit aisément; or, ε étant imaginaire, $\frac{\varepsilon^2}{n}$ ne peut être égal à l'unité, ni à l'infini.

On peut se servir de plusieurs méthodes pour débarrasser l'équation $F(\xi, \xi) = 0$ des racines étrangères à la question. Dans beaucoup de cas les modules du degré n seuls sont des racines simples, ce qui fournit un moyen de les isoler. On peut, dans tous les cas, calculer préalablement les équations dont dépendent les racines étrangères, et les supprimer par une série de divisions. Enfin, si l'on connaît l'équation du multiplicateur ε, on peut en éliminer ε au moyen de l'équation $\varepsilon^2 + n = 0$ ou $\varepsilon^2 \pm \varepsilon + n = 0$, suivant qu'il s'agit de modules de la première ou de la seconde espèce; en cherchant le plus grand commun diviseur des premiers membres de l'équation résultante et de l'équation $F(\xi, \xi) = 0$, on obtient un polynôme qui, égalé à zéro, donne évidemment l'équation des modules du degré n.

Pour n'avoir pas un trop grand nombre de cas à distinguer, nous nous occuperons principalement des équations en k^2, quoiqu'il soit souvent préférable dans les calculs de passer par des équations en $\sqrt{k}$, ou même en $\sqrt[4]{k}$.

9. Supposons que n soit impair. Nous choisissons pour transformations principales celles qui sont définies par les équations

$$\varepsilon_0 . 2\omega = \quad \delta . 2\omega_0,$$
$$\varepsilon_0 . \ \omega' = -\ell . 2\omega_0 + n'\omega'_0, \qquad \frac{\omega'_0}{2\omega_0} = \zeta_0 = \frac{\ell + \delta\zeta}{n'},$$

qui donnent les formules bien connues

$$Y = \lambda(\varepsilon_0 0, k_0) = \varepsilon_0 \lambda(0) \prod_1^{\frac{n-1}{2}} \frac{1 - \frac{\lambda^2 0}{\lambda^2\left(\frac{p\Omega}{n}\right)}}{1 - k^2\lambda^2(0)\lambda^2\left(\frac{p\Omega}{n}\right)},$$

$$\varepsilon_0 = (-1)^{\frac{n-1}{2}} \prod_1^{\frac{n-1}{2}} \frac{\lambda^2\left(\frac{p\Omega}{n}\right)\nu^2\left(\frac{p\Omega}{n}\right)}{\mu^2\left(\frac{p\Omega}{n}\right)}, \qquad \sqrt{k_0} = (\sqrt{k})^n \prod_1^{\frac{n-1}{2}} \frac{\mu^2\left(\frac{p\Omega}{n}\right)}{\nu^2\left(\frac{p\Omega}{n}\right)}.$$

Le nombre ℓ n'est déterminé que par rapport au module n' : nous

pouvons donc le supposer divisible par 4; de plus, δ étant impair et de signe arbitraire, nous supposerons

$$\delta \equiv 1 \pmod 4, \qquad \text{d'où} \qquad n' \equiv n \pmod 4;$$

par là les équations (24) donnent

$$(29) \quad r_1 \equiv r, \qquad s_1 \equiv s, \qquad r'_1 \equiv (-1)^{\frac{n-1}{2}} r', \qquad s'_1 \equiv (-1)^{\frac{n-1}{2}} s'.$$

Nous supposerons l'équation modulaire écrite entre $\sqrt{k_0}$ et $\sqrt{k}$: nous la désignerons par

$$(30) \qquad f(\sqrt{k}, \sqrt{k_0}) = 0;$$

si on la combine avec une des transformations linéaires du Tableau, on a une équation entre $\sqrt{k}$ et $\sqrt{k_1}$ dont les racines correspondent une à une aux racines de l'équation (30). On sait que dans l'équation (30) les coefficients des diverses puissances de $\sqrt{k_0}$ sont des fonctions entières de $\sqrt{k}$ à coefficients entiers, le premier terme étant $(\sqrt{k_0})^N$, le dernier $(\sqrt{k})^N$. De plus, si n n'est pas un carré parfait, les termes du plus haut et du plus petit degré en $\sqrt{k}$ et $\sqrt{k_0}$ ont pour coefficients une même puissance de 2. Cela a été démontré par Sohnke pour les transformations de degré premier (*Journal de Crelle*, t. 16), et il n'est pas difficile de le démontrer en général. En effet, pour les petites valeurs de k, on peut développer $\sqrt{k_0}$ en une série ordonnée suivant les puissances croissantes de $(\sqrt{k})^{\frac{1}{n'}}$, dont le premier terme est

$$e^{2\pi i \frac{t}{4n'}} 2^{\frac{n'-\delta}{n'}} (\sqrt{k})^{\frac{\delta}{n'}}$$

(*voir* la *Théorie des fonctions elliptiques* de MM. Briot et Bouquet, p. 631, où cette propriété est démontrée pour les degrés premiers). On a donc, pour les petites valeurs de k,

$$f(\sqrt{k}, \sqrt{k_0}) = \Pi\left(\sqrt{k_0} - e^{2\pi i \frac{t}{4n'}} 2^{\frac{n'-\delta}{n'}} \sqrt{k}^{\frac{\delta}{n'}} - \dots\right);$$

or on a le terme du plus petit degré, en prenant de chaque facteur le terme dont le degré est le plus petit, c'est-à-dire, le premier terme si $\delta > n'$, le second si $\delta < n'$; donc, le coefficient du terme cherché de la fonction $f(\sqrt{k}, \sqrt{k_0})$, étant un nombre entier, est bien une puissance de 2. De plus, ayant

$$f(\sqrt{k}, \sqrt{k_0}) = (\sqrt{k})^N (\sqrt{k_0})^N f\left(\frac{1}{\sqrt{k}}, \frac{1}{\sqrt{k_0}}\right),$$

le coefficient du terme du plus haut degré est égal à celui du terme du plus petit degré.

Par la remarque faite à la fin du n° 6, il est facile de voir qu'en supposant $\sqrt{k}$ égal à l'une des valeurs

$$0, \quad \infty, \quad 1, \quad -1, \quad i, \quad -i,$$

$\sqrt{k_0}$ sera respectivement égal à

$$0, \quad \infty, \quad 1, \quad -1, \quad (-1)^{\frac{n-1}{2}} i, \quad -(-1)^{\frac{n-1}{2}} i,$$

c'est-à-dire qu'on aura, pour les valeurs critiques de $\sqrt{k}$,

$$\sqrt{k_0} = (\sqrt{k})^n.$$

Soit, pour un moment, $\sqrt{k} = x$, $\sqrt{k_0} = y$, et faisons subir à x la transformation linéaire $\begin{pmatrix} r & 1 \\ -1 & 0 \end{pmatrix}$, et soit ξ la racine carrée du module transformé; on aura

$$\xi = i^{-r} \frac{1-x}{1+x}, \qquad x = \frac{i^{-r} - \xi}{i^{-r} + \xi};$$

soit de plus η la valeur de $\sqrt{k_0}$ correspondant à ξ, de sorte qu'on ait

$$f(\xi, \eta) = 0.$$

Évidemment η se déduit de x par une transformation du degré n, c'est-à-dire qu'on l'obtient par une transformation principale du

degré n suivie d'une transformation linéaire; donc on a

$$\eta_1 = i^m y \qquad \text{ou} \qquad \eta_1 = \frac{i^m}{y}$$

ou enfin

$$\eta_1 = i^m \frac{1 - i^\mu y}{1 + i^\mu y};$$

or, par la remarque précédente, il est facile de voir qu'on a effectivement

$$\eta_1 = i^{-nr} \frac{1 - y}{1 + y}, \qquad y = \frac{i^{-nr} - \eta_1}{i^{-nr} + \eta_1}.$$

En reportant les valeurs de x et de y dans l'équation $f(x, y) = 0$, on voit que l'équation $f(\xi, \eta_1) = 0$ entraîne celle-ci :

$$f\left(\frac{i^{-r} - \xi}{i^{-r} + \xi}, \quad \frac{i^{-nr} - \eta_1}{i^{-nr} + \eta_1}\right) = 0.$$

Voici encore une remarque qui nous sera utile. On a

$$\prod_1^{\frac{n-1}{2}} \frac{\mu^2\left(\frac{p\omega}{n}\right)}{\nu^2\left(\frac{p\omega}{n}\right)} = \frac{\sqrt{k_0}}{\sqrt{k}} \frac{1}{k^{\frac{n-1}{2}}} = \frac{\sqrt{k_0}\sqrt{k}}{k^{\frac{n+1}{2}}},$$

et l'on sait que le premier membre est racine d'une équation du degré N dont les coefficients sont rationnels en k^2; par suite, en substituant à l'inconnue de cette équation, soit $\frac{\sqrt{k_0}}{\sqrt{k}} \frac{1}{k^{\frac{n-1}{2}}}$, soit $\frac{\sqrt{k_0}\sqrt{k}}{k^{\frac{n+1}{2}}}$, on obtient l'équation modulaire. Donc celle-ci peut être mise sous la forme

$$(31) \qquad \Phi\left(\frac{\sqrt{k_0}}{\sqrt{k}}, k^2\right) = 0, \qquad \text{si } n \equiv 1 \pmod 4,$$

et sous la forme

$$(32) \qquad \Phi(\sqrt{k_0}\sqrt{k}, k^2) = 0, \qquad \text{si } n \equiv -1 \pmod 4.$$

10. *Considérons les modules de la première espèce et de la première catégorie d'un degré de la forme* $4h+1$. — Le coefficient a est nécessairement congru à $2 \pmod 4$, b et c sont impairs; les équations (29) deviennent

$$r_1 \equiv b, \qquad s_1 \equiv a \equiv 2, \qquad r'_1 \equiv -c, \qquad s'_1 \equiv -b \pmod 4.$$

Il faut donc employer le cas B du tableau des transformations linéaires, c'est-à-dire qu'il faut faire

$$\sqrt{k} = \frac{i^{-bc}}{\sqrt{k_0}}, \qquad \varepsilon' = (-1)^{\frac{b-1}{2}+c} k_0, \qquad \lambda(\varepsilon' \varepsilon_0 0) = \varepsilon' \lambda(\varepsilon_0 0) = \varepsilon' Y;$$

d'où l'on tire

$$\sqrt{k_0} = \frac{i^{-bc}}{\sqrt{k}}, \qquad \varepsilon_0 = i^b k \sqrt{n}, \qquad \lambda(i\sqrt{n}\,0) = \frac{(-1)^{\frac{b-1}{2}}}{k} Y.$$

En substituant l'expression de $\sqrt{k_0}$ dans l'équation modulaire principale, on obtient donc deux équations en $\sqrt{k}$, dont les coefficients, qui sont de la forme $p+qi$, ne se distinguent que par le signe de i; le premier et le dernier coefficient sont ± 1. L'équation (31) fait voir que les équations trouvées peuvent être mises sous la forme

$$\Phi\left(\frac{1}{i^{bc}k}, k^2\right) = 0$$

ou bien

$$f(i^{bc}k) = 0,$$

f dénotant une fonction entière à coefficients entiers.

Cette équation n'est satisfaite ni par $k=0$, ni par $k=\pm 1$.

Soit l un module singulier de la première espèce et du degré n_1, satisfaisant à l'équation $f(i^{bc}k)=0$, on aura, d'après (27) et (29),

$$x^2 + y^2 n_1 = n, \qquad R_1 \equiv x + y b_1, \qquad S_1 \equiv y a_1$$
$$R'_1 \equiv -y c_1, \qquad S'_1 \equiv x - y b_1 \pmod 4.$$

Or on doit avoir (n° 8)

$$S_1 \equiv s_1 \equiv 2, \qquad R'_1 S'_1 \equiv r'_1 s'_1 \equiv bc \pmod 4;$$

donc les conditions à remplir pour que l satisfasse à l'équation sont les suivantes :

$$(33)\qquad \left\{\begin{array}{rl} x^2+y^2n_1=n, & ya_1\equiv 2 \\ -xyc_1+y^2b_1c_1\equiv bc & \end{array}\right\} \pmod 4.$$

On en conclut que y et c_1 sont impairs, et que $a_1\equiv 2 \pmod 4$; b_1 est nécessairement impair; car, dans le cas contraire, on aurait,

$$n_1=a_1c_1-b_1^2\equiv 2 \pmod 4;$$

d'où

$$x^2+y^2n_1\equiv 3 \quad \text{ou} \quad \equiv 2,$$

contre l'hypothèse. Donc n_1 est de la forme $4h+1$, x pair. Si $x>0$, on peut changer son signe sans troubler les congruences (mod 4); donc, dans ces cas, l est une racine double ou multiple; l est en effet racine multiple s'il existe plus de quatre solutions de l'équation indéterminée $x^2+y^2n_1=n$ en nombres premiers entre eux.

Aucun module de la seconde espèce ne satisfait à nos équations. En effet, d'après (28), on aurait

$$R_1\equiv \frac{x+y}{2}+yb_1\equiv\pm 1, \qquad S_1\equiv ya_1\equiv 2 \pmod 4,$$

$$R'_1\equiv -yc_1\equiv\pm 1, \qquad S'_1\equiv \frac{x-y}{2}-yb_1\equiv\pm 1 :$$

donc y serait impair; or on trouve $R_1-S'_1\equiv y(2b_1+1)$, ce qui est impossible, $R_1-S'_1$ devant être pair.

Par ce qui précède il est démontré que les racines de l'équation $f(i^{bc}k)=0$ sont les modules de la première espèce et de la première catégorie dont les degrés, nécessairement de la forme $4h+1$, vérifient l'équation $n=x^2+y^2n_1$, x et y étant premiers entre eux, x pair, et pour lesquels le nombre b_1c_1 satisfait à la congruence

$$b_1c_1\equiv bc+x \pmod 4,$$

issue de (33). Parmi ces racines les modules du degré n seuls sont des

racines simples. Si l'on a calculé préalablement les équations des modules de première espèce et de première catégorie des degrés $4h+1$ inférieurs à n, on peut obtenir l'équation relative au degré n par de simples divisions; dans ce cas, on remarquera qu'il faudra alterner le signe de i dans les équations des degrés inférieurs. On trouve donc finalement deux équations en k,

$$F(ik)=0, \qquad F(-ik)=0,$$

équivalentes à une seule équation en k^2

$$F_1(k^2)=0,$$

qui est réciproque, et dont les coefficients sont des nombres entiers, le premier et le dernier étant 1. Les degrés de ces équations sont égaux au double du nombre des classes primitives du déterminant $-n$, comme on le sait *a priori*. Les deux équations

$$F(i^{bc}k)=0 \qquad \text{et} \qquad F(i^{-bc}k)=0$$

n'ayant pas de racine commune, on peut conclure qu'on aura

$$i^{bc}k=\psi(k^2),$$

ψ dénotant une fonction rationnelle à coefficients entiers, qui est identiquement la même pour toutes les racines de l'équation $F_1(k^2)=0$.

Si, par exemple, on fait $n=5$, et qu'on pose $k=u^4$, $k_0=v^4$, l'équation modulaire principale peut s'écrire comme il suit :

$$(u^6+5u^4v^2-5u^2v^4-v^6)^2=16u^2v^2(1-u^4v^4)^2.$$

En y faisant $u^2=\sqrt{k}$, $v^2=\dfrac{-i}{\sqrt{k}}$, on trouve

$$k^6-10ik^5-15k^4+12ik^3+15k^2-10ik-1=0$$

ou bien

$$(k-i)^2(k^4-8ik^3+2k^2+8ik+1)=0.$$

Égalant à zéro le second facteur, on a l'équation $F(ik) = 0$; en la résolvant, on trouve

$$k = i\left(2 + \sqrt{5} + 2\sqrt{2 + \sqrt{5}}\right)$$

ou

$$k^2 = -\left[\tfrac{1}{2}(\sqrt{5}+1) + \sqrt{\tfrac{1}{2}(\sqrt{5}+1)}\right]^2.$$

C'est le module trouvé par *Abel* dans les *Recherches sur les fonctions elliptiques*.

De l'analyse précédente on tire facilement une formule d'Arithmétique. En effet, l'équation que nous avons décomposée est du degré N. D'autre part, on obtient ce degré, en prenant pour chaque valeur paire de x, figurant dans l'équation $n = x^2 + y^2 n_1$, le nombre des classes de formes quadratiques du déterminant $-(n - x^2)$, dans lesquelles le plus grand commun diviseur des trois coefficients a, b, c sont premiers à n, multipliant ce nombre par 2 si $x = 0$, et si $n_1 = 1$ (puisqu'il n'y a qu'une seule valeur de k^2 de la première espèce et de la première catégorie du degré 1), par 4 dans les autres cas, et faisant la somme des produits formés. On peut conserver le facteur 4 dans le cas où $n_1 = 1$, si l'on ajoute à N la correction nécessaire. Pour écrire la formule, désignons, pour un moment, par $F_1(m)$ le nombre des classes du déterminant $-m$ où les trois coefficients n'ont pas un même diviseur commun avec n, et désignons par $2\varphi_1(n)$ le nombre des solutions de l'équation $n = 4x^2 + y^2$ en nombres premiers entre eux; la correction à ajouter sera $\varphi_1(n)$, et, par suite, on aura, en supposant $n = 4h + 1$,

$$2F_1(n) + 4F_1(n - 2^2) + 4F_1(n - 4^2) + \ldots = N + \varphi_1(n).$$

Au fond cette équation ne diffère pas de celle qu'on obtient en ajoutant les formules V et VI de M. Kronecker (*Journal de Crelle*, t. 57, p. 249), et faisant $m \equiv 1 \pmod 4$. On trouve des corollaires analogues dans tous les cas que nous avons à considérer dans la suite; dans un Mémoire inséré aux *Comptes rendus*, t. L, le P. Joubert en a développé plusieurs. Nous les passerons ordinairement sous silence, pour y revenir dans un paragraphe spécial.

11. *Modules de la première espèce et de la première catégorie d'un degré de la forme* $4h-1$. — On a $a\equiv 0 \pmod 4$, b et c sont impairs; par suite les congruences (29) deviennent

$$r_1\equiv b\equiv \pm 1, \qquad s_1\equiv 0, \qquad r'_1\equiv c\equiv \pm 1,$$
$$s'_1\equiv b\equiv \pm 1, \qquad (\mathrm{mod.}\,4),$$

et, par conséquent, on a

$$\sqrt{k}=i^{-bc}\sqrt{k_0}, \qquad \varepsilon'=(-1)^{\frac{b-1}{2}},$$

d'où

$$\sqrt{k}\sqrt{k_0}=i^{bc}k, \qquad \varepsilon_0=i^b\sqrt{n}, \qquad \lambda(i\sqrt{n}\,0)=(-1)^{\frac{b-1}{2}}\mathrm{Y}.$$

En substituant dans l'équation modulaire, on obtient une équation en k, qui, en vertu de l'équation (32), prend la forme

$$f(i^{bc}k)=0.$$

Les coefficients des diverses puissances de $i^{bc}k$ sont des nombres entiers, le premier et le dernier étant égaux à une même puissance de 2. L'équation admet la racine, en général multiple, $k=0$, mais elle n'est pas satisfaite par $k=\pm 1$. Quant aux autres racines, on a des résultats complètement analogues à ceux du numéro précédent. Finalement on trouve les équations

$$\mathrm{F}(i^{bc}k)=0, \qquad \mathrm{F}_1(k^2)=0,$$

qui ne sont satisfaites que par les modules du degré n; la seule différence est que le premier et le dernier coefficient sont une même puissance de 2. Cependant, si n est de la forme $8h'+3$, cette puissance de 2 disparaît comme diviseur commun à tous les coefficients, de sorte que dans ce cas le premier et le dernier coefficient de $\mathrm{F}_1(k^2)$ deviennent 1. C'est ce que nous démontrerons plus tard.

Exemples. — Pour $n=3$ l'équation modulaire

$$u^4-v^4+2uv(1-u^2v^2)=0$$

donne, en chassant les puissances impaires de uv et faisant $u^2=\sqrt{k}$, $v^2=\sqrt{k_0}$

$$k^2-4\sqrt{k^3}\sqrt{k_0^3}+6kk_0-4\sqrt{k}\sqrt{k_0}+k_0^2=0;$$

en y faisant $\sqrt{k_0}=i\sqrt{k}$, on a

$$4k(k^2+ik-1)=0;$$

le dernier facteur donne pour les modules du degré 3 les deux valeurs

$$k^2=\tfrac{1}{2}(1\pm i\sqrt{3})=e^{\pm\frac{\pi i}{3}}.$$

Pour $n=7$, l'équation modulaire est

$$(u^8-1)(v^8-1)-(uv-1)^8=0.$$

En y faisant $v=u\sqrt{i}$, $u^2=\sqrt{k}$, on a

$$\left[k^2-1-(\sqrt{i}\sqrt{k}-1)^4\right]\left[k^2-1+(\sqrt{i}\sqrt{k}-1)^4\right]=0$$

ou bien, en chassant les radicaux,

$$4k(k^2-ik-1)^2(4k^2+ik-4)=0.$$

Le dernier facteur donne, pour les modules du degré 7, l'expression

$$k^2=\left[\tfrac{1}{8}(i\pm 3\sqrt{7})\right]^2.$$

12. *Modules de la seconde espèce du déterminant* $-n$. — De l'équation modulaire répondant à la transformation principale du degré $n=4h-1$, on peut tirer tous les modules de la seconde espèce du déterminant $-n$, c'est-à-dire du degré $\frac{n+1}{4}$. En faisant $x=0$, $y=2$ et, remplaçant $4n-1$ par n, les équations (10) donnent

$$i\sqrt{n}\,.\,2\omega=(2b+1)\,2\omega+2a\,\omega',$$
$$i\sqrt{n}\,.\;\omega'=-2\,.\,c\,2\omega-(2b+1)\omega',$$
$$n=4ac-(2b+1)^2.$$

On fera donc

$$r_1 \equiv s'_1 \equiv 2b+1, \qquad s_1 \equiv 2a, \qquad r'_1 \equiv 2c \qquad (\mathrm{mod}4).$$

La première catégorie n'existe que si n est de la forme $8h-1$; de plus a est pair, et par conséquent s_1 est divisible par 4; on a donc

$$\sqrt{k} = (-1)^c \sqrt{k_0}, \qquad \varepsilon' = (-1)^b,$$

d'où

$$\sqrt{k_0} = (-1)^c \sqrt{k}, \qquad \varepsilon_0 = i^{2b+1}\sqrt{n}, \qquad \lambda(i\sqrt{n}\,0) = (-1)^b \mathrm{Y}.$$

En substituant dans l'équation modulaire, on obtient une équation de la forme

$$f[(-1)^c k] = 0$$

(32), dont les coefficients sont des entiers, le premier et le dernier étant égaux à une même puissance de 2. Elle admet évidemment les racines $k=0$ et $k=(-1)^c$; mais elle n'est satisfaite par aucun module de la première espèce; en effet, les équations (27) et (29) donneraient

$$\mathrm{S}_1 \equiv y a_1 \equiv 0, \qquad \mathrm{R}'_1 \equiv y c_1, \qquad \mathrm{R}'_1 \mathrm{S}'_1 \equiv 2c \qquad (\mathrm{mod}4).$$

Or, S_1 étant pair, S'_1 serait impair, et par suite $\mathrm{R}'_1 = y c_1$ serait pair; donc, a_1 et c_1 n'étant pas tous les deux pairs, y serait pair, ce qui rendrait impossible la relation $x^2 + y^2 n_1 = n$. Pour les modules de la seconde espèce, satisfaisant à l'équation trouvée, on doit avoir [équations (28), (29)]

$$\left.\begin{aligned} &\mathrm{R}_1 \equiv \frac{x+y}{2} + y b_1, \qquad \mathrm{S}_1 \equiv y a_1, \\ &\mathrm{R}'_1 \equiv y c_1, \qquad\qquad \mathrm{S}'_1 \equiv -\frac{x-y}{2} + y b_1 \end{aligned}\right\} (\mathrm{mod}4),$$

et (n° 8)

$$\mathrm{S}_1 \equiv 0, \qquad \mathrm{R}'_1 \mathrm{S}'_1 \equiv 2c.$$

S étant pair, R_1 et S'_1 seront impairs; or, ayant

$$\mathrm{R}_1 + \mathrm{S}'_1 \equiv y(2b_1+1),$$

y et par suite x seront pairs. En remplaçant $4n_1 - 1$ par n_1, et faisant par suite $n_1 = 4a_1c_1 - (2b_1 + 1)^2$, on a

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 n_1 = n,$$

d'où l'on conclut que $\frac{x}{2}$ est pair, $\frac{y}{2}$ impair; par suite a_1 sera pair, n_1 de la forme $8h - 1$: donc enfin $\frac{x}{2}$ est divisible par 4. L'équation

$$f[(-1)^c k] = 0$$

admet donc comme racines, outre 0 et $(-1)^c$, les modules de la seconde espèce et de la première catégorie dont les déterminants $-n_1$ satisfont à la relation $n = 16\xi^2 + \eta^2 n_1$, ξ et η étant premiers entre eux, pourvu toutefois qu'on détermine le signe de chaque module conformément à la congruence $c_1 \equiv c \pmod 2$. Si $\xi > 0$, son signe est arbitraire : donc les modules du déterminant $-n$ seuls sont des racines simples. En les isolant, on obtient une équation en k, $F[(-1)^c k] = 0$, à coefficients entiers, le premier et le dernier étant une même puissance de 2. On a donc une seule équation en k^2. D'ailleurs ces équations sont réductibles, comme on le verra plus bas.

Pour $n = 7$, l'équation modulaire est

$$(u^8 - 1)(v^8 - 1) - (uv - 1)^8 = 0;$$

au lieu de faire $u^2 = v^2$ après avoir chassé les puissances impaires de uv, faisons simplement $u = v$, ce qui d'ailleurs modifie la multiplicité de la racine $u^2 = 0$; on trouve

$$[u^8 - 1 + (u^2 - 1)^4][u^8 - 1 - (u^2 - 1)^4] = 0$$

ou bien

$$u^2(u^2 - 1)^2(u^4 - u^2 + 2)(2u^4 - u^2 + 1) = 0.$$

Par conséquent les carrés des modules de la seconde espèce et de la première catégorie du déterminant -7 sont compris dans les expressions

$$k^2 = \left[\tfrac{1}{2}(1 \pm i\sqrt{7})\right]^4, \qquad k^2 = \left[\tfrac{1}{4}(1 \pm i\sqrt{7}\right]^4.$$

On a les mêmes valeurs de k^2 en faisant $u = -v$.

Dans la seconde catégorie a est impair; c est pair ou impair suivant que n est de la forme $8h-1$ ou $8h+3$: donc on a

$$s_1 \equiv 2, \qquad r'_1 \equiv \frac{n+1}{2} \pmod 4,$$

$$\sqrt{k} = \frac{(-1)^{\frac{n+1}{4}}}{\sqrt{k_0}}, \qquad \varepsilon' = (-1)^b k_0,$$

ce qui donne

$$\sqrt{k_0}\sqrt{k} = (-1)^{\frac{n+1}{4}}, \qquad \varepsilon_0 = i^{2b+1} k \sqrt{n}, \qquad \lambda(i\sqrt{n}\,0) = (-1)^b \frac{1}{k} Y.$$

En substituant la valeur de $\sqrt{k_0}$ dans l'équation modulaire, on obtient une équation en k^2 [équation (32)]

$$f(k^2) = 0,$$

qui est satisfaite par $k^2 = 1$ seulement si $n = 8h-1$, mais qui n'est jamais satisfaite par $k^2 = 0$. Au reste, elle admet pour racines les carrés des modules de la seconde espèce et de la seconde catégorie dont les déterminants $-n_1$ vérifient la relation

$$n = 16\xi^2 + \eta^2 n_1,$$

ξ et η étant premiers entre eux, les modules du déterminant $-n$ seuls étant des racines simples. En débarrassant l'équation $f(k^2) = 0$ de la racine $k^2 = 1$ et des racines doubles ou multiples, on trouve finalement une équation en k^2, réciproque, à coefficients entiers, dont évidemment le premier et le dernier sont 1.

Exemples : $n = 3$. — Faisant, dans l'équation modulaire

$$u^4 - v^4 + 2uv(1 - u^2v^2) = 0,$$

$uv = \pm i$, on a

$$u^8 \mp 4iu^4 - 1 = 0,$$

ou bien

$$k^2 \mp 4ik - 1 = 0; \qquad \text{d'où} \qquad k^2 = -(2 \pm \sqrt{3})^2.$$

$n = 7$. — En faisant, dans l'équation

$$(u^8 - 1)(v^8 - 1) - (uv - 1)^8 = 0,$$

$uv = 1$, on a seulement la racine double $k^2 = 1$; mais, en faisant $uv = -1$, on trouve

$$(u^8 - 1)^2 + 2^8 u^8 = 0; \qquad \text{d'où} \qquad u^8 \pm 16iu^4 - 1 = 0 :$$

donc

$$k^2 = -\tfrac{1}{4}(3 \pm \sqrt{7})^4.$$

$n = 11$. — On trouve, en faisant, dans l'équation modulaire $uv = \pm i$, $u^2 = \sqrt{k}$,

$$k^6 \pm 44ik^5 + 77k^4 \mp 152ik^3 - 77k^2 \pm 44ik - 1 = 0;$$

d'où, en chassant les puissances impaires de k,

$$k^{12} + 2090k^{10} - 7601k^8 + 15116k^6 - 7601k^4 + 2090k^2 + 1 = 0.$$

13. *Modules de la première espèce et de la seconde catégorie, d'un degré impair.* — Puisque, dans les congruences,

$$\left.\begin{aligned} r_1 &\equiv b, & s_1 &\equiv a \equiv \pm 1, \\ r'_1 &\equiv (-1)^{\frac{n+1}{2}} c, & s'_1 &= (-1)^{\frac{n+1}{2}} b \end{aligned}\right\} \pmod 4,$$

a et, par suite, s_1 sont impairs, on a

$$\sqrt{k} = i^{-ab}\frac{1 - i^{nab}\sqrt{k_0}}{1 + i^{nab}\sqrt{k_0}}, \qquad \varepsilon' = \frac{i^a}{2}(1 + i^{nab}\sqrt{k_0})^2;$$

d'où l'on tire, en faisant, pour abréger, $\Delta Y = \mu(\varepsilon_0 0, k_0)\nu(\varepsilon_0 0, k_0)$,

$$\sqrt{k_0} = i^{-nab}\frac{1 - i^{ab}\sqrt{k}}{1 + i^{ab}\sqrt{k}}, \qquad \varepsilon' = \frac{2i^a}{(1 + i^{ab}\sqrt{k})^2},$$

$$\varepsilon_0 = (-1)^{\frac{n-1}{2}}\frac{1}{2}\sqrt{n}(1 + i^{ab}\sqrt{k})^2, \qquad \lambda(i\sqrt{n}\,0) = \frac{2\varepsilon' Y}{1 + \Delta Y - i^{3nab}k_0 Y^2}.$$

En substituant l'expression de $\sqrt{k_0}$ dans l'équation modulaire, on obtient quatre équations répondant aux quatre valeurs de $ab \pmod 4$; mais il est facile de voir, au moyen des formules (31), (32), que ces équations ne donnent qu'une seule équation en k^2.

En effet, si $n \equiv 1 \pmod 4$, l'équation deviendra

$$\Phi\left(\frac{1 - i^{ab}\sqrt{k}}{i^{ab}\sqrt{k} + i^{2ab}k}, k^2\right) = 0,$$

et, si $n \equiv -1 \pmod 4$,

$$\Phi\left(\frac{i^{ab}\sqrt{k} - i^{2ab}k}{1 + i^{ab}\sqrt{k}}, k^2\right) = 0.$$

Donc, en désignant par

$$f(\sqrt{k}) = 0$$

l'équation qui répond à $b \equiv 0 \pmod 4$, on aura généralement

$$f(i^{ab}\sqrt{k}) = 0.$$

L'équation $f(\sqrt{k}) = 0$ n'est pas satisfaite par $k = 0$, $\sqrt{k} = \pm 1$; elle est satisfaite par $\sqrt{k} = \pm i$ seulement si $n \equiv -1 \pmod 4$. On voit aussi facilement qu'elle n'est satisfaite par aucun module de la seconde espèce. Pour les modules de la première espèce, on doit avoir

$$S_1 \equiv y a_1 \equiv \pm 1 \pmod 4;$$

donc y et a_1 sont impairs; de plus, il faut que

$$R_1 S_1 \equiv S_1 S'_1 \equiv 0;$$

d'où

$$x + y b_1 \equiv x - y b_1 \equiv 0 \pmod 4.$$

On en conclut que $2x \equiv 0 \pmod 4$, et que par suite x est pair et $b_1 \equiv x \pmod 4$. Par conséquent les racines de l'équation $f(z) = 0$ sont $\pm i$ (seulement si $n = 4h - 1$) et les racines carrées des modules de

la première espèce et de la seconde catégorie dont le degré n_1 vérifie la relation $n = x^2 + y^2 n_1$, x et y étant premiers entre eux, le premier pair et le dernier impair, et dont le coefficient b_1 est congru à $x \pmod 4$.) Évidemment les modules du degré n sont seuls des racines simples. En débarrassant l'équation des autres racines, on a finalement une équation $F(\sqrt{k}) = 0$, répondant au cas où $b \equiv 0 \pmod 4$; généralement on a

$$F(i^{ab}\sqrt{k}) = 0.$$

En chassant $\sqrt{k}$ et les puissances impaires de k, on a une seule équation en k^2, $F_1(k^2) = 0$. Remarquons encore que, puisque deux quelconques des quatre équations $F(\pm\sqrt{k}) = 0$, $F(\pm i\sqrt{k}) = 0$ n'ont pas de racines communes, $i^{ab}\sqrt{k}$ peut être exprimé en fonction rationnelle de k^2 :

$$i^{ab}\sqrt{k} = \psi(k^2),$$

la fonction ψ étant la même pour toutes les racines de l'équation

$$F_1(k^2) = 0.$$

Exemples. — Pour $n = 3$, on obtient, en écrivant z au lieu de $\sqrt{k}$, l'équation suivante

$$(z^2 + 1)^2(z^4 + 8z^3 + 2z^2 - 8z + 1) = 0;$$

le dernier facteur, qui répond aux modules du troisième degré, donne

$$z = \sqrt{k} = (\sqrt{3} + \sqrt{2})(\sqrt{2} + 1).$$

Pour $n = 5$, on trouve

$$(z^2 - 2z - 1)^2 \times (z^8 + 16z^7 - 12z^6 + 16z^5 + 38z^4 - 16z^3 - 12z^2 - 16z + 1) = 0,$$

où le premier facteur donne les modules linéaires de la seconde catégorie, le second ceux du cinquième degré. Pour trouver ces derniers,

on peut faire $z - \frac{1}{z} = p$; on a ainsi

$$p^4 + 16p^3 - 8p^2 + 64p + 16 = (p^2 + 8p + 4)^2 - 80p^2 = 0;$$

d'où

$$p = -4 - 2\sqrt{5} - 4\sqrt{2 + \sqrt{5}},$$

$$-z = 2 + \sqrt{5} + 2\sqrt{2 + \sqrt{5}} + \sqrt{2 + \sqrt{5}}\sqrt{4 + 2\sqrt{5} + 2\sqrt{2 + \sqrt{5}}}$$

$$= \tfrac{1}{2}\left[4 + 2\sqrt{5} + 3\sqrt{2} + \sqrt{10} + (4 + \sqrt{2} + \sqrt{10})\sqrt{2 + \sqrt{5}}\right].$$

14. *Modules de la seconde espèce d'un degré impair.* — Le degré n étant donné par la relation $n = ac - b(b+1)$, a et c sont impairs. On peut employer à volonté le premier ou le second des deux systèmes (9); si l'on choisit le premier, on a

$$\left.\begin{array}{ll} r_1 \equiv b + 1, & s_1 \equiv a \equiv \pm 1, \\ r'_1 \equiv (-1)^{\frac{n+1}{2}} c, & s'_1 \equiv (-1)^{\frac{n+1}{2}} b \end{array}\right\} \pmod 4;$$

donc on doit faire

$$\sqrt{k_0} = i^{-nab}\frac{1 - i^{a(b+1)}\sqrt{k}}{1 + i^{a(b+1)}\sqrt{k}},$$

$$\varepsilon' = \frac{2\,i^a}{\left[1 + i^{a(b+1)}\sqrt{k}\right]^2},$$

$$\varepsilon_0 = (-1)^{\frac{a-1}{2}}\tfrac{1}{4}\left(-i + \sqrt{4n-1}\right)\left[1 + i^{a(b+1)}\sqrt{k}\right]^2,$$

$$\lambda\left(\frac{1 + i\sqrt{4n-1}}{2}\,0\right) = \frac{2\varepsilon' Y}{1 + \Delta(Y) - i^{2nab}k_0 Y^2}.$$

On en tire, pour $n \equiv 1 \pmod 4$,

$$\frac{\sqrt{k_0}}{\sqrt{k}} = i^a\frac{1 - i^{a(b+1)}\sqrt{k}}{i^{a(b+1)}\sqrt{k} + i^{2a(b+1)}k}$$

et, pour $n \equiv -1$,

$$\sqrt{k_0}\sqrt{k} = i^{-a}\frac{i^{a(b+1)}\sqrt{k} - i^{2a(b+1)}k}{1 + i^{a(b+1)}\sqrt{k}}.$$

Donc, en vertu des formules (31) et (32), on a une équation de la forme

$$f\left[i^{a(b+1)}\sqrt{k}, i^a\right] = 0, \tag{34}$$

le polynôme $f(z, i)$ étant le même pour tous les cas appartenant au même degré.

Si l'on emploie le second système (9), on trouve

$$r_1 \equiv b, \qquad s'_1 \equiv (-1)^{\frac{n+1}{2}}(b+1);$$

on est ainsi conduit à l'équation

$$f(i^{ab}\sqrt{k}, i^{-a}) = 0, \tag{35}$$

qui, par conséquent, est satisfaite par les mêmes valeurs de $\sqrt{k}$ appartenant au degré n que la précédente.

En chassant le radical $\sqrt{k}$ et les puissances impaires de k, on obtient donc, pour toutes les valeurs de b, une même équation en k^2, qui semble contenir encore i^a; mais on verra tout à l'heure que i^a disparaît avec k.

Cherchons les racines de l'équation (34). Évidemment elle n'est satisfaite par aucune des valeurs $\sqrt{k} = 0, \pm 1, \pm i$. Elle n'est pas non plus satisfaite par des modules de la première espèce; c'est une conséquence de ce que les nombres r_1, s'_1 sont de parités contraires. Pour que le carré d'un module de seconde espèce satisfasse à l'équation (34), il faut évidemment que, dans l'équation (28), a_1, c_1, x et y soient des nombres impairs, x et y premiers entre eux. Réciproquement, si ces conditions sont remplies, et si le degré n_1 du module vérifie la relation

$$4n = x^2 + y^2(4n_1 - 1),$$

on peut déterminer les signes de l et $\sqrt{l}$, de sorte que $\sqrt{l}$ soit une racine de l'équation. En effet, les autres conditions à remplir sont

$$\frac{xy+1}{2}a_1 + a_1 b_1 \equiv a(b+1), \qquad \frac{xy-1}{2}a_1 - a_1 b_1 \equiv -ab \pmod 4$$

ou bien

$$x \equiv y a a_1, \qquad b_1 \equiv a a_1 (b+1) - \frac{xy+1}{2};$$

or on satisfait à ces congruences en choisissant arbitrairement le signe de y, déterminant le signe de x par la première congruence, et la valeur de $b_1 \pmod 4$ par la seconde. Cette dernière détermination est possible sans changer l^2 ni a_1, et la valeur de $\sqrt{l}$ se trouve par là complètement déterminée. Puisque, le signe de y étant choisi, celui de x est déterminé, la multiplicité de la racine $\sqrt{l}$ est égale au quart du nombre des solutions de l'équation $4n = x^2 + y^2(4n_1 - 1)$ en nombres premiers entre eux.

En cherchant de la même manière les racines de l'équation (35), on trouve, en désignant par x' et b'_1 les valeurs de x et de b_1 qui s'y rapportent,

$$x' \equiv -y a a_1 \pmod 4;$$

d'où

$$x' \equiv -x, \qquad b'_1 \equiv a a_1 (b+1) + \frac{x'y-1}{2} \equiv a a_1 (b+1) - \frac{xy+1}{2} \equiv b_1.$$

Il s'ensuit que les équations (34), (35) ont les mêmes racines, et, comme d'ailleurs leur degré 2N est divisible par 4, excepté pour $n = 1$, les deux polynômes formant les premiers membres sont identiques, à cette exception près.

En faisant $b \equiv -1$, on trouve

$$f(\sqrt{k}, i^a) = f(i^{-a}\sqrt{k}, i^{-a});$$

d'où l'on peut conclure qu'on a

$$f(\sqrt{k}, i^a) = \varphi(k^2) + (1 + i^a) k \sqrt{k}\, \varphi_1(k^2) + i^a k \varphi_2(k^2) + (1 - i^a)\sqrt{k}\, \varphi_3(k^2),$$

$\varphi, \varphi_1, \varphi_2, \varphi_3$ dénotant des polynômes à coefficients entiers; de plus, le premier et le dernier coefficient de $\varphi(k^2)$ sont égaux à 1, comme il est facile de le voir. Pour $n = 1$, on a

$$k + (1 + i^a)\sqrt{k} - i^a = 0.$$

En chassant $\sqrt{k}$, on obtient une équation de la forme $f_1(i^a k) = 0$, et en chassant, de plus, les puissances impaires de k, une équation de la forme $f_2(k^2) = 0$, où i a disparu.

Les équations trouvées n'ont pas, comme celles des numéros précédents, la propriété que les modules du degré n sont les seules racines simples; mais, si l'on connaît déjà les équations répondant aux degrés inférieurs à n, on peut débarrasser les équations des racines étrangères par une série de divisions. En considérant spécialement l'équation $f(\sqrt{k}, i) = 0$, qui répond à $a \equiv -b \equiv 1 \pmod 4$, on fera $x \equiv y a_1$, ou bien, puisque, d'après ce qui a été dit, il suffit de prendre $a_1 \equiv 1$,

$$x \equiv y, \qquad b_1 \equiv -\frac{xy+1}{2}.$$

On obtient ainsi finalement une équation $F(\sqrt{k}, i) = 0$, qui n'est satisfaite que par les modules de la seconde espèce du degré n; on en déduit une équation en k, $F_1(ik) = 0$, et enfin une en k^2, $F_2(k^2) = 0$; il est facile de voir que, dans cette dernière équation, le premier et le dernier coefficient sont 1. On voit aussi que $(1 - i^a)\sqrt{k}$ s'exprime en fonction rationnelle de k^2, et que généralement, sans aucune hypothèse sur les valeurs de a et de b, on a

$$(1 - i^a) i^{a(b+1)} \sqrt{k} = \psi(k^2),$$

la fonction rationnelle ψ étant la même pour toutes les valeurs de ces nombres.

Exemple. — En faisant, dans l'équation modulaire répondant à $n = 3$,

$$k^2 - 4\sqrt{k^3}\sqrt{k_0^3} + 6kk_0 - 4\sqrt{k}\sqrt{k_0} + k_0^2 = 0,$$

$$\sqrt{k_0} = -i\frac{1-\sqrt{k}}{1+\sqrt{k}},$$

et écrivant z au lieu de $\sqrt{k}$, on trouve

$$z^8 + 4(1+i)z^7 - 8iz^6 + 4(1-i)z^5 + 14z^4 - 4(1+i)z^3 + 8iz^2 - 4(1-i)z + 1 = 0.$$

Puisque

$$4.3 = 3^2 + 1^2.3,$$

on a

$$y = 1,$$

donc on doit prendre

$$x = -3, \qquad b_1 \equiv \frac{-3+1}{2} \equiv 1,$$

c'est-à-dire qu'il faut diviser l'équation trouvée par

$$z^2 - (1+i)z - i,$$

ce qui donne

$$z^6 + 5(1+i)z^5 + 3iz^4 - 4(1-i)z^3 + 3z^2 - 5(1+i)z + i = 0;$$

en chassant les puissances impaires de z et écrivant k au lieu de z^2, on retrouve l'équation du n° **12**.

Le corollaire d'Arithmétique qu'on peut tirer de ce qui précède est des plus simples; en égalant le degré de l'équation $F_2(k^2) = 0$ au nombre de ses racines, on trouve

$$F_1(4n-1) + F_1(4n-3^2) + F_1(4n-5^2) + \ldots = N.$$

Dans cette formule, n désigne un nombre impair; F_1 a la même signification qu'au n° **10**, seulement on ne doit compter que les classes dans lesquelles l'un au moins des coefficients extérieurs est impair.

13. Pour les degrés pairs, le nombre N des transformations qui ne se déduisent pas linéairement les unes des autres est exprimé par la même formule que pour les degrés impairs, c'est-à-dire qu'en faisant

$$n = 2^\pi q_1^{\beta_1} q_2^{\beta_2} \ldots,$$

$2, q_1, q_2, \ldots$ étant les facteurs premiers de n, on a

$$N = 2^{\pi-1}.3\, q_1^{\beta_1-1}(q_1+1)\, q_2^{\beta_2-1}(q_2+1)\ldots;$$

mais on sait que les N modules correspondants ne sont pas, comme pour

les degrés impairs, racines d'une même équation irréductible. Il faut d'abord distinguer le cas où le nombre δ [équat. (20)] est pair de celui où δ est impair, et l'on vérifie sans peine que, des N transformations linéairement indépendantes, un tiers répond au premier cas, les deux tiers au second.

Cas 1 : *Si δ est un nombre pair.* — Pour avoir les équations modulaires les plus simples, nous choisirons les transformations principales un peu autrement que pour les degrés impairs.

En désignant par δ' le plus grand commun diviseur des nombres r', s', qui figurent dans l'équation (18) du n° **8**, nous ferons

$$r' = \rho'\delta', \qquad s' = \sigma'\delta', \qquad n' = \rho s' - r'\sigma = \delta'(\rho\sigma' - \rho'\sigma) = \delta' n'';$$

d'où

$$n = \delta\delta' n''.$$

En remplaçant les équations (21) par les suivantes

$$\mu\rho - m\sigma = t',$$
$$-\mu\rho' + m\sigma' = 1,$$

l'expression (19) devient

$$\lambda\left(0 + \frac{\delta'.2\omega + t'\delta\omega'}{n}\right) \quad \text{ou bien} \quad \lambda\left(0 + \frac{\Omega'}{n}\right),$$

en posant

$$\Omega' = \delta'.2\omega + t'\delta\omega'.$$

Comme au n° **8**, nous pouvons rendre t' premier à δ'; les valeurs de l'expression (19) peuvent donc être écrites sous la forme

$$\lambda\left(0 + \frac{p\Omega'}{n}\right), \qquad \text{où} \qquad p = 0, 1, 2, \ldots, (n-1).$$

De plus, nous choisirons le signe de δ' de manière à avoir $\delta' \equiv 1 \pmod 4$. Cela posé, nous prendrons pour transformations principales celles qui sont définies par les équations

$$(36) \qquad \begin{cases} \varepsilon_0.2\omega = t'\delta.2\omega_0 + \delta n''\omega'_0, \\ \varepsilon_0.\ \omega' = -\delta'.2\omega_0. \end{cases}$$

En faisant

$$\varphi(0)=\prod_{0}^{n-1}\lambda\left(0+p\frac{\Omega'}{n}\right)=-\lambda^2(\theta)\prod_{1}^{\frac{n}{2}-1}\frac{\lambda^2(0)-\lambda^2\left(\frac{p}{n}\Omega'\right)}{1-k^2\lambda^2(\theta)\lambda^2\left(\frac{p}{n}\Omega'\right)},$$

on est conduit aux formules suivantes

$$(37)\qquad \begin{cases} \lambda\left(\varepsilon_0 0+\frac{\omega_0}{2},k_0\right)=\dfrac{1+(-k)^{\frac{n}{2}}\varphi(0)}{1-(-k)^{\frac{n}{2}}\varphi(0)}, \\ k_0=\dfrac{1-(-k)^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)}{1+(-k)^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)}. \end{cases}$$

L'expression $\varphi\left(\frac{1}{2n}\Omega'\right)$ est une fonction rationnelle des quantités $\lambda^2\left(\frac{p}{2n}\Omega'\right)$; or $\lambda^2\left(\frac{n}{2}\frac{1}{2n}\Omega'\right)$ ou $\lambda^2\left(\frac{1}{4}\Omega'\right)$ est égal à 1 si $\frac{t'\delta}{2}$ est pair, mais égal à $\frac{1}{k^2}$ si $\frac{t'\delta}{2}$ est impair.

Donc, en faisant

$$\lambda^2\left(\frac{n}{2}0\right)=f[\lambda^2(0)],$$

les quantités $\lambda^2\left(\frac{p}{2n}\Omega'\right)$ sont racines de l'équation $f(x)=1$ dans le premier cas, mais de l'équation $f(x)=\frac{1}{k^2}$ dans le second; par suite, les équations modulaires sont différentes dans les deux cas.

Si maintenant n est impairement pair, $\frac{\delta}{2}$ et n'' sont impairs; le nombre t', n'étant déterminé que par rapport au module n'', peut être choisi pair ou impair à volonté. Nous le supposerons pair; l'équation modulaire principale sera donc déterminée par les équations

$$k_0=\frac{1+k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)}{1-k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)},\qquad \lambda^2\left(\frac{1}{4}\Omega'\right)=1;$$

on a ainsi une équation en k_0 du degré $\frac{1}{3}N$, dont les coefficients sont des fonctions rationnelles de k à coefficients entiers. La première des équations (37) peut être remplacée par la suivante :

$$(38)\quad \lambda(\varepsilon_0 0, k_0) = \frac{\varepsilon_0 \lambda(0)}{\mu(0)\nu(0)} \prod_1^{\frac{n-2}{4}} \frac{\left[1 - \frac{\lambda^2(0)}{\lambda^2\left(\frac{p}{n}\Omega'\right)}\right]\left[1 - k^2\lambda^2\left(\frac{p}{n}\Omega'\right)\lambda^2(0)\right]}{\left[1 - \frac{\lambda^2(0)}{\lambda^2\left(\frac{2p-1}{2n}\Omega'\right)}\right]\left[1 - k^2\lambda^2\left(\frac{2p-1}{2n}\Omega'\right)\lambda^2(0)\right]};$$

en employant cette équation, le multiplicateur ε_0 est complètement déterminé,

$$\varepsilon_0 = i\left[1 - k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)\right]\prod_1^{\frac{n-2}{4}} \frac{\lambda^2\left(\frac{p}{n}\Omega'\right)}{\lambda^2\left(\frac{2p-1}{2n}\Omega'\right)};$$

dans l'équation (37), son signe est arbitraire.

En faisant abstraction du facteur ε_0, les coefficients du second membre de (38) sont des fonctions rationnelles de k et de k_0 à coefficients entiers, tandis que ε_0 est égal à une telle fonction multipliée par i.

Si, au contraire, n est divisible par 4, $\frac{\delta}{2}$ peut être pair ou impair, et, dans ce dernier cas, n'' est pair, et, par suite, t' est impair. On a donc, pour les valeurs pairement paires de n, deux équations modulaires principales, définies par l'équation

$$k_0 = \frac{1 - k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)}{1 + k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)}$$

avec

$$\lambda^2\left(\frac{1}{4}\Omega'\right) = 1 \qquad \text{ou} \qquad \lambda^2\left(\frac{1}{4}\Omega'\right) = \frac{1}{k^2}.$$

Nous appellerons la première l'équation modulaire Ia, la seconde l'équation Ib; leurs coefficients sont évidemment des fonctions rationnelles de k^2 à coefficients entiers.

On a, dans les deux cas,

$$(39)\quad \left\{\begin{array}{l} \lambda(\varepsilon_0\theta, k_0) = \varepsilon_0\,\lambda(\theta)\,\mu(\theta)\,\nu(\theta) \\ \qquad \times \dfrac{\prod_1^{\frac{n}{4}-1}\left[1-\dfrac{\lambda^2(\theta)}{\lambda^2\left(\frac{p}{n}\Omega'\right)}\right]\left[1-k^2\lambda^2\left(\frac{p}{n}\Omega'\right)\lambda^2(\theta)\right]}{\prod_0^{\frac{n}{4}-1}\left[1-\dfrac{\lambda^2(\theta)}{\lambda^2\left(\frac{2p+1}{2n}\Omega'\right)}\right]\left[1-k^2\lambda^2\left(\frac{2p+1}{2n}\Omega'\right)\lambda^2(\theta)\right]} \end{array}\right.$$

et, de plus,

$$\varepsilon_0 = i\left[1+k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)\right]\frac{\prod_1^{\frac{n}{4}-1}\lambda^2\left(\frac{p}{n}\Omega'\right)}{\prod_0^{\frac{n}{4}-1}\lambda^2\left(\frac{2p+1}{2n}\Omega'\right)} \qquad \text{pour le cas I}a,$$

$$\varepsilon_0 = \frac{i}{k}\left[1+k^{\frac{n}{2}}\varphi\left(\frac{1}{2n}\Omega'\right)\right]\frac{\prod_1^{\frac{n}{4}-1}\lambda^2\left(\frac{p}{n}\Omega'\right)}{\prod_0^{\frac{n}{4}-1}\lambda^2\left(\frac{2p+1}{2n}\Omega'\right)} \qquad \text{pour le cas I}b.$$

En désignant pour un moment par $2\omega_1$, ω_1' un couple de périodes elliptiques appartenant au module $-k_0$, on peut faire

$$2\omega_0 = 2\omega_1, \qquad \omega_0' = \delta'.2\omega_1 + \omega_1';$$

d'où

$$\varepsilon_0.2\omega = (l' + n''\delta')\delta.2\omega_1 + \delta n''\omega_1',$$
$$\varepsilon_0.\ \omega' = -\delta'.2\omega_1.$$

De ces équations on conclut que, lorsque $\frac{n}{2}$ est impair, $-k_0$ ne satisfait pas à l'équation modulaire I, puisque, dans ce cas, $l' + n''\delta'$ est

impair; par conséquent, cette équation contient des puissances impaires de k_0. Au contraire, si $\frac{n}{2}$ est pair, les équations modulaires Ia et Ib ne contiennent que des puissances paires de k_0. De plus, en désignant par Ω'' la nouvelle valeur de Ω', on a

$$\Omega'' = \Omega' + \omega' n;$$

d'où

$$\lambda\left(\frac{p}{n}\Omega''\right) = \lambda\left(\frac{p}{n}\Omega'\right), \qquad \lambda\left(\frac{2p+1}{2n}\Omega''\right) = \frac{1}{k\lambda\left(\frac{2p+1}{2n}\Omega'\right)},$$

de sorte que les formules (38), (39) ne sont pas altérées quand on change le signe de k_0. Donc, abstraction faite du facteur ε_0, les coefficients des seconds membres sont des fonctions rationnelles de k et de k_0^2 si $\frac{n}{2}$ est impair, de k^2 et de k_0^2 si $\frac{n}{2}$ est pair; ε_0 est évidemment de la forme $i\psi(k, k_0^2)$ si $\frac{n}{2}$ est impair; mais, si $\frac{n}{2}$ est pair, il est des formes $i\psi(k^2, k_0^2)$ ou $\frac{i}{k}\psi(k^2, k_0^2)$, suivant que la transformation appartient au cas Ia ou au cas Ib. Il est d'ailleurs facile de voir que ces dernières transformations se déduisent l'une de l'autre, en remplaçant k par $\frac{1}{k}$.

Voici les équations modulaires dans les cas les plus simples :

$n = 2 \ldots$ $\quad k_0 = \frac{1-k}{1+k}$;

$n = 4 \ldots$ $\quad$ équat. Ia : $k_0^2 = k'^2$; $\quad$ équat. Ib : $k_0^2 k^2 + k'^2 = 0$;

$n = 8 \ldots$ $\quad$ équat. Ia : $k^4 k_0^4 = 16 k'^2 k_0'^2$; $\quad$ équat. Ib : $k_0^4 + 16 k_0'^2 k^2 k'^2 = 0$.

Cas II : *Si δ est impair.* — Nous poserons, dans le reste de ce numéro,

$$n = 2^\pi n_0,$$

n_0 étant impair, et nous désignerons par k_0 le module qu'on déduit de k par une transformation principale du degré n_0 et généralement par k_r celui qu'on obtient par une transformation principale du degré $2^r n_0$. Comme pour les degrés impairs, nous définissons la transformation

principale du degré n par les équations

$$(40)\qquad \begin{cases} \varepsilon_\pi . 2\omega = \delta . 2\omega_\pi, \\ \varepsilon_\pi . \ \omega' = -t . 2\omega_\pi + n'\omega'_\pi; \end{cases}$$

nous supposons le signe de δ défini par la congruence $\delta \equiv 1 \pmod 4$, et nous faisons $t . 2\omega + \delta\omega' = \Omega$. Cela posé, on a

$$\lambda(\varepsilon_\pi \theta, k_\pi) = \varepsilon_\pi \lambda(\theta) \prod \frac{1 - k^2\lambda^2\left(\frac{p}{n}\Omega\right)\lambda^2(\theta)}{1 - k^2\lambda^2\left(\frac{2p+1}{2n}\Omega\right)\lambda^2(\theta)},$$

$$\varepsilon_\pi = \prod \frac{\nu^2\left(\frac{2p+1}{2n}\Omega\right)}{\nu^2\left(\frac{p}{n}\Omega\right)},$$

$$k_\pi = \frac{1}{\lambda\left(\frac{\omega}{2} + \frac{1}{2n}\Omega\right)} \prod \frac{\nu^2\left(\frac{p}{n}\Omega\right)}{\nu^2\left(\frac{2p+1}{2n}\Omega\right)} \frac{1 - k^2\lambda^2\left(\frac{2p+1}{2n}\Omega\right)\lambda^2\left(\frac{\omega}{2} + \frac{1}{2n}\Omega\right)}{1 - k^2\lambda^2\left(\frac{p}{n}\Omega\right)\lambda^2\left(\frac{\omega}{2} + \frac{1}{2n}\Omega\right)},$$

où il faut donner à p les valeurs $0, 1, 2, \ldots, \left(\frac{n}{2} - 1\right)$.

Le module transformé k_π est lié à k par une équation algébrique entre k_π et $i^t\sqrt{k}$, dont les coefficients sont des nombres entiers. Pour le démontrer, posons

$$(41)\qquad \begin{cases} \varepsilon_0 . 2\omega = \delta_0 . 2\omega_0, \\ \varepsilon_0 \quad \omega' = -t_0 . 2\omega_0 + n'_0\omega'_0, \end{cases}$$

où $n_0 = \delta_0 n'_0$, $\delta_0 \equiv 1 \pmod 4$, t_0 premier à δ_0 et divisible par 4; soit, de plus,

$$(42)\qquad \begin{cases} \varepsilon' . 2\omega_0 = 2\omega_1, \\ \varepsilon' \quad \omega'_0 = -m . 2\omega_1 + 2\omega'_1. \end{cases}$$

On en tire

$$(43)\qquad k_1 = \frac{2i^m\sqrt{k_0}}{1 + i^{2m}k_0}$$

et

$$\varepsilon_0\varepsilon'.2\omega = \delta_0.2\omega_1,$$
$$\varepsilon_0\varepsilon' \quad \omega' = -(t_0 + mn'_0)2\omega_1 + 2n'_0\omega'_1. \quad .$$

Ces équations définissent une transformation du degré $2n_0$ appartenant au cas que nous considérons; en les comparant aux équations (40), on a

$$\pi = 1, \qquad t = t_0 + mn'_0 \equiv mn'_0 \qquad (\mathrm{mod}4);$$

l'équation modulaire entre k_1 et $\sqrt{k}$ s'obtient en éliminant $\sqrt{k_0}$ entre l'équation (43) et l'équation modulaire principale appartenant au degré n_0

$$f_0(\sqrt{k_0}, \sqrt{k}) = 0.$$

Or il suit de ce qui a été dit au n° 9 qu'on a

$$f_0(i^m\sqrt{k_0}, i^{mn_0}\sqrt{k}) = 0,$$

donc l'élimination de $\sqrt{k_0}$ donnera une équation de la forme

$$f_1(k_1, i^{mn_0}\sqrt{k}) = f_1(k_1, i^t\sqrt{k}) = 0,$$

ce qui démontre l'assertion faite plus haut pour le cas où $\pi = 1$. Il est à remarquer que, pour $\pi = 1$, il suffit de distinguer deux cas au lieu de quatre, en se bornant, par exemple, à faire $t \equiv 0$ et $t \equiv 1 \pmod 4$, puisque, en changeant le signe de $\sqrt{k}$, on ne fait que changer celui de k_1, de sorte que les deux autres cas se déduisent de ceux-ci par une transformation linéaire.

Pour achever la démonstration, on n'a qu'à faire subir au module k_1 une série de transformations successives, définies par les équations

$$\varepsilon^{(j+1)}2\omega_j = 2\omega_{j+1},$$
$$\varepsilon^{(j+1)} \quad \omega'_j = 2\omega'_{j+1},$$
$$k_{j+1} = \frac{2\sqrt{k_j}}{1 + k_j},$$

et qui n'altèrent pas la valeur de $t \pmod 4$. Il est facile de voir que l'équation finale est du degré $\frac{1}{3}N$ en k_π, et qu'à partir de $\pi = 2$ elle ne contient que des puissances paires de k_π.

En chassant $\sqrt{k}$ et les puissances impaires de k, on obtient une équation en k_π^2 et k^2, qui a la propriété de ne pas être altérée en changeant k_π et k respectivement en k', k'_π. Soient, en effet,

$$F_\pi(k_\pi^2, k^2) = 0, \qquad F_0(k_0^2, k^2) = 0, \qquad \varphi_\pi(k_\pi^2, k^2) = 0$$

les équations entre les carrés des modules appartenant respectivement aux degrés $2^\pi n_0$, n_0 et 2^π; on trouve d'abord

$$\varphi_1(k_1^2, k^2) = k_1^4 k'^4 - 16 k_1'^2 k^2,$$

ce qui démontre la proposition pour $n = 2$. De plus, l'équation $\varphi_\pi(k_\pi^2, k^2) = 0$ résulte de l'élimination de $k_1, k_2, \ldots, k_{\pi-1}$ entre les équations

$$k_\pi^4 k'^4_{\pi-1} = 16 k_\pi'^2 k_{\pi-1}^2, \qquad k_{\pi-1}^4 k'^4_{\pi-2} = 16 k_{\pi-1}'^2 k_{\pi-2}^2, \qquad \ldots, \qquad k_1^4 k'^4 = 16 k_1'^2 k^2;$$

or, en changeant k_j en $k'_{\pi-j}$, ces équations sont reproduites dans l'ordre inverse; d'où l'on conclut qu'on a

$$\varphi_\pi(k'^2, k_\pi'^2) = 0 :$$

donc la proposition est démontrée pour $n = 2^\pi$. L'équation

$$F_\pi(k_\pi^2, k^2) = 0$$

s'obtient en éliminant k_0 entre les équations

$$F_0(k_0^2, k^2) = 0, \qquad \varphi_\pi(k_\pi^2, k_0^2) = 0;$$

on trouve la même équation en éliminant x entre les équations

$$\varphi_\pi(x^2, k^2) = 0, \qquad F_0(k_\pi^2, x^2) = 0;$$

c'est ce qu'on voit aisément au moyen des relations entre les périodes.

Mais ce dernier système entraîne le suivant

$$F_0(x'^2, k_\pi'^2) = 0, \qquad \varphi_\pi(k'^2, x'^2) = 0,$$

qui donne enfin

$$F_\pi(k'^2, k_\pi'^2) = 0. \qquad \text{C. Q. F. D.}$$

En désignant par N_0 le degré de l'équation $F_0(k_0^2, k^2) = 0$, par $\Psi_\pi(k_\pi^2, k^2)$ un polynôme à coefficients entiers, l'équation $F_\pi(k_\pi^2, k^2) = 0$ peut être mise sous la forme suivante

$$k_\pi^{2^{\pi+1}N_0} k'^{2^{\pi+1}N_0} + 4\,k_\pi^2 k^2 \Psi_\pi(k_\pi^2, k^2) \pm 16^{(2^\pi-1)N_0} k^{2N_0} k'^{(2^{\pi+1}-4)N_0} = 0,$$

où les plus hautes puissances de k_π et de k n'entrent que dans le premier terme. En effet, on a vu qu'on obtient l'équation $F_1(k_1^2, k^2) = 0$ en faisant, dans l'équation $F_0(k_1^2, x^2) = 0$, $x^2 = \frac{4k}{(1+k)^2}$ et chassant les puissances impaires de k, c'est-à-dire qu'on a

$$F_1(k_1^2, k^2) = (1-k^2)^{2N_0} F_0\left[k_1^2, \frac{4k}{(1+k)^2}\right] F_0\left[k_1^2, \frac{-4k}{(1-k)^2}\right].$$

Or, en développant $(1 \pm k)^{2N_0} F_0\left[k_1^2, \frac{\pm 4k}{(1\pm k)^2}\right]$, on a, comme on le voit aisément, un résultat de la forme

$$k_1^{2N_0}(1 \pm k)^{2N_0} \pm 4k_1^2 k\psi(k_1^2, \pm k) + 4^{N_0}(\pm k)^{N_0} = 0,$$

où les plus hautes puissances de k_1 et de k ne se trouvent qu'au premier terme. En faisant le produit, on a

$$F_1(k_1^2, k^2) = k_1^{4N_0} k'^{4N_0} + 4k_1^2 k^2 \Psi_1(k_1^2, k^2) + (-1)^{N_0} 16^{N_0} k^{2N_0}.$$

Donc la proposition est démontrée pour $\pi = 1$, et l'on démontre aisément de la même manière qu'elle a lieu pour $\pi = m+1$, si elle a lieu pour $\pi = m$.

Ainsi le terme du plus haut degré a le coefficient 1. Le terme du plus petit degré a pour coefficient une puissance de 16; on le démontre en remarquant que le premier terme du développement de k_π^2 suivant les

puissances fractionnaires croissantes de k^2 est $16^{\frac{n'-\delta}{n'}} e^{\frac{2i\pi i}{n'}} k^{\frac{2\delta}{n'}}$, de sorte que, pour les petites valeurs de k, on a

$$F_\pi(k_\pi^2, k^2) = (1-k^2)^{2^\pi N_0} \prod \left(k_\pi^2 - 16^{\frac{n'-\delta}{n'}} e^{\frac{2i\pi i}{n'}} k^{\frac{2\delta}{n'}} - \dots\right).$$

Évidemment dans l'équation entre k_π et $i^t\sqrt{k}$ le terme du plus haut degré a pour coefficient 1, celui du plus petit une puissance de 2.

Pour mettre l'équation I*a* sous une forme semblable, on peut remarquer qu'on trouve le module transformé k_π en posant $k = \frac{1-k_1}{1+k_1}$ et faisant subir au module k_1 une transformation principale du cas II, appartenant au degré $2^{\pi-1}$ et à une valeur paire du nombre t; on le démontre aisément par les relations qui ont lieu entre les rapports des périodes. Il s'ensuit qu'on a l'équation cherchée en éliminant k_2 et k_1 entre les équations

$$F_{\pi-2}(k_\pi^2, k_2^2) = 0, \qquad k_2^2 = \frac{4k_1}{(1+k_1)^2}, \qquad k_1 = \frac{1-k}{1+k};$$

or on trouve $k_2^2 = k'^2$: donc l'équation I*a* est

$$F_{\pi-2}(k_\pi^2, k'^2) = 0;$$

par conséquent, si $\pi > 2$, elle peut être écrite sous la forme suivante

$$k_\pi^{2^{\pi-1}N_0} k^{3^{\pi-1}N_0} + 4k_\pi^2 k'^2 \Psi_{\pi-2}(k_\pi^2, k'^2) \pm 16^{(2^{\pi-2}-1)N_0} k'^{2N_0} k^{(2^{\pi-1}-4)N_0} = 0,$$

où les plus hautes puissances de k_π et de k ne se trouvent qu'au premier terme; évidemment cette équation n'est pas altérée en échangeant entre eux k_π et k.

16. *Modules de la première espèce et de la première catégorie d'un degré pair.* — Puisque a est pair, b est aussi pair; d'où l'on conclut que c est impair, δ pair. Par suite, il faut employer les transformations principales du cas I, qui sont définies par les équations

$$\varepsilon_0 . 2\omega = t'\delta . 2\omega_0 + \delta n'' \omega_0',$$
$$\varepsilon_0 . \omega' = -\delta' . 2\omega_0;$$

donc les équations (24) deviennent

$$t'\delta r_1 + \delta n'' r'_1 = b, \qquad t'\delta s_1 + \delta n'' s'_1 = a, \qquad \delta' r_1 = c, \qquad \delta' s_1 = b.$$

Supposons d'abord que $\frac{n}{2}$ soit impair. Dans ce cas on a évidemment $a + \delta \equiv 2 \pmod 4$, n'' est impair; en se rappelant que nous supposons t' pair, $\delta' \equiv 1$, on voit de plus qu'on a $2r'_1 \equiv b \equiv s_1 \pmod 4$. Si maintenant b est divisible par 4, s_1 l'est aussi, et r'_1 est pair; donc il faut faire

$$(14) \qquad k_0 = k, \qquad \varepsilon_0 = i^c \sqrt{n}, \qquad \lambda(i\sqrt{n}0) = (-1)^{\frac{c-1}{2}} \mathrm{Y}.$$

Si, au contraire, $b \equiv 2 \pmod 4$, on a $s_1 \equiv 2$, r'_1 est impair; par suite, on fera

$$k_0 = -\frac{1}{k}, \qquad \varepsilon_0 = i^c k \sqrt{n}, \qquad \lambda(i\sqrt{n}0) = \frac{(-1)^{\frac{c-1}{2}}}{k} \mathrm{Y}.$$

En substituant dans l'équation modulaire les valeurs de k_0, on obtient deux équations en k. On trouve les mêmes équations en remplaçant dans l'équation modulaire en k et en k_0, appartenant au degré $\frac{n}{2}$, le module transformé k_0 respectivement par $\frac{1-k}{1+k}$, $-\frac{1+k}{1-k}$; par suite les premiers et les derniers coefficients des équations sont ± 1. On en peut aussi conclure que si la première des deux équations est satisfaite par un module l, elle est aussi satisfaite par $-\frac{1}{l}$, pendant que la seconde équation a les racines $-l$, $\frac{1}{l}$; donc les deux équations en k ne donnent qu'une seule équation k^2. Aucune de ces équations n'est satisfaite par $k = 0$, $k = \pm 1$.

Cherchons maintenant les racines des équations trouvées. Pour que les formules (27) définissent un module de la première espèce, l, satisfaisant à l'une des équations, il faut qu'on ait (n° 8)

$$\mathrm{S}_1 \equiv s_1 \equiv b \pmod 4, \qquad \mathrm{R}'_1 \mathrm{S}'_1 \equiv r'_1 s'_1 \pmod 2;$$

les nombres R_1, S_1, R'_1, S'_1 étant déterminés de la manière suivante

$$\begin{aligned} l'\delta R_1 + \delta n'' R'_1 &= x + b_1 y, & \delta' R_1 &= y c_1, \\ l'\delta S_1 + \delta n'' S'_1 &= y a_1, & \delta' S_1 &= -x + b_1 y; \end{aligned}$$

on en conclut que, pour la première équation,

$$x + y b_1 \equiv x - y b_1 \equiv 0 \pmod 4$$

et, pour la seconde,

$$x + y b_1 \equiv x - y b_1 \equiv 2,$$

et que $y a_1$ est pair, $y c_1$ impair. Donc x sera pair, y impair, b_1 pair. La relation

$$x^2 + y^2 n_1 = n$$

fait voir que $n_1 \equiv 2$ et, par suite,

$$a_1 \equiv 2 \pmod 4.$$

Puisque $b_1 \equiv x \pmod 4$ pour la première équation, $b_1 \equiv x + 2$ pour la seconde, l appartiendra alternativement à la première ou à la seconde équation relative au degré n_1, quand on donne à x les valeurs $0, 2, 4, \ldots$. Évidemment l n'est racine simple que pour $x = 0$. Enfin on voit sans peine que les équations ne sont satisfaites par aucun module de la seconde espèce.

En se débarrassant des modules dont les degrés sont moindres que n, on obtient donc deux équations qui, en chassant les puissances impaires de k, se réunissent en une seule équation en k^2, dont évidemment le premier et le dernier coefficient sont 1. De plus on voit que k peut être exprimé en fonction rationnelle de k^2.

Exemples. — Pour $n = 2$, on a les équations

$$k = \frac{1-k}{1+k} \qquad \text{et} \qquad -\frac{1}{k} = \frac{1-k}{1+k}$$

ou

$$k^2 + 2k - 1 = 0, \qquad k^2 - 2k - 1 = 0;$$

d'où

$$k^2 = 3 + 2\sqrt{2}.$$

$n = 6$. — Si dans l'équation modulaire appartenant au degré 3

$$(k^2 + 6kk_0 + k_0^2)^2 - 16kk_0(1 + kk_0)^2 = 0,$$

on fait $k_0 = \frac{1-k}{1+k}$, on a

$$(k^2 - 2k - 1)^2(k^4 + 12k^3 + 2k^2 - 12k + 1) = 0;$$

le second facteur donne les modules de sixième degré; on trouve

$$k^2 = (2 + \sqrt{3})^2(\sqrt{2} + \sqrt{3})^2.$$

Supposons maintenant que $\frac{n}{2}$ soit pair; a étant divisible par 4, il faut employer l'équation modulaire $1a$ ou $1b$, suivant que b est divisible par 4 ou non. Dans le premier cas, il faut faire $k_0^2 = k^2$; dans le second, $k_0^2 = \frac{1}{k^2}$. Au moyen de la relation

$$\zeta_0 = \cdots \frac{\delta' + \iota'\delta\zeta}{\delta n''\zeta},$$

on peut se convaincre que les deux équations, qu'on obtient en substituant dans les équations modulaires les valeurs de k_0^2, ne sont jamais satisfaites par $k^2 = 1$, et que la première équation admet la racine $k^2 = 0$, quand n est divisible par 16, la seconde quand $n \equiv 4 \pmod 8$. En supposant les équations débarrassées de la racine zéro, les carrés des modules du degré n sont les seules racines simples; les autres racines sont les modules de la première espèce et de la première catégorie dont le degré n_1 vérifie la relation $n = x^2 + y^2 n_1$, x et y étant premiers entre eux, et x pair; par suite, n_1 est toujours divisible par 4. Ces modules sont distribués entre les deux équations de la manière suivante : dans la première équation un module du degré n_1, qui lui satisfait, appartient à la première ou à la seconde équation relative au degré n_1, suivant que x est divisible par 4 ou non; l'inverse a lieu

pour la seconde équation. Tout cela se démontre de la même manière que dans le cas où $\frac{n}{2}$ est impair. En débarrassant les équations des racines appartenant à des degrés moindres que n, on a donc deux équations en k^2 qui n'admettent d'autres racines que les modules cherchés. Il est facile de voir que les racines de l'une de ces équations sont les réciproques de celles de l'autre. Des remarques faites au numéro précédent sur la forme des équations modulaires, il suit que, si $n \equiv 4 \pmod 8$, le premier coefficient de la première équation est une puissance de 2, le dernier est 1. Si n est divisible par 8, le premier coefficient de la première équation est évidemment 1. Quant au dernier, il ne peut être qu'une puissance de 2; on peut le démontrer par la considération de l'équation qu'on obtient en faisant $\sqrt{k_0} = -\sqrt{k}$ dans l'équation modulaire appartenant au degré $4n+1$. Les expressions de ε_0 et de $\lambda(i\sqrt{n}0)$ en $\sqrt{n}$ et en Y sont les mêmes que pour les valeurs impairement paires de n. Remarquons qu'en vertu de la congruence évidente $a - 2b \equiv n \pmod 8$, la valeur de $a \pmod 8$ est déterminée par celle de $b \pmod 4$, de telle manière que le premier ou le dernier coefficient de l'équation est égal à 1, suivant que $a \equiv 0$ ou $4 \pmod 8$.

Exemples. — Pour $n = 4$ on trouve

$$k^2 = \tfrac{1}{2}, \qquad k^2 = 2.$$

$n = 8$. — On trouve les deux équations

$$k^8 = 16k'^4, \qquad 1 - 16k'^4k^4 = 0$$

ou bien

$$(k^2-2)^2(k^4+4k^2-4) = 0, \qquad (2k^2-1)^2(4k^4-4k^2-1) = 0;$$

les derniers facteurs donnent les modules de huitième degré

$$k^2 = 2(\sqrt{2}-1), \qquad k^2 = \frac{1+\sqrt{2}}{2}.$$

Voici encore les modules du douzième et du seizième degré.

$n = 12$:

$$k^2 = \frac{2+\sqrt{3}}{4}, \qquad k^2 = 4(2+\sqrt{3}).$$

$n = 16$:

$$k^2 = 4(3\sqrt{2}-4), \qquad k^2 = \frac{3\sqrt{2}+4}{8}.$$

17. *Modules de la première espèce et de la seconde catégorie d'un degré pair.* — Dans ce cas a est impair, b et c sont de la même parité. Le nombre δ étant par conséquent impair, l'équation modulaire principale appartient au cas II; en remplaçant dans les équations (10) les indices π par o, elle est définie par les relations

$$\varepsilon_0 . 2\omega = \hat{\delta} . 2\omega_0,$$
$$\varepsilon_0 . \omega' = -t . 2\omega_0 + n'\omega'_0.$$

Les équations (24) deviennent

$$(15) \qquad \begin{cases} b = r_1\delta, & a = s_1\delta, \\ -c = -r_1 t + r'_1 n', & -b = -s_1 t + s'_1 n'; \end{cases}$$

on voit que les deux premières déterminent complètement les nombres r_1, s_1, δ, en se rappelant que $\hat{\delta}$ désigne le plus grand commun diviseur de a et de b, et que son signe est déterminé par la congruence $\hat{\delta} \equiv 1 \pmod 4$. Ensuite on choisit les nombres r'_1 et s'_1 de manière à vérifier la relation $r_1 s'_1 - r'_1 s_1 = 1$; or, s_1 étant impair, on peut choisir s'_1 pair. En éliminant n' des deux dernières équations, on a

$$(16) \qquad t = cs'_1 - br'_1,$$

ce qui achève la résolution du système (15). En effet, l'équation $ac - b^2 = n$ donne

$$(17) \qquad n' = cs_1 - br_1,$$

et évidemment les deux dernières des équations (15) sont des consé-

quences de (46) et (47). De plus on tire de la dernière équation (45)

$$t \equiv s, b \equiv ab \pmod 4.$$

Cela posé, le Tableau des transformations linéaires donne

$$(48)\quad \begin{cases} k_0 = \left(\dfrac{1 - i^{ab}\sqrt{k}}{1 + i^{ab}\sqrt{k}}\right)^2, \\ \varepsilon' = \dfrac{2\,i^a}{(1 + i^{ab}\sqrt{k})^2}, \qquad \varepsilon_0 = (-1)^{\frac{a-1}{2}} \tfrac{1}{2}\sqrt{n}\,(1 + i^{ab}\sqrt{k})^2, \end{cases}$$

$$\lambda(i\sqrt{n}\,0) = \frac{2\varepsilon' Y}{1 + \Delta Y - k_0 Y^2}.$$

En substituant la valeur de k_0 dans l'équation modulaire répondant à $t \equiv ab \pmod 4$, on obtient une équation de la forme

$$f(i^{ab}\sqrt{k}) = 0,$$

f dénotant un polynôme à coefficients entiers, dont le premier est égal à 1. Ici, comme dans les deux numéros suivants, on a le cas où chaque racine de l'équation modulaire principale répond à deux ou à quatre racines de l'équation $F(\xi, \eta) = 0$ du n° 8; mais, comme nous l'avons fait remarquer, cette circonstance n'infirme pas les conclusions de ce numéro. Puisqu'on n'a qu'une seule équation en k^2, il suffira de chercher les racines de l'équation

$$f(\sqrt{k}) = 0.$$

Au moyen de la relation

$$\zeta_0 = \frac{t + \delta\zeta}{n'},$$

on vérifie sans peine qu'elle admet la racine $\sqrt{k} = -1$, quand $\pi = 2$, et la racine $\sqrt{k} = 1$, quand $\pi > 3$, et qu'elle n'est pas satisfaite par $\sqrt{k} = 0$, ni par $\sqrt{k} = \pm i$. De plus, on verra aisément que les autres racines étrangères dont il faut débarrasser l'équation, toutes des racines au moins doubles, sont les racines carrées des modules de la première espèce et de la seconde catégorie dont le degré n_1 vérifie la relation

$n = x^2 + y^2 n_1$, x et y étant premiers entre eux, et x pair. On remarquera cependant que, lorsque x n'est pas divisible par 4, il faut prendre les racines carrées des modules correspondants avec le signe opposé à celui qu'on obtient en les calculant d'après la règle qui vient d'être donnée. Dans l'équation finale

$$F(\sqrt{k}) = 0,$$

le premier coefficient est évidemment 1; en chassant $\sqrt{k}$ et les puissances impaires de k, on a une équation en k^2, nécessairement réciproque, dont par conséquent et le premier et le dernier coefficient sont égaux à l'unité. Remarquons enfin que, puisque deux quelconques des quatre équations $F(\pm\sqrt{k}) = 0$, $F(\pm i\sqrt{k}) = 0$ ne peuvent avoir des racines communes, on a

$$i^{ab}\sqrt{k} = \psi(k^2),$$

ψ dénotant une fonction rationnelle à coefficients entiers, identiquement la même dans tous les cas appartenant au même degré.

Exemples. — Pour $n = 2$, on a

$$\frac{2\sqrt{k}}{1+k} = \left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^2$$

ou bien

$$k^2 - 4k\sqrt{k} - 2k - 4\sqrt{k} + 1 = 0,$$

ce qui donne

$$\sqrt{k} = 1 + \sqrt{2} + \sqrt{2 + 2\sqrt{2}}.$$

$n = 4$. — L'équation modulaire est

$$k_0^2(1+\sqrt{k})^4 = 8\sqrt{k}(1+k);$$

en y faisant

$$k_0^2 = \left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^4$$

et supprimant la racine quadruple $\sqrt{k} = -1$, on trouve

$$k^2 - 12k\sqrt{k} + 6k - 12\sqrt{k} + 1 = 0,$$

d'où

$$\sqrt{k} = 3 + 2\sqrt{2} + 2\sqrt{4 + 3\sqrt{2}} = -\frac{1+\sqrt[4]{2}}{1-\sqrt[4]{2}}.$$

18. *Modules de la seconde espèce et de la première catégorie.* — On peut réunir les deux systèmes d'équations (9) à un seul, en écrivant

$$(49)\qquad \begin{cases} \varepsilon.2\omega = \beta.2\omega + a\,\omega', \\ \varepsilon.\ \omega' = -c.2\omega - \beta'\omega', \\ \varepsilon = \dfrac{\beta - \beta' + i\sqrt{4n-1}}{2}, \end{cases}$$

où $\beta + \beta' = 2b + 1$, $\beta - \beta' = \pm 1$, $n = ac - \beta\beta'$, et où, par conséquent, on peut à volonté supposer β pair ou impair. Pour la première catégorie a est pair et nous supposons β impair. Par suite, il faut employer les équations modulaires du cas II; on a, comme au numéro précédent,

$$(50)\qquad \begin{cases} \beta = r_1\delta, \qquad a = s_1\delta, \\ -c = -r_1 t + r'_1 n', \qquad -\beta' = -s_1 t + s'_1 n', \end{cases}$$

où $\delta \equiv 1 \pmod 4$, s_1 est pair, r_1 et s'_1 impairs. On peut profiter de l'indétermination de l'équation $r_1 s'_1 - r'_1 s_1 = 1$ pour rendre r'_1 pair; le nombre t est déterminé par l'équation

$$t = cs'_1 - \beta' r'_1,$$

et l'on a

$$t \equiv cr_1 \equiv \beta c \pmod 4.$$

Si maintenant a est divisible par 4, on a

$$k_0 = k, \qquad \varepsilon_0 = (-1)^{\frac{\beta-1}{2}} \frac{\beta - \beta' + i\sqrt{4n-1}}{2}$$

$$\lambda\left(\frac{\beta - \beta' + i\sqrt{4n-1}}{2}\theta\right) = (-1)^{\frac{\beta-1}{2}} Y.$$

et, si $a \equiv 2 \pmod 4$,

$$k_0 = \frac{1}{k}, \qquad \varepsilon_0 = (-1)^{\frac{\beta-1}{2}} k \frac{\beta - \beta' + i\sqrt{4n-1}}{2},$$

$$\lambda\left(\frac{\beta - \beta' + i\sqrt{4n-1}}{2}\theta\right) = (-1)^{\frac{\beta-1}{2}} \frac{1}{k} Y.$$

Les valeurs de k_0 doivent être substituées dans l'équation modulaire en $\sqrt{k}$ et en k_0 répondant à $t \equiv \beta c \pmod 4$; on obtient ainsi deux équations à coefficients entiers

$$f(i^{\beta c}\sqrt{k}) = 0, \qquad f'(i^{\beta c}\sqrt{k}) = 0,$$

dont la première a lieu si $a \equiv 0$, l'autre si $a \equiv 2 \pmod 4$; dans la première le coefficient de la plus haute puissance de $i^{\beta c}\sqrt{k}$ est 1, le dernier coefficient est une puissance de 2; dans la seconde équation l'inverse a lieu.

Il suffira de chercher les racines des équations

$$f(\sqrt{k}) = 0, \qquad f'(\sqrt{k}) = 0,$$

répondant à $c \equiv 0 \pmod 4$. Au moyen de la relation $\zeta_0 = \frac{t + \delta\zeta}{n'}$, on trouve que les deux équations admettent la racine $\sqrt{k} = 1$, et qu'en outre la première a la racine $\sqrt{k} = 0$, mais qu'aucune d'elles n'est satisfaite par $\sqrt{k} = -1$, ni par $\sqrt{k} = \pm i$. De la manière ordinaire on démontre que les autres racines sont les racines carrées des modules de la seconde espèce et de la première catégorie, dont le degré n_1 satisfait à la relation

$$4n = x^2 + y^2(4n_1 - 1),$$

x et y étant premiers entre eux et impairs, et que la multiplicité de chacune d'elles est égale à la quatrième partie du nombre des solutions de cette équation; on voit en même temps qu'il faut supposer pour chacun de ces modules le coefficient c_1 divisible par 4, et qu'il faut prendre $a_1 \equiv 0 \pmod 4$ pour la première équation, $a_1 \equiv 2$ pour la seconde.

En supprimant les racines étrangères, on a deux équations

$$F(\sqrt{k}) = 0, \qquad F'(\sqrt{k}) = 0;$$

si l'on ne fait pas d'hypothèse sur la valeur de c, on a évidemment

$$F(i^{\beta c}\sqrt{k}) = 0, \qquad F'(i^{\beta c}\sqrt{k}) = 0,$$

c'est-à-dire qu'il y a quatre équations pour $a \equiv 0 \pmod 4$ et autant pour $a = 2$, mais qu'en chassant $\sqrt{k}$ et les puissances impaires de k, on n'a que deux équations finales

$$F_1(k^2) = 0, \qquad F_1'(k^2) = 0.$$

Dans la première de ces équations le premier coefficient est 1, le dernier une puissance de 2, l'inverse ayant lieu pour la seconde. Au moyen des transformations linéaires, on démontre facilement que, $\sqrt{k}$ satisfaisant à l'équation $F(\sqrt{k}) = 0$, $\frac{1-\sqrt{k}}{1+\sqrt{k}}$ lui satisfera aussi, et que $\frac{1}{\sqrt{k}}$, $\frac{1+\sqrt{k}}{1-\sqrt{k}}$ seront racines de l'équation $F'(\sqrt{k}) = 0$.

Évidemment $(-1)^c k$ s'exprime en fonction rationnelle de k^2.

Exemples. — En faisant

$$k = \frac{2\sqrt{k}}{1+k},$$

on a

$$\sqrt{k}(\sqrt{k}-1)(k+\sqrt{k}+2) = 0,$$

où le dernier facteur donne la première équation relative à $n = 2$; on en tire

$$\sqrt{k} = \frac{-1+i\sqrt{7}}{2}.$$

Faisant, au contraire,

$$\frac{1}{k} = \frac{2\sqrt{k}}{1+k},$$

on a

$$(\sqrt{k}-1)(2k+\sqrt{k}+1) = 0;$$

d'où

$$\sqrt{k} = \frac{-1 + i\sqrt{7}}{4}.$$

$n = 4$. — L'équation modulaire est

$$k_0^2(1+\sqrt{k})^8 = 8\sqrt{k}(1+k);$$

en y faisant $k_0 = k$, on trouve

$$\sqrt{k}(\sqrt{k}-1)(k+\sqrt{k}+2)(k^2+4k\sqrt{k}+5k+2\sqrt{k}+4) = 0;$$

donc, pour $n = 4$, la première équation est

$$k^2+4k\sqrt{k}+5k+2\sqrt{k}+4 = 0.$$

Pour en faciliter la résolution, on peut remarquer que, $\sqrt{k}$ étant une racine, $\frac{1-\sqrt{k}}{1+\sqrt{k}}$ en est une autre, de sorte que l'équation se décompose en deux facteurs de la forme $k - \alpha\sqrt{k} - (\alpha - 1) = 0$; on trouve ainsi $\alpha = -2 - \sqrt{5}$,

$$\sqrt{k} = \frac{2+\sqrt{5}+i\sqrt{3}}{2}.$$

En faisant $k_0 = \frac{1}{k}$, on a

$$(\sqrt{k}-1)(2k+\sqrt{k}+1)(4k^2+2k\sqrt{k}+5k+4\sqrt{k}+1) = 0,$$

où le dernier facteur donne la seconde équation; on trouve

$$\sqrt{k} = \frac{-1+\sqrt{5}+3i\sqrt{3}+i\sqrt{15}}{8}.$$

19. *Modules de la seconde espèce et de la seconde catégorie d'un degré pair.* — Dans les équations (49), (50) le nombre α est impair, de sorte qu'il faut employer les équations modulaires du cas II; de plus, s_1 étant impair, nous pouvons rendre $s'_1 \equiv 0 \pmod 4$. On a donc

$$\beta \equiv r_1, \qquad \alpha \equiv s_1, \qquad t \equiv s_1\beta' \equiv \alpha\beta' \pmod 4,$$

et, par suite, le Tableau des transformations linéaires donne

$$\sqrt{k_0} = \frac{1 - i^{\alpha\beta}\sqrt{k}}{1 + i^{\alpha\beta}\sqrt{k}},$$

$$\varepsilon' = \frac{2 i^{\alpha}}{(1 + i^{\alpha\beta}\sqrt{k})^2},$$

$$\varepsilon_0 = (-1)^{\frac{\alpha-1}{2}} \frac{1}{4}\left[(\beta' - \beta)i + \sqrt{4n-1}\right](1 + i^{\alpha\beta}\sqrt{k})^2,$$

$$\lambda\left(\frac{\beta - \beta' + i\sqrt{4n-1}}{2}\,0\right) = \frac{2\varepsilon' Y}{1 + \Delta(Y) - k_0 Y^2}.$$

En dénotant par $f(k_0, \sqrt{k}) = 0$ l'équation modulaire du cas II qui répond à $l \equiv 0 \pmod 4$, on a

$$f\left[\left(\frac{1 - i^{\alpha\beta}\sqrt{k}}{1 + i^{\alpha\beta}\sqrt{k}}\right)^2, i^{\alpha\beta'}\sqrt{k}\right] = 0. \tag{51}$$

En cherchant les modules singuliers qui satisfont à cette équation, on voit facilement qu'ils sont tous de la seconde espèce; par conséquent, les nombres R_1, S_1, R'_1, S'_1 sont déterminés par les équations

$$\begin{aligned}
\frac{x+y}{2} + y b_1 &= R_1 \delta, \\
y a_1 &= S_1 \delta, \\
-y c_1 &= -R_1 t + R'_1 n', \\
\frac{x-y}{2} - y b_1 &= -S_1 t + S'_1 n'.
\end{aligned}$$

S_1 étant nécessairement impair, nous pouvons toujours supposer $S'_1 \equiv 0 \pmod 4$; d'où

$$\left.\begin{aligned}
S_1 &\equiv y a_1 \\
t &\equiv -a_1 \frac{xy-1}{2} + a_1 b_1 \\
R_1 S_1 &\equiv a_1 \frac{xy+1}{2} + a_1 b_1
\end{aligned}\right\} \pmod 4.$$

Donc les conditions nécessaires et suffisantes pour que $\sqrt{l}$ soit une

racine de l'équation (51) sont

$$a_1 \frac{xy+1}{2} + a_1 b_1 \equiv a\beta, \qquad -a_1 \frac{xy-1}{2} + a_1 b_1 \equiv a\beta' \pmod 4 :$$

d'où l'on tire

$$a_1 xy \equiv a(\beta - \beta'), \qquad b_1 \equiv a\beta a_1 - \frac{xy+1}{2}$$

et

$$a_1(2b_1+1) = a_1(\beta_1 + \beta'_1) \equiv a(\beta + \beta') \pmod 4.$$

Considérons spécialement l'équation

$$f\left[\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^2, i\sqrt{k}\right] = 0, \tag{52}$$

qui, comme il est facile de le voir, donne toutes les valeurs de k^2; on doit faire $\beta \equiv 0$, $\beta' \equiv a$, et l'on a, par conséquent,

$$xy \equiv -a_1, \qquad a_1(\beta_1 + \beta'_1) \equiv 1 \pmod 4,$$
$$b_1 \equiv -\frac{xy+1}{2}, \qquad b_1 + 1 \equiv -\frac{xy-1}{2}.$$

Nous pouvons maintenant faire $\beta_1 = b_1$ ou $\beta_1 = b_1 + 1$ à volonté; supposons β_1 pair, et remarquons que, si β_1 est divisible par 4, on aura $a_1\beta'_1 \equiv 1$; si, au contraire, $\beta_1 \equiv 2 \pmod 4$, on aura $a_1\beta'_1 \equiv -1$. Il s'ensuit que l'équation (52) est satisfaite par les racines carrées des modules de la seconde espèce et de la seconde catégorie dont le degré n_1, nécessairement pair, vérifie l'équation

$$4n = x^2 + y^2(4n_1 - 1), \tag{53}$$

x et y étant impairs et premiers entre eux, et lesquelles satisfont à une équation de la forme (52) correspondant au degré n_1, pourvu qu'on ait soin de changer le signe de $\sqrt{l}$ toutes les fois que $\frac{xy \pm 1}{2}$ est pair, sans être divisible par 4. Puisque, le signe de y étant choisi, celui de x est déterminé par la congruence $xy \equiv -a_1$, la multiplicité de la racine $\sqrt{l}$

est égale au quart du nombre des solutions de l'équation (53). Outre ces racines, l'équation (52) admet encore les suivantes :

$$\text{si } \frac{n}{2} \text{ est impair}, \qquad \sqrt{k} = -1, \qquad \sqrt{k} = i,$$

$$\text{si } \frac{n}{2} \text{ est pair}, \qquad \sqrt{k} = 1, \qquad \sqrt{k} = -i.$$

Ce qui précède suffit pour montrer comment on peut débarrasser l'équation des racines étrangères et obtenir ainsi une équation $F(\sqrt{k}, i) = 0$ qui n'est satisfaite que par les modules du degré n.

En considérant l'équation

$$f\left[\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^2, -i\sqrt{k}\right] = 0,$$

qu'on obtient en faisant $\beta \equiv 0$, $\beta' \equiv -a$, on voit qu'elle donne les mêmes valeurs de k^2 que l'équation (52); en supprimant les racines étrangères, on a évidemment $F(\sqrt{k}, -i) = 0$. Il s'ensuit que, en chassant des équations $F(\sqrt{k}, \pm i) = 0$, le radical $\sqrt{k}$ et les puissances impaires de k, on obtient une seule équation en k^2

$$F_1(k^2) = 0,$$

dont les coefficients sont, par conséquent, des entiers. Cette équation est réciproque, et, d'après ce qui a été dit au n° **15**, son premier et son dernier coefficient sont 1.

On voit facilement que, si $\sqrt{k} = \varkappa$ satisfait à l'équation $F(\sqrt{k}, i) = 0$, la valeur $\sqrt{k} = i\varkappa$ satisfait à l'équation $F(\sqrt{k}, -i) = 0$, de sorte qu'on a $F(\sqrt{k}, i) = F(i\sqrt{k}, -i)$; on en conclut que le polynôme $F(\sqrt{k}, i)$ a la forme suivante

$$F(\sqrt{k}, i) = \varphi(k^2) + (1-i)k\sqrt{k}\,\varphi_1(k^2) + ik\,\varphi_2(k^2) + (1+i)\sqrt{k}\,\varphi_3(k^2),$$

φ, φ_1, φ_2, φ_3 dénotant des polynômes à coefficients entiers. De plus, puisque, des quatre équations $F(\pm\sqrt{k}, \pm i) = 0$, deux n'ont pas de ra-

cines communes, on voit que $(1+i)\sqrt{k}$ s'exprime en fonction rationnelle de k^2. Généralement, en ne faisant aucune supposition relative à β et à β', on trouve

$$F\left[i^{\alpha\beta}\sqrt{k},\, i^{\alpha(\beta'-\beta)}\right]=0,$$

et l'on a une équation de la forme

$$i^{\alpha\beta}\left[1+i^{\alpha\beta'-\beta}\right]\sqrt{k}=\psi(k^2),$$

$\psi(k^2)$ étant une fonction rationnelle, la même pour toutes les racines de l'équation $F_1(k^2)=0$.

En faisant, par exemple, $n=2$, on a

$$\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^2=\frac{2i\sqrt{k}}{1-k};$$

d'où

$$(\sqrt{k}+1)(\sqrt{k}-i)\left[k-3(1-i)\sqrt{k}-i\right]=0;$$

le dernier facteur donne

$$\sqrt{k}=\frac{1-i}{2}(3+\sqrt{7}),\qquad k^2=-\frac{1}{4}(3+\sqrt{7})^4.$$

En faisant $n=4$, on obtient

$$\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^4=\frac{8i\sqrt{k}(1-k)}{(1+i\sqrt{k})^4}$$

ou bien

$$(\sqrt{k}-1)(\sqrt{k}+i)\left[k+3(1-i)\sqrt{k}-i\right]$$
$$\times\left[k^2-6(1-i)k\sqrt{k}+20ik+6(1+i)\sqrt{k}-1\right]=0,$$

où le dernier facteur donne

$$\sqrt{k}=\frac{1-i}{2}(2+\sqrt{3})(\sqrt{3}+\sqrt{5}),\qquad k^2=-\frac{1}{4}(2+\sqrt{3})^4(\sqrt{3}+\sqrt{5})^4.$$

20. Si, dans l'équation modulaire Ib appartenant au degré $4n$, on

fait $k_0^2 = k^2$, on obtient une équation, $F(k^2) = 0$, qui, comme on le démontre aisément, est satisfaite par les modules de la première espèce et de la première catégorie dont le degré n_1 vérifie la condition

$$4n = x^2 + y^2 n_1,$$

x et y étant impairs et premiers entre eux; la multiplicité de chacune de ces racines est égale au quart du nombre des solutions de l'équation de condition. En outre, elle n'admet que la racine $k^2 = 0$, et seulement si n est pair. Supposons que n soit impair, et soit $f(k_0^2, k^2) = 0$ l'équation modulaire appartenant au degré n, N le degré de cette équation; l'équation modulaire Ia correspondant au degré $4n$ est $f(k_0'^2, k^2) = 0$ (n° **15**), et, par conséquent, l'équation Ib est $f\left(k_0'^2, \frac{1}{k^2}\right) = 0$. Donc on a

$$F(k^2) = k^{2N} f\left(k'^2, \frac{1}{k^2}\right) = 0.$$

Dans cette équation, le premier et le dernier coefficient sont égaux à 1, propriété qui est conservée, quand on supprime les racines appartenant aux degrés moindres que $4n - 1$. Cela justifie l'assertion faite au n° **11** sur l'équation des modules de la première espèce et de la première catégorie dont le degré est de la forme $8h + 3$.

Au fond, la règle qui vient d'être démontrée est la même que la troisième règle de M. Hermite (*Théor. d'équat. mod.*, p. 44, 45); on peut démontrer les autres par des considérations analogues.

21. Nous supposerons dès à présent le rapport des périodes défini par une équation de la forme

$$a\zeta^2 + 2b\zeta + c = 0,$$

même pour les modules de la seconde espèce, de sorte que, pour ces modules, a et c sont pairs, b impair; nous désignerons par $-D$ le déterminant du module, en faisant

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

Cela posé, examinons de plus près les formules de multiplication

complexe. Pour tous les modules de la première espèce et de la première catégorie et pour tous les modules de la seconde espèce, on a des équations de la forme

$$\lambda(i\sqrt{D}\,0) = AY;$$

pour ceux de la seconde espèce et de la première catégorie, on a, en outre,

$$\lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right) = AY,$$

où A désigne une constante, Y ayant la même signification que dans les numéros précédents. En faisant converger 0 vers zéro, on en tire respectivement

$$i\sqrt{D} = A\varepsilon_0, \qquad \frac{1+i\sqrt{D}}{2} = A\varepsilon_0;$$

d'où

$$(54)\qquad \lambda(i\sqrt{D}\,0) = i\sqrt{D}\,\frac{Y}{\varepsilon_0}, \qquad \lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right) = \frac{1+i\sqrt{D}}{2}\,\frac{Y}{\varepsilon_0}.$$

Pour la seconde catégorie de la première espèce, on trouve, en remettant la valeur de k_0,

$$(55)\qquad \lambda(i\sqrt{D}\,0) = \frac{2i\sqrt{D}(1+i^{ab}\sqrt{k})^2\,\frac{Y}{\varepsilon_0}}{(1+i^{ab}\sqrt{k})^2[1+\Delta(Y)] - (1-i^{ab}\sqrt{k})^2 Y^2},$$

et, pour la seconde catégorie de la seconde espèce, en ayant égard à la dénomination changée,

$$(56)\qquad \lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right) = \frac{(1+i\sqrt{D})\left(1+i^{\frac{ab+1}{4}}\sqrt{k}\right)^2\,\frac{Y}{\varepsilon_0}}{\left(1+i^{\frac{ab+1}{4}}\sqrt{k}\right)^2[1+\Delta(Y)] - \left(1-i^{\frac{ab+1}{4}}\sqrt{k}\right)^2 Y^2}.$$

La fonction Y a des formes différentes dans les différents cas. En désignant par F et F_1 des fonctions rationnelles, on a, si la transformation appartient à un degré impair,

$$Y = \varepsilon_0 F[\lambda(0)], \qquad \Delta(Y) = \mu(0)\nu(0)F_1[\lambda(0)].$$

Cela a encore lieu si le degré est pair, et que la transformation appar-

tienne au second cas; mais, si elle appartient au premier cas, on a, si le degré est impairement pair,

$$Y = \frac{\varepsilon_0 F[\lambda(\theta)]}{\mu(\theta)\nu(\theta)}, \qquad \Delta(Y) = F_1[\lambda(\theta)],$$

et, si le degré est divisible par 4,

$$Y = \varepsilon_0 \mu(\theta)\nu(\theta) F[\lambda(\theta)], \qquad \Delta(Y) = F_1[\lambda(\theta)].$$

Tant qu'on regarde le module primitif k comme une quantité indéterminée, les coefficients de la fonction Y, à l'exception du multiplicateur ε_0, s'expriment toujours ou en fonction entière de k^2 et de k_0^2 à coefficients entiers, ou bien, s'il s'agit d'une transformation d'un degré impairement pair et appartenant au premier cas, en fonction entière de k et de k_0^2; la même chose a lieu à l'égard de ε_0^2 et des coefficients de $F_1[\lambda(\theta)]$. Cette propriété des transformations principales est fondée sur la circonstance que k_0^2 et les coefficients dont il est question sont des fonctions symétriques des quantités $\lambda^2\left(\frac{p\Omega}{n}\right)$ ou $\lambda^2\left[\frac{(2p+1)\Omega}{2n}\right]$, et que k_0^2 a autant de valeurs différentes que le permet la nature d'une fonction de cette forme; par conséquent, elle ne peut faire défaut pour des modules spéciaux que si k_0^2 est racine double ou multiple de l'équation modulaire correspondante. Or, d'après ce qui a été dit au n° **8**, il est facile de voir que, si l'on fait k égal à un module singulier appartenant au déterminant $-D$, k_0^2 est effectivement racine simple de l'équation modulaire principale; donc la propriété générale des transformations dont nous parlions ne cesse pas d'avoir lieu dans notre cas spécial. En l'appliquant aux équations (54), on a ou $k_0^2 = k^2$ ou $k_0^2 = \frac{1}{k^2}$, et, par suite, les coefficients de $F[\lambda(\theta)]$, $F_1[\lambda(\theta)]$ sont rationnels en k^2; les formules qui appartiennent aux degrés impairement pairs ne font pas exception, puisque, dans ces cas, k s'exprime rationnellement en k^2 (n^{os} **16, 18**). Quand les équations (55) ou (56) ont lieu, on a respectivement (n^{os} **13, 14, 17, 19**)

$$k_0^2 = \left(\frac{1 - i^{ab}\sqrt{k}}{1 + i^{ab}\sqrt{k}}\right)^4, \qquad k_0^2 = \left(\frac{1 - i^{\frac{a(b+1)}{4}}\sqrt{k}}{1 + i^{\frac{a(b+1)}{4}}\sqrt{k}}\right)^4,$$

et, de plus, on a vu que, dans le cas de l'équation (55), $i^{ab}\sqrt{k}$ s'exprime rationnellement en k^2, et que, dans celui de l'équation (56), $i^{\frac{a(b+1)}{4}}\sqrt{k}$ s'exprime rationnellement en k^2 et en $i^{\frac{a}{2}}$.

De ce qui précède il suit qu'on a, pour tout module du déterminant — D, une équation de la forme suivante

$$(57)\qquad \lambda(i\sqrt{D}\,0) = \frac{i\sqrt{D}\,\psi[\lambda(0), k^2]}{\psi_1[\lambda(0), k^2] + \mu(0)\nu(0)\psi_2[\lambda(0), k^2]},$$

et qu'on a, en outre, pour les modules de la seconde espèce s'ils sont de la première catégorie,

$$(58)\qquad \lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right) = \frac{1+i\sqrt{D}}{2}\,\frac{\psi[\lambda(0), k^2]}{\psi_1[\lambda(0), k^2]},$$

et, s'ils sont de la seconde catégorie,

$$(59)\qquad \lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right) = \frac{1+i\sqrt{D}}{2}\,\frac{\psi\left[\lambda(0), k^2, i^{\frac{a}{2}}\right]}{\psi_1\left[\lambda(0), k^2, i^{\frac{a}{2}}\right] + \mu(0)\nu(0)\psi_2\left[\lambda(0), k^2, i^{\frac{a}{2}}\right]},$$

ψ, ψ_1, ψ_2 dénotant des polynômes à coefficients entiers qu'on peut supposer dépourvus de diviseurs communs. Pour les modules de la première catégorie, $\psi_2[\lambda(0), k^2] = 0$ si D est impair; si D est pair, on a $\psi_1[\lambda(0), k^2] = 0$.

L'introduction de l'irrationnelle $i\sqrt{D}$ dans les seconds membres de ces formules a pour effet de faire disparaître le double signe qui, dans les numéros précédents, affecte partout les expressions de $\lambda(i\sqrt{D}\,0)$, $\lambda\left(\frac{1+i\sqrt{D}}{2}\,0\right)$; par là, les formules (57), (58) sont devenues indépendantes des coefficients a, b, c de l'équation en ζ, de sorte qu'elles sont identiquement les mêmes pour tous les modules qui satisfont à la même équation en k^2. Dans l'équation (59), une ambiguïté subsiste encore; mais, comme on le verra au numéro suivant, elle peut être levée au moyen d'une équation de la forme

$$i^{\frac{a}{2}} = i\sqrt{D}\,\chi(k^2).$$

Par différentiation on tire de l'équation (57) une expression de

$$\mu(i\sqrt{D}\theta)\nu(i\sqrt{D}\theta);$$

au moyen des théorèmes d'addition et de multiplication on peut ensuite déduire l'expression de $\lambda[(r+si\sqrt{D})\theta]$, qui évidemment peut être réduite à la forme

$$\lambda[(r+si\sqrt{D})\theta] = \frac{P}{Q+\mu(\theta)\nu(\theta)R},$$

P, Q et R étant des fonctions entières de $\lambda(\theta)$, k^2, $i\sqrt{D}$ à coefficients entiers, et qu'on peut supposer sans diviseurs communs. Pour les modules de la seconde espèce, on aura une expression semblable de

$$\lambda\left(\frac{r+si\sqrt{D}}{2}\theta\right),$$

r et s étant impairs.

22. Les équations algébriques qui déterminent les carrés des modules singuliers se décomposent toutes en deux équations partielles par l'adjonction ou de $\sqrt{D}$ ou de $i\sqrt{D}$, à moins que D ne soit un carré parfait. Cela découle immédiatement des relations qui ont lieu entre $i\sqrt{D}$ et le multiplicateur ε_0 de la transformation principale employée.

Soit $\Phi(k^2)=0$ une de ces équations, et supposons d'abord qu'elle appartienne à la première catégorie, le déterminant étant de la forme $-(4h+1)$. On a, dans ce cas (n° **10**), $\varepsilon_0 = i^b k\sqrt{D}$; or, ε_0 s'exprimant en fonction rationnelle de k^2, on peut faire

$$i^b k\sqrt{D} = \varphi(k^2);$$

de plus, on a

$$i^{bc}k = \psi(k^2);$$

d'où l'on tire, en se rappelant que b et c sont impairs,

$$\varphi(k^2) - (-1)^{\frac{c-1}{2}}\sqrt{D}\,\psi(k^2) = 0.$$

Les coefficients des fonctions rationnelles φ et ψ étant des entiers, on en peut évidemment conclure que, si D n'est pas un carré parfait, l'équation $\Phi(k^2) = 0$ se décompose par l'adjonction de $\sqrt{D}$ en deux autres du degré sous-double, et qu'un module satisfait à l'une ou l'autre de ces équations, suivant que $(-1)^{\frac{c-1}{2}}$ est égal à $+1$ ou à -1.

Pour les modules de la première catégorie d'un déterminant pair, on peut se borner aux équations (44), puisque, si $D \equiv 2 \pmod 4$, il n'y a qu'une seule équation en k^2, et que, si $D \equiv 0 \pmod 4$, l'une des deux équations a pour racines les réciproques de celles de l'autre, de sorte que la décomposition de la première équation entraîne celle de l'autre. On a donc

$$\varepsilon_0 = i^c \sqrt{D} = i\varphi(k^2)$$

ou bien

$$\varphi(k^2) - (-1)^{\frac{c-1}{2}} \sqrt{D} = 0;$$

d'où l'on peut faire les mêmes conclusions que pour $D = 4h + 1$; seulement il faut se rappeler que, si $D \equiv 2 \pmod 4$, on a supposé b divisible par 4; si l'on veut se délivrer de cette restriction, il faut remplacer $(-1)^{\frac{c-1}{2}}$ par $(-1)^{\frac{c-b-1}{2}}$.

Pour tous les modules de la première espèce et de la seconde catégorie, on a (n^{os} **13**, **17**) une équation de la forme

$$\varepsilon_0 = (-1)^{\frac{a-1}{2}} \tfrac{1}{2}(1 + i^{ab}\sqrt{k})^2 \sqrt{D} = \varphi(k^2),$$

et l'on peut faire

$$\tfrac{1}{2}(1 + i^{ab}\sqrt{k})^2 = \psi(k^2),$$

donc

$$\varphi(k^2) - (-1)^{\frac{a-1}{2}} \sqrt{D}\,\psi(k^2) = 0.$$

Donc, si D n'est pas un carré, l'équation $\Phi(k^2) = 0$ se décompose par l'adjonction de $\sqrt{D}$ en deux équations partielles, un module donné satisfaisant à l'une ou à l'autre, suivant qu'on a $(-1)^{\frac{a-1}{2}} = +1$ ou $= -1$.

Pour la seconde catégorie de la seconde espèce, on a (n° **12**), en

ayant égard au changement fait dans la signification des lettres a, b, c,

$$\varepsilon_0 = i^b k\sqrt{D} = \varphi(k^2);$$

de plus, on a (n^{os} **14**, **19**)

$$-2i^{\frac{a}{2}b+a}k = \psi(k^2);$$

d'où l'on tire, en remarquant que $\frac{a}{2}$ et b sont des nombres impairs,

$$\varphi(k^2) - \tfrac{1}{2}(-1)^{\frac{a-2}{4}}\sqrt{D}\,\psi(k^2) = 0.$$

Il y a donc, encore dans ce cas, décomposition par $\sqrt{D}$, les modules se groupant suivant la valeur de $(-1)^{\frac{a-2}{4}}$. On trouve aussi

$$i^{\frac{a}{2}} = \tfrac{1}{2}i\sqrt{D}\frac{\psi(k^2)}{\varphi(k^2)},$$

ce qui justifie une assertion faite au numéro précédent.

En considérant, au contraire, les modules de la première catégorie d'un déterminant de la forme $4h-1$, on a, pour les deux espèces (n^{os} **11**, **12**),

$$\varepsilon_0 = (-1)^{\frac{b-1}{2}}i\sqrt{D} = \varphi(k^2);$$

donc l'équation $\Phi(k^2) = 0$ se décompose par l'adjonction de $i\sqrt{D}$, les racines se groupant suivant la valeur de $(-1)^{\frac{b-1}{2}}$.

Si l'on fait subir au module k, défini par l'équation

$$a\zeta^2 + 2b\zeta + c = 0,$$

la transformation linéaire $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, le module transformé sera $\frac{1}{k}$, et il répondra à l'équation

$$(a + 4b + 4c)\zeta^2 + 2(b + 2c)\zeta + c = 0.$$

En considérant séparément les divers cas, on démontre aisément que, pour la première catégorie d'un déterminant de la forme $-(4h+1)$ et pour la seconde catégorie de la première espèce de tous les déterminants, k^2 et $\frac{1}{k^2}$ satisfont à la même équation partielle, tandis que, pour la première catégorie de la première espèce des déterminants $-(4h-1)$, $-(4h+2)$ et pour la seconde catégorie de la seconde espèce, k^2 satisfait à l'une des équations partielles, $\frac{1}{k^2}$ à l'autre. Quant à la première catégorie de la seconde espèce et à la première catégorie des déterminants divisibles par 4, on se rappelle qu'il y a déjà, avant la décomposition, deux équations, satisfaites l'une par k^2, l'autre par $\frac{1}{k^2}$.

IV. — Digression sur les formules d'Arithmétique de M. Kronecker.

23. Nous avons déjà donné deux exemples des formules d'Arithmétique qu'on peut tirer des considérations du paragraphe précédent, et évidemment toute équation modulaire donne lieu à un corollaire de cette espèce. Mais, si l'on veut obtenir ces formules sous la forme choisie par leur illustre auteur, il faut employer, non pas les équations modulaires irréductibles, mais les équations qui embrassent toutes les transformations définies par des équations de la forme

$$\varepsilon.2\omega = n'.2\omega_0,$$
$$\varepsilon.2\omega' = -l.2\omega_0 + n''\omega'_0,$$

d'un degré impair donné, ou toutes celles qu'on en déduit par une transformation principale du degré 2^π. On trouve par cette méthode, indiquée par M. Hermite dans son célèbre travail *Sur les équations modulaires* (p. 46, note), un certain nombre de formules qui se résument toutes par les formules I-VI de M. Kronecker (*Journal de Crelle*, t. 57, p. 249). Nous en déduirons quelques-unes, en commençant par celles qui correspondent à des transformations de degrés

impairs. Voici d'abord les notations dont nous ferons usage dans ce paragraphe : nous désignerons par

$G(n)$ le nombre des classes de formes quadratiques du déterminant $-n$, en faisant toutefois $G(0)=\frac{1}{4}$;

$F(n)$ le nombre des classes du déterminant $-n$ dont les coefficients extérieurs ne sont pas, les deux, pairs, en faisant $F(0)=0$;

$\Phi(n)$ la somme des facteurs de n;

$\Psi(n)$ l'excès de la somme des facteurs de n qui surpassent $\sqrt{n}$, sur la somme de ceux qui sont moindres que $\sqrt{n}$;

$\varphi(n)$ la moitié du nombre des solutions de l'équation indéterminée $n=\xi^2+4\eta^2$;

$\varphi''(n)$ la moitié du nombre des solutions de l'équation $n=\xi^2+16\eta^2$;

$\psi(n)$ la moitié du nombre des solutions de l'équation $n=\xi^2+3\eta^2$.

Ce sont, à l'exception de φ'', les notations employées par M. Kronecker dans le travail cité. Les expressions $G(n)$, $F(n)$ satisfont aux égalités suivantes, où les termes qui se trouvent entre parenthèses ou entre doubles parenthèses doivent être omis, les premiers si n n'est pas un carré impair, les derniers si n n'est pas le triple d'un carré impair

$$F(4n)=2F(n)-(1), \qquad G(4n)-F(4n)=G(n);$$

pour $n=4h+1$, $4h+2$, on a

$$G(n)=F(n),$$

pour $n=8h-1$

$$G(n)=2F(n),$$

et pour $n=8h+3$

$$3G(n)=4F(n)+((2)).$$

24. Soit n un nombre impair, et désignons par

$$f(\sqrt{k}, \sqrt{k_0})=0$$

l'équation qui a lieu entre les racines carrées du module k et de son transformé k_0, la transformation étant du degré n et définie par des

équations de la forme

$$(60)\qquad \begin{cases} \varepsilon . 2\omega = n' . 2\omega_0, \\ \varepsilon \omega' = -t . 2\omega_0 + n'' \omega'_0, \end{cases}$$

où $n = n' n''$, $n' \equiv 1$, $t \equiv 0 \pmod 4$, et où t, n', n'' peuvent avoir un diviseur commun. On sait que le degré de cette équation, en $\sqrt{k_0}$ aussi bien qu'en $\sqrt{k}$, est égal à $\Phi(n)$. Pour les petites valeurs de $\sqrt{k}$ les valeurs de $\sqrt{k_0}$ se développent en séries convergentes, dont les premiers termes sont de la forme $e^{\frac{2\pi i t}{4n''}} 2^{\frac{n''-n'}{n''}} \sqrt{k}^{\frac{n'}{n''}}$; donc, pour les petites valeurs de x, l'équation $f(x, y) = 0$ peut être remplacée par la suivante

$$\Pi(y^{n''} - 2^{n''-n'} x^{n'}) = 0,$$

où n' doit être égalé à tous les diviseurs de n. On en conclut que le plus petit degré d'un terme du développement du polynôme $f(x, y)$ suivant les puissances de x et de y, est égal à $\Phi(n) - \Psi(n)$; c'est donc la multiplicité du point $x = y = 0$ de la courbe $f(x, y) = 0$. Dans le cas où n est un carré parfait nous devons quelquefois faire abstraction de la racine $y = x$, et, dans ce cas, il faudra diminuer d'une unité le nombre trouvé. L'équation ayant la propriété de ne pas être altérée quand on remplace x et y par $\frac{1}{x}$ et $\frac{1}{y}$, on a

$$f(x, y) = C x^{\Phi(n)} y^{\Phi(n)} f\left(\frac{1}{x}, \frac{1}{y}\right),$$

d'où l'on conclut que l'ordre de la courbe est égal à $\Phi(n) + \Psi(n)$, nombre qui doit aussi être diminué d'une unité, si, dans les cas où n est un carré, on supprime la racine $x = y$. Enfin, nous aurons besoin de connaître les multiplicités des points

$$x = y = \pm 1, \qquad x = (-1)^{\frac{n-1}{2}} y = \pm i;$$

on les trouve égales à celle du point

$$x = y = 0.$$

On a vu, en effet, au n° 9, que dans le cas des équations modulaires irréductibles l'équation $f(x, y) = 0$ peut s'écrire

$$f\left(\frac{i^r - x}{i^r + x}, \frac{i^{nr} - y}{i^{nr} + y}\right) = 0;$$

par conséquent la même équation a évidemment lieu dans le cas qui nous occupe. En développant suivant les puissances de $i^r - x$, $i^{nr} - y$, on voit qu'on a, pour les valeurs infiniment petites de ces quantités,

$$f(x, y) = \Pi[(i^{nr} - y)^{n''} - 2^{2(n''-n')}(i^r - x)^{n''}],$$

ce qui justifie notre assertion.

En supposant maintenant que le module k_0 se ramène à k par une transformation linéaire, on obtient une équation en $\sqrt{k}$, dont le degré peut être évalué au moyen des déterminations précédentes. Si cette équation admet les racines 0, ± 1 ou $\pm i$, on les supprimera, et l'on déterminera le degré de l'équation finale, satisfaite par les racines carrées des modules qui admettent une multiplication complexe du degré n et d'une forme spéciale, déterminée par la transformation linéaire employée. Or ces modules sont définis par les équations (27) et (28); seulement, dans notre cas, les nombres x et y ne sont pas assujettis à la condition d'être premiers entre eux.

Faisons dans les équations (27)

$$ya_1 = a, \qquad yb_1 = b, \qquad yc_1 = c, \qquad y^2 n_1 = ac - b^2 = \Delta,$$

on aura, en écrivant ω et ω' au lieu de ϖ et ϖ',

$$(61) \qquad \begin{cases} (x + i\sqrt{\Delta}).2\omega = (x + b).2\omega + a\omega', \\ (x + i\sqrt{\Delta})\ \omega' = \quad -c.2\omega + (x - b)\omega', \end{cases}$$
$$n = x^2 + \Delta.$$

En supposant x et y pairs, les équations (28) donnent un résultat de la même forme; mais, si x et y sont impairs, et qu'on fasse

$$2ya_1 = a, \qquad y(2b_1 + 1) = b,$$
$$2yc_1 = c, \qquad y^2(4n_1 - 1) = ac - b^2 = \Delta,$$

on a

$$(62)\qquad \begin{cases} \dfrac{x+i\sqrt{\Delta}}{2}\cdot 2\omega = \left(\dfrac{x+b}{2}\right)\cdot 2\omega + \dfrac{a}{2}\omega', \\ \dfrac{x+i\sqrt{\Delta}}{2}\ \omega' = \quad -\dfrac{c}{2}\cdot 2\omega + \dfrac{x-b}{2}\omega', \end{cases}$$

$$4n = x^2 + \Delta,$$

où x est impair. Dans les deux cas le module est déterminé par l'équation

$$a\zeta^2 + 2b\zeta + c = 0.$$

Par là nous avons rapporté les modules aux déterminants $-\Delta$, au lieu de les rapporter à leurs degrés, et nous n'avons plus à distinguer les deux espèces de modules, mais seulement les multiplicateurs des formes $x + i\sqrt{\Delta}$ et $\frac{1}{2}(x + i\sqrt{\Delta})$, dont la dernière n'existe que si Δ est de la forme $4h - 1$ et x impair. On remarquera que dans les équations (61) le premier et le dernier coefficient $x + b$ et $x - b$ sont de la même parité, tandis que dans (62) les coefficients correspondants sont de parités contraires.

En faisant usage de (61) et (62), il arrive quelquefois qu'un même module est rapporté à plusieurs déterminants; mais on voit que sa multiplicité comme racine est intacte, en se rappelant que cette multiplicité est égale à la moitié du nombre des multiplicateurs avec lesquels le module satisfait à l'équation. Pour chaque déterminant auquel un module se trouve rapporté, il doit donc être compté comme racine simple si x est zéro, ou si x doit être pris avec un signe déterminé, comme racine double si $x^2 > 0$ et le signe de x est arbitraire.

En égalant le nombre des racines ainsi déterminé au degré connu de l'équation finale, on a une relation entre certains nombres de classes appartenant à une série de déterminants de la forme $-(n - x^2)$ ou de la forme $-(4n - x^2)$.

25. En faisant $\sqrt{k_0} = \sqrt{k}$, on obtient une équation en $\sqrt{k}$ du degré $\Phi(n) + \Psi(n)$, pourvu que n ne soit pas un carré parfait; dans ce cas il faut préalablement débarrasser l'équation modulaire du facteur $\sqrt{k_0} - \sqrt{k}$. Pour comprendre les deux cas dans une même formule, nous

écrirons entre crochets les termes qui doivent être omis, quand n n'est pas un carré; ainsi notre équation sera du degré $\Phi(n)+\Psi(n)-[1]$. Elle admet les racines $0, \pm 1$ et, si n est de la forme $4h+1$, encore $\pm i$. Or, puisque dans les points

$$x=y=0, \qquad x=y=\pm 1, \qquad x=y=\pm i,$$

les directions des tangentes de la courbe $f(x,y)=0$ ne coïncident pas avec la droite $x=y$, la multiplicité de chacun de ces points, considéré comme point d'intersection de la courbe et de la droite, est égale à $\Phi(n)-\Psi(n)-[1]$. Donc, en supprimant ces racines, le degré de l'équation finale sera

$$6\Psi(n)-4\Phi(n)+[4]$$

si n est de la forme $4h+1$,

$$4\Psi(n)-2\Phi(n)$$

si n est de la forme $4h-1$.

Pour que la racine carrée d'un module singulier définie par les formules (61) ou (62) satisfasse à l'équation finale, il faut que l'une ou l'autre de ces multiplications complexes se déduise d'une transformation de la forme (60) suivie d'une transformation linéaire $\begin{pmatrix} r & s \\ r' & s' \end{pmatrix}$, c'est-à-dire que les quatre coefficients de la multiplication complexe doivent être respectivement égaux aux nombres

$$rn', \quad sn', \quad -rt+r'n'', \quad -st+s'n''.$$

Dans notre cas on a

$$s\equiv r'\equiv 0 \pmod 4,$$

de sorte que rn' et $-st+s'n''$ sont impairs; donc il ne peut être question que des équations (61). On doit donc poser

$$x+b=rn', \qquad a=sn',$$
$$-c=-rt+r'n'', \qquad x-b=-st+s'n''.$$

Par suite $x+b$ et $x-b$ seront impairs, a et c divisibles par 4, et l'on aura

$$\Delta = ac - b^2 \equiv 0 \qquad \text{ou} \qquad \equiv -1 \qquad (\text{mod } 4).$$

Réciproquement on voit sans peine que ces conditions sont suffisantes.

Supposons d'abord que n soit de la forme $4h+1$; dans ce cas x sera nécessairement impair, b pair, puisque autrement

$$\Delta = n - x^2 \equiv 1 \qquad (\text{mod } 4)$$

ce qui est impossible. Donc les modules peuvent correspondre à toute forme quadratique (a, b, c) du déterminant

$$-|n-(2\xi+1)^2|$$

dans laquelle a et c sont divisibles par 4, b pair, en d'autres termes, à toute forme quadratique du déterminant

$$-\tfrac{1}{4}|n-(2\xi+1)^2|$$

dont les coefficients extérieurs sont pairs. Ainsi on a pour chaque valeurs de $(2\xi+1)^2$ un nombre de classes égal à

$$G\left[\frac{n-(2\xi+1)^2}{4}\right] - F\left[\frac{n-(2\xi+1)^2}{4}\right].$$

A l'exception des modules linéaires qui pourront se présenter, il y a pour chaque classe vingt-quatre valeurs de $\sqrt{k}$, toutes des racines doubles, puisque le signe de $2\xi+1$ est arbitraire. Mais nous conserverons au premier membre de l'équation le coefficient 48 devant tous les termes en ajoutant au second membre une correction C. On a donc

$$48\sum\left\{G\left[\frac{n-(2\xi+1)^2}{4}\right] - F\left[\frac{n-(2\xi+1)^2}{4}\right]\right\}$$
$$= 6\Psi(n) - 4\Phi(n) + |4| + C.$$

Déterminons maintenant la correction. Pour rencontrer des modules linéaires de la première espèce, il faut que $\frac{n-(2\xi+1)^2}{4}$ soit un carré

parfait; mais, puisque a et c doivent être pairs, ce carré sera lui-même pair : donc il faut que $n=(2\xi+1)^2+16\eta^2$. Si cette équation a lieu, on a les valeurs

$$\sqrt{k}=\pm\sqrt{\pm i},\qquad \sqrt{k}=\pm(\sqrt{2}\pm 1),\qquad \sqrt{k}=\pm i(\sqrt{2}\pm 1):$$

douze valeurs de $\sqrt{k}$ au lieu de vingt-quatre; ces racines étant doubles, la partie correspondante de la correction sera $12\varphi''(n)-[12]$. On a des modules linéaires de la seconde espèce si $n=(2\xi+1)^2+3(2\eta)^2$, et dans ce cas on a compté vingt-quatre valeurs de $\sqrt{k}$ au lieu de huit, ce qui amène une correction de $16\psi(n)-[16]$. Enfin un dernier terme de correction égal à $[12]$ est exigé par la circonstance qu'on a $G(0)=\frac{1}{4}$. Donc enfin on a

$$C=12\varphi''(n)+16\psi(n)-[16].$$

En substituant et divisant par 2, on a, pour $n=4h+1$,

$$(63)\quad \begin{cases} 24\sum G\left[\dfrac{n-(2\xi+1)^2}{4}\right]-24\sum F\left[\dfrac{n-(2\xi+1)^2}{4}\right] \\ \qquad =3\Psi(n)-2\Phi(n)+6\varphi''(n)+8\psi(n)-[6], \end{cases}$$

où le nombre $2\xi+1$ doit prendre toutes les valeurs impaires et positives qui ne surpassent pas $\sqrt{n}$.

Si $n=4h-1$, x est pair, b impair, et par suite $\Delta=ac-b^2$ est de la forme $8h-1$. Il s'ensuit que x aura les valeurs 0, 4, 8, 12, ..., si n est de la forme $8h-1$, mais les valeurs 2, 6, 10, ..., si n est de la forme $8h+3$. Or, si dans une forme (a, b, c) du déterminant $-(8h-1)$, les coefficients a et c sont pairs, l'un d'eux sera divisible par 4, et b sera impair; de plus, il y aura toujours une forme de la même classe dans laquelle a et c sont, les deux, divisibles par 4; en effet, si l'on a, par exemple, $c\equiv 2 \pmod 4$, on déduira par la transformation linéaire $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ une nouvelle forme a_1, b_1, c_1 dans laquelle

$$a_1=a,$$
$$c_1=a+2b+c\equiv 0 \pmod 4.$$

Il y a donc, parmi les racines de l'équation, des valeurs de $\sqrt{k}$ appartenant à chaque classe de formes du déterminant $-\Delta$ dont les coefficients extérieurs sont pairs. Le nombre de ces classes est

$$G(\Delta) - F(\Delta) = F(\Delta).$$

Or, si $\sqrt{k}$ est une de ces racines, les autres racines appartenant à la même classe s'en déduisent par les transformations linéaires $\begin{pmatrix} r & s \\ r' & s' \end{pmatrix}$ qui conservent les congruences $a \equiv c \equiv 0 \pmod 4$; il faut pour cela que rr' et ss' soient pairs, c'est-à-dire que r' et s soient pairs, ce qui donne les racines

$$\pm\sqrt{k}, \quad \pm\frac{1}{\sqrt{k}},$$

ou que r et s' soient pairs, ce qui donne

$$\pm\frac{1\pm\sqrt{k}}{1\mp\sqrt{k}}.$$

Il y a donc huit racines par classe; elles sont racines doubles, excepté pour $x = 0$. On ne rencontre pas de modules linéaires.

On est ainsi conduit aux deux formules suivantes :

Pour $n = 8h - 1$, on a

$$(64)\quad 4\left|F(n) + 2F(n-4^2) + 2F(n-8^2) + \ldots\right| = 2\Psi(n) - \Phi(n),$$

et pour $n = 8h + 3$

$$(65)\quad \left\{\begin{array}{l} 4\left[2F(n-2^2) + 2F(n-6^2) + 2F(n-10^2) + \ldots\right| \\ \qquad = 2\Psi(n) - \Phi(n). \end{array}\right.$$

26. Faisons $\sqrt{k_1} = -\frac{1}{\sqrt{k}}$. En substituant, on a une équation en $\sqrt{k}$ du degré $2\Phi(n)$, qui n'est satisfaite ni par $\sqrt{k} = 0$, ni par $\sqrt{k} = \pm 1$. Mais, si $n = 4h + 1$, elle admet les racines $\sqrt{k} = \pm i$, et l'on voit comme précédemment que leur multiplicité est $\Phi(n) - \Psi(n)$; donc, en sup-

primant ces racines, on obtient, pour $n = 4h + 1$, une équation finale du degré $2\Psi(n)$.

En poursuivant l'analyse de la même manière qu'au numéro précédent, on est conduit aux trois équations suivantes :

Pour $n = 4h + 1$, on a

$$(66) \qquad 2[2F(n-1^2)+2F(n-3^2)+2F(n-5^2)+\ldots] = \Psi(n);$$

pour $n = 8h - 1$,

$$(67) \qquad 4[2F(n-2^2)+2F(n-6^2)+2F(n-10^2)+\ldots] = \Phi(n);$$

et, pour $n = 8h + 3$,

$$(68) \qquad 4[F(n)+2F(n-4^2)+2F(n-8^2)+\ldots] = \Phi(n).$$

De même, en faisant $\sqrt{k_1} = \frac{i}{\sqrt{k}}$, on trouve :

Pour $n = 4h + 1$,

$$(69) \qquad 2[F(n)+2F(n-2^2)+2F(n-4^2)+\ldots] = \Phi(n)+\psi(n);$$

et, pour $n = 4h - 1$,

$$(70) \qquad 2[2F(n-1^2)+2F(n-3^2)+2F(n-5^2)+\ldots] = \Phi(n).$$

Enfin, faisant dans l'équation modulaire

$$f(k, k_1) = 0,$$

qui a lieu entre k et k_1,

$$k_1 = \left(\frac{1+i\sqrt{k}}{1-i\sqrt{k}}\right)^2$$

et chassant le radical $\sqrt{k}$, on obtient une équation en k du degré $4\Phi(n)$, qui n'est satisfaite ni par $k = 0$, ni par $k = \pm 1$. En raisonnant sur cette équation, on ne rencontre que des multiplicateurs de la forme $\frac{1}{2}(x + i\sqrt{\Delta})$, et l'on obtient facilement

$$(71) \qquad F(4n-1^2)+F(4n-3^2)+F(4n-5^2)+\ldots = \Phi(n).$$

27. Des équations (63) à (70) on déduit les formules IV, V, VI de M. Kronecker. En effet, les équations (64) à (70) donnent, pour toute valeur impaire de n,

$$(72)\quad \begin{cases} 2[F(n)+2F(n-1^2)+2F(n-2^2)+2F(n-3^2)+\dots] \\ \quad =\Phi(n)+\Psi(n)+\varphi(n), \end{cases}$$

$$(73)\quad \begin{cases} 2[F(n)-2F(n-1^2)+2F(n-2^2)-2F(n-3^2)+\dots] \\ \quad =(-1)^{\frac{n-1}{2}}[\Phi(n)-\Psi(n)]+\varphi(n), \end{cases}$$

c'est-à-dire les équations V et VI. Pour avoir l'équation IV, remarquons qu'au moyen de la formule $2F(\Delta)=F(4\Delta)+1$, où le dernier terme doit être omis si Δ n'est pas un carré impair, on trouve

$$24\sum F\left[\frac{n-(2\xi+1)^2}{4}\right] = 12\sum F[n-(2\xi+1)^2]+6\varphi(n)-6\varphi'(n);$$

donc, en vertu de l'équation (66), on a, pour $n=4h+1$,

$$24\sum F\left[\frac{n-(2\xi+1)^2}{4}\right] = 3\Psi(n)+6\varphi(n)-6\varphi'(n)$$

et, en ajoutant cette équation à (63),

$$24\sum G\left[\frac{n-(2\xi+1)^2}{4}\right] = 6\Psi(n)-2\Phi(n)+6\varphi(n)+8\psi(n)-[6].$$

Or l'équation (72) peut s'écrire de la manière suivante

$$\begin{aligned} &2[G(n)+2G(n-1^2)+2G(n-2^2)+2G(n-3^2)+\dots] \\ &\quad -4\sum G\frac{n-(2\xi+1)^2}{4} \\ &\quad =\Phi(n)+\Psi(n)+\varphi(n); \end{aligned}$$

donc enfin

$$\begin{aligned} &3[G(n)+2G(n-1^2)+2G(n-2^2)+2G(n-3^2)+\dots] \\ &\quad =\Phi(n)+3\Psi(n)+3\varphi(n)+2\psi(n)-\left[\tfrac{3}{2}\right]; \end{aligned}$$

c'est là l'équation IV démontrée pour $n=4h+1$ (¹). Pour $n=h-1$, on la tire des formules (64), (65), (67), (68), (70), en y exprimant $F(\Delta)$ par $G(\Delta)$.

28. Pour avoir des formules dans lesquelles le nombre impair n est remplacé par $2n$, partons toujours de la transformation du degré n

$$\begin{aligned}\varepsilon_1 2\omega &= n'.2\omega_0,\\ \varepsilon_1\omega' &= -t.2\omega_0+n''\omega_0',\end{aligned}$$

qui donne l'équation modulaire

$$f(k,k_0)=0,$$

et faisons-y

$$\begin{aligned}\varepsilon'.2\omega_0 &= 2\omega_1', & \varepsilon''.2\omega_1 &= \rho.2\omega+4\sigma\omega',\\ \varepsilon'\omega_0' &= -2\omega_1, & \varepsilon''\omega_1' &= 2\rho'.2\omega+\sigma'\omega'.\end{aligned}$$

$$\rho\sigma'-8\rho'\sigma=1,$$

ou bien

$$(74)\qquad \begin{cases}\varepsilon'\varepsilon''.2\omega_0 = 4\rho'.2\omega+2\sigma'\omega',\\ \varepsilon'\varepsilon''\ \omega_0' = -\rho.2\omega-4\sigma\omega',\end{cases}$$

ce qui donne

$$k=\frac{1-k_0}{1+k_0},\qquad k_0=\frac{1-k}{1+k}.$$

Évidemment l'équation en k est du degré $2\Phi(n)$; elle a pour racines les modules qui admettent une multiplication de la forme suivante :

$$(75)\qquad \begin{cases}\varepsilon.2\omega = 4\rho'n'.2\omega+2\sigma'n'\omega',\\ \varepsilon\ \ \omega' = -(4\rho't+\rho'n'').2\omega-(2\sigma't+4\sigma n'')\omega'.\end{cases}$$

En raisonnant sur cette équation comme dans les nos **25** et **26**, on trouve facilement

$$F(2n)+2F(2n-2^2)+2F(2n-4^2)+\ldots=\Phi(n).$$

(¹) Dans le Mémoire de M. Kronecker le dernier terme $-[\frac{3}{4}]$ a été omis.

De même, en écrivant, dans les équations (74), (75), $4\sigma+2$ au lieu de 4σ, c'est-à-dire, en faisant

$$k=\frac{1+k_0}{1-k_0}, \qquad k_0=-\frac{1-k}{1+k},$$

on obtient

$$2F(2n-1^2)+2F(2n-3^2)+2F(2n-5^2)+\ldots=2\Phi(n)+\varphi(n).$$

En ajoutant et soustrayant membre à membre les équations trouvées, on a, pour toute valeur impaire de n,

$$(76)\quad \begin{cases} F(2n)+2F(2n-1^2)+2F(2n-2^2)+2F(2n-3^2)+\ldots \\ \quad =2\Phi(n)+\varphi(n), \end{cases}$$

$$F(2n)-2F(2n-1^2)+2F(2n-2^2)-2F(2n-3^2)+\ldots=-\varphi(n).$$

c'est-à-dire les équations II et III de M. Kronecker.

29. Des équations (71) et (72) on tire aisément la suivante

$$(77)\quad \begin{cases} F(4n)+2F(4n-1^2)+2F(4n-2^2)+2F(4n-3^2)+\ldots \\ \quad =3\Phi(n)+\Psi(n), \end{cases}$$

qui est un cas spécial de la formule I de Kronecker. Mais, pour la démontrer généralement, il nous faut une nouvelle équation, que nous tirerons de la considération d'une transformation de degré pair, appartenant au second cas (*voir* n° **15**). En conservant la lettre n pour désigner un nombre impair, nous dénotons le degré de la transformation par $m=2^\pi n$; en faisant comme précédemment $n=n'n''$, la transformation dont il s'agit est définie par les relations

$$\varepsilon_0 2\omega = n'.2\omega_0,$$
$$\varepsilon_0\ \omega'=-l.2\omega_0+2^\pi n''\omega_0'.$$

L'équation modulaire correspondante

$$(78)\qquad f(k^2,k_0^2)=0$$

est le produit de plusieurs équations modulaires, principales et irréductibles, du cas II, dont les degrés sont des facteurs de m de la forme $2^{\pi}(2h+1)$. De ce qui est dit au n° **15** nous pouvons conclure que notre équation est du degré $2^{\pi}\Phi(n)$ en k^2, aussi bien qu'en k_0^2, et que les plus hautes puissances de k^2 et de k_0^2 se trouvent multipliées ensemble. Donc, en faisant $k_0^2 = k^2$, on obtient une équation en k^2 du degré $2^{\pi+1}\Phi(n)$. Comme le fait voir la relation $\zeta_0 = \frac{t + n'\zeta}{n''2^{\pi}}$, cette équation a la racine $k^2 = 0$.

Pour en trouver la multiplicité, il suffit de remarquer que, pour les infiniment petites valeurs de k^2, l'équation peut être écrite

$$\Pi\left[(k_0^2)^{2^{\pi}n''} - A(k^2)^{n''}\right] = 0,$$

où n doit être égalé successivement à tous les diviseurs de n. Il en résulte, en effet, qu'on trouve la multiplicité de la racine zéro en décomposant le nombre m de toutes les manières possibles en deux facteurs dont l'un est impair, et faisant la somme de ceux qui sont moindres que $\sqrt{m}$. Nous désignerons cette somme par $S(m)$. Enfin, puisque l'équation (78) peut aussi être écrite $f(k_0', k'^2) = 0$ (**15**), on voit que l'équation $f(k^2, k^2) = 0$ admet la racine $k^2 = 1$ avec la multiplicité $S(m)$. Donc, en supprimant les racines 0 et 1, on a une équation finale du degré

$$2^{\pi+1}\Phi(n) - 2S(m).$$

En égalant ce degré au nombre des racines de l'équation, on trouve facilement la formule suivante :

$$(79)\qquad \begin{cases} F(4m-1^2) + F(4m-3^2) + F(4m-5^2) + \dots \\ \qquad = 2^{\pi}\Phi(n) - S(m). \end{cases}$$

Faisant $m = 2n$, l'équation (76) donne

$$F(4m) + 2F(4m-2^2) + 2F(4m-4^2) + \dots = 4\Phi(n);$$

donc, ayant, pour $m = 2n$,

$$2S(m) = \Phi(m) - \Psi(m) = 3\Phi(n) - \Psi(m);$$

on trouve

$$(80)\quad \begin{cases} F(4m) + 2F(4m-1^2) + 2F(4m-2^2) + \dots \\ \quad = 5\Phi(n) + \Psi(m) = \Phi(m) + \Psi(m) + 2\Phi(n); \end{cases}$$

cette équation a aussi lieu pour $\pi = 0$, $m = n$, puisque dans ce cas elle rentre dans (77). Par là la formule (I) de M. Kronecker est démontrée pour $\pi = 0$ et $\pi = 1$. Pour achever la démonstration, il suffit maintenant de faire voir qu'elle subsiste pour le nombre $4m$, si elle subsiste pour le nombre m. En multipliant l'équation (80) par 2, on obtient

$$\begin{aligned} &F(16m) + 2F(16m-2^2) + 2F(16m-4^2) + \dots \\ &\quad = 2\Phi(m) + 2\Psi(m) + 4\Phi(n); \end{aligned}$$

de plus l'équation (79) donne

$$\begin{aligned} &2F(16m-1^2) + 2F(16m-3^2) + 2F(16m-5^2) + \dots \\ &\quad = 2^{\pi+3}\Phi(n) - 2S(4m), \end{aligned}$$

donc

$$(81)\quad \begin{cases} F(16m) + 2F(16m-1^2) + 2F(16m-2^2) + \dots \\ \quad = (2^{\pi+3}+4)\Phi(n) + 2\Phi(m) + 2\Psi(m) - 2S(4m). \end{cases}$$

Or, si l'on désigne pour un moment par $T(m)$ la somme des facteurs de m qui sont moindres que $\sqrt{m}$, on a

$$T(4m) = 2T(m) + S(4m);$$

donc

$$\begin{aligned} 2S(4m) &= 2T(4m) - 4T(m) \\ &= \Phi(4m) - \Psi(4m) - 2\Phi(m) + 2\Psi(m). \end{aligned}$$

En substituant cette expression de $S(4m)$ dans le second membre de l'équation (81), il devient

$$(2^{\pi+3}+4)\Phi(n) - \Phi(4m) + \Psi(4m) + 4\Phi(m)$$

ou bien, en vertu de la relation $\Phi(m) = (2^{\pi+1} - 1)\Phi(n)$,

$$\Phi(4m) + \Psi(4m) + 2\Phi(n),$$

ce qui achève la démonstration de l'équation (80).

V. — L'ÉQUATION DE LA DIVISION DES PÉRIODES; L'ÉQUATION MODULAIRE.

30. Soit k un module singulier du déterminant $-D$, défini par l'équation

$$a\zeta^2 + 2b\zeta + c = 0,$$

le plus grand commun diviseur des nombres a, $2b$, c étant 1 ou 2 suivant l'espèce du module, et soit pour abréger $\varepsilon = i\sqrt{D}$. Supposons de plus que k^2 satisfait à une équation algébrique

$$\Phi(k^2) = 0,$$

du nombre de celles que nous avons déduites dans le § III, n^{os} **10**, **11**, **13**, **14**, **16-19**. Regardons k^2 comme une quantité connue; soit p un nombre impair, et considérons l'équation du degré $p^2 - 1$

$$F(z) = 0,$$

dont les racines sont les quantités $\lambda\left(\frac{r.2\omega + s\omega'}{p}\right)$, et dont les coefficients sont, comme on le sait, des polynômes en k^2 à coefficients entiers.

Si l'on désigne par Ω une période quelconque, on a (n^o **21**)

$$\lambda\left[\frac{(r+s\varepsilon)\Omega}{p}\right] = \frac{P}{Q + \mu\left(\frac{\Omega}{p}\right)\nu\left(\frac{\Omega}{p}\right)R},$$

P, Q, R étant des fonctions entières de $\lambda\left(\frac{\Omega}{p}\right)$, k^2 et de ε. Or on sait que $\mu\left(\frac{\Omega}{p}\right)\nu\left(\frac{\Omega}{p}\right)$ peut être exprimé en fonction rationnelle de $\lambda^2\left(\frac{\Omega}{p}\right)$ et de k^2 : donc on peut déduire de l'équation précédente une relation

de la forme

$$\lambda\left[\frac{(r+s\varepsilon)\Omega}{p}\right] = f\left[\lambda\left(\frac{\Omega}{p}\right)\right], \tag{82}$$

f dénotant une fonction rationnelle dont les coefficients sont des polynômes en k^2 et en ε à coefficients entiers. Il importe de remarquer que l'expression $f\left[\lambda\left(\frac{\Omega}{p}\right)\right]$ est identiquement la même pour toutes les périodes et pour tous les modules qui satisfont à l'équation $\Phi(k^2) = 0$.

Au moyen des relations (82), il est facile de faire voir que l'équation $F(z) = 0$ est abélienne, au moins après l'adjonction de ε. En faisant

$$\varpi = m.2\omega + m'\omega',$$

d'où

$$\varepsilon\varpi = (mb - m'c)2\omega + (ma - m'b)\omega',$$

on voit aisément que l'aire du parallélogramme $(\varpi, \varepsilon\varpi)$ est égale à celle du parallélogramme $(2\omega, \omega')$ multiplié par $(am^2 - 2bmm' + cm'^2)$. Or, si la classe de formes quadratiques, à laquelle correspond le module, contient la forme $x^2 + y^2 D$, on peut faire $am^2 - 2bmm' + cm'^2 = 1$; par cela le parallélogramme $(\varpi, \varepsilon\varpi)$ devient élémentaire, et, par suite, toutes les périodes sont contenues dans l'expression $(r + s\varepsilon)\varpi$. Pour les autres modules, cela n'est pas possible; mais dans tous les cas on peut rendre $am^2 - 2bmm' + cm'^2$ premier à p. La période ϖ étant choisie de cette manière, on démontre facilement que l'égalité

$$\lambda\left[\frac{(r+s\varepsilon)\varpi}{p}\right] = \lambda\left[\frac{(r'+s'\varepsilon)\varpi}{p}\right]$$

exige qu'on ait

$$r \equiv r', \qquad s \equiv s' \pmod{p},$$

et que, par conséquent, toutes les racines de l'équation $F(z) = 0$ sont contenues dans l'expression $\lambda\left[\frac{(r+s\varepsilon)\varpi}{p}\right]$. Or, en remplaçant, dans les équations

$$\lambda\left[\frac{(r+s\varepsilon)\varpi}{p}\right] = f\left[\lambda\left(\frac{\varpi}{p}\right)\right], \qquad \lambda\left[\frac{(r'+s'\varepsilon)\varpi}{p}\right] = f_1\left[\lambda\left(\frac{\varpi}{p}\right)\right],$$

ϖ respectivement par $(r'+s'\varepsilon)\varpi$, $(r+s\varepsilon)\varpi$, on trouve

$$\lambda\left[\frac{(r+s\varepsilon)(r'+s'\varepsilon)\varpi}{p}\right]=f\left\{f_1\left[\lambda\left(\frac{\varpi}{p}\right)\right]\right\}=f_1\left\{f\left[\lambda\left(\frac{\varpi}{p}\right)\right]\right\},$$

ce qui fait voir que l'équation $F(z)=0$ est abélienne, si ε est une quantité connue, ou si elle a été adjointe à l'équation. Dans les cas de la première catégorie d'un déterminant de la forme $-(4h-1)$, ε s'exprime rationnellement en k^2; dans les autres cas, l'adjonction de ε peut être remplacée par celle de i (n° 22). Mais, comme nous l'avons déjà dit, l'introduction de ε dans le second membre de l'égalité (82) a eu pour effet de rendre les mêmes formules applicables à tous les modules qui satisfont à l'équation $\Phi(k^2)=0$. Cela n'a pas d'importance quand il s'agit seulement de la résolution de l'équation $F(z)=0$; mais c'est un point essentiel pour les applications que nous avons à faire des propriétés de cette équation.

D'ailleurs les modules de la seconde espèce peuvent être traités, ici et plus bas, d'une manière spéciale, en faisant usage des multiplicateurs de la forme $\frac{1+i\sqrt{D}}{2}$; mais, puisque cela n'exige que des modifications légères, il suffit de l'avoir indiqué.

31. En étudiant de plus près la résolution de l'équation de division des périodes, nous nous bornerons au cas où p est un nombre premier impair; la résolution étant connue pour ce cas, on en tire celle des équations plus générales par la théorie de la division de l'argument et le théorème d'addition. On sait que, pour les modules indéterminés, le groupe de l'équation proposée est le groupe linéaire du degré p^2-1, et qu'en adjoignant à l'équation les racines $p^{\text{ièmes}}$ de l'unité, il se réduit au groupe de monodromie, qui contient les substitutions linéaires dont les déterminants sont congrus à l'unité suivant le module p (¹).

(¹) Voyez le *Traité des substitutions* de M. JORDAN, n° 476. Dans une Note insérée aux *Comptes rendus de la Société des Sciences de Christiania*, année 1871, j'ai démontré que le groupe algébrique contient toutes les substitutions linéaires, et qu'il se réduit au groupe de monodromie par l'adjonction de $e^{\frac{2\pi i}{p}}$. M. KRONECKER a donné une autre démonstration dans les *Monatsberichte de l'Académie de Berlin*, année 1875. M. H. WEBER y en a joint une troisième dans son travail sur la multiplication complexe (*Acta mathematica*, t. VI).

Par conséquent, si k est un module singulier, le groupe de l'équation $F(z) = 0$ est contenu dans le groupe linéaire, et si l'on adjoint la quantité $e^{\frac{2\pi i}{p}}$, il est contenu dans le groupe des substitutions linéaires dont les déterminants sont congrus à 1 (mod p). On sait de plus que pour les modules de la première catégorie dont le déterminant est de la forme $-(4h-1)$ le groupe ne peut contenir que des substitutions compatibles avec les relations (82); la même chose a lieu pour les autres modules, quand on adjoint à l'équation l'irrationnelle $i\sqrt{D}$. En faisant

$$z_{x,y} = \lambda\left(\frac{x.2\omega + y\omega'}{p}\right),$$

on a la relation

$$\lambda\left(\varepsilon\,\frac{x.2\omega + y\omega'}{p}\right) = f\left[\lambda\left(\frac{x.2\omega + y\omega'}{p}\right)\right]$$

ou bien

$$z_{bx-cy,\,ax-by} = f(z_{x,y}).$$

Soit

$$S = \left| \begin{matrix} x, y \end{matrix} \quad \begin{matrix} rx + sy,\ r'x + s'y \end{matrix} \right|$$

une substitution du groupe; on a, en exprimant qu'elle laisse subsister la relation ci-dessus

$$(83) \qquad \left\{ \begin{array}{l} r(bx - cy) + s(ax - by) \\ \quad \equiv b(rx + sy) - c(r'x + s'y), \\ r'(bx - cy) + s'(ax - by) \\ \quad \equiv a(rx + sy) - b(r'x + s'y) \end{array} \right\} \pmod{p},$$

congruences qui doivent être vérifiées pour toute combinaison de valeurs de x et de y, et qui expriment en même temps que S est échangeable à la substitution

$$\left| \begin{matrix} x, y \end{matrix} \quad \begin{matrix} bx - cy,\ ax - by \end{matrix} \right|,$$

si d'ailleurs ce symbole désigne réellement une substitution. On en tire

$$(84) \qquad \frac{r'}{a} \equiv \frac{r - s'}{2b} \equiv -\frac{s}{c} \pmod{p}.$$

De même les conditions à remplir pour que S soit échangeable à la substitution

$$| \ x, y \quad r_1 x + s_1 y, r'_1 x + s'_1 y \ |$$

sont les suivantes

$$\frac{r'}{r'_1} \equiv \frac{r - s'}{r_1 - s'_1} \equiv \frac{s}{s_1} \pmod p.$$

Il s'ensuit que les substitutions définies par les congruences (84) sont échangeables entre elles; elles forment évidemment un groupe, que nous désignerons par G. De ce qui précède on conclut que, pour les modules de la première catégorie dont le déterminant est de la forme $-(4h-1)$, le groupe de l'équation $F(z) = 0$ est contenu dans le groupe G, et que, pour les autres modules, cela a aussi lieu, pourvu qu'on adjoigne à l'équation la quantité ε. Pour trouver quel peut être, pour ces derniers modules, le groupe avant l'adjonction de ε, considérons la relation

$$\lambda^2\left(\varepsilon \frac{x.2\omega + y\omega'}{p}\right) = f_1\left[\lambda^2\left(\frac{x.2\omega + y\omega'}{p}\right)\right],$$

qu'on obtient de la précédente en l'élevant au carré, et dans laquelle ε n'entre pas [n° **21**, équation (57)]. On voit immédiatement que les substitutions du groupe vérifient ou les congruences (84) ou celles qu'on en déduit en changeant le signe des seconds membres; on trouve ainsi les substitutions de G et celles de la forme suivante

$$T = | \ x, y \quad rx + sy, r'x - ry \ |,$$

r, r', s satisfaisant à la congruence

$$as + 2br - cr' \equiv 0 \pmod p.$$

Ces substitutions forment un groupe H, contenant G, et l'on sait que, pour les modules en question, le groupe de l'équation $F(z) = 0$, sans adjonction préalable, est contenu dans H. Enfin nous désignons par Γ le groupe contenant celles des substitutions de G dont les déterminants sont congrus à $1 \pmod p$.

Dans ce qui précède on peut remplacer les périodes 2ω et ω' par la période ϖ, définie au numéro précédent, et $\varpi' = \varepsilon\varpi$, pourvu qu'on remplace les nombres a, b, c respectivement par 1, 0, $-D$; par là on obtient pour S la forme suivante

$$S = | \ x, y \quad rx - r'Dy, r'x + ry \ |,$$

et l'on trouve qu'elle remplace $\lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right]$ par $\lambda\left[\frac{(r+r'\varepsilon)(x+y\varepsilon)\varpi}{p}\right]$. La substitution T devient

$$T = | \ x, y \quad rx + r'Dy, r'x - ry \ |;$$

elle remplace $\lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right]$ par $\lambda\left[\frac{(r+r'\varepsilon)(x-y\varepsilon)\varpi}{p}\right]$. Parmi les substitutions de H se trouve la suivante

$$T_0 = | \ x, y \quad x, -y \ |,$$

et l'on a

$$T = T_0 S,$$

$$\begin{aligned} T_0^{-1} S T_0 &= | \ x, y \quad rx + r'Dy, -r'x + ry \ | \\ &= S^{-1} | \ x, y \quad (r^2 + r'^2 D)x, (r^2 + r'^2 D)y \ |; \end{aligned}$$

on en conclut que les substitutions de H sont permutables à G, et que son ordre est le double de celui de G, comme cela doit être, si le groupe de l'équation $F(z) = 0$ se confond effectivement avec H (*voir* le Traité de M. Jordan, nos 376, 378).

L'ordre du groupe G est différent, suivant que $-D$ est résidu quadratique de p, divisible par p, ou non-résidu quadratique de p; on le trouve égal à $(p-1)^2$ dans le premier cas, à $p^2 - p$ dans le deuxième, et à $p^2 - 1$ dans le troisième. Examinons séparément ces trois cas.

A. Supposons que $-D$ soit résidu quadratique de p et faisons

$$\rho^2 + D = pq.$$

On a

$$z_{x,y} = \lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right] = \lambda\left[\frac{q(x+y\varepsilon)\varpi}{\rho^2+D}\right],$$

et l'on remarque les deux systèmes contenant chacun $p-1$ racines d'une forme spéciale

$$\lambda\left(\frac{tq\varpi}{\rho-\varepsilon}\right) \quad \text{et} \quad \lambda\left(\frac{tq\varpi}{\rho+\varepsilon}\right),$$

où $t = 1, 2, \ldots, (p-1)$.

Par les substitutions de G les racines de chacun de ces systèmes s'échangent entre elles; en effet, on a

$$\lambda\left[\frac{tq(r+r'\varepsilon)\varpi}{\rho\mp\varepsilon}\right] = \lambda\left[\frac{tq(r+r'\varepsilon)\varpi}{\rho\mp\varepsilon} \pm tqr'\varpi\right] = \lambda\left[\frac{tq(r\pm r'\rho)\varpi}{\rho\mp\varepsilon}\right].$$

Par la substitution T_0 les deux systèmes s'échangent entre eux. Donc l'équation $F(z) = 0$ est réductible et se partage en deux autres

$$F_1(z) = 0, \qquad F_2(z) = 0,$$

dont la première est du degré $2(p-1)$, la seconde du degré $(p-1)^2$. Quand le groupe est contenu dans G, soit originairement, soit par adjonction de ε, la première se partage de nouveau en deux équations du degré $p-1$,

$$F'_1(z) = 0, \qquad F''_1(z) = 0,$$

dont la première a pour racines les $\lambda\left(\frac{tq\varpi}{\rho-\varepsilon}\right)$, la seconde les $\lambda\left(\frac{tq\varpi}{\rho+\varepsilon}\right)$. En adjoignant à l'équation $F(z) = 0$ les deux quantités $\lambda\left(\frac{q\varpi}{\rho-\varepsilon}\right)$, $\lambda\left(\frac{q\varpi}{\rho+\varepsilon}\right)$, son groupe se réduit à la substitution identique; par conséquent les racines de l'équation $F(z) = 0$ s'expriment rationnellement par $\lambda\left(\frac{q\varpi}{\rho-\varepsilon}\right)$ et $\lambda\left(\frac{q\varpi}{\rho+\varepsilon}\right)$. Et, en effet, on peut faire

$$\lambda\left[\frac{q(x+y\varepsilon)\varpi}{\rho^2+D}\right] = \lambda\left(\frac{\xi q\varpi}{\rho-\varepsilon} + \frac{\eta q\varpi}{\rho+\varepsilon}\right),$$

et trouver ainsi l'expression en question. D'ailleurs c'est là une propriété générale de l'équation de la division des périodes. Les nombres ξ et η sont déterminés par les congruences

$$\xi \equiv \frac{x+y\rho}{2\rho}, \qquad \eta \equiv \frac{x-y\rho}{2\rho} \pmod{p};$$

si on les prend pour indices, les substitutions du groupe G se réduisent simultanément à leurs formes canoniques, car évidemment on a

$$S = | \ \xi, \eta \quad (r + r'\rho)\xi, (r - r'\rho)\eta \ |;$$

la substitution T_0 devient

$$T_0 = | \ \xi, \eta \quad \eta, \xi \ |.$$

Le calcul des polynômes $F'_1(z)$, $F''_1(z)$ peut être fait de la manière suivante. On voit aisément que les $p-1$ quantités $\lambda\left(\frac{tq\varpi}{\rho-\varepsilon}\right)$ sont les seules valeurs de $\lambda(0)$ qui satisfassent en même temps aux équations

$$\lambda[(\rho-\varepsilon)0] = 0, \qquad \frac{\lambda(p0)}{\lambda(0)} = 0.$$

On a

$$\lambda[(\rho-\varepsilon)0] = \frac{\psi[\lambda(0)]}{\psi_1[\lambda(0)] + \mu(0)\nu(0)\psi_2[(\lambda(0)]}, \tag{85}$$

ψ, ψ_1, ψ_2 dénotant des fonctions entières dont les coefficients sont rationnels en k^2 et ε; donc $\lambda[(\rho-\varepsilon)0]$ ne peut s'annuler que quand on a

$$\psi[\lambda(0)] = 0 \quad \text{ou} \quad \lambda(0) = \infty;$$

mais $\lambda(0) = \infty$ donne

$$\frac{\lambda(p0)}{\lambda(0)} = \frac{1}{p};$$

donc l'équation $\lambda[(\rho-\varepsilon)0] = 0$ peut être remplacée par $\psi[\lambda(0)] = 0$. Par conséquent on trouve $F'_1(z)$ en cherchant le plus grand commun diviseur des polynômes $\psi(z)$ et $F(z)$; en y changeant le signe de ε, on a $F''_1(z)$. On voit que les expressions qu'on trouve de cette manière sont applicables indistinctement à toutes les valeurs de k^2 qui satisfont à l'équation $\Phi(k^2) = 0$.

En adjoignant ε, si cela simplifie le groupe, et en outre les racines $p^{\text{ièmes}}$ de l'unité, le groupe se réduit à être contenu dans Γ, dont les substitutions, réduites à leurs formes canoniques, sont les suivantes

$$\left| \ \xi, \eta \qquad m\xi, \frac{1}{m}\eta \ \right|.$$

Par cette adjonction $F_1(z) = 0$, $F_1'(z) = 0$ ne se décomposent pas; mais $F_2(z) = 0$ est décomposée en $p-1$ équations du degré $p-1$. De plus, on voit que toutes les racines de l'équation $F(z) = 0$ s'expriment rationnellement en $\lambda\left(\frac{q\varpi}{\rho-\varepsilon}\right)$, k^2, $e^{\frac{2\pi i}{p}}$ et ε (si cette dernière quantité a dû être adjointe).

B. Supposons D divisible par p, et faisons

$$D = pq.$$

Les substitutions de G sont réduites à leurs formes canoniques par l'introduction des périodes ϖ et $\varepsilon\varpi$; on a, en effet,

$$S = | \; x, y \quad rx, ry + r'x \; |.$$

Les quantités $\lambda\left(\frac{y\varepsilon\varpi}{p}\right)$ s'échangent entre elles par les substitutions du groupe H; par conséquent, elles sont les racines d'une équation

$$F_1(z) = 0,$$

du degré $(p-1)$. On peut calculer $F_1(z)$ par la méthode indiquée dans le cas précédent; on n'a qu'à faire $\rho = 0$ dans la formule (85); car les $\lambda\left(\frac{y\varepsilon\varpi}{p}\right)$ sont les seules racines communes aux deux équations $\psi(z) = 0$ et $F(z) = 0$, et, par conséquent, $F_1(z)$ est le plus grand diviseur commun à $\psi(z)$ et à $F(z)$; évidemment ε n'y entre pas. En faisant

$$F(z) = F_1(z) F_2(z),$$

l'équation $F_2(z) = 0$ se décompose par l'adjonction de $\lambda\left(\frac{\varepsilon\varpi}{p}\right)$ en $p-1$ équations du degré p. Et, en effet, nous avons

$$\lambda\left(\frac{\varepsilon x\varpi}{p}\right) = f\left[\lambda\left(\frac{x\varpi}{p}\right)\right] = f\left\{\lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right]\right\},$$

y ayant les valeurs $0, 1, 2, \ldots, (p-1)$, de sorte que les p quantités $\lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right]$ sont racines de l'équation

$$f(z) - \lambda\left(\frac{\varepsilon x\varpi}{p}\right) = 0,$$

et il est facile de voir qu'elles sont les seules racines communes à cette équation et à l'équation $F(z) = 0$. On trouve donc, par le procédé du plus grand commun diviseur, une équation

$$\varphi\left[z, \lambda\left(\frac{\varepsilon x \varpi}{p}\right)\right] = 0,$$

dont les racines sont les p quantités $\lambda\left[\frac{(x + y\varepsilon)\varpi}{p}\right]$.

Adjoignons maintenant ε (si cela simplifie le groupe) et $e^{\frac{2\pi i}{p}}$; par cela le groupe est réduit à ne contenir que des substitutions de la forme

$$| x, y \quad x, y + r'x |.$$

On voit immédiatement que l'équation $F_1(z) = 0$ se trouve résolue, c'est-à-dire que les quantités $\lambda\left(\frac{y\varepsilon\varpi}{p}\right)$ s'expriment rationnellement en k^2, $e^{\frac{2\pi i}{p}}$ et ε (si, d'ailleurs, cette dernière quantité a dû être adjointe). Les équations $\varphi\left[z, \lambda\left(\frac{\varepsilon x \varpi}{p}\right)\right] = 0$ ne se décomposent pas; mais leurs coefficients sont rationnels en k^2, $e^{\frac{2\pi i}{p}}$ et ε.

C. Supposons enfin $-D$ non résidu quadratique de p. Dans ce cas, la congruence

$$\varepsilon^2 + D \equiv 0 \pmod{p}$$

étant irréductible, on peut distinguer les racines de l'équation proposée par un seul indice de la forme $x + y\varepsilon$, pris suivant le module p. Faisons donc

$$z_\xi = \lambda\left(\frac{\xi\varpi}{p}\right) = \lambda\left[\frac{(x + y\varepsilon)\varpi}{p}\right].$$

Les substitutions du groupe G prennent évidemment la forme

$$| \xi \quad M\xi |,$$

où

$$M = r + r'\varepsilon;$$

on aura, de plus,

$$T_0 = | \xi \quad \xi^p |,$$

de sorte que les substitutions du groupe H auront la forme

$$| \xi \quad M\xi^{p^\nu} |,$$

ν étant égal à 1 ou à 2. En adjoignant ε, dans les cas où cela simplifie le groupe, et, en outre, $e^{\frac{2\pi i}{p}}$, le groupe se réduit à être contenu dans Γ. Or, ayant $M = r + r'\varepsilon$, $M^p \equiv r - r'\varepsilon \pmod p$, on en conclut que

$$M^{p+1} \equiv r^2 + r'^2 D \equiv 1 \qquad (\mathrm{mod}\, p).$$

Donc, en désignant par j une racine primitive de la congruence $\xi^{p^2-1} \equiv 1 \pmod p$, les substitutions de Γ auront la forme

$$| \xi \quad j^{h(p-1)}\xi |,$$

où $h = 0, 1, 2, \ldots, p$; par conséquent, l'ordre de Γ est égal à $p+1$. Il s'ensuit que par l'adjonction de $e^{\frac{2\pi i}{p}}$ et de ε (si cela simplifie le groupe), l'équation $F(z) = 0$ se décompose en $p-1$ équations du degré $p+1$.

Dans tous les trois cas, une fonction rationnelle des quantités $\lambda\left[\frac{(x+y\varepsilon)\varpi}{p}\right]$, invariable par les substitutions du groupe G, s'exprime rationnellement en k^2 et en $i\sqrt{D}$ d'une manière identique pour toutes les valeurs de k^2, racines de l'équation $\Phi(k^2) = 0$. On le démontre facilement, en remarquant que la fonction s'exprime, pour tous ces modules, d'une manière identique, sous la forme

$$U = \varphi_1\left[\lambda\left(\frac{\varpi}{p}\right)\right] + i\sqrt{D}\,\varphi_2\left[\lambda\left(\frac{\varpi}{p}\right)\right],$$

et que, si une substitution de G change U en U_1, $\lambda\left(\frac{\varpi}{p}\right)$ en $\lambda\left(\frac{\varpi_1}{p}\right)$, on a

$$U_1 = \varphi_1\left[\lambda\left(\frac{\varpi_1}{p}\right)\right] + i\sqrt{D}\,\varphi_2\left[\lambda\left(\frac{\varpi_1}{p}\right)\right].$$

32. De ce qui précède on tire facilement des conséquences importantes relatives aux équations modulaires principales. Nous ne considérerons que les équations entre les carrés des modules.

Il est d'abord évident que, pour les modules singuliers, l'équation modulaire qui répond à une transformation d'un degré impair est abélienne, au moins après l'adjonction de ε.

Supposons que p soit un nombre premier impair. En désignant par k_u le module transformé qu'on obtient par la division en p parties égales de la période $x.2\omega + y\omega'$, $\frac{x}{y}$ étant congru à $u \pmod p$, on sait qu'*en général* le groupe de l'équation modulaire contient les substitutions de la forme

$$\left| u \quad \frac{ru+s}{r'u+s'} \right|;$$

on sait, de plus, que l'adjonction du radical $\sqrt{(-1)^{\frac{p-1}{2}}p}$ réduit le groupe à ne contenir que les substitutions dont les déterminants $rs' - r's$ sont résidus quadratiques de p. [Voir le *Traité des substitutions* de M. Jordan, n° 480 (1).] Pour les modules singuliers, les nombres r, s, r', s' ont évidemment les mêmes valeurs que dans le groupe de l'équation de la division des périodes sous les mêmes hypothèses relatives aux quantités adjointes. On obtient ainsi trois groupes H', G', I' correspondant aux groupes H, G, I du numéro précédent. Avec les indices relatifs aux périodes ϖ et $\varepsilon\varpi$, le groupe H' contient les substi-

(1) La démonstration de M. Jordan est fondée sur le théorème, dû à M. Hermite, que le discriminant de l'équation modulaire est égal à $(-1)^{\frac{p-1}{2}}p$ multiplié par le carré d'un polynôme en k^2 à coefficients entiers. Ce théorème est une conséquence de la réduction du groupe de l'équation de division des périodes par l'adjonction de $e^{\frac{2\pi i}{p}}$. En effet, d'après une remarque de M. Jordan (*Traité*, p. 343), le produit des différences des racines de l'équation modulaire est une fonction rationnelle des racines de l'équation de la division des périodes, invariable par toute substitution linéaire dont le déterminant est résidu quadratique et, par conséquent, invariable par le groupe de monodromie de l'équation modulaire. Donc le produit est fonction rationnelle de k^2, et, puisqu'il ne devient pas infini pour des valeurs finies de k^2, cette fonction est entière. Les coefficients sont évidemment rationnels en $e^{\frac{2\pi i}{p}}$, et, comme ils n'ont que deux valeurs, numériquement égales et de signes contraires, il est facile de voir qu'ils sont de la forme $a\sqrt{(-1)^{\frac{p-1}{2}}p}$, a étant un entier.

tutions

$$\left| u \quad \frac{ru \mp r'D}{r'u \pm r} \right|;$$

G′ contient celles qu'on obtient en prenant, dans l'expression ci-dessus, les signes supérieurs. Enfin Γ′ contient les substitutions de G′ dont le déterminant $r^2 + r'^2 D$ est un résidu quadratique; mais il faut remarquer que, en vertu du théorème de M. Jordan, cité plus haut, le groupe de l'équation modulaire se réduit d'être contenu dans G′ à être contenu dans Γ′, déjà par l'adjonction de $\sqrt{(-1)^{\frac{p-1}{2}} p}$.

Cela posé, considérons les trois cas du numéro précédent.

A. Soit $-D$ résidu quadratique de p. Nous désignerons par k_u le module transformé obtenu par la division de la période

$$[(\xi + \eta_1)\rho + (\xi - \eta_1)\varepsilon]\varpi,$$

$\frac{\xi}{\eta_1}$ étant congru à $u \pmod p$. On voit immédiatement que le groupe Π′ contient les substitutions

$$\left| u \quad \frac{r + r'\rho}{r - r'\rho} u \right|, \quad \left| u \quad \frac{1}{u} \right|.$$

Donc, $\frac{r + r'\rho}{r - r'\rho}$ pouvant avoir toutes les valeurs $(\bmod p)$, excepté ∞ et 0, le groupe Π′ consiste dans les $2(p-1)$ substitutions suivantes

$$\left| u \quad mu \right|, \quad \left| u \quad \frac{m}{u} \right|.$$

Il s'ensuit que l'équation modulaire est réductible, k_∞^2 et k_0^2 satisfaisant à une équation du second degré, les autres k_u^2 à une équation du degré $p-1$. Le groupe G′ contient seulement les substitutions

$$\left| u \quad mu \right|;$$

donc, quand le groupe de l'équation modulaire est contenu dans G′, k_∞^2 et k_0^2 sont rationnels. On peut faire le calcul des expressions de k_∞^2 et de k_0^2 en k^2 et ε, en les regardant respectivement comme fonctions symétriques des racines des équations $F_1'(z) = 0$, $F_1''(z) = 0$ du numéro

précédent. Enfin le groupe Γ' contient les substitutions $| u \quad m^2 u |$; on en conclut que, par l'adjonction de ε (si cela simplifie le groupe) et de $\sqrt{(-1)^{\frac{p-1}{2}} p}$, la seconde équation se partage en deux autres du degré $\frac{1}{2}(p-1)$.

B. Soit $D = p.q$; en désignant par k_u le module obtenu par la division de la période $(x + y\varepsilon)\varpi$, $\frac{y}{x}$ étant $\equiv u \pmod p$, le groupe G' contient les substitutions

$$| u \quad u + r' |,$$

le groupe H', en outre, les substitutions

$$| u \quad -u + r' |.$$

Ces substitutions ne déplaçant pas k_*^2, cette racine est rationnelle en k^2; on peut calculer son expression de la même manière que dans le cas A. Les autres racines satisfont à une équation du degré p, qui est abélienne dans le cas du groupe G'. Γ' se confond avec G'.

C. Supposons enfin que $-D$ soit un résidu quadratique. Posons

$$\xi = x + y\varepsilon \equiv j^u \pmod p,$$

et désignons par k_u le module transformé correspondant à la division de la période $(x + y\varepsilon)\varpi$. Puisque j^{p+1} est congru à un nombre réel, on a $k^2_{u+p+1} = k^2_u$, de sorte que l'indice u doit être pris suivant le module $(p+1)$. Si, dans les k^2_u, considérés comme fonctions rationnelles de l'équation de division des périodes, on effectue la substitution

$$| \xi \quad j\xi |,$$

on a une substitution entre ces quantités qui a évidemment la forme

$$| u \quad u + 1 |.$$

De même la substitution T_0 produit entre les k^2_u la substitution $| u \quad -u |$. Donc le groupe H' contient les $2(p+1)$ substitutions $| u \quad \pm u + h |$, le groupe G' les $| u \quad u + h |$, et enfin les substitutions de Γ' seront les $| u \quad u + h(p-1) |$ ou bien les $| u \quad u + 2h |$. Donc, par l'adjonction

de ε (s'il y a lieu) et de $\sqrt{(-1)^{\frac{p-1}{2}}p}$, l'équation modulaire se décompose en deux équations abéliennes du degré $\frac{1}{2}(p+1)$.

Évidemment une fonction rationnelle des k_u^2, invariable par les substitutions de G', s'exprime en k^2 et en $i\sqrt{D}$ d'une manière identique pour tous les modules qui satisfont à l'équation $\Phi(k^2)=0$.

Parmi ces résultats, ceux qui concernent les racines rationnelles de l'équation modulaire sont les plus importants. Ils se résument par la proposition suivante :

Si l'on fait subir à un module singulier k^2 du déterminant $-D$, racine de l'équation $\Phi(k^2)=0$, une transformation principale du degré premier impair p, $-D$ étant résidu quadratique de p, deux racines de l'équation modulaire s'expriment rationnellement en k^2, pourvu que D soit de la forme $4h-1$ et que k appartienne à la première catégorie; si D est pair ou de la forme $4h+1$, ou que k appartienne à la seconde catégorie, deux racines s'expriment rationnellement en k^2 et en $i\sqrt{D}$. Si le degré divise D, une racine s'exprime rationnellement en k^2. On peut donner aux expressions des racines rationnelles de l'équation modulaire une telle forme qu'elles sont applicables indistinctement à tous les modules satisfaisant à l'équation $\Phi(k^2)=0$; il suffit, pour cela, que, dans les cas où $-D$ est résidu quadratique de p et de la forme $(4h-1)$ et où k appartient à la première catégorie, on laisse subsister, dans les expressions, l'irrationnelle $i\sqrt{D}$.

Cherchons quelles sont, dans le système primitif d'indices, ces racines rationnelles de l'équation modulaire. En exprimant que la substitution

$$\left|\begin{array}{cc} u & \frac{ru+s}{r'u+s'} \end{array}\right|$$

ne déplace pas k_u^2, on a la condition

$$r'u^2-(r-s')u-s\equiv 0 \pmod p$$

ou bien, en vertu des relations (84),

$$au^2-2bu+c\equiv 0;$$

d'où

$$u \equiv \frac{\pm\rho + b}{a} \equiv \frac{c}{\mp\rho + b} \pmod{p}, \tag{86}$$

formule qui, pour $a \equiv 0$, peut être remplacée par

$$u \equiv \infty, \qquad u \equiv \frac{c}{2b}; \tag{87}$$

dans les cas où p divise D, les doubles valeurs coïncident.

VI. — Transformations des modules singuliers.

33. En transformant un module singulier du déterminant $-\mathrm{D}$, on obtient toujours un autre module singulier; ordinairement le déterminant du module transformé est égal à $-\mathrm{D}$ multiplié par le carré du degré de la transformation. En effet, si, dans l'équation

$$a\zeta^2 + 2b\zeta + c = 0,$$

on fait

$$\zeta = \frac{r' + s'\zeta_1}{r + s\zeta_1},$$

on obtient une nouvelle équation

$$a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0,$$

où

$$a_1c_1 - b_1^2 = (ac - b^2)(rs' - r's)^2.$$

Mais, dans des cas spéciaux, il arrive que les coefficients a_1, b_1, c_1 ont un diviseur commun, de sorte que, en désignant par $-\mathrm{D}_1$ le déterminant du module transformé, on ait $\mathrm{D}_1 < \mathrm{D}(rs' - r's)^2$, quelquefois même $\mathrm{D}_1 < \mathrm{D}$. Évidemment le rapport $\frac{\mathrm{D}_1}{\mathrm{D}}$ est toujours un carré parfait.

Considérons spécialement les transformations principales d'un degré premier impair p. Le module k_u s'obtient par la division de la période $\Omega = t.2\omega + \delta\omega'$ (n^{os} **8**, **9**), pourvu qu'on ait $\frac{t}{\delta} \equiv u \pmod{p}$; donc, en

désignant par ζ_u le rapport des périodes correspondant à k_u, on a généralement

$$\zeta = \frac{-t + n'\zeta_u}{\delta}, \qquad \zeta_u = \frac{\delta\zeta + t}{n'}.$$

Par conséquent, k_∞ répond aux valeurs $\delta = p$, $n' = 1$, $\zeta_\infty = p\zeta$. Les autres k_u répondent aux valeurs $\delta = 1$, $n' = p$, $t = u$. On a donc

$$\zeta = \frac{\zeta_\infty}{p} = p\zeta_u - u.$$

En substituant ces valeurs dans l'équation en ζ, on trouve

$$a\zeta_\infty^2 + 2bp\zeta_\infty + cp^2 = 0,$$
$$ap^2\zeta_u^2 + 2p(b - au)\zeta_u + au^2 - 2bu + c = 0.$$

Évidemment p est le seul nombre premier qui puisse diviser à la fois les trois coefficients de l'une ou de l'autre de ces équations. Si, dans la première, a est divisible par p, on a

$$\frac{a}{p}\zeta_\infty^2 + 2b\zeta_\infty + cp = 0,$$

et, par suite, k_∞ appartient, dans ce cas, généralement au déterminant $-$ D. De même, si, dans la seconde équation

$$au^2 - 2bu + c \equiv 0 \pmod{p},$$

on a

$$ap\zeta_u^2 + 2(b - au)\zeta_u + \frac{au^2 - 2bu + c}{p} = 0,$$

et k_u appartient généralement au déterminant $-$ D. Or cette congruence exige que $-$ D soit un résidu quadratique ou un multiple de p; en posant, comme plus haut,

$$\rho^2 + \mathrm{D} \equiv 0 \pmod{p},$$

elle donne

$$u \equiv \frac{\rho + b}{a}, \qquad \text{si } a \text{ est premier à } p,$$

$$u \equiv \frac{c}{2b}, \qquad \text{si } a \text{ est divisible par } p.$$

Donc, si $-D$ est résidu quadratique de p, il y a, parmi les $p+1$ modules transformés, deux qui appartiennent à un déterminant dont la valeur absolue est égale ou moindre que D; si D est multiple de p, il y en a un seul. On voit, de plus, que ces modules sont précisément les racines rationnelles de l'équation modulaire. Ordinairement, ils appartiennent au déterminant $-D$; mais, si a est divisible par p^2, b par p, k_{∞} appartient à $-\frac{D}{p^2}$; si $au^2-2bu+c$ est divisible par p^2, $b-au$ par p, $k_{\frac{b}{a}}$ appartient à $-\frac{D}{p^2}$. Or les égalités

$$D=ac-b^2=a(au^2-2bu+c)-(b-au)^2$$

font voir que ces conditions ne peuvent être remplies que quand D est divisible par p^2, et que, réciproquement, dans ce cas, l'unique racine rationnelle de l'équation modulaire appartient toujours au déterminant $-\frac{D}{p^2}$.

La notation k_u ayant l'inconvénient de dépendre des coefficients a, b, c qui peuvent avoir une infinité de valeurs différentes pour chaque valeur de k^2, nous adopterons, pour les racines rationnelles, une notation spéciale : p étant, comme ci-dessus, un nombre premier dont $-D$ est un résidu quadratique ou un multiple, ρ une racine déterminée de la congruence $\rho^2+D\equiv 0 \pmod p$, $k_{p,\rho}$ désignera, si a est premier à p, la racine rationnelle de l'équation modulaire du degré $p+1$ qui correspond à $u\equiv\frac{\rho+b}{a}\pmod p$; si a est divisible par p, on a $\rho=\pm b$; dans ce cas, $k_{p,-b}$ correspondra à $u\equiv\frac{c}{2b}$, $k_{p,+b}$ sera le module que nous avons désigné plus haut par k_{∞}. Nous poserons, de plus,

$$k_{p,\rho}^2=\varphi_{p,\rho}(k^2, i\sqrt{D}),$$

où $\varphi_{p,\rho}$, d'après ce qu'on a vu au n° **29**, désigne une fonction rationnelle à coefficients entiers; cette formule est, comme on se rappelle, applicable à toute valeur de k^2, racine de l'équation $\Phi(k^2)=0$; si l'on a $\rho\equiv 0$, elle ne contient pas effectivement $i\sqrt{D}$.

En désignant par ζ_1 un rapport de périodes correspondant au mo-

dule $k_{p,\rho}$ et supposant que p^2 ne divise pas D, on a, par conséquent,

$$a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0,$$

où

$$a_1c_1 - b_1^2 = \mathrm{D},$$

et, si p ne divise pas a,

$$(88)\qquad a_1 = ap, \qquad b_1 \equiv b \pmod{a}, \qquad b_1 \equiv -\rho \pmod{p};$$

ces déterminations ont encore lieu si p divise a et qu'on prenne $\rho = -b$; mais, en faisant $\rho \equiv b$, on a

$$(89)\qquad a_1 = \frac{a}{p}, \qquad b_1 = b.$$

Remarquons encore que $k_{p,\rho}$ est toujours de la même espèce et de la même catégorie que k; de plus, dans les cas où il y a deux équations en k^2 répondant au même déterminant, à la même espèce et à la même catégorie (n^{os} **16**, **18**), k et $k_{p,\rho}$ satisfont en même temps à la première ou à la seconde équation. Donc, si D n'est pas divisible par p^2, $k_{p,\rho}^2$ ou $\varphi_{p,\rho}(k^2, i\sqrt{\mathrm{D}})$ est racine de l'équation $\Phi(k^2) = 0$, résultat important pour la résolution de celle-ci.

54. On a vu que, si, dans l'équation modulaire

$$\Psi(k^2, k_0^2) = 0$$

du degré $p+1$, on fait k égal à un module singulier du déterminant $-\mathrm{D}$, les $p+1$ valeurs de k_0^2 seront, à quelques exceptions près, des carrés de modules singuliers du déterminant $-p^2\mathrm{D}$; démontrons maintenant qu'on obtient, de cette manière, tous les modules du déterminant $-p^2\mathrm{D}$.

Soit k_0 un de ces modules, et soit

$$(90)\qquad a_0\zeta_0^2 + 2b_0\zeta_0 + c_0 = 0$$

l'équation qui définit le rapport des périodes. Le coefficient a_0 est ou divisible par p^2 ou premier à p; dans le dernier cas, on peut substituer

à l'équation (90) une autre

$$a'_0\zeta_0'^2 + 2b'_0\zeta'_0 + c'_0 = 0,$$

donnant la même valeur de k_0^2, où a'_0 est divisible par p^2. En effet, en posant

$$\zeta_0 = \frac{r' + s'\zeta'_0}{r + 4s\zeta'_0}, \qquad \text{où} \qquad rs' - 4r's = 1,$$

on a

$$a'_0 = a_0 s'^2 + 8b_0 s's + 16c_0 s^2,$$

d'où

$$a_0 a'_0 = (a_0 s' + 4b_0 s)^2 + 16p^2 \mathrm{D} s^2;$$

or on peut choisir s et s', de manière à rendre $a_0 s' + 4b_0 s$ divisible par p, ce qui donne $a'_0 \equiv 0 \pmod{p^2}$. Nous pouvons donc, dans l'équation (90), supposer a_0 divisible par p^2 et, par suite, b divisible par p. Faisant maintenant $\zeta_0 = \frac{1}{p}\zeta$, on a

$$\frac{a_0}{p^2}\zeta^2 + 2\frac{b_0}{p}\zeta + c_0 = 0,$$

ce qui fait voir que k_0 se déduit du module k correspondant au rapport ζ et appartenant au déterminant $-\mathrm{D}$ par une transformation du degré p.

Les valeurs de k_0^2 sont des racines simples de l'équation modulaire. En effet, dans le cas contraire, k_0 se transformerait en lui-même par une transformation du degré p^2, laquelle ne serait pas une multiplication ordinaire; c'est ce qu'on démontre aisément par les relations entre les rapports des périodes; mais on verra que cela conduirait à l'équation impossible $p^2 = (2x+1)^2 + y^2 p^2 \mathrm{D}$, y étant différent de zéro. Il est également facile de voir que deux valeurs de k_0^2, déduites de valeurs différentes de k^2, ne sauront être égales; car, si cela avait lieu, on pourrait, par des transformations principales du degré p, déduire d'un seul module du déterminant $-p^2\mathrm{D}$ deux modules différents du déterminant $-\mathrm{D}$, ce qui est impossible.

Donc, en faisant, dans l'équation $\Psi(k^2, k_0^2) = 0$, k^2 successivement égal à toutes les racines de l'équation $\Phi(k^2) = 0$, débarrassant les

équations des racines qui appartiennent aux déterminants $-D$, $-\frac{D}{p^2}$, si $-D$ est résidu quadratique ou multiple de p, on obtiendra, par la résolution des équations résultantes, toutes les racines de l'équation $\Phi(k^2)=0$ relative au déterminant $-p^2D$, chaque module ne se présentant qu'une seule fois. Il s'ensuit que le nombre des modules appartenant au déterminant $-p^2D$ est $p-1$, p ou $p+1$ fois plus grand que le nombre des modules du déterminant $-D$, suivant que $-D$ est résidu quadratique, multiple ou non résidu de p.

En désignant par $F_1(D)$ le nombre de classes proprement primitives du déterminant $-D$, on en tire la relation connue

$$F_1(p^2D)=\left[p-\left(\frac{-D}{p}\right)\right]F_1(D),$$

où $\left(\frac{-D}{p}\right)$ est le symbole de Legendre, et où, pour $D=1$, le second membre doit être précédé du facteur $\frac{1}{2}$.

Soit maintenant k_0 un module de la première catégorie du déterminant $-4D$; alors, dans l'équation (90), a_0 est divisible par 4, b_0 est pair, c_0 impair. En faisant $\zeta_0=-\frac{1}{2\zeta}$, ce qui répond à la première transformation du degré 2, on obtient

$$c_0\zeta^2-2\left(\frac{b_0}{2}\right)\zeta+\frac{a_0}{4}=0,$$

équation qui définit un module de la première espèce et de la seconde catégorie du déterminant $-D$, et l'on a

$$k_0=\frac{1-k}{1+k}.$$

On voit qu'à chaque valeur de k^2 répondent deux valeurs de k_0^2, et que, pour deux valeurs différentes de k^2, on a des valeurs différentes de k_0^2, à moins que l'une des valeurs de k^2 ne soit la réciproque de l'autre. Donc, si, dans les deux équations en k (n^{os} **13**, **17**), on fait $k=\frac{1-k_0}{1+k_0}$, on obtient les deux équations en k_0^2 du n° **16**; il est, en effet, facile de voir que les puissances impaires de k_0 disparaissent. Cela revient d'ail-

leurs à faire, dans les équations en k de la première espèce et de la première catégorie, $k = \frac{1-k'_0}{1+k'_0}$, $k = \frac{k_0 - ik'_0}{k_0 + ik'_0}$.

Il est évident, d'après ce qui vient d'être dit, que le nombre des modules de la première catégorie du déterminant $-4D$ est égal au nombre des modules de la première espèce et de la seconde catégorie du déterminant $-D$ ou, ce qui revient au même, égal au double du nombre des modules de la première espèce et de la première catégorie.

On en tire l'équation

$$F_1(4D) = 2F_1(D), \tag{91}$$

où il faut omettre le facteur 2 du second membre si $D = 1$.

On voit encore que, par la même transformation, les modules de la première espèce et de la première catégorie d'un déterminant de la forme $-(4h-1)$ se déduisent de ceux de la seconde espèce et de la seconde catégorie, et *vice versa*. Par conséquent, on obtient l'équation en k^2 relative à la première espèce et à la première catégorie si, dans l'équation en k de la seconde espèce et de la seconde catégorie, on remplace k par $\frac{1-k}{1+k}$ et qu'on chasse les puissances impaires de k. Ainsi tous les modules du déterminant $-(4h-1)$ peuvent être trouvés au moyen de l'équation modulaire relative au degré h.

Soit, par exemple, $D = 11$; de l'équation de la seconde espèce, trouvée au n° **12**,

$$k^6 + 11ik^5 + 77k^4 - 152ik^3 - 77k^2 + 11ik + 1 = 0,$$

on déduit la suivante :

$$k^{12} - 3k^{10} + 134k^8 - 263k^6 + 134k^4 - 3k^2 + 1 = 0.$$

Pour $D = 15$, on tire de l'équation

$$k^2 - 6(1-i)k\sqrt{k} + 20ik + 6(1+i)\sqrt{k} - 1 = 0,$$

trouvée au n° **19**,

$$16k^4 - 28ik^3 - 33k^2 + 28ik + 16 = 0;$$

d'où

$$k^2 = -\tfrac{1}{256}(1+i\sqrt{3})^2(7+i\sqrt{15})^2.$$

On a évidemment la proposition suivante : Pour un déterminant de la forme $-(4h-1)$, le nombre des modules singuliers de la première espèce et de la première catégorie est égal au nombre de ceux de la seconde espèce et de la seconde catégorie. En désignant par $G_1(D)$ le nombre des classes primitives du déterminant $-D$, on peut conclure, en se rappelant ce qui a été dit du nombre des modules appartenant à chaque classe (n° 5), que, si $D = 8h-1$, on a

$$G_1(D) = 2F_1(D) \tag{92}$$

et, si $D = 8h+3$,

$$3G_1(D) = 4F_1(D), \tag{93}$$

formule qui, pour $D = 3$, doit être remplacée par $G_1(D) = 2F_1(D)$. Des relations (91), (92), (93) on obtient aisément les équations entre $G(4n)$, $F(4n)$, $G(n)$, $F(n)$ dont il a été parlé au n° **23**. On voit que les règles relatives au nombre des modules s'énoncent plus simplement que celles qui regardent le nombre des classes.

VII. — Résolution des équations des modules singuliers.

35. En nous occupant de la résolution des équations des modules singuliers, nous supposerons adjointe l'irrationnelle $i\sqrt{D}$. Sous cette hypothèse, on a le théorème suivant : *Le carré de tout module singulier s'exprime rationnellement par le carré de tout autre module appartenant au même déterminant, à la même espèce et à la même catégorie.*

Dans la démonstration, nous supposerons que, dans les équations de la forme $a\zeta^2 + 2b\zeta + c = 0$, définissant les modules singuliers, les coefficients a ne soient divisibles par aucun nombre premier impair dont le carré divise D. On sait, en effet, qu'on peut trouver une forme quadratique (a_1, b_1, c_1), équivalente à (a, b, c), telle que a_1 soit pre-

mier à un nombre donné quelconque, et il est facile de voir qu'on peut en même temps obtenir qu'elle réponde au même module que (a, b, c).

Cela posé, commençons la démonstration par le cas de la première espèce et de la seconde catégorie. Soit

$$a\zeta^2 + 2b\zeta + c = 0$$

l'équation du rapport des périodes appartenant au module k; soient, de plus, p un nombre premier divisant a, k_1 le module correspondant au rapport $\zeta_1 = p\zeta$; alors on a

$$\frac{a}{p}\zeta_1^2 + 2b\zeta_1 + cp = 0;$$

de plus, p^2 ne divisant pas D, k_1^2 appartient au déterminant $-$ D et s'exprime rationnellement par k^2. En désignant par p_1 un nombre premier divisant $\frac{a}{p}$, par k_2 le module appartenant au rapport $\zeta_2 = p_1\zeta_1$, on a de même

$$\frac{a}{pp_1}\zeta_2^2 + 2b\zeta_2 + cpp_1 = 0,$$

k_2^2 s'exprimant rationnellement en k_1^2 et, par suite, en k^2. En continuant ainsi, on finit par avoir l'équation

$$\zeta_n^2 + 2b\zeta_n + ac = 0$$

et le module k_n, et l'on sait exprimer k_n^2 rationnellement en k^2; d'ailleurs, cette équation peut être remplacée par la suivante

$$\zeta_n'^2 + \mathrm{D} = 0,$$

qui donne la même valeur de k_n^2. Soient maintenant k_m un module quelconque de la première espèce, de la seconde catégorie et du déterminant $-$ D, ζ_m le rapport de ses périodes, et soit

$$a_m\zeta_m^2 + 2b_m\zeta_m + c_m = 0;$$

on démontre, par une marche inverse, que k_m^2 s'exprime rationnellement en k_n^2 et, par suite, en k^2. En effet, faisant $\zeta_n' = \zeta_n'' + b_m$, ce qui

ne change pas k_n^2, on a

$$\zeta_n''^2 + 2b_m\zeta_n'' + a_m c_m = 0;$$

en désignant, de plus, par p', p_1', p_2', ... les facteurs premiers de a_m, faisant $\zeta_n'' = p'\zeta_{n+1}$, $\zeta_{n+1} = p_1'\zeta_{n+2}$, ..., on obtient une série d'équations

$$p'\zeta_{n+1}^2 + 2b_m\zeta_{n+1} + \frac{a_m c_m}{p'} = 0, \qquad p'p_1'\zeta_{n+2}^2 + 2b_m\zeta_{n+2} + \frac{a_m c_m}{p'p_1'} = 0, \qquad \ldots,$$

et la série des modules correspondants k_{n+1}, k_{n+2}, ... Or les derniers termes de ces séries sont l'équation

$$a_m\zeta_m^2 + 2b_m\zeta_m + c_m = 0$$

et le module k_m; de plus, le carré de chaque module s'exprimant en fonction rationnelle du carré du précédent, on obtient k_m^2 en fonction rationnelle de k^2.

Considérons ensuite les modules de la première espèce et de la première catégorie. On voit immédiatement que le coefficient a est impairement pair si D est de l'une des formes $4h+1$, $4h+2$, et que, pour $D = 8h+3$, on a $a \equiv 4 \pmod 8$. Pour $D = 8h+7$, on peut, comme on le démontre aisément, sans nuire à la généralité, supposer

$$a \equiv 8 \pmod{16};$$

ainsi ce cas se subdivise en deux autres : $D = 16h+7$ avec $b = 8h' \pm 1$ et $D = 16h+15$ avec $b = 8h' \pm 3$. Enfin, dans le cas où D est divisible par 4, les modules se partagent entre deux équations, suivant que $a \equiv 4$ ou $a \equiv 0 \pmod 8$; mais, puisque les racines de l'une de ces équations sont les réciproques de celles de l'autre, il suffit de considérer celle où $a \equiv 4$. Nous pouvons donc supposer que, en posant

$$a = 2^\pi(2l+1),$$

on ait

$\pi = 1$ si $D = 4h+1, 4h+2$,

$\pi = 2$ si $D = 8h+3, 4h$,

$\pi = 3$ si $D = 8h+7$.

Cela posé, considérons les divers cas. Soit d'abord $D = 4h + 1$; par le procédé employé plus haut, on déduit de l'équation

$$a\zeta^2 + 2b\zeta + c = 0,$$

correspondant au module k, l'équation

$$2\zeta_n^2 + 2\zeta_n + \frac{D+1}{2} = 0,$$

qui répond à un module k_n, k_n^2 étant rationnel en k^2. De ce module et de cette équation, on déduit le module k_m et l'équation

$$a_m\zeta_m^2 + 2b_m\zeta_m + c_m = 0,$$

k_m^2 étant fonction rationnelle de k_n^2 et, par suite, de k^2.

Si D est pair, les choses se passent de la même manière, avec la seule différence que l'équation $2\zeta_n^2 + 2\zeta_n + \frac{D+1}{2} = 0$ est remplacée par

$$2\zeta_n^2 + \frac{D}{2} = 0, \qquad \text{si } D \equiv 2 \pmod 4,$$

par

$$4\zeta_n^2 + \frac{D}{4} = 0, \qquad \text{si } D \equiv 4 \pmod 8$$

et par

$$4\zeta_n^2 + 4\zeta_n + \frac{D+4}{4} = 0, \qquad \text{si } D \equiv 0 \pmod 8.$$

Si $D = 8h + 3$, on obtient l'équation

$$4\zeta_n^2 \pm 2\zeta_n + \frac{D+1}{4} = 0;$$

si $D = 16h + 7$, on trouve

$$8\zeta_n^2 \pm 2\zeta_n + \frac{D+1}{8} = 0,$$

et, si $D = 16h + 15$,

$$8\zeta_n^2 \mp 6\zeta_n + \frac{D+9}{8} = 0,$$

où l'on doit prendre les signes supérieurs si $b \equiv 1$, les inférieurs si

$b \equiv -1 \pmod 4$. On voit par là que les carrés des modules k et k_m s'expriment rationnellement l'un par l'autre, si $b \equiv b_m \pmod 4$. Pour compléter la démonstration, il suffit de remarquer que les modules pour lesquels $b \equiv 1$ sont les réciproques de ceux pour lesquels $b \equiv -1$, ce qu'on vérifie par une transformation linéaire.

Examinons enfin les modules de la seconde espèce. Dans la seconde catégorie, a est impairement pair, b impair; par conséquent, la démonstration se fait comme pour les modules de la première espèce et de la première catégorie d'un déterminant de la forme $4h+1$. Dans la première catégorie, les modules se partagent entre deux équations, dont l'une correspond aux valeurs de a divisibles par 8, l'autre aux valeurs qui ne le sont pas; mais les racines de la seconde étant les réciproques de celles de la première, on peut se borner à celle-ci. De plus, c étant pair, b impair, on a

$$b = 8h' \pm 1, \qquad \text{si } D = 16h + 15;$$
$$b = 8h' \pm 3, \qquad \text{si } D = 16h + 7.$$

On obtient, dans le premier cas,

$$8\zeta_n^2 \pm 2\zeta_n + \frac{D+1}{8} = 0;$$

dans le second,

$$8\zeta_n^2 \pm 6\zeta_n + \frac{D+9}{8} = 0;$$

donc, comme plus haut, k^2 et k_m^2 s'expriment rationnellement l'un en l'autre, pourvu que $b \equiv b_m \pmod 4$. Or les modules pour lesquels $b \equiv -1$ sont les compléments de ceux pour lesquels $b \equiv +1$; pour le faire voir, il suffit d'employer la transformation $\zeta = -\frac{1}{4\zeta'}$, qui change le module en son complément, et l'équation $a\zeta^2 + 2b\zeta + c = 0$ en $4c\zeta'^2 - 2b\zeta' + \frac{a}{4} = 0$, où maintenant $4c$ est divisible par 8, $\frac{a}{4}$ par 2. Par suite, k_m^2 s'exprime rationnellement en k^2, même si

$$b_m \equiv -b \pmod 4.$$

Le théorème est donc démontré dans tous les cas.

36. Par l'adjonction de $i\sqrt{D}$, l'équation $\Phi(k^2) = 0$, qui détermine le carré du module singulier, est devenue abélienne. Il résulte de ce qui est dit au numéro précédent qu'on passe d'une racine à une autre en opérant sur la première plusieurs fois de suite avec les symboles $\varphi_{p,\rho}$, φ_{p_1,ρ_1}, ... du n° **33**, ou en prenant le module réciproque ou le complément du module ainsi obtenu. Pour démontrer le théorème ci-dessus, il suffit donc de faire voir : 1° que les symboles $\varphi_{p,\rho}$, φ_{p_1,ρ_1} sont échangeables, c'est-à-dire qu'on a

$$(k^2_{p,\rho})_{p_1,\rho_1} = (k^2_{p_1,\rho_1})_{p,\rho};$$

2° que

$$\left(\frac{1}{k^2}\right)_{p,\rho} = \frac{1}{k^2_{p,\rho}}, \qquad (1 - k^2)_{p,\rho} = 1 - k^2_{p,\rho}.$$

Remarquons d'abord, pour abréger la démonstration, que dans l'équation $a\zeta^2 + 2b\zeta + c = 0$, qui définit le module k, on peut supposer que a soit premier à pp_1. Cela posé, désignons par ζ', ζ_1, ζ'', ζ_2 les rapports des périodes appartenant respectivement à $k^2_{p,\rho}$, $k^2_{p_1,\rho_1}$, $(k^2_{p,\rho})_{p_1,\rho_1}$, $(k^2_{p_1,\rho_1})_{p,\rho}$, et soit

$$a'\zeta'^2 + 2b'\zeta' + c' = 0, \qquad a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0,$$
$$a''\zeta''^2 + 2b''\zeta'' + c'' = 0, \qquad a_2\zeta_2^2 + 2b_2\zeta_2 + c_2 = 0.$$

Or, si p et p_1 sont différents, on a, d'après les équations (88),

$$a'' = a_2 = app_1$$

et

$$b' \equiv b \pmod{a}, \qquad b' \equiv -\rho \pmod{p},$$
$$b'' \equiv b' \pmod{ap}, \qquad b'' \equiv -\rho_1 \pmod{p_1},$$

d'où

$$b'' \equiv b \pmod{a}, \qquad b'' \equiv -\rho \pmod{p}, \qquad b'' \equiv -\rho_1 \pmod{p_1};$$

de la même manière, on a

$$b_2 \equiv b \pmod{a}, \qquad b_2 \equiv -\rho \pmod{p}, \qquad b_2 \equiv -\rho_1 \pmod{p_1};$$

donc

$$b_2 = b'' + happ_1,$$

h étant un entier. En substituant, on trouve

$$app_1\zeta''^2 + 2b''\zeta'' + c'' = 0,$$
$$app_1\zeta_2^2 + 2(b'' + happ_1)\zeta_2 + c_2 = 0;$$

d'où l'on conclut, en se rappelant que les déterminants sont les mêmes,

$$\zeta_2 = \zeta'' - h,$$

ce qui donne

$$(k^2_{p,\rho})_{p_1,\rho_1} = (k^2_{p_1,\rho_1})_{p,\rho}.$$

Si $p = p_1$, il y a deux cas : on peut avoir $\rho_1 = \rho$, et dans ce cas l'échangeabilité est évidente. On peut aussi avoir $\rho_1 = -\rho$: alors on a, pour la première transformation, comme plus haut,

$$a' = ap, \qquad b' \equiv b \pmod{a}, \qquad b' \equiv -\rho \pmod{p};$$

mais, a' étant divisible par p, on doit, pour le passage de ζ' à ζ'', employer l'équation (89) : donc

$$a'' = a, \qquad b'' = b' \equiv b \pmod{a}.$$

Il s'ensuit $\zeta'' = \zeta + h$, h étant entier; donc

$$(k^2_{p,\rho})_{p,-\rho} = k^2. \tag{94}$$

L'échangeabilité est donc démontrée encore dans ce cas.

Démontrons maintenant l'égalité $\left(\frac{1}{k^2}\right)_{p,\rho} = \frac{1}{k^2_{p,\rho}}$. En désignant par ζ' la même chose que plus haut, on a (**35**)

$$\zeta = p\zeta' - u, \qquad \text{où} \qquad u \equiv \frac{b+\rho}{a} \pmod{p}.$$

La transformation linéaire $\begin{pmatrix} 1 & 2p \\ 0 & 1 \end{pmatrix}$ change k^2 en $\frac{1}{k^2}$; donc, en désignant par ζ_1 un rapport de périodes elliptiques appartenant à $\frac{1}{k^2}$, on a

$$\zeta = \frac{\zeta_1}{1 + 2p\zeta_1};$$

donc, en faisant

$$a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0,$$

on trouve

$$a_1 = a + 4bp + 4cp^2,$$
$$b_1 = b + 2cp.$$

Soit enfin ζ'_1 le rapport des périodes appartenant à $\left(\frac{1}{k^2}\right)_{p,\rho}$; on a

$$\zeta_1 = p\zeta'_1 - u_1, \qquad \text{où} \qquad u_1 \equiv \frac{b_1+\rho}{a_1} \equiv \frac{b+\rho}{a} \equiv u \pmod p.$$

En exprimant ζ' en ζ'_1, on trouve

$$\zeta' = \frac{\frac{u-u_1}{p} - 2uu_1 + (1+2pu)\zeta'_1}{1 - 2pu_1 + 2p^2\zeta'_1},$$

relation qui définit une transformation linéaire conduisant de $k^2_{p,\rho}$ à $\left(\frac{1}{k^2}\right)_{p,\rho}$; comme, de plus, on a

$$2p^2 \equiv 2 \pmod 4,$$

on conclut

$$\left(\frac{1}{k^2}\right)_{p,\rho} = \frac{1}{k^2_{p,\rho}}.$$

Démontrons enfin qu'on a, pour les modules de la seconde espèce et de la première catégorie,

$$(1-k^2)_{p,\rho} = 1 - k^2_{p,\rho}.$$

En conservant la signification des lettres ζ, ζ', u, soit

$$\zeta = -\frac{1}{4\zeta_1}, \qquad \text{d'où} \qquad 4c\zeta_1^2 - 2b\zeta_1 + \frac{a}{4} = 0,$$

de sorte que ζ_1 réponde à $1-k^2$, et soit ζ'_1 le rapport des périodes appartenant à $(1-k^2)_{p,\rho}$. Si maintenant c est premier à p, on a

$$\zeta_1 = p\zeta'_1 - u_1, \qquad \text{où} \qquad u_1 \equiv \frac{-b+\rho}{4c} \pmod p;$$

on en tire, en remarquant que $4uu_1 \equiv -1 \pmod p$,

$$\zeta' = \frac{\frac{1+4uu_1}{p} - 4u\zeta'_1}{4u_1 - 4p\zeta'_1}.$$

Or, cette équation définit une transformation du quatrième degré et du cas $Ia(\mathbf{15})$: donc on a

$$(1-k^2)_{p,\rho}=1-k_{p,\rho}^2.$$

Si c est divisible par p, on a

$$\rho \equiv \pm b.$$

Avec le signe supérieur, on a

$$u \equiv \frac{2b}{a}, \qquad u_1 \equiv -\frac{a}{8b};$$

donc $4uu_1 \equiv -1$, comme plus haut. Avec le signe inférieur, on a

$$u=0, \qquad \zeta = p\zeta', \qquad \zeta_1 = \frac{\zeta_1}{p},$$

et par conséquent $\zeta' = -\frac{1}{4\zeta_1}$, ce qui donne encore

$$(1-k^2)_{p,\rho}=1-k_{p,\rho}^2.$$

Ce n'est qu'en traitant les équations de la première catégorie d'un déterminant de la forme $-(4h+3)$ qu'il est nécessaire d'employer les fonctions $\frac{1}{k^2}$, $1-k^2$. Or, dans ce cas, l'équation $\Phi(k^2)=0$ se décompose par l'adjonction de $i\sqrt{\mathrm{D}}$ en deux autres $\Phi_1(k^2, i\sqrt{\mathrm{D}})=0$, $\Phi_1(k^2, -i\sqrt{\mathrm{D}})=0$; les fonctions $\frac{1}{k^2}$, $1-k^2$ servent à exprimer les racines de l'une de ces équations par celles de l'autre; les fonctions $\varphi_{p,\rho}$ suffisent pour exprimer les racines de chacune d'elles, les unes par les autres.

37. Désignons par $\mathrm{S}_{p,\rho}$ la substitution qu'on obtient en remplaçant chaque racine k_j^2 de l'équation $\Phi(k^2)=0$ par la racine $\varphi_{p,\rho}(k_j^2, i\sqrt{\mathrm{D}})$.

L'ensemble des substitutions renfermées dans l'expression

$$\mathrm{S}_{p,\rho}^{m}\cdot \mathrm{S}_{p_1,\rho_1}^{m_1}\cdot \mathrm{S}_{p_2,\rho_2}^{m_2}\cdots$$

forme évidemment un groupe G, dont l'ordre est égal au degré de l'équation, à moins qu'elle n'appartienne à la première catégorie et à un déterminant de la forme $-(4h+3)$; dans ce cas, l'ordre du groupe G

est égal à la moitié du degré de l'équation. Après l'adjonction de $i\sqrt{D}$, le groupe de l'équation est contenu dans G. En effet, posons

$$k_j^2 = \theta_j(k_0^2),$$

les fonctions rationnelles θ_j étant choisies parmi celles qu'on obtient par le procédé du n° **35**; si une substitution T du groupe de l'équation remplace k_0^2 par $\theta_p(k_0^2)$, elle remplacera k_j^2 par $\theta_j[\theta_p(k_0^2)]$ ou, ce qui est la même chose (**36**), par $\theta_p(k_j^2)$; par suite, la substitution T appartient au groupe G.

De l'équation (91) on tire

$$S_{p,\rho} = S_{p,-\rho}^{-1};$$

en supposant que p divise D, on a

$$\rho \equiv 0 \pmod{p},$$

donc

$$S_{p,0} = S_{p,0}^{-1}, \qquad S_{p,0}^2 = 1.$$

Cherchons l'ordre de $S_{p,\rho}$. En faisant subir au module k la substitution $S_{p,\rho}^m$, on obtient un module k_m qui, en supposant a premier à p, est défini par l'équation

$$ap^m\zeta_m^2 + 2b_m\zeta_m + c_m = 0,$$

où

$$b_m^2 \equiv -D \pmod{ap^m},$$
$$b_m \equiv b \pmod{a},$$
$$b_m \equiv -\rho \pmod{p},$$

congruences qui déterminent b_m aux multiples de ap^m près. Pour que $S_{p,\rho}^m$ soit la substitution identique, il faut et il suffit que $k_m^2 = k^2$, c'est-à-dire qu'il soit possible de trouver quatre entiers r, s, r', s' satisfaisant aux équations

$$rs' - r's = 1,$$
$$ap^m = as'^2 + 2bss' + cs^2,$$
$$b_m = b + ar's' + 2br's + crs,$$

s étant divisible par 4. Si l'on avait

$$s \equiv 2 \pmod 4,$$

on aurait

$$k_m^2 = \frac{1}{k^2}$$

et, si s était impair,

$$k_m^2 = \left(\frac{1 + i^t\sqrt{k}}{1 - i^t\sqrt{k}}\right)^4.$$

De ces équations on tire

$$2bss' + cs^2 \equiv 0,$$

$$2br's + crs \equiv 0 \pmod a;$$

d'où

$$2bs \equiv 0, \qquad cs \equiv 0 \pmod a.$$

S'il s'agit de la première espèce, a, $2b$, c n'ont pas de diviseur commun : donc on a

$$s \equiv 0 \pmod a;$$

en faisant

$$s = ya,$$

on trouve

$$p^m = s'^2 + 2bs'y + acy^2 = (s' + by)^2 + Dy^2,$$

y et $s' + by$ étant premiers entre eux.

Au contraire, s'il s'agit de la seconde espèce, on peut seulement conclure que s est divisible par $\frac{a}{2}$; en faisant alors

$$s = \frac{a}{2}y,$$

on a

$$4p^m = 4s'^2 + 4bs'y + acy^2 = (2s' + by)^2 + Dy^2,$$

y et $2s' + by$ ne pouvant avoir un autre diviseur commun que 2.

Si $D = 8h - 1$, y ne peut être impair, car l'équation donnerait

$$4p^m \equiv 0 \pmod 8,$$

ce qui est absurde; si $D = 8h + 3$, $\frac{a}{2}$ est impair et, par suite, y pair.

Donc, en faisant pour la seconde espèce $y = 2\eta$, on a

$$p^m = (s' + b\eta)^2 + D\eta^2,$$

comme pour la première. Pour que $S_{p,\rho}$ soit de l'ordre m, il faut donc que p^m puisse être représenté par la forme principale en nombres premiers entre eux.

Supposons que cette condition soit remplie et qu'on ait

$$p^m = x^2 + y^2 D,$$

x et y étant premiers entre eux. En faisant

$$s = ay, \qquad s' = x - by,$$

on a

$$p^m = s'^2 + 2bs'y + acy^2;$$

s et s' seront premiers entre eux; en effet, un diviseur de y ne peut diviser s', et, si un diviseur de a divisait s', il diviserait p^m, ce qui est contre l'hypothèse. Donc, il est possible de choisir les nombres r, r' de manière à rendre $rs' - r's$ égal à 1. Cela posé, on a

$$ap^m = as'^2 + 2bs's + cs^2,$$

et, en faisant

$$b' = b + ar's' + 2br's + crs,$$

on a, de plus,

$$b'^2 \equiv -D \pmod{ap^m},$$
$$b' \equiv b \pmod{a},$$
$$b' \equiv \pm\rho \pmod{p}.$$

En supposant qu'on ait

$$b' \equiv -\rho \pmod{p}.$$

on en conclut

$$b' \equiv b_m \pmod{ap^m},$$

de sorte que le carré du module défini par l'équation

$$ap^m\zeta'^2 + 2b'\zeta' + \frac{D + b'^2}{ap^m} = 0$$

est égal à k_m^2; donc, k_m appartient à la même classe de formes que k, et

si de plus ay est divisible par 4, on a

$$k_m^2 = k^2, \qquad S_{p,\rho}^m = 1.$$

Si l'on a

$$b' \equiv +\rho,$$

on a évidemment

$$S_{p,-\rho}^m = 1,$$

ce qui entraîne $S_{p,\rho}^m = 1$.

On trouve des considérations parfaitement analogues dans le Mémoire du P. Joubert (*Comptes rendus des séances de l'Académie des Sciences*, t. L).

De l'analyse précédente, on déduit ces règles : en désignant respectivement par m, m_1, m_2 les exposants des plus petites puissances de p qui puissent être représentées par les formes $x^2 + Dy^2$, $x^2 + 4Dy^2$, $x^2 + 16Dy^2$, l'ordre de la substitution $S_{p,\rho}$ est égal à m pour les équations de la première catégorie, si $D = 4h - 1$ ou $= 4h$; il est égal à m_1 pour les équations de la première catégorie, si $D = 4h + 1$ ou $= 4h + 2$, et pour les équations de la seconde espèce et de la seconde catégorie; enfin il est égal à m_2 pour les équations de la première espèce et de la seconde catégorie.

Supposons que, D étant de la forme $8h + 3$, on ait

$$4p^n = x^2 + y^2 D,$$

x et y étant impairs, et que n soit le plus petit exposant pour lequel cette équation puisse être résolue. Alors $S_{p,\rho}^n$ est, pour l'équation de la seconde espèce, la plus petite puissance de $S_{p,\rho}$ qui remplace chaque module par un autre appartenant à la même classe de formes. Or on a

$$p^{3n} = \left(\frac{x^3 - 3xy^2 D}{8}\right)^2 + \left(\frac{3x^2 y - y^3 D}{8}\right)^2 D.$$

On en conclut que $S_{p,\rho}$ est de l'ordre $3n$ si, pour $D = 16h' + 3$, on a

$$x^2 \equiv y^2 \pmod{16},$$

et si, pour $D = 16h' + 11$, on a

$$x^2 \equiv 9y^2 \pmod{16}.$$

Dans les cas contraires, $S_{p,\rho}$ est évidemment de l'ordre $6n$.

On peut aussi conclure de ce qui précède que $S_{p,0}$ est de l'ordre 2, à moins qu'on n'ait

$$p = D = 4h - 1$$

et que l'équation appartienne à la première catégorie.

38. Nous considérerons, dans les numéros suivants, la décomposition des équations des modules singuliers en équations partielles correspondant aux divers genres de formes quadratiques. Soit, comme plus haut, $\Phi(k^2) = 0$ une des équations appartenant au déterminant $-D$, k_1^2 une de ses racines que nous supposerons définie par les équations

$$i\sqrt{D}.2\omega_1 = b_1.2\omega_1 + a_1\omega_1',$$
$$i\sqrt{D}\ \omega_1' = -c_1.2\omega_1 - b_1\omega_1';$$

d'où

$$a_1\zeta_1^2 + 2b_1\zeta_1 + c_1 = 0.$$

Soit, de plus, p un nombre premier impair, diviseur de D, et désignons par $l_{1,\infty}$, $l_{1,0}$, $l_{1,1}$, ..., $l_{1,p-1}$ les modules qu'on déduit de k_1 par les transformations principales du degré $p+1$, $l_{1,\frac{\gamma}{x}}$ étant celui qu'on obtient par la division de la période $(x + yi\sqrt{D})\varpi$ (n° **30**). Nous supposerons enfin que a_1 soit premier à p, ce qui est permis, de sorte que nous pouvons faire $\varpi = 2\omega_1$. Cela posé, considérons, en suivant la voie indiquée par M. Kronecker dans sa célèbre Communication de 1862, le produit Δ_1 des différences des $l_{1,m}^2$, formé d'une manière déterminée, par exemple la suivante :

$$\begin{aligned}\Delta_1 = {} & (l_{1,\infty}^2 - l_{1,0}^2)(l_{1,\infty}^2 - l_{1,1}^2)\dots(l_{1,\infty}^2 - l_{1,p-1}^2),\\ & \times(l_{1,0}^2 - l_{1,1}^2)(l_{1,1}^2 - l_{1,2}^2)\dots(l_{1,p-1}^2 - l_{1,0}^2),\\ & \times(l_{1,0}^2 - l_{1,2}^2)(l_{1,1}^2 - l_{1,3}^2)\dots(l_{1,p-1}^2 - l_{1,1}^2),\\ & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ & \times\left(l_{1,0}^2 - l_{1,\frac{p-1}{2}}^2\right)\left(l_{1,1}^2 - l_{1,\frac{p+1}{2}}^2\right)\dots\left(l_{1,p-1}^2 - l_{1,\frac{p-3}{2}}^2\right).\end{aligned}$$

Plus loin, on verra que la valeur de Δ_1 est indépendante des coefficients a_1, b_1, c_1, le carré du module primitif k_1^2 étant déterminé. On

sait que Δ_1 n'est pas altéré par une substitution linéaire

$$\left| u \quad \frac{\alpha u + \beta}{\gamma u + \delta} \right|$$

relative aux seconds indices, pourvu que $\alpha\delta - \beta\gamma$ soit un résidu quadratique de p, mais qu'il se change en $-\Delta_1$ dans le cas contraire. Or, d'après le n° **32** B, le groupe G′ contient les substitutions $|u \quad u + \beta|$, et le groupe H′ en outre les substitutions $|u \quad -u + \beta|$; donc Δ_1 est invariable par les substitutions de G′, et si $p \equiv 1 \pmod 4$, il l'est aussi par les substitutions de H′; au contraire, si $p \equiv -1 \pmod 4$, la substitution $|u \quad -u|$ change Δ_1 en $-\Delta_1$.

Dans le premier cas, Δ_1 s'exprime en fonction rationnelle et entière de k_1^2. Dans le second, il s'exprime en fonction entière de k_1^2 et de $i\sqrt{D}$; or, puisque la valeur qu'induit Δ_1 par la substitution $|u \quad -u|$ se déduit de la valeur primitive en changeant le signe de $i\sqrt{D}$, on conclut que Δ_1 est égal à une fonction entière de k^2 multipliée par $i\sqrt{D}$. Nous pouvons donc écrire

$$\Delta_1 = \psi(k_1^2), \qquad \text{si } p \equiv 1 \pmod 4,$$
$$\Delta_1 = i\sqrt{D}\,\psi(k_1^2), \qquad \text{si } p \equiv -1 \pmod 4.$$

On se rappelle que, pour un nombre p donné, la fonction $\psi(k^2)$ est identiquement la même pour toutes les racines de l'équation

$$\Phi(k^2) = 0.$$

En désignant par k^2 un module *indéterminé*, par Δ le produit des différences des racines $l_\infty^2, l_0^2, l_1^2, \ldots, l_{p-1}^2$ de l'équation modulaire du degré $p+1$, on a

$$\Delta = \sqrt{(-1)^{\frac{p-1}{2}} p}\,\chi(k^2),$$

χ dénotant une fonction entière. Pour faire coïncider Δ avec Δ_1 pour $k^2 = k_1^2$, nous supposerons que Δ dépende de $l_\infty^2, l_0^2, \ldots, l_{p-1}^2$ de la même manière que Δ_1 dépend des $l_{1,\infty}^2, l_{1,0}^2, \ldots, l_{1,p-1}^2$, et que l_∞ désigne le module obtenu par la division de la période $b_1 . 2\omega + a_1\omega'$, l_u celui qui

répond à $(1 + b_1 u)2\omega + a_1 u\omega'$. On a donc

$$(95)\quad \begin{cases} \psi(k_1^2) = \sqrt{p}\,\chi(k_1^2), & \text{si } p \equiv 1 \pmod 4, \\ \psi(k_1^2) = \sqrt{\frac{p}{D}}\,\chi(k_1^2), & \text{si } p \equiv -1 \pmod 4. \end{cases}$$

Soit maintenant k_2^2 une autre racine de l'équation $\Phi(k^2) = 0$ déterminée par l'équation

$$a_2\zeta_2^2 + 2b_2\zeta_2 + c_2 = 0,$$

a_2 étant premier à p, et soient $l_{2,u}$, Δ_2 les quantités qui correspondent à $l_{1,u}$, Δ_1; nous avons

$$\Delta_2 = \psi(k_2^2), \qquad \text{si } p \equiv 1 \pmod 4,$$
$$\Delta_2 = i\sqrt{D}\,\psi(k_2^2), \qquad \text{si } p \equiv -1 \pmod 4.$$

D'autre côté, faisons varier ζ de ζ_1 à ζ_2, et appelons Δ', l'_u les valeurs de Δ et de l_u pour $\zeta = \zeta_2$; nous avons ainsi

$$\Delta' = \sqrt{(-1)^{\frac{p-1}{2}} p}\,\chi(k_2^2).$$

Puisque les l'_u coïncident, à l'ordre près, avec les $l_{2,u}$, on a

$$\Delta' = \pm\Delta_2.$$

Pour déterminer le signe, remarquons qu'en faisant $\zeta = \zeta_2$, 2ω et ω' deviennent respectivement $2\omega_2$ et ω'_2; donc l'_u correspond à la période $(1 + b_1 u)2\omega_2 + a_1 u\omega'_2$, tandis que $l_{2,u}$ correspond à

$$(1 + ub_2)2\omega_2 + a_2 u\omega'_2;$$

donc, en faisant $l'_{u'} = l_{2,u}$, on a

$$u' \equiv \frac{a_2 u}{(a_1 b_2 - a_2 b_1)u + a_1} \pmod p.$$

Ainsi, Δ' se déduisant de Δ_2 par une substitution linéaire sur les $l_{2,u}$, dont le déterminant est $a_1 a_2$, on a

$$\Delta' = \Delta_2 \qquad \text{ou} \qquad \Delta' = -\Delta_2,$$

suivant que $a_1 a_2$ est résidu quadratique de p ou non. Dans le cas spécial où k_2^2 coïncide avec k_1^2, $a_1 a_2$ est résidu, les deux formes (a_1, b_1, c_1) et (a_2, b_2, c_2) étant proprement équivalentes; donc, k_1^2 étant déterminé, la valeur de Δ_1 est indépendante du choix des coefficients a_1, b_1, c_1, comme nous l'avons dit. En général, on trouve

$$(96)\quad \begin{cases} \psi(k_2^2) = \left(\frac{a_1 a_2}{p}\right)\sqrt{p}\,\chi(k_2^2), & \text{si } p \equiv 1 \pmod 4, \\ \psi(k_2^2) = \left(\frac{a_1 a_2}{p}\right)\sqrt{\frac{p}{D}}\,\chi(k_2^2), & \text{si } p \equiv -1 \pmod 4, \end{cases}$$

$\left(\frac{a_1 a_2}{p}\right)$ étant le symbole de Legendre.

Avant de faire usage des équations (95), (96), il faut démontrer que leurs deux membres ne s'annulent pas séparément, ce qui ne présente pas de difficulté. En effet, si l'on avait $\Delta_1 = 0$, deux racines $l_1'^2$, $l_1''^2$ de l'équation modulaire seraient égales; en désignant par ζ_1', ζ_1'' les valeurs de ζ qui correspondent, on aurait

$$\zeta_1 = p\zeta_1' + m' = p\zeta_1'' + m''$$

ou

$$\zeta_1 = p\zeta_1' + m' = \frac{\zeta_1''}{p};$$

on en tire respectivement

$$\zeta_1'' = \frac{p\zeta_1' + m' - m''}{p} \qquad \text{ou} \qquad \zeta_1'' = p^2\zeta_1' + pm',$$

d'où l'on peut conclure que le module l_1' admettrait une multiplication complexe du degré p^2. Or, l_1' appartenant nécessairement au déterminant $-p^2 D$, on aurait l'une des deux équations

$$p^2 = x^2 + y^2 p^2 D, \qquad 4p^2 = x^2 + y^2 p^2 D,$$

y n'étant pas zéro; mais ces équations sont impossibles, à moins qu'on n'ait

$$D = 1 \qquad \text{ou} \qquad D = 3,$$

deux cas dont nous n'aurons pas à nous occuper.

En supposant que p soit $\equiv 1 \pmod 4$, on voit que toute racine de

l'équation $\Phi(k^2) = 0$ satisfait à l'une des équations

$$\psi(k^2) = \sqrt{p}\,\chi(k^2) \qquad \text{ou} \qquad \psi(k^2) = -\sqrt{p}\,\chi(k^2).$$

Désignons par

$$F(k^2, \sqrt{p})$$

le plus grand commun diviseur des polynômes $\Phi(k^2)$ et

$$\psi(k^2) - \sqrt{p}\,\chi(k^2);$$

alors $F(k^2, -\sqrt{p})$ sera le plus grand commun diviseur de $\Phi(k^2)$ et de $\psi(k^2) + \sqrt{p}\,\chi(k^2)$, et puisque l'équation des modules singuliers n'a pas de racines doubles ou multiples, on a

$$\Phi(k^2) = F(k^2, \sqrt{p})\,F(k^2, -\sqrt{p}); \tag{97}$$

de plus, on voit que les racines se distribuent entre les deux facteurs du second membre d'après les valeurs de $\left(\frac{a_1}{p}\right)$, en d'autres termes, suivant le caractère relatif au module p que possède la forme quadratique correspondante. Pour abréger, nous attribuerons dans la suite ce caractère au module lui-même.

Pareillement, si $p \equiv -1 \pmod 4$, et que $\frac{p}{D}$ ne soit pas un carré parfait, on trouve

$$\Phi(k^2) = F\left(k^2, \sqrt{\frac{p}{D}}\right) F\left(k^2, -\sqrt{\frac{p}{D}}\right), \tag{98}$$

les modules se groupant suivant leurs caractères (mod p). Dans le cas où D est un carré parfait, cette formule peut être remplacée par (97).

On a vu, au n° **22**, que si D n'est pas un carré, $\Phi(k^2)$ se décompose en deux facteurs par l'adjonction de $\sqrt{D}$ ou de $i\sqrt{D}$. Supposons d'abord que la première décomposition ait lieu, et faisons

$$\Phi(k^2) = \Phi_1(k^2, \sqrt{D})\,\Phi_1(k^2, -\sqrt{D});$$

si maintenant $p \equiv 1 \pmod 4$, on a en même temps l'équation (97); il s'ensuit évidemment qu'à l'exception des cas où $D = p$, $\Phi_1(k^2, \sqrt{D})$

se décompose par l'adjonction de $\sqrt{p}$ en deux facteurs, de sorte qu'on a

$$\Phi_1(k^2, \sqrt{D}) = f(k^2, \sqrt{p}, \sqrt{D}) f(k^2, -\sqrt{p}, \sqrt{D}),$$
$$F(k^2, \sqrt{p}) = f(k^2, \sqrt{p}, \sqrt{D}) f(k^2, \sqrt{p}, -\sqrt{D}).$$

Ainsi $\Phi(k^2)$ est décomposé en quatre facteurs $f(k^2, \pm\sqrt{p}, \pm\sqrt{D})$, de manière que les racines de $f(k^2, \pm\sqrt{D}, \sqrt{p}) = 0$ possèdent le même caractère (mod p), celles de $f(k^2, \pm\sqrt{D}, -\sqrt{p}) = 0$, le caractère opposé.

Si $p \equiv -1 \pmod 4$, l'équation (97) est remplacée par (98); on aura, pourvu que $\frac{D}{p}$ ne soit pas un carré,

$$\Phi_1(k^2, \sqrt{D}) = f(k^2, \sqrt{p}, \sqrt{D}) f(k^2, -\sqrt{p}, \sqrt{D});$$
$$F\left(k^2, \sqrt{\frac{p}{D}}\right) = f(k^2, \sqrt{p}, \sqrt{D}) f(k^2, -\sqrt{p}, -\sqrt{D}).$$

Donc $\Phi(k^2)$ est encore décomposé en quatre facteurs, mais ici les racines des équations

$$f(k^2, \sqrt{p}, \sqrt{D}) = 0, \qquad f(k^2, -\sqrt{p}, -\sqrt{D}) = 0$$

possèdent le même caractère, celle des autres le caractère opposé.

Dans les cas où la décomposition par $i\sqrt{D}$ a lieu, on a

$$\Phi(k^2) = \Phi_1(k^2, i\sqrt{D}) \Phi_1(k^2, -i\sqrt{D}),$$

et, si $p \equiv 1 \pmod 4$:

$$\Phi_1(k^2, i\sqrt{D}) = f(k^2, \sqrt{p}, i\sqrt{D}) f(k^2, -\sqrt{p}, i\sqrt{D}),$$
$$F(k^2, \sqrt{p}) = f(k^2, \sqrt{p}, i\sqrt{D}) f(k^2, \sqrt{p}, -i\sqrt{D});$$

si $p = -1 \pmod 4$,

$$\Phi_1(k^2, i\sqrt{D}) = f(k^2, i\sqrt{p}, i\sqrt{D}) f(k^2, -i\sqrt{p}, i\sqrt{D}),$$
$$F\left(k^2, \sqrt{\frac{p}{D}}\right) = f(k^2, i\sqrt{p}, i\sqrt{D}) f(k^2, -i\sqrt{p}, -i\sqrt{D});$$

d'où l'on tire des conclusions analogues à l'égard des caractères propres aux racines des quatre équations partielles.

39. Soit maintenant $D = m^2 D'$, m^2 étant le plus grand carré divisant D, et désignons par $p_1, p_2, \ldots, p_\mu$ les nombres premiers impairs qui divisent D; dans les cas où $D' > 2$, nous supposons que p_μ soit un diviseur de D'. Choisissons de plus pour chaque module singulier l'équation $a\zeta^2 + 2b\zeta + c = 0$, de telle manière qu'on puisse reconnaître l'ensemble des caractères du module par l'un des coefficients extérieurs; ce sera c ou a qui servira de nombre caractéristique, suivant que le module appartient à la première ou à la seconde catégorie. Cela posé, étudions la décomposition du polynôme $\Phi(k^2)$ par l'adjonction simultanée des radicaux $\sqrt{\pm p_1}, \sqrt{\pm p_2}, \ldots, \sqrt{\pm p_\mu}$. Il faudra pour cela distinguer plusieurs cas.

Soit d'abord $D = 4h + 1$. Si $D' > 1$, on a

$$\Phi(k^2) = \Phi_1(k^2, \sqrt{D})\,\Phi_1(k^2, -\sqrt{D});$$

d'après le n° **22**, on peut supposer que, pour les modules qui appartiennent au premier facteur, on ait $c \equiv 1$ ou $a \equiv 1 \pmod 4$, ou bien, en faisant usage de l'expression de Gauss, que les modules qui possèdent le caractère $(1, 4)$ appartiennent au premier facteur, ceux qui ont le caractère $(3, 4)$ au second. A son tour le polynôme $\Phi_1(k^2, \sqrt{D})$ admet une décomposition relative à chacun des radicaux $\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\mu}$:

$$\begin{aligned}\Phi_1(k^2, \sqrt{D}) &= f_1(k^2, \sqrt{p_1}, \sqrt{D})\, f_1(k^2, -\sqrt{p_1}, \sqrt{D}) = \ldots \\ &= f_{\mu-1}(k^2, \sqrt{p_{\mu-1}}, \sqrt{D})\, f_{\mu-1}(k^2, -\sqrt{p_{\mu-1}}, \sqrt{D}).\end{aligned}$$

On en conclut que $\Phi_1(k^2, \sqrt{D}) = 0$ se décompose en $2^{\mu-1}$ équations partielles de la forme

$$f'(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{\mu-1}}, \sqrt{D}) = 0, \tag{99}$$

où le premier membre est le plus grand commun diviseur de

$$f_1(k^2, \sqrt{p_1}, \sqrt{D}), \quad f_2(k^2, \sqrt{p_2}, \sqrt{D}), \quad \ldots, \quad f_{\mu-1}(k^2, \sqrt{p_{\mu-1}}, \sqrt{D}).$$

Si, dans l'équation (99), on change le signe de l'un des radicaux

$\sqrt{p_1}, \ldots, \sqrt{p_{\mu-1}}$, par exemple celui de $\sqrt{p_1}$, en conservant les autres signes, on obtient une nouvelle équation, dont les racines ont conservé les caractères relatifs aux modules $p_2, \ldots, p_{\mu-1}$, pendant que leur caractère (mod p_1) est changé. Par cela le caractère (mod p_μ) est changé ou conservé, suivant que p_1 divise D′ ou non. En mettant l'équation (99) sous la forme

$$\varphi(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\mu}) = 0, \tag{100}$$

la nouvelle équation sera

$$\varphi(k^2, -\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{\mu-1}}, \mp\sqrt{p_\mu}) = 0,$$

où évidemment il faut prendre le signe supérieur si p_1 divise D′, l'inférieur dans le cas contraire. Donc le signe de $\sqrt{p_\mu}$ doit aussi être déterminé suivant le caractère que possèdent les racines de la nouvelle équation par rapport au module p_μ. L'équation $\Phi_1(k^2, -\sqrt{\mathrm{D}}) = 0$ se décompose de la même manière; si dans une de ses équations partielles on veut avoir les mêmes caractères (mod p_1), ..., (mod $p_{\mu-1}$) que dans l'équation (99), le caractère (mod p_μ) sera changé; en vertu de ce qui a été dit au numéro précédent, on a ainsi l'équation

$$f'\left[k^2, (-1)^{\frac{1}{2}(p_1-1)}\sqrt{p_1}, (-1)^{\frac{1}{2}(p_2-1)}\sqrt{p_2}, \ldots, (-1)^{\frac{1}{2}(p_{\mu-1}-1)}\sqrt{p_{\mu-1}}, -\sqrt{\mathrm{D}}\right] = 0$$

ou bien

$$\varphi\left[k^2, (-1)^{\frac{1}{2}(p_1-1)}\sqrt{p_1}, (-1)^{\frac{1}{2}(p_2-1)}\sqrt{p_2}, \ldots, (-1)^{\frac{1}{2}(p_{\mu-1}-1)}\sqrt{p_{\mu-1}}, -(-1)^{\frac{1}{2}(p_\mu-1)}\sqrt{p_\mu}\right] = 0;$$

on démontre la dernière équation en remarquant que les diviseurs premiers de D′ qui sont de la forme $4h-1$ sont en nombre pair. L'équation $\Phi(k^2) = 0$ est ainsi décomposée en 2^μ équations partielles du même degré, répondant chacune à un genre déterminé de formes quadratiques du déterminant $-\mathrm{D}$. Supposons que l'équation proposée soit de la première catégorie, et déterminons les signes des radicaux $\sqrt{p_1}, \ldots, \sqrt{p_\mu}$ de telle manière que l'équation (100) réponde au genre principal; on en déduit l'équation partielle satisfaite par le module défini par la relation $a\zeta^2 + 2b\zeta + c = 0$, en changeant $\sqrt{p_r}$ en $\left(\frac{c}{p_r}\right)\sqrt{p_r}$,

quand $c \equiv 1 \pmod 4$; en $(-1)^{\frac{1}{2}(p_r-1)}\left(\frac{c}{p_r}\right)\sqrt{p_r}$, quand $c \equiv -1 \pmod 4$, c'est-à-dire qu'on obtient l'équation partielle cherchée en remplaçant $\sqrt{p_r}$ par $\left(\frac{p_r}{c}\right)\sqrt{p_r}$. S'il s'agit d'une équation de la seconde catégorie, c doit être remplacé par a. C'est la règle indiquée par M. Kronecker, à l'occasion des déterminants — 21, — 105; il faut pourtant remarquer que la classification des modules singuliers que nous avons adoptée ne coïncide pas avec celle de M. Kronecker. Ces résultats sont encore valables si $D' = 1$; en effet, on trouve dans ce cas l'équation (100) par décomposition immédiate de $\Phi(k^2) = 0$, et il n'existe pas de genre ayant le caractère (3, 4).

Supposons $D = 4h - 1$. On a aussi $D' \equiv -1 \pmod 4$ et, par suite, D' contient au moins un diviseur premier de la forme $(4h - 1)$; nous pouvons donc supposer $p_\mu \equiv -1 \pmod 4$. Pour écrire plus simplement les formules, nous poserons

$$p_1 \equiv p_2 \equiv \ldots \equiv p_\lambda \equiv 1, \qquad p_{\lambda+1} \equiv p_{\lambda+2} \equiv \ldots \equiv p_\mu \equiv -1 \pmod 4.$$

Considérons d'abord les équations de la première espèce et de la première catégorie. L'équation $\Phi(k^2) = 0$ se décompose en deux autres $\Phi_1(k^2, i\sqrt{D}) = 0$ et $\Phi_1(k^2, -i\sqrt{D}) = 0$, où il est permis de supposer que les modules pour lesquels le coefficient b est congru à $1 \pmod 4$ satisfassent à la première, les autres à la seconde équation (n° **22**). Chacune de ces équations se décompose de nouveau comme dans le cas précédent; en désignant par

$$(101) \qquad \varphi(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\lambda}, i\sqrt{p_{\lambda+1}}, \ldots, i\sqrt{p_\mu}) = 0,$$

l'une des équations partielles provenant de la première, celle-ci

$$(102) \qquad \varphi(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\lambda}, -i\sqrt{p_{\lambda+1}}, \ldots, -i\sqrt{p_\mu}) = 0$$

appartient à la seconde; les racines de ces deux équations partielles présentent le même ensemble de caractères et répondent, par suite, à un même genre de formes; les racines de l'une sont les réciproques de celles de l'autre (n° **22**). Quand D est de la forme $8h + 3$, il y a aussi une autre relation entre les racines des deux équations; en effet, si l'on

fait $\zeta = -\frac{1}{4\zeta'}$, ce qui donne le module transformé k', on a

$$4c\zeta'^2 - 2b\zeta' + \frac{a}{4} = 0,$$

où $\frac{a}{4}$ est impair; on en conclut que k' appartient non seulement au même déterminant, à la même espèce et à la même catégorie, mais aussi au même genre. Donc k^2 satisfaisant à (101), k'^2 satisfait à (102); de plus (101) sera satisfaite par k^2, $\frac{1}{k'^2}$, $\frac{-k'^2}{k^2}$; (102) par $\frac{1}{k^2}$, k'^2, $\frac{-k^2}{k'^2}$. Si l'on suppose les radicaux tellement déterminés que l'équation (101) réponde au genre principal, avec $b \equiv 1 \pmod 4$, on en tire celle qui est satisfaite par k^2 en changeant $\sqrt{p_r}$ en $\left(\frac{c}{p_r}\right)\sqrt{p_r}$, i en i^b.

Pour les équations de la première espèce et de la seconde catégorie, les équations (101), (102) sont remplacées par les suivantes

$$(103) \qquad \varphi(k^2, \sqrt{p_1}, \ldots, \sqrt{p_\lambda}, \quad \sqrt{p_{\lambda+1}}, \ldots, \quad \sqrt{p_\mu}) = 0,$$

$$(104) \qquad \varphi(k^2, \sqrt{p_1}, \ldots, \sqrt{p_\lambda}, -\sqrt{p_{\lambda+1}}, \ldots, -\sqrt{p_\mu}) = 0,$$

dont la première a lieu si $a \equiv 1$, la seconde si $a \equiv -1 \pmod 4$. Il est facile de voir que les deux équations sont réciproques. Si (103) répond au genre principal, on en déduit l'équation qui est satisfaite par le module k, en remplaçant $\sqrt{p_r}$ par $\left(\frac{p_r}{a}\right)\sqrt{p_r}$.

Dans la première catégorie de la seconde espèce il y a deux équations, dont l'une a lieu pour $a \equiv 0 \pmod 8$, l'autre pour $a \equiv 4 \pmod 8$, les racines de l'une étant les réciproques de celles de l'autre. Chacune de ces équations se décompose comme dans la première catégorie de la première espèce; on a donc deux équations appartenant à chaque genre, définies par les formules (101), (102). Si $a \equiv 0 \pmod 8$, les racines de l'une sont les compléments de celles de l'autre. En partant des équations qui répondent au genre contenant la forme $\left(\frac{D+1}{2}, 1, 2\right)$, la règle des signes est évidemment aussi la même que dans la première catégorie de la première espèce, en y remplaçant c par $\frac{1}{2}c$.

Dans la seconde catégorie de la seconde espèce, on a

$$a \equiv 2 \pmod 4.$$

On a, pour chaque genre de formes, deux équations définies par les formules (103), (104), dont la première répond à $\frac{a}{2} \equiv 1 \pmod 4$, la seconde à $\left(\frac{a}{2}\right) \equiv 3$, les racines de l'une étant les réciproques de celle de l'autre (n° **22**). En partant de l'équation qui répond au genre contenant la forme $\left(2, 1, \frac{D+1}{2}\right)$, la règle des signes est la même que pour la seconde catégorie de la première espèce, en remplaçant seulement a par $\frac{a}{2}$.

Soit maintenant $D = 8h \pm 2$. On a

$$\Phi(k^2) = \Phi_1(k^2, \sqrt{D})\,\Phi_1(k^2, -\sqrt{D}).$$

En poursuivant les décompositions comme pour $D = 4h + 1$, on voit que chacun des deux facteurs donne 2^μ équations partielles respectivement des formes

$$(105)\quad \varphi(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\lambda}, \sqrt{p_{\lambda+1}}, \ldots, \sqrt{p_\mu}, \sqrt{2}) = 0,$$

$$(106)\quad \varphi(k^2, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\lambda}, -\sqrt{p_{\lambda+1}}, \ldots, -\sqrt{p_\mu}, \mp\sqrt{2}) = 0,$$

dont (105) a lieu si $c \equiv 1$ pour la première catégorie (en supposant b divisible par 4, *voir* n° **22**), si $a \equiv 1$ pour la seconde, pendant que (106) a lieu dans les cas contraires; le double signe correspond à celui de $8h \pm 2$. Les modules qui satisfont à ces équations ont les mêmes caractères $(\bmod p_1), (\bmod p_2), \ldots, (\bmod p_\mu)$; or les formes du déterminant $-D$ possèdent en outre un caractère (mod 8), qui est déterminé par les autres caractères, tandis que les valeurs de $(-1)^{\frac{c-1}{2}}$ ou $(-1)^{\frac{a-1}{2}}$ ne le sont pas; donc les équations (105), (106) répondent au même genre de formes. On voit aisément que dans la première catégorie les racines de l'une de ces équations sont les réciproques de celles de l'autre, et que dans la seconde catégorie k^2 et $\frac{1}{k^2}$ satisfont à la même équation. En remarquant qu'on a, pour la première catégorie,

$$\Pi\left(\frac{c}{q_r}\right) = (\mp 1)^{\frac{c-1}{2}}(-1)^{\frac{c^2-1}{8}},$$

où q_r doit être égalé à tous les diviseurs premiers impairs de D′, on trouve facilement la règle des signes : l'équation (105) répondant au genre principal, on obtient celle qui est satisfaite par un module k en changeant $\sqrt{p_r}$ en $\left(\frac{p_r}{c}\right)\sqrt{p_r}$, $\sqrt{2}$ en $(-1)^{\frac{c^2-1}{8}}\sqrt{2}$. Pour la seconde catégorie c est remplacé par a.

Si $D = 4(2h+1)$ il y a deux équations appartenant à la première catégorie, une à la seconde. Chacune de ces équations se décompose en 2^μ équations partielles répondant aux 2^μ genres; celles de la seconde catégorie sont réciproques. Quant à la forme des équations partielles et à la règle des signes, tout est comme pour $D = 4h+1$.

Si $D = 2^{2\pi+1}(4h \pm 1)$, où $\pi > 0$, la forme des équations partielles et la règle des signes sont les mêmes que pour $D = 8h \pm 2$. Mais puisque les formes peuvent avoir quatre caractères différents par rapport au module 8 : (1, 8), (3, 8), (5, 8), (7, 8), les deux équations (105), (106) répondent à des genres différents; il n'y a donc qu'une équation partielle pour chaque genre.

Enfin, si $D = 2^{2\pi}(2h+1)$, π surpassant 1, on a la même décomposition et la même règle des signes que pour $D = 4h+1$; mais, comme chaque classe a un caractère par rapport au module 8, qui n'est pas déterminé par les caractères relatifs aux modules $4, p_1, p_2, \ldots, p_\mu$, chacune des 2^μ équations partielles répond à l'ensemble de deux genres distincts. Dans ces seuls cas la décomposition dont il s'agit ne suffit pas pour séparer les modules appartenant aux divers genres.

40. L'analogie fait présumer qu'il existe, pour les déterminants de la forme $-2^{2\pi}(2h+1)$, une nouvelle décomposition qui sépare complètement les genres, et l'on est porté à croire qu'elle aura lieu par l'adjonction de $\sqrt{2}$. On peut le démontrer par les considérations suivantes, qui éclaircissent en même temps quelques autres points.

Soit k un module quelconque, k_0 celui qu'on en déduit par la transformation principale du degré impair n; on a une équation de la forme

$$F\left[\frac{\sqrt[4]{k_0}}{(\sqrt[4]{k})^n},\ k^2\right] = 0$$

ou bien, si $n = 8h + 1$,

$$F_1\left(\frac{\sqrt[4]{k_0}}{\sqrt[4]{k}},\ k^2\right) = 0;$$

si $n = 8h + 3$,

$$F_1\left(\frac{1}{k}\sqrt[4]{k_0}\sqrt[4]{k},\ k^2\right) = 0;$$

si $n = 8h + 5$,

$$F_1\left(\frac{1}{k}\frac{\sqrt[4]{k_0}}{\sqrt[4]{k}},\ k^2\right) = 0;$$

si $n = 8h + 7$,

$$F_1(\sqrt[4]{k_0}\sqrt[4]{k},\ k^2) = 0.$$

Pour avoir une équation en $\sqrt{k}$ satisfaite par les modules de la première espèce et de la première catégorie du déterminant impair $-D$, on peut faire $n = D$, et (n^{os} **10, 11**) $\frac{\sqrt[4]{k_0}}{\sqrt[4]{k}} = \pm\frac{1}{\sqrt{i^{bc}}\sqrt{k}}$, si $n = 8h + 1$ ou $= 8h + 5$; mais $\sqrt[4]{k_0}\sqrt[4]{k} = \pm\sqrt{i^{bc}}\sqrt{k}$, si $n = 8h + 3$ ou $= 8h + 7$. On obtient ainsi deux équations, qui, pour $D = 8h \pm 1$, sont de la forme

$$f(\sqrt{i^{bc}}\sqrt{k}) = 0, \qquad f(-\sqrt{i^{bc}}\sqrt{k}) = 0;$$

pour $D = 8h \pm 3$, de la forme

$$f\left(\frac{\sqrt{k}}{\sqrt{i^{bc}}}\right) = 0, \qquad f\left(-\frac{\sqrt{k}}{\sqrt{i^{bc}}}\right) = 0$$

ou bien

$$(107) \qquad f\left(\frac{1 \pm i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0, \qquad f\left(-\frac{1 \pm i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0,$$

où il faut prendre le signe supérieur si $D = 8h \pm 1$, l'inférieur si $D = 8h \pm 3$.

Multipliées membre à membre, ces équations reproduisent les équations en $i^{bc}k$ des n^{os} **10** et **11**. L'équation modulaire n'étant pas altérée quand on remplace $\sqrt[4]{k}$ et $\sqrt[4]{k_0}$ par $\frac{1}{\sqrt[4]{k}}$ et $\frac{1}{\sqrt[4]{k_0}}$, il est facile de voir que les modules réciproques satisfont respectivement aux équations

$$f\left(\frac{1 \mp i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0, \qquad f\left(-\frac{1 \mp i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0.$$

En se servant de l'équation $\Phi(k^2) = 0$, on peut débarrasser les équations (107) des racines qui n'appartiennent pas au déterminant $-D$; soient

$$\varphi\left(\frac{1 \pm i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0, \qquad \varphi\left(-\frac{1 \pm i^{bc}}{2}\sqrt{2}\sqrt{k}\right) = 0$$

les équations ainsi obtenues. En chassant maintenant i, on obtient deux équations nouvelles

$$\varphi_1(\sqrt{2}\sqrt{k}) = 0, \qquad \varphi_1(-\sqrt{2}\sqrt{k}) = 0, \tag{108}$$

qui, multipliées membre à membre, reproduisent l'équation $\Phi(k^2) = 0$. Elles sont évidemment réciproques, et d'ailleurs elles n'ont pas de racine commune, de sorte que $\sqrt{2}$ ne peut disparaître; car, si $\sqrt{k}$ satisfaisait aux deux équations, k^2 serait racine double de l'équation $\Phi(k^2) = 0$, ce qui n'a pas lieu. En désignant par m le degré du polynôme Φ, celui de φ_1 est évidemment $2m$.

Par exemple, pour $D = 3$ et $D = 5$, on a, en écrivant z au lieu de $\sqrt{k}$,

$$z^4 + \sqrt{2}z^3 + z^2 + \sqrt{2}z + 1 = 0,$$

$$z^8 - 2\sqrt{2}z^7 + 4z^6 + 6\sqrt{2}z^5 + 2z^4 + 6\sqrt{2}z^3 + 4z^2 - 2\sqrt{2}z + 1 = 0.$$

Il faut maintenant déterminer le signe du radical $\sqrt{2}$. Pour cela, nous supposons, suivant l'usage, que $\sqrt[4]{k}$ soit généralement défini par la formule

$$\sqrt[4]{k} = \sqrt{2}\cdot\sqrt[8]{q}\prod_1^\infty \frac{1+q^{2m}}{1+q^{2m-1}}, \qquad \text{où} \qquad \sqrt[8]{q} = e^{\frac{1}{4}\pi i\zeta}.$$

Sans nuire à la généralité, nous pouvons, de plus, supposer que les coefficients a des équations $a\zeta^2 + 2b\zeta + c = 0$ soient premiers à D; sous cette hypothèse, le rapport des périodes qui répond à la racine $\sqrt[4]{k_0}$ de l'équation modulaire dont nous sommes partis est $\frac{t+\zeta}{D}$, où nous pouvons prendre $t \equiv 0 \pmod 8$, puisque t n'est déterminé que par rapport au module D (n° 9). Les équations (24) deviennent

$$b = r_1, \qquad a = s_1, \qquad -c = -tr_1 + Dr'_1, \qquad -b = -ts_1 + Ds'_1.$$

Or il résulte des formules de M. Hermite (*Sur la théorie des équations modulaires*, p. 4) que la transformation linéaire $\begin{pmatrix} r_1 & s_1 \\ r'_1 & s'_1 \end{pmatrix}$ donne

$$\sqrt[4]{k_1} = (-1)^{\frac{1}{8}(s_1^2-1)} e^{-\frac{1}{4}r_1 s_1 \pi i} \sqrt[4]{k} \qquad \text{si} \quad s_1 \equiv 0 \pmod 4,$$

$$\sqrt[4]{k_1} = (-1)^{\frac{1}{8}(s_1^2-1)} e^{-\frac{1}{4}r_1 s_1 \pi i} \frac{1}{\sqrt[4]{k}} \qquad \text{si} \quad s_1 \equiv 2.$$

En remplaçant k par k_0, k_1 par k, nous avons donc :

$$\text{Pour D} = 8h+1,\ 8h+5 \ldots\ldots \quad \frac{\sqrt[4]{k_0}}{\sqrt[4]{k}} = (-1)^{\frac{1}{8}(s_1^2-1)} e^{-\frac{1}{4}r_1 s_1 \pi i} \frac{1}{\sqrt{k}},$$

$$\text{Pour D} = 8h+3,\ 8h+7 \ldots\ldots \quad \sqrt[4]{k_0}\sqrt[4]{k} = (-1)^{\frac{1}{8}(s_1^2-1)} e^{\frac{1}{4}r_1 s_1 \pi i} \sqrt{k}.$$

Ayant $s'_1 \equiv -\mathrm{D}b$, $r'_1 s'_1 = bc \pmod 8$, on trouve

$$(-1)^{\frac{1}{8}(s_1^2-1)} e^{\pm\frac{1}{4}r_1 s_1 \pi i} = \frac{1 \pm i^{bc}}{2} (-1)^{\frac{1}{8}\mathrm{D}b^2 - \frac{1}{8} + \frac{1}{8}(c^2-1)} \sqrt{2}.$$

On en peut conclure que les valeurs de $\sqrt{k}$ se distribuent entre les deux équations (108) suivant la valeur de l'expression $(-1)^{\frac{1}{8}(c^2-1)}$. Il est, d'ailleurs, facile de voir que ce résultat est indépendant de l'hypothèse faite sur les coefficients α; en effet, si l'on effectue une transformation linéaire $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ ne changeant pas $\sqrt{k}$, la valeur nouvelle c_1 de c sera

$$a\gamma^2 + 2b\gamma\alpha + c\alpha^2;$$

or, ayant $\gamma \equiv 0$, $\alpha \equiv \pm 1 \pmod 4$, on a

$$c_1 \equiv c \pmod 8, \qquad \text{d'où} \qquad (-1)^{\frac{1}{8}(c_1^2-1)} = (-1)^{\frac{1}{8}(c^2-1)}.$$

En faisant $\zeta = -\frac{1}{\zeta_1}$, $\sqrt{k} = \frac{1-\sqrt{k_1}}{1+\sqrt{k_1}}$, on a

$$c\zeta_1^2 - 2b\zeta_1 + a = 0,$$

et, par suite, le module transformé k_1 appartient à la seconde catégorie et à la première espèce. Puisque $\sqrt{k_1}$ se change en $-\sqrt{k_1}$ quand

$\sqrt{k}$ est remplacé par $\frac{1}{\sqrt{k}}$, les équations (108) donnent, en substituant, deux équations en k_1 du degré m

$$\psi(k_1, \sqrt{2}) = 0, \qquad \psi(k_1, -\sqrt{2}) = 0;$$

en changeant le signe de $\sqrt{2}$, celui de $\sqrt{k}$ est aussi changé, et, par suite, k_1 est remplacé par $\frac{1}{k_1}$. En chassant les puissances impaires de k_1, on obtient deux équations en k_1^2 du degré m

$$\psi_1(k_1^2, \sqrt{2}) = 0, \qquad \psi_1(k_1^2, -\sqrt{2}) = 0,$$

qui, multipliées, reproduisent évidemment l'équation $\Phi(k^2) = 0$ relative à la seconde catégorie.

On a ainsi le résultat suivant : L'équation $\Phi(k^2) = 0$ relative à la première espèce et à la seconde catégorie se décompose par l'adjonction de $\sqrt{2}$ en deux équations partielles

$$\psi_1(k^2, \sqrt{2}) = 0, \qquad \psi_1(k^2, -\sqrt{2}) = 0;$$

on peut déterminer la valeur de $\sqrt{2}$ de telle manière que le module défini par l'équation $a\zeta^2 + 2b\zeta + c = 0$ satisfasse à l'équation

$$\psi_1\left[k^2, (-1)^{\frac{1}{2}(a^2-1)}\sqrt{2}\right] = 0,$$

le module réciproque étant racine de l'autre équation.

Le module k étant de la première espèce et de la seconde catégorie, posons

$$\zeta = -\frac{1}{2\zeta_1}, \qquad \text{d'où} \qquad 4c\zeta_1^2 - 4b\zeta_1 + a = 0;$$

alors le module transformé k_1 appartient à la première catégorie et au déterminant $-4D$. Donc, si, dans les équations $\psi(k, \pm\sqrt{2}) = 0$, on fait $k = \frac{1-k_1}{1+k_1}$, on obtient deux équations en k_1

$$\chi(k_1, \pm\sqrt{2}) = 0;$$

d'ailleurs, on a $\chi(k_1, -\sqrt{2}) = \pm\chi(-k_1, \sqrt{2})$, comme on le voit aisément; donc les équations prennent la forme

$$\chi(\pm\sqrt{2}k_1) = 0.$$

Par suite, chacune des deux équations en k^2 de la première catégorie d'un déterminant de la forme $-4(2h+1)$ se décompose en deux équations en k par l'adjonction de $\sqrt{2}$; on peut déterminer la valeur de $\sqrt{2}$ de manière que le module défini par la relation $a\zeta^2 + 2b\zeta + c = 0$ soit racine de l'équation

$$\chi[(-1)^{\frac{1}{8}(a^2-1)}\sqrt{2}k] = 0.$$

Les décompositions des équations $\Phi(k^2) = 0$ dont nous venons de parler entraînent évidemment des décompositions analogues des équations partielles du numéro précédent.

Considérons enfin les déterminants de la forme $2^{2\pi}(2h+1)$, où $\pi > 1$. Soit, comme plus haut, k un module de la première espèce et de la seconde catégorie du déterminant impair $-D$, défini par l'équation $a\zeta^2 + 2b\zeta + c = 0$ et, par suite, satisfaisant à l'équation

$$\psi_1[k^2, (-1)^{\frac{1}{8}(a^2-1)}\sqrt{2}] = 0.$$

En faisant $\zeta = -\frac{1}{4\zeta_1}$, ce qui donne $k_1^2 = 1 - k^2$, on a

$$16c\zeta_1^2 - 8b\zeta_1 + a = 0;$$

par conséquent, k_1 appartient au déterminant $-16D$ et à la première des deux équations de la première catégorie. Évidemment, on trouve, de cette manière, toutes les racines de cette équation. Il s'ensuit que, si k est un module de la première catégorie du déterminant $-16D$, racine de la première des deux équations, et défini par l'équation $a\zeta^2 + 2b\zeta + c = 0$, il satisfait à l'équation

$$\psi_1[1 - k^2, (-1)^{\frac{1}{8}(a^2-1)}\sqrt{2}] = 0.$$

En égalant à zéro le plus grand commun diviseur des premiers membres de cette équation et de l'équation partielle du numéro précédent,

on a une nouvelle équation partielle $\varphi(k^2) = 0$, répondant à un seul genre de formes.

Posons maintenant $\zeta = 2\zeta_1 + t$; on aura

$$4a\zeta_1^2 + 4(b + at)\zeta_1 + at^2 + 2bt + c = 0, \qquad k_1^4 k'^4 = 16 k_1'^2 k^2;$$

le nouveau module k_1 appartient donc au déterminant $-64D$ et à la première des deux équations de la première catégorie; évidemment, ses caractères sont les mêmes que ceux du module k. En éliminant k^2 entre les équations $\varphi(k^2) = 0$ et $k_1^4 k'^4 = 16 k_1'^2 k^2$, on obtient donc une équation partielle répondant à un seul genre de formes du déterminant $-64D$. En continuant de la même manière, on finit par trouver les équations partielles qui répondent à un seul genre du déterminant $-2^{2\pi}D$. On voit que le signe de $\sqrt{2}$ doit être déterminé par la même règle que pour les déterminants de la forme $8h \pm 2$.

La décomposition de la première équation de la première catégorie donne immédiatement celle de la seconde équation. On a aussi une décomposition analogue de l'équation de la seconde catégorie, puisque celle-ci se déduit de l'équation traitée en remplaçant k^2 par $\left(\frac{1-\sqrt{k}}{1+\sqrt{k}}\right)^4$ et chassant le radical et les puissances impaires de k.

La décomposition des équations des modules singuliers fournit évidemment une démonstration de ces deux théorèmes d'Arithmétique : Tous les genres de formes d'un déterminant négatif contiennent le même nombre de classes; le nombre des genres est égal à la moitié du nombre des caractères totaux assignables.

Remarque sur la classification des modules singuliers.

La classification dont nous avons fait usage repose sur la considération de l'équation $a\zeta^2 + 2b\zeta + c = 0$, où ζ est le rapport des périodes elliptiques de la fonction $\lambda(z)$. On peut la remplacer par une autre, qui est, sans doute, celle de M. Kronecker et qui présente à certains égards un avantage, en introduisant, au lieu de ζ, le rapport $\frac{\omega'}{\omega}$ des pé-

riodes des carrés des trois fonctions elliptiques. Faisons, en effet,

$$\rho = \frac{\omega'}{\omega} = 2\zeta, \qquad a\rho^2 + 2b\rho + c = 0, \qquad ac - b^2 = \Delta,$$

et classons les modules d'après les valeurs de Δ. En considérant d'abord l'ordre proprement primitif, on a, comme on le voit sans peine, pour chaque valeur de Δ, trois équations différentes en k^2, toutes du degré $2N$, N étant le nombre des classes proprement primitives du déterminant $-\Delta$. Parmi ces équations, deux correspondent aux valeurs impaires de c; ce sont celles que nous avons appelées les équations de la première catégorie du déterminant -4Δ. La troisième équation correspond aux valeurs paires de c; si Δ a l'une des formes $4h+1$, $4h+2$, c'est l'équation de la première catégorie du déterminant $-\Delta$; si $\Delta = 4h-1$, c'est l'équation de la seconde espèce et de la seconde catégorie du déterminant $-\Delta$; enfin, si $\Delta = 4h$, c'est l'équation de la première espèce et de la seconde catégorie du déterminant $-\frac{1}{4}\Delta$.

Quant à l'ordre improprement primitif, le résultat est différent suivant que $\Delta = 8h-1$ ou $= 8h+3$. Pour $\Delta = 8h-1$, on a trois équations du degré $2N$, savoir les trois équations de la première catégorie du déterminant $-\Delta$. Si, au contraire, $\Delta = 8h+3$, on n'a qu'une seule équation, celle de la première espèce et de la première catégorie du déterminant $-\Delta$; le degré de cette équation est encore $2N$, c'est-à-dire qu'il est égal au sextuple du nombre des classes improprement primitives. Pour $\Delta = 1$, $\Delta = 3$, il y a des exceptions évidentes à l'égard des degrés des équations.

D'après cette classification, les équations qui appartiennent à l'ordre proprement primitif se décomposent en deux équations partielles par l'adjonction de $\sqrt{\Delta}$, pourvu que Δ ne soit pas un carré; celles qui répondent à l'ordre improprement primitif, au contraire, par l'adjonction de $i\sqrt{\Delta}$; de plus, les valeurs réelles de k^2 appartiennent toutes à l'ordre proprement primitif.