ANNALES SCIENTIFIQUES DE L'É.N.S.

KRONECKER

Sur la multiplication complexe des fonctions elliptiques

Annales scientifiques de l'É.N.S. 1re série, tome 3 (1866), p. 295-302

<http://www.numdam.org/item?id=ASENS_1866_1_3__295_0>

SUR LA MULTIPLICATION COMPLEXE DES FONCTIONS ELLIPTIQUES,

PAR M. KRONECKER.

(*Monatsbericht der Akademie der Wissenschaften zu Berlin*, 26 juin 1862, p. 363.)

TRADUIT PAR M. HOÜEL,

PROFESSEUR A LA FACULTÉ DES SCIENCES DE BORDEAUX.

Dans le cours de mes recherches sur les fonctions elliptiques pour lesquelles a lieu la multiplication complexe, j'ai été conduit par le sujet même à étudier principalement les propriétés arithmétiques des modules correspondants, pour approfondir la nature de ces remarquables irrationnelles numériques. J'ai pu m'appuyer, dans ce travail, sur une théorie nouvelle et générale des formes décomposables, dont je m'étais occupé peu de temps auparavant au point de vue le plus étendu possible, et dont j'ai retiré tous les avantages que j'en attendais dans l'application à la question particulière qui nous occupe. Comme j'ai déjà annoncé, au mois de juillet de l'année dernière, les résultats des recherches en question, et que cependant les travaux algébriques qui m'absorbent en ce moment ne me permettront pas, sans doute, d'ici à quelque temps, de développer devant l'Académie ces recherches dans toute leur étendue, je vais communiquer aujourd'hui quelques-uns de ces résultats, dont le sens et la portée pourront être compris sans de plus amples explications.

J'ai déjà indiqué, dans le *Compte rendu* d'octobre 1857 (*), quelques propriétés de l'équation dont les racines sont les divers modules pour lesquels a lieu une multiplication des fonctions elliptiques par $\sqrt{-n}$. J'y ai mentionné ce fait, que

(*) Une traduction de cette Note a été insérée dans le *Journal de M. Liouville*, 2e série, t. III, p. 265. (*Note du traducteur.*)

cette équation se décompose en facteurs correspondants aux divers ordres de formes quadratiques qui appartiennent au déterminant $-n$, et que le facteur qui répond à l'ordre proprement primitif est décomposable à son tour en six facteurs, de degrés égaux, dont les coefficients ne renferment que des nombres entiers avec le radical $\sqrt{n}$, et dont le degré commun est précisément égal au nombre total des classes de formes proprement primitives de déterminant $-n$. L'étude spéciale de ces équations partielles fournit encore une décomposition ultérieure de ces équations en d'autres, qui correspondent à chacune des *espèces* de formes quadratiques; et, par là, la division des classes en genres, déjà si importante pour la pure théorie des nombres (*Disquis. arithm.*, art. 227), se trouve encore appelée, de la manière la plus surprenante, à jouer son rôle dans une autre branche des Mathématiques, qui appartient aussi bien à l'Algèbre qu'à l'Analyse. Le but principal de la présente Note est d'expliquer brièvement le caractère essentiel de cette décomposition des équations.

Soient n un nombre positif impair, plus grand que 3, et N le nombre des classes de formes proprement primitives de déterminant $-n$. Donnons, de plus, aux lettres $\varkappa$ et q la signification qu'elles ont habituellement dans la théorie des fonctions elliptiques, et posons $\varkappa^2 = k$. Il y a 6N valeurs différentes de k, pour lesquelles la multiplication complexe par $\sqrt{-n}$ a lieu, et qui correspondent à l'ordre proprement primitif des formes quadratiques de déterminant $-n$. Ces valeurs se partagent en trois groupes de 2N chacun, les valeurs d'un même groupe étant racines d'une seule et même équation à coefficients numériques rationnels; et si, dans les trois équations correspondantes, de degré 2N, on rend tous les coefficients *entiers*, alors, dans l'une d'elles, le premier et le dernier coefficient seront égaux tous les deux à l'unité, tandis que, dans l'une des deux autres équations, le premier coefficient étant 1, le dernier sera une puissance de 2, l'inverse ayant lieu pour la troisième équation. L'une de ces trois équations a pour racine la valeur connue de k qui répond à

$$q = e^{-\pi\sqrt{n}}.$$

Soient maintenant $p_1, p_2, p_3, \ldots, p_\nu$ les divers facteurs premiers du nombre n. L'équation en question, de degré 2N, se décomposera, par l'introduction de $\sqrt{p_1}$, $\sqrt{p_2}, \ldots, \sqrt{p_\nu}$, en 2^ν facteurs, dont chacun sera du degré

$$\left(\frac{1}{2}\right)^{\nu-1} \mathrm{N}.$$

Le degré de chacune de ces équations partielles sera donc, suivant que l'on aura

$$n \equiv 3 \quad \text{ou} \quad \equiv 1, \quad \text{mod. } 4,$$

égal au *nombre* ou au *double du nombre* des formes quadratiques de déterminant $-n$, contenues dans un genre. Dans le second de ces deux cas, pour chaque valeur de k que donne l'équation, elle admet aussi la racine $1-k$; de sorte qu'il existe des équations en $k(1-k)$, dont le degré est encore égal à une fois le nombre des classes appartenant à un genre. On peut donc formuler notre résultat comme il suit :

Les modules singuliers pour lesquels a lieu la multiplication complexe par $\sqrt{-n}$ *sont déterminés par des équations en k ou en* $k(1-k)$, *suivant que n est* $\equiv 3$ *ou* $\equiv 1$ *par rapport au module* 4; *les coefficients de ces équations sont formés rationnellement au moyen des racines carrées des divers facteurs premiers de n, et leur degré est précisément égal au nombre des classes de formes proprement primitives, de déterminant* $-n$, *appartenant à un seul et même genre.*

Cette nouvelle décomposition des équations d'où dépendent ces modules singuliers des fonctions elliptiques n'est pas seulement de la plus haute importance par la lumière qu'elle jette sur la nature de ces modules eux-mêmes, mais encore elle complète les applications, que j'ai rappelées plus haut, de la théorie des fonctions elliptiques aux formes quadratiques, les théorèmes arithmétiques relatifs à la division en genres devant être tirés désormais des recherches analytiques en question. Il existe, en effet, une dépendance mutuelle parfaite entre ces équations partielles et les diverses espèces de formes quadratiques, de telle sorte qu'à chaque genre correspond une équation partielle déterminée, et à chaque classe de formes quadratiques renfermée dans ce genre, une racine déterminée de cette équation. Au genre principal, par exemple, correspond l'équation partielle qui admet pour racine la valeur de k ou de $k(1-k)$ relative à $q=e^{-\pi\sqrt{n}}$, et l'on en déduit les équations partielles correspondantes aux autres genres, en changeant, d'après les caractères propres à ces genres, les signes des racines carrées de $p_1, p_2, \ldots, p_\nu$, qui entrent dans les coefficients. Il faut observer cependant que, pour $n=4m+3$, il n'existe point de caractère suivant le module 4, et que par suite, dans ce cas, il manque *une* détermination pour les changements de signes. Cette détermination se trouve remplacée par cette règle, que le changement de $+\sqrt{n}$ en $-\sqrt{n}$ doit se faire en même temps que celui de k en $1-k$. On obtient d'ailleurs des résultats tout à fait analogues pour les valeurs *paires* de n, et afin d'éclaircir par quelques exemples la décomposition des équations pour les diverses sortes de valeurs

$$n \equiv 1,\ 2,\ 3,\ \text{mod. } 4,$$

je donnerai ici les déterminations relatives aux modules qui correspondent à la multiplication complexe par $\sqrt{-n}$. J'ai choisi à dessein, pour n, des valeurs des natures les plus diverses, parmi lesquelles il se trouve aussi bien des nombres pre-

miers que des nombres composés, et, parmi ces derniers, des nombres contenant un facteur carré.

1° $n \equiv 2$, mod. 4.

Pour $n = 6$, $k = (1+\sqrt{2})^2(1+\sqrt{2}+\sqrt{6})^2$,

$n = 10$, $k = (1+\sqrt{2})^4(3+\sqrt{10})^2$.

2° $n \equiv 3$, mod. 4.

Pour $n = 15$, $2^5(2k-1) = \sqrt{3}(7+\sqrt{5})$,

$n = 39$, $2^7(2k-1)^2 + 2^4\sqrt{3}(7+2\sqrt{13})(2k-1) + 21(5+3\sqrt{13}) = 0$,

$n = 63$, $2^7(2k-1)^2 + 8(7\sqrt{3}+9\sqrt{7})(2k-1) + \sqrt{3}(155\sqrt{3}+109\sqrt{7}) = 0$.

3° $n \equiv 1$, mod. 4.

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

$n = 13$, $4k(1-k) = (18+5\sqrt{13})^2$,

$n = 21$, $4k(1-k) = (8+3\sqrt{7})^2(3\sqrt{3}+2\sqrt{7})^2$,

$n = 37$, $4k(1-k) = (6+\sqrt{37})^6$,

$n = 49$, $2\varkappa\varkappa' + 4(11+4\sqrt{7})\sqrt{\varkappa\varkappa'} + 1 = 0$;

$n = 105$, $4k(1-k) = (3\alpha-2\gamma)^4(5+9\alpha+16\beta+4\gamma+7\beta\gamma+12\alpha\beta+3\alpha\beta\gamma)^2$,

α, β, γ désignant respectivement les racines carrées des trois facteurs premiers de 105, c'est-à-dire $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$. Dans la valeur de k, donnée pour $n = 21$, le signe $+$ de $\sqrt{3}$ et le signe $-$ de $\sqrt{7}$ correspondent au genre principal, c'est-à-dire à la détermination $a = 1$ dans la relation

$$\frac{1}{\pi i}\log q = \frac{b+\sqrt{-21}}{a},$$

et en général, pour les quatre valeurs de $k(1-k)$, les déterminations des signes de $\sqrt{3}$ et de $\sqrt{7}$ se déduisent respectivement des signes de Legendre $\left(\frac{3}{a}\right)$, $\left(\frac{7}{a}\right)$, en désignant par $\sqrt{3}$ la valeur positive et par $\sqrt{7}$ la valeur négative. De même, pour $n = 105$, on mettra, dans l'expression de $k(1-k)$, pour α, β, γ, les valeurs négatives de $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, si l'on veut avoir la valeur de cette expression correspondante à $a = 1$. En désignant ces valeurs négatives par α', β', γ', on devra prendre alors, pour un nombre quelconque a,

$$\alpha = \left(\frac{3}{a}\right)\alpha', \quad \beta = \left(\frac{5}{a}\right)\beta', \quad \gamma = \left(\frac{7}{a}\right)\gamma'.$$

Dans les cas de $n = 21, 37, 105$, le calcul des valeurs des modules par les méthodes algébriques ne serait guère praticable. J'ai obtenu ces valeurs par une tout autre marche, après avoir préalablement trouvé la forme du résultat par la théorie. La décomposition des équations, que j'ai exposée ci-dessus, fournit un moyen d'arriver aux valeurs des modules par un calcul assez simple, surtout lorsque le nombre des classes appartenant à un même genre n'est pas trop considérable. Ainsi, dans le cas de $n = 21$, par exemple, des quatre valeurs de $\frac{1}{\pi i}\log q$, connues *à priori*, j'ai tiré les valeurs correspondantes de $2\varkappa\varkappa'$, calculées avec un petit nombre de décimales seulement; j'ai identifié ces valeurs, d'après ce que nous venons de voir, avec une expression de la forme

$$A \pm B\sqrt{3} \pm C\sqrt{7} \pm D\sqrt{21},$$

et j'en ai conclu facilement les valeurs, en nombres entiers, de A, B, C, D. La nouvelle méthode que j'indique ici pour le calcul des modules pour lesquels a lieu la division complexe, et des coefficients des équations d'où dépendent ces modules, peut encore s'appliquer pratiquement à des valeurs de n plus grandes que 105; je me propose de faire construire, par ce moyen, un tableau pour les nombres consécutifs $n = 1, 2, 3, \ldots$, et de prolonger ce tableau aussi loin que possible.

Une des questions les plus difficiles qui se soient présentées à moi au sujet de ces mêmes équations particlles est celle qui est relative à leur irréductibilité. Pour des valeurs particulières du nombre n, l'irréductibilité de ces équations est facile à établir; mais pour arriver à une démonstration générale de cette propriété, les méthodes connues et employées jusqu'à présent ne suffisent plus. Cela tient à une circonstance tout à fait singulière qui se rencontre dans les équations en question, et qui prouve encore une fois, comme je l'ai souvent répété, que les progrès de l'Algèbre et de ses méthodes ont toujours pour occasion des questions relatives à des équations fournies par les autres branches des Mathématiques, et, si je puis m'exprimer ainsi, ils sont causés par la diversité des phénomènes algébriques que présente l'Analyse dans ses développements successifs.

Les méthodes par lesquelles on a démontré jusqu'ici l'irréductibilité des équations à coefficients numériques s'appuient presque toutes sur la nature des facteurs premiers essentiels contenus dans le discriminant. Mais les discriminants des équations partielles d'où dépendent les modules correspondants à la multiplication par $\sqrt{-n}$ ne contiennent, à quelques exceptions près, aucuns nombres premiers comme facteurs essentiels, mais seulement des unités. Ce n'est, il est vrai, que par induction que j'ai trouvé cette propriété remarquable de ces équations, et je n'ai pu encore la démontrer généralement; mais ce que je venais de constater suffisait

déjà pour me faire renoncer à l'emploi des méthodes ordinaires, et pour me faire rechercher d'autres moyens de démonstration pour l'irréductibilité des équations en question. J'y suis effectivement parvenu, après avoir déterminé, à l'aide des principes de Dirichlet, le nombre de classes des nombres complexes formés avec ces modules. Par cette méthode, ce n'est plus, comme dans les cas habituels, au commencement, mais seulement à la fin de la théorie arithmétique, que se trouve démontrée l'irréductibilité de l'équation qui sert de point de départ, et l'on obtient en même temps la démonstration de cette autre proposition, liée étroitement à la précédente, que toute forme quadratique proprement primitive de déterminant négatif peut représenter une infinité de nombres premiers.

La théorie des nombres complexes dont je viens de parler, et dont j'ai achevé de traiter la plus grande partie, renferme, comme cas particulier, la théorie des formes quadratiques à coefficients complexes, $a + b\sqrt{-n}$, et ainsi, entre autres résultats, se trouve rétabli ce qui, selon toute probabilité, devait former le contenu de la seconde partie, non publiée, du Mémoire de Dirichlet sur les nombres $a + b\sqrt{-1}$ (*Journal de Crelle*, t. XXIV). Cette théorie des nombres complexes renferme encore, comme autre cas particulier, la théorie des nombres formés par l'extraction de la racine carrée des nombres entiers. Je ne saurais entrer dans plus de détails sur les résultats arithmétiques obtenus, sans m'écarter du but de cette courte Note; mais je ne puis passer sous silence une conséquence *algébrique* que l'on tire de la décomposition des équations en k et en $k(1-k)$, indiquée plus haut. L'*affection* des équations partielles, dont les coefficients renferment les racines carrées des divers facteurs premiers de n, a, pour toute valeur du nombre n, une relation très-simple avec la régularité du déterminant correspondant, relation que, dans ma Note d'octobre 1857, je n'ai pu indiquer que pour le cas où n est un nombre premier. Le nombre des différentes périodes des racines est précisément égal à l'exposant de l'irrégularité, et l'équation partielle elle-même, dans le cas où le déterminant $-n$ est régulier, devient une équation abélienne, en ce sens que les fonctions cycliques de ses racines sont des fonctions rationnelles de $\sqrt{-1}$ et des racines carrées des divers facteurs premiers du nombre n. On aperçoit ici quelle est encore, sous ce nouveau point de vue, la signification de la décomposition ultérieure des équations qui déterminaient primitivement ces modules singuliers des fonctions elliptiques; et je vais maintenant, pour terminer, indiquer brièvement la méthode qui m'a conduit à ce résultat, et dont la découverte m'a présenté assez de difficultés.

Le principe que j'ai appliqué est celui-là même qui m'avait déjà servi à séparer les modules d'après les différents déterminants des formes quadratiques correspondantes, et à établir généralement les équations de degré N, mentionnées ci-dessus, dont les coefficients ne renferment que $\sqrt{n}$, et dont les racines sont toutes expri-

mables en fonctions rationnelles d'une seule d'entre elles et de coefficients entiers de la forme $a + bi$. Dans l'équation

$$\varphi(\mu, k) = 0,$$

à laquelle satisfont les divers multiplicateurs de la transformation du $n^{ième}$ ordre, et dont les coefficients sont des fonctions de nombres entiers et de $\varkappa^2 = k$, remplaçons le multiplicateur μ par la valeur $\sqrt{n}$. Comme l'équation modulaire de la transformation du $n^{ième}$ ordre,

$$\psi(\lambda^2, \varkappa^2) = 0,$$

devient, par la substitution de la valeur $\lambda^2 = 1 - \varkappa^2$, l'équation

$$\psi(1 - k, k) = 0,$$

qui donne les valeurs de k pour lesquelles a lieu la multiplication par $\sqrt{-n}$, le facteur commun aux deux fonctions $\varphi(\sqrt{n}, k)$ et $\psi(1 - k, k)$ contiendra précisément les valeurs de k pour lesquelles le multiplicateur est égal à $\sqrt{n}$. Toutes ces quantités k sont donc liées entre elles par une équation dont les coefficients renferment $\sqrt{n}$, et non-seulement on isole, de cette manière, les valeurs de k correspondantes aux formes quadratiques de déterminant $-n$, mais encore on sépare l'une de l'autre, pour $n \equiv 3$, mod. 4, les deux espèces de couples de modules complémentaires, et pour $n \equiv 1$, mod. 4, les deux espèces de modules pour lesquelles les formes quadratiques correspondantes se distinguent entre elles par leur caractère relatif au nombre 4.

Pour parvenir à la séparation générale des genres, et par suite à celle des formes quadratiques de caractère opposé par rapport à un nombre premier p, facteur de n, il s'agissait maintenant d'établir une équation en k, dont les coefficients continssent la racine carrée de p, et cela de telle manière que le signe de cette racine fût déterminé par le caractère des formes correspondantes aux diverses valeurs de k. Pour obtenir une semblable équation, on fera usage des considérations suivantes. En désignant par p un nombre premier impair, et par λ un des modules qui se déduisent de k par une transformation d'ordre p, et posant de plus $\varkappa^2 = k$, $\lambda^2 = l$, il existe, comme on sait, entre l et k, une équation de degré $p + 1$, à coefficients numériques entiers. La racine carrée du discriminant de cette équation est, comme on le voit aisément, une fonction de k à coefficients entiers, multipliée par $\sqrt{\pm p}$, où l'on doit prendre le signe supérieur ou le signe inférieur, suivant que l'on a $p \equiv 1$ ou $\equiv 3$, mod. 4. D'après cela, pour l'équation de degré p, dont les racines sont p des modules transformés, savoir, $l_0, l_1, \ldots, l_{p-1}$, et dont les coefficients sont des fonctions rationnelles du $(p+1)^{ième}$ module trans-

formé l' et de k, la racine carrée du discriminant, abstraction faite du facteur $\sqrt{\pm p}$, deviendra une fonction rationnelle de k et de l', de sorte qu'il existe une relation de la forme

$$\Pi(l_r - l_s) = \sqrt{\pm p}.f(k, l').$$

Si l'on prend pour la valeur de k une de celles pour lesquelles a lieu la multiplication complexe par $\sqrt{-n}$, et que l'on ait $n \equiv 0$, mod. p, alors, parmi les $p+1$ valeurs de l, il y en aura une, et *une seule*, qui fera également partie de ces mêmes valeurs. En la désignant par l', l' pourra être mise sous la forme d'une fonction rationnelle de k et de $\sqrt{n}$, et l'équation en $l_0, l_1, \ldots, l_{p-1}$ sera telle, que ses coefficients contiendront rationnellement les seules quantités k et $\sqrt{n}$. Cette équation est maintenant, dans le sens relatif, une équation abélienne, comme cela ressort immédiatement de ce qui a été dit plus haut, en ayant égard à ce que les racines donnent en même temps des valeurs du module pour la multiplication par $\sqrt{-np^2}$. Donc chacun des $\frac{1}{2}(p-1)$ produits

$$(l_0 - l_m)(l_1 - l_{m+1}) \ldots (l_{p-1} - l_{m-1})$$

est une fonction rationnelle des quantités k, $\sqrt{n}$ et $\sqrt{-1}$. De là résulte aussi, en s'appuyant sur la forme du discriminant indiquée plus haut, une équation en k dont les coefficients, outre $\sqrt{n}$ et $\sqrt{-1}$, contiennent $\sqrt{\pm p}$, et, en l'étudiant de plus près, on reconnaît que *la même* équation continue de subsister pour toutes les valeurs de k correspondantes à la multiplication par $\sqrt{-n}$, de telle sorte toutefois que, pour la moitié de ces valeurs, il faut changer le signe du produit Π, et par suite celui de $\sqrt{\pm p}$. Ce changement lui-même dépend du caractère par rapport à p de la forme relative au module correspondant, si bien que, pour les valeurs de k auxquelles répond un même caractère des formes corrélatives de déterminant $-n$, il faut conserver à $\sqrt{\pm p}$ le même signe, et, pour les autres valeurs, remplacer ce signe par son opposé. Alors il ne reste plus qu'à faire voir, par des considérations simples, que la racine carrée de -1 disparaît des coefficients de l'équation en k, pour en conclure la forme que nous avons indiquée pour les équations partielles qui représentent séparément chaque genre de formes quadratiques. Le développement spécial de la méthode en question est seulement rendu un peu long par la nécessité où l'on est, pour démontrer la vérité de l'équation, d'employer la composition des formes quadratiques pour toutes les valeurs de k ou pour la moitié de ces valeurs. Cependant la théorie de la multiplication complexe fournit pour cet objet quelques points de vue simples et nouveaux, comme je le ferai voir dans la suite, en exposant complétement cette théorie.