RECHERCHES SUR DIVERSES APPLICATIONS DE L'ANALYSE INFINITÉSIMALE A LA THÉORIE DES NOMBRES.

En m'occupant, il y a deux ans*), à prouver que toute progression arithmétique indéfinie dont les termes n'ont pas tous un même diviseur commun, renferme une infinité de nombres premiers, ce qui n'avait pas encore été fait d'une manière rigoureuse, j'ai été conduit à envisager un grand nombre de questions relatives aux nombres, sous un point de vue entièrement nouveau, et qui les rattache aux principes de l'analyse infinitésimale et aux propriétés remarquables d'une classe de séries et de produits infinis qui ont beaucoup d'analogie avec les expressions que l'illustre EULER a considérées dans le chapitre de son Introduction à l'analyse de l'infini, ayant pour titre „De seriebus ex evolutione factorum ortis." Dans une note insérée dans le Journal de CRELLE**), j'ai déjà indiqué plusieurs des questions auxquelles ce genre d'analyse peut être appliqué. Je me propose maintenant d'exposer mes recherches sur cette matière avec tous les développements nécessaires, dans une suite de mémoires dont celui que je soumets aujourd'hui au jugement des géomètres, sera particulièrement destiné à l'examen d'une question dont la solution n'avait pas encore été donnée, et qui a pour objet de déterminer le nombre des formes quadratiques différentes dont le déterminant D est un entier quelconque positif ou négatif, ou ce qui est la même chose, le nombre des diviseurs quadratiques qui appartiennent à l'expression $x^2 - Dy^2$. L'analyse qui nous conduira à la solution complète de cette question intéressante, nous fournira en même temps et pour ainsi dire, chemin faisant, des démonstrations nouvelles et très simples de plusieurs beaux théorèmes dus à M. GAUSS, mais que cet illustre géomètre

*) Le mémoire que j'ai lu sur cette question à l'Académie de Berlin, vient d'être imprimé dans la collection de l'Académie, année 1837.[1])

**) Tome XVIII. p. 259.[2])

[1]) S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. [2]) S. 357 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

n'avait établis qu'au moyen de considérations très compliquées dans la seconde partie de la 5ième section de ses Disquisitiones arithmeticae.

Cette section de l'ouvrage de M. GAUSS, qui est consacrée à la théorie des formes du second degré, se compose de deux parties très distinctes, dont la première, qui se termine à l'art. 223, peut être considérée comme l'exposition de la partie élémentaire de cette théorie, et renferme tous les résultats antérieurement donnés par EULER, LAGRANGE et LEGENDRE, complétés et étendus à beaucoup d'égards et déduits d'ailleurs de principes nouveaux. La seconde partie qui commence, à proprement parler, à l'art. 234, (les art. 223—233 contenant des définitions et des lemmes qui servent d'introduction à la seconde partie) se compose presque exclusivement de recherches propres à l'illustre auteur. Ces recherches, aussi remarquables par la profondeur des méthodes que par le nombre et la variété des résultats, forment sans contredit la partie de tout l'ouvrage dont l'étude présente le plus de difficultés. Aussi sont-elles très peu connues des géomètres, et l'on doit y rapporter particulièrement ce que LEGENDRE dit dans la préface de la seconde édition de sa Théorie des Nombres, lorsqu'après avoir indiqué les découvertes de M. GAUSS qu'il avait fait entrer dans son ouvrage, il ajoute:

„On aurait désiré enrichir cet Essai d'un plus grand nombre des excellents matériaux qui composent l'ouvrage de M. GAUSS: mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très étendus, et sans s'assujettir au simple rôle de traducteur, profiter de ses autres découvertes."

J'ose donc espérer qu'indépendamment des résultats nouveaux qu'il fait connaître, mon travail pourra encore contribuer à l'avancement de la science, en établissant sur de nouvelles bases et en rapprochant des éléments, de belles et importantes théories qui n'ont été jusqu'à présent à la portée que du petit nombre de géomètres capables de la contention d'esprit nécessaire pour ne pas perdre le fil des idées dans une longue suite de calculs et de raisonnements très composés.

§. 1.

Les lettres k et ϱ désignant deux quantités positives, la première constante, la seconde variable, considérons la somme de la série infinie:

$$(1) \qquad \frac{1}{k^{1+\varrho}} + \frac{1}{(k+1)^{1+\varrho}} + \frac{1}{(k+2)^{1+\varrho}} + \cdots$$

Cette somme croissant au delà de toute limite finie, lorsque la variable ϱ devient infiniment petite, voyons quelle est la fonction de ϱ la plus simple qui puisse servir de mesure à cette augmentation, ou en d'autres termes, dont le rapport à l'expression précédente converge vers l'unité, lorsque ϱ convergera vers zéro. Pour cela, nous aurons recours à la formule connue:

$$\int_0^1 x^{k-1} \log^{\varrho}\left(\frac{1}{x}\right) dx = \frac{\Gamma(1+\varrho)}{k^{1+\varrho}}.$$

En mettant successivement k, $k+1$, $k+2$, ... à la place de k et faisant la somme de toutes ces équations, la série (1) se trouvera exprimée comme il suit:

$$\frac{1}{\Gamma(1+\varrho)} \int_0^1 \frac{x^{k-1}}{1-x} \log^{\varrho}\left(\frac{1}{x}\right) dx.$$

Si l'on ajoute $\frac{1}{\varrho}$ à cette expression et que l'on en retranche la quantité égale:

$$\frac{\Gamma(\varrho)}{\Gamma(1+\varrho)} = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\varrho-1}\left(\frac{1}{x}\right) dx,$$

elle deviendra:

$$\frac{1}{\varrho} + \frac{1}{\Gamma(1+\varrho)} \int_0^1 \left[\frac{x^{k-1}}{1-x} - \frac{1}{\log\left(\frac{1}{x}\right)}\right] \log^{\varrho}\left(\frac{1}{x}\right) dx.$$

Comme le second terme converge vers la limite finie:

$$\int_0^1 \left[\frac{x^{k-1}}{1-x} - \frac{1}{\log\left(\frac{1}{x}\right)}\right] dx,$$

k étant > 0, on conclut que le rapport de la somme (1) à la fraction $\frac{1}{\varrho}$ a l'unité pour limite, lorsque la variable positive ϱ devient moindre que toute grandeur donnée.

Au moyen du résultat précédent, il nous sera facile de démontrer le théorème suivant, dont nous ferons un usage très fréquent dans nos recherches.

„Soient:

$$(2) \qquad l_1, \; l_2, \; l_3, \; \ldots, \; l_n, \; \ldots$$

des constantes en nombre infini, positives, différentes de zéro, inégales ou en partie égales; soit encore $f(t)$ une fonction discontinue de la variable positive t, qui exprime combien il y a dans la suite (2) de termes dont la valeur ne surpasse pas celle de t. Cela posé, si la fonction $f(t)$ peut être mise sous

la forme:

$$f(t) = ct + t^{\gamma}\psi(t), \tag{3}$$

c et γ désignant des constantes positives dont la seconde est inférieure à l'unité, et la nouvelle fonction $\psi(t)$, abstraction faite de son signe et quelque grande qu'on y suppose la variable t, restant toujours moindre que la constante positive C, je dis que la somme:

$$\varphi(\varrho) = \frac{1}{l_1^{1+\varrho}} + \frac{1}{l_2^{1+\varrho}} + \frac{1}{l_3^{1+\varrho}} + \cdots, \tag{4}$$

dans laquelle ϱ désigne une variable positive, sera telle qu'on aura pour une valeur infiniment petite de ϱ:

$$\varphi(\varrho) = \frac{c}{\varrho}, \tag{5}$$

c'est-à-dire que le rapport de la somme $\varphi(\varrho)$ à la fraction $\frac{c}{\varrho}$ convergera vers l'unité, lorsque ϱ devient moindre que toute grandeur donnée."

Le nombre des termes de la suite (2) qui ne surpassent pas l'unité, est limité (ce nombre étant égal à $c+\psi(1)$), et comme parmi ces termes il n'y en a aucun dont la valeur soit zéro, il est évident par la nature de la proposition qu'il s'agit d'établir, que nous pouvons omettre la partie de l'expression $\varphi(\varrho)$, qui correspond à ces termes. Ce qui reste après ce retranchement, étant toujours désigné par $\varphi(\varrho)$, choisissons une constante δ supérieure à $\frac{1}{1-\gamma}$, et partageons la somme $\varphi(\varrho)$ en une infinité de sommes partielles, en comprenant dans la $m^{\text{ième}}$ de ces sommes partielles tous les termes qui satisfont à la double condition:

$$m^{\delta} < l_n \leqq (m+1)^{\delta},$$

et par suite à celle-ci:

$$\frac{1}{m^{\delta(1+\varrho)}} > \frac{1}{l_n^{1+\varrho}} \geqq \frac{1}{(m+1)^{\delta(1+\varrho)}}.$$

Le nombre de ces termes sera évidemment:

$$f((m+1)^{\delta}) - f(m^{\delta}).$$

La valeur numérique de $t^{\gamma}\psi(t)$, lorsqu'on suppose successivement $t = m^{\delta}$ et $t = (m+1)^{\delta}$, étant inférieure à $C(m+1)^{\gamma\delta}$, on aura ces deux inégalités:

$$f((m+1)^{\delta}) - f(m^{\delta}) < c((m+1)^{\delta} - m^{\delta}) + 2C(m+1)^{\gamma\delta}$$
$$f((m+1)^{\delta}) - f(m^{\delta}) > c((m+1)^{\delta} - m^{\delta}) - 2C(m+1)^{\gamma\delta}.$$

En combinant ces inégalités avec celles que nous venons d'écrire, on conclura que la somme partielle dont il s'agit, est respectivement inférieure et supérieure aux quantités:

$$c\frac{(m+1)^{\delta} - m^{\delta}}{m^{\delta(1+\varrho)}} + 2C\frac{(m+1)^{\gamma\delta}}{m^{\delta(1+\varrho)}}, \quad c\frac{(m+1)^{\delta} - m^{\delta}}{(m+1)^{\delta(1+\varrho)}} - 2C\frac{(m+1)^{\gamma\delta}}{(m+1)^{\delta(1+\varrho)}}.$$

Il suit de là qu'on a:

$$\varphi(\varrho) < c\Sigma\frac{(m+1)^{\delta} - m^{\delta}}{m^{\delta(1+\varrho)}} + 2C\Sigma\frac{(m+1)^{\gamma\delta}}{m^{\delta(1+\varrho)}},$$

le signe Σ s'étendant depuis $m = 1$ jusqu'à $m = \infty$.

Puisqu'on a en vertu d'un théorème connu:

$$(m+1)^{\delta} - m^{\delta} = \delta m^{\delta-1} + \frac{\delta(\delta-1)}{2}(m+\varepsilon_m)^{\delta-2},$$

ε_m désignant une fraction positive, l'inégalité précédente pourra se mettre sous la forme:

$$\varphi(\varrho) < c\delta\Sigma\frac{1}{m^{1+\delta\varrho}} + \tfrac{1}{2}c\delta(\delta-1)\Sigma\left(1+\frac{\varepsilon_m}{m}\right)^{\delta}\frac{1}{m^{\delta\varrho}(m+\varepsilon_m)^2} + 2C\Sigma\left(1+\frac{1}{m}\right)^{\gamma\delta}\frac{1}{m^{\delta(1-\gamma)+\delta\varrho}}.$$

Or, ϱ devenant infiniment petit, les deux dernières sommes resteront finies, car elles seront constamment inférieures à celles-ci:

$$\Sigma\left(1+\frac{1}{m}\right)^{\delta}\frac{1}{m^2}, \quad \Sigma\left(1+\frac{1}{m}\right)^{\gamma\delta}\frac{1}{m^{\delta(1-\gamma)}},$$

qui le sont elles-mêmes, comme il est facile de le voir au moyen des principes connus, si l'on se rappelle que, d'après la supposition faite sur la constante δ, on a $\delta(1-\gamma) > 1$. Quant à la première somme, comme elle a une forme analogue à l'expression (1) considérée plus haut, elle sera évidemment $\frac{1}{\delta\varrho}$, ϱ étant supposé infiniment petit. On voit donc que la limite supérieure de $\varphi(\varrho)$ prend la forme $\frac{c}{\varrho}$, lorsque ϱ devient moindre que toute grandeur donnée, et comme le même raisonnement peut s'appliquer à la limite inférieure et conduit au même résultat, la proposition énoncée se trouve établie.

On pourrait donner au théorème que nous venons de démontrer, beaucoup plus d'étendue, mais comme ce théorème tel que nous l'avons énoncé, suffit aux applications que nous avons en vue, quant à présent, nous ne nous arrêterons pas à cette généralisation qui ne présente d'ailleurs aucune difficulté.

Nous aurons encore besoin de deux autres lemmes qui appartiennent, comme le précédent, à l'analyse infinitésimale. Le premier de ces nouveaux lemmes est tellement simple que nous nous contenterons de l'énoncer, sans en donner la démonstration qui est très facile à suppléer.

Tous les points d'un plan infini étant rapportés à deux axes rectangulaires des x et des y, concevons dans ce plan une courbe fermée assujettie ou non à une même loi analytique dans toutes ses parties, supposons que les dimensions de cette courbe augmentent de plus en plus et au-delà de toute limite, de manière cependant que la courbe variable reste toujours semblable à elle-même, et désignons par σ l'aire également variable à laquelle la courbe sert de contour.

Soient maintenant a, b, α, β quatre constantes dont les deux premières ont des valeurs positives, et supposons que l'on construise tous les points dont les coordonnées x et y ont la forme:

$$x = av+\alpha, \quad y = bw+\beta, \tag{6}$$

où v et w désignent tous les entiers depuis $-\infty$ jusqu'à ∞. Cela posé, si l'on désigne par $F(\sigma)$ le nombre de ces points situés dans l'intérieur de la courbe, on aura évidemment pour des valeurs infinies de σ:

$$F(\sigma) = \frac{1}{ab}\sigma,$$

c'est-à-dire que le rapport des deux membres de cette équation convergera vers l'unité lorsque σ croît au-delà de toute limite positive. Il est également facile de voir que la différence $F(\sigma)-\frac{\sigma}{ab}$ croîtra moins rapidement que la puissance σ^γ, l'exposant γ étant supposé $>\frac{1}{2}$. Nous pouvons donc poser:

$$F(\sigma) = \frac{1}{ab}\sigma+\sigma^\gamma\psi(\sigma), \tag{7}$$

où l'on a $\frac{1}{2}<\gamma<1$, et l'on sera assuré que la fonction $\psi(\sigma)$, abstraction faite de son signe, restera toujours moindre qu'une certaine constante finie C.

Le dernier des lemmes que nous emprunterons à l'analyse infinitésimale, se rapporte à la théorie des séries. On sait que les séries infinies convergentes sont de deux espèces très différentes, les séries de la première espèce étant convergentes indépendamment des signes dont leurs termes sont affectés; tandis que celles de la seconde ne jouissent de cette propriété que parce que les termes se détruisent en partie par l'opposition de leurs signes.

La convergence d'une série de la première espèce subsiste et sa somme conserve toujours la même valeur, quel que soit l'ordre que l'on établisse entre ses termes. Les séries de la seconde espèce se comportent d'une manière entièrement différente. Une série de cette espèce, convergente pour un certain arrangement de ses termes, peut perdre cette propriété lorsque cet ordre vient à être changé. Il peut arriver aussi que la série soit encore convergente après ce changement, mais que sa somme ait varié en même temps que l'ordre de ses termes. Ces remarques intimement liées à notre sujet, comme on le verra plus loin, ne sont pas sans importance pour d'autres recherches. Il en résulte par exemple et pour le dire en passant, que si l'on parvient à sommer une série qui appartient à la seconde espèce, et que l'on trouve pour la somme de la série une valeur entièrement déterminée, sans que l'ordre dans lequel les termes sont supposés se suivre, entre comme un élément essentiel dans l'analyse dont on fait usage, la méthode de sommation doit renfermer quelque vice caché, ou du moins a besoin d'être complétée par quelque considération qui indique clairement quel est l'arrangement des termes auquel la somme obtenue correspond.

Pour revenir à notre objet, soit s une variable positive et considérons la série dont le terme général est:

$$c_n \frac{1}{n^s},$$

l'entier n étant susceptible de toutes les valeurs depuis $n=1$ jusqu'à $n=\infty$. Si nous supposons que c_n, abstraction faite de son signe, et quel que soit l'indice n, soit toujours moindre que la constante C, notre série appartiendra à la première espèce tant que l'on aura $s>1$. En posant donc $s=1+\varrho$, ϱ étant une variable positive aussi petite que l'on voudra, la somme:

$$\psi(1+\varrho) = \Sigma c_n \frac{1}{n^{1+\varrho}}$$

aura une valeur unique et entièrement indépendante de l'arrangement de ses termes. Concevons maintenant qu'il s'agisse d'obtenir la limite vers laquelle la fonction $\psi(1+\varrho)$, évidemment continue tant que la variable ϱ reste positive, converge lorsque ϱ devient moindre que toute grandeur donnée, en supposant toutefois qu'une pareille limite existe, ce qui peut n'avoir pas lieu. D'après les remarques faites plus haut, on ne serait pas fondé à dire que cette limite

soit exprimée par:

$$\Sigma c_n \frac{1}{n},$$

l'ordre des termes étant arbitraire, car il est évident que cette dernière série appartient à la seconde espèce, et n'a par conséquent pas de somme déterminée.

Les suppositions énoncées plus haut étant conservées, soit k un entier positif, et concevons que c_n satisfasse à l'équation:

$$c_{n+k} = c_n, \tag{8}$$

ou en d'autres termes, que la suite:

$$c_1,\ c_2,\ \ldots,\ c_k;\quad c_{k+1},\ c_{k+2},\ \ldots,\ c_{2k};\quad c_{2k+1},\ \ldots$$

soit périodique, le nombre des termes qui composent une période étant égal à k. Supposons encore que la somme de ces termes soit zéro, c'est-à-dire que l'on ait:

$$c_1+c_2+\cdots+c_k = 0. \tag{9}$$

Cela étant, je dis que la somme:

$$\Sigma c_n \frac{1}{n^{1+\varrho}}$$

qui ne dépend pas de l'ordre des termes, converge vers une limite finie, donnée par l'expression:

$$\Sigma c_n \frac{1}{n},$$

où les termes sont supposés se suivre dans l'ordre naturel, c'est-à-dire de manière à ce que les valeurs de n croissent constamment depuis $n = 1$ jusqu'à $n = \infty$. Pour démontrer cette assertion, il suffira évidemment de faire voir que la série:

$$\Sigma c_n \frac{1}{n^s},$$

les termes étant rangés dans l'ordre indiqué, reste convergente et exprime une fonction continue de s, depuis $s = \infty$ jusqu'à $s = 1$ inclusivement. Or il est facile de prouver que cette double propriété subsiste non seulement entre les limites précédentes, mais plus généralement tant que s reste supérieur à zéro. En effet, h étant un entier positif quelconque, exprimons par une intégrale définie la somme des hk premiers termes de la série précédente. Au moyen de

la formule:

$$\int_0^1 x^{n-1}\log^{s-1}\left(\frac{1}{x}\right)dx = \frac{\Gamma(s)}{n^s},$$

et en ayant égard à l'équation (8), on trouvera pour cette somme:

$$\frac{1}{\Gamma(s)}\int_0^1 \frac{\Sigma c_n x^{n-1}}{1-x^k}\log^{s-1}\left(\frac{1}{x}\right)dx - \frac{1}{\Gamma(s)}\int_0^1 \frac{\Sigma c_n x^{n-1}}{1-x^k}x^{hk}\log^{s-1}\left(\frac{1}{x}\right)dx,$$

le signe sommatoire s'étendant depuis $n = 1$ jusqu'à $n = k$. Le polynôme $\Sigma c_n x^{n-1}$ étant divisible par $1-x$, comme on le voit par l'équation (9), la fraction algébrique sous le signe d'intégration reste finie. Soit K la plus grande valeur numérique de cette fraction depuis $x = 0$ jusqu'à $x = 1$; la seconde intégrale sera donc moindre que:

$$\frac{K}{\Gamma(s)}\int_0^1 x^{hk}\log^{s-1}\left(\frac{1}{x}\right)dx = \frac{K}{(hk+1)^s},$$

et s'évanouira pour $h = \infty$. Il résulte de là que la série prolongée à l'infini est convergente, et l'on voit avec la même facilité que sa somme exprimée par la première intégrale, est une fonction de s, qui varie d'une manière continue avec cette variable tant que l'on a $s > 0$.

§. 2.

p étant un nombre premier impair, positif ou négatif, et k un entier non-divisible par p, qui peut être aussi positif ou négatif, nous désignons avec LEGENDRE par $\left(\frac{k}{p}\right)$ l'unité prise avec le signe plus ou avec le signe moins, suivant que k sera ou ne sera pas résidu quadratique relativement à p. L'illustre auteur définit le symbole $\left(\frac{k}{p}\right)$ comme le reste que donne la puissance $k^{\frac{1}{2}(p-1)}$, lorsqu'on la divise par p; la définition précédente, quoique la même au fond, est préférable pour notre objet en ce qu'elle ne suppose pas que p soit un nombre positif. Si nous désignons par l un second entier non-divisible par p et par q un nombre premier impair dont la valeur numérique diffère de celle de p, on aura suivant la notation précédente:

$$(1)\quad \begin{cases} \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{kl}{p}\right), \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}, \\ \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}. \end{cases}$$

Ces équations qui renferment toute la théorie des résidus quadratiques, supposent de plus, la seconde que p est positif, la quatrième que p et q n'ont pas simultanément le signe négatif.

Les entiers k et P, positifs ou négatifs, n'ayant pas de diviseur commun, et le second P, que nous supposons impair, étant décomposé en ses facteurs simples $p, p', p'', \ldots$ égaux ou inégaux, de sorte que $P = pp'p''\ldots$, nous aurons souvent à distinguer si ceux des nombres premiers $p, p', p'', \ldots$ à l'égard desquels k est non-résidu quadratique, sont en nombre pair ou impair, ou ce qui est la même chose, si le produit:

$$\left(\frac{k}{p}\right)\left(\frac{k}{p'}\right)\left(\frac{k}{p''}\right)\ldots$$

a la valeur $+1$ ou -1. M. JACOBI a proposé d'étendre la notation de LEGENDRE à de semblables produits et d'écrire:

$$\left(\frac{k}{P}\right) = \left(\frac{k}{p}\right)\left(\frac{k}{p'}\right)\left(\frac{k}{p''}\right)\ldots$$

Comme cette généralisation de la notation de LEGENDRE, dont l'illustre géomètre que je viens de citer, a fait des applications ingénieuses*), est très propre à simplifier les formules et à abréger les démonstrations, nous l'adopterons dans ce qui suivra. On aura suivant cette notation:

$$(2)\quad \begin{cases} \left(\frac{k}{P}\right)\left(\frac{l}{P}\right) = \left(\frac{kl}{P}\right), \quad \left(\frac{k}{P}\right)\left(\frac{k}{Q}\right) = \left(\frac{k}{PQ}\right), \quad \left(\frac{-1}{P}\right) = (-1)^{\frac{1}{2}(P-1)}, \\ \left(\frac{2}{P}\right) = (-1)^{\frac{1}{4}(P^2-1)}, \quad \left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right)(-1)^{\frac{1}{4}(P-1)\cdot\frac{1}{2}(Q-1)}, \end{cases}$$

en supposant que les entiers k et l n'ont pas de diviseur commun avec les nombres impairs P et Q, que P est positif dans la troisième, et enfin que P et Q sont premiers entre eux et n'ont pas simultanément le signe négatif dans la dernière de ces équations. Toutes ces équations sont ou évidentes ou se déduisent facilement des relations (1), et il serait d'autant plus inutile de nous arrêter à les démontrer que les théorèmes qu'elles expriment se trouvent déjà, à la notation près, dans l'ouvrage de M. GAUSS art. 133. Pour éviter des distinctions inutiles il conviendra de ne pas exclure le cas où P dans le symbole $\left(\frac{k}{P}\right)$ a la valeur ± 1, en supposant $\left(\frac{k}{\pm 1}\right) = 1$. Il est évident que cette

*) Compte rendu des séances de l'Académie de Berlin, Oct. 1837.

nouvelle convention est compatible avec les équations précédentes, et qu'en l'adoptant, la troisième de ces équations se trouvera comprise dans la cinquième et répondra à $Q = -1$.

Nous terminerons ce paragraphe, en posant les équations évidentes qui suivent, et dans lesquelles k et l désignent des nombres impairs et ϑ la valeur ± 1:

$$(3)\quad \vartheta^{\frac{1}{2}(k-1)}\vartheta^{\frac{1}{2}(l-1)} = \vartheta^{\frac{1}{2}(kl-1)}, \quad \vartheta^{\frac{1}{2}(k^2-1)}\vartheta^{\frac{1}{2}(l^2-1)} = \vartheta^{\frac{1}{2}((kl)^2-1)}.$$

§. 3.

Nous avons maintenant à rappeler quelques résultats connus qui se rapportent à la théorie des formes quadratiques. En désignant par D un entier positif ou négatif (le cas de $D = 0$ sera excepté), nous appellerons avec M. GAUSS forme du déterminant D, toute expression comme:

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

a, b, c étant des entiers donnés, liés entre eux par la condition $b^2 - ac = D$, et x et y désignant des entiers indéterminés. Lorsque le déterminant D est un nombre négatif, les coefficients extrêmes seront toujours de même signe. Nous ne considérons, dans ce cas, que les formes pour lesquelles ce signe est $+$, c'est-à-dire les formes qui n'expriment que des nombres positifs. M. GAUSS range les formes qui appartiennent à un même déterminant en différents ordres, en comprenant dans un même ordre toutes celles pour lesquelles le plus grand diviseur commun de a, b, c a la même valeur. Nous supposerons toujours qu'un pareil diviseur n'existe pas ou plutôt qu'il est égal à l'unité, les autres cas pouvant être immédiatement ramenés à celui-ci. Les formes dont il s'agit et dont l'ensemble forme l'ordre appelé primitif, peuvent elles-mêmes présenter deux cas. Il peut arriver que a et c soient simultanément pairs ou que cette condition n'ait pas lieu. Dans le second de ces cas, les formes constituent ce que M. GAUSS appelle l'ordre proprement primitif, l'autre cas étant celui de l'ordre improprement primitif. Quand nous parlerons de formes quadratiques sans autre désignation, nous sous-entendrons toujours que ces formes appartiennent à l'ordre proprement primitif. On sait d'ailleurs que l'ordre improprement primitif n'existe que lorsqu'on a $D \equiv 1 \pmod 4$.

Deux formes:

$$ax^2+2bxy+cy^2, \quad a'x'^2+2b'x'y'+c'y'^2$$

étant telles que la première se change dans la seconde, au moyen de la sub-

stitution:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

où l'on a:

$$\alpha\delta - \beta\gamma = \pm 1,$$

sont dites équivalentes et cette équivalence est appelée propre ou impropre, suivant que le signe supérieur ou le signe inférieur a lieu. Cette distinction que M. GAUSS a introduite dans la théorie des formes quadratiques, et qui est analogue à celle que l'on fait en géométrie entre l'égalité par superposition et l'égalité par symétrie*), a beaucoup d'importance en ce qu'elle conserve à la théorie des formes du second degré une simplicité que cette théorie n'aurait pas, à beaucoup près, si l'on n'y avait pas égard. Nous n'aurons pas à considérer l'équivalence impropre; en disant donc simplement que deux formes sont équivalentes, nous sous-entendrons toujours qu'il s'agit de l'équivalence propre.

Les formes (positives et proprement primitives) dont le déterminant est un nombre donné D, et qui sont toujours en nombre infini, peuvent se distribuer en un nombre limité de classes, en plaçant deux formes dans la même classe ou dans des classes différentes suivant que ces formes sont ou ne sont pas équivalentes. Si l'on prend dans chaque classe l'une quelconque des formes qui la composent, on aura ce que nous appellerons le système complet des formes différentes, ou plus simplement, les formes différentes du déterminant D. Ce système étant construit, il est évident que toute forme dont le déterminant est D, aura toujours son équivalente et n'en aura qu'une dans ce système. Il est également facile de voir que si l'on construit un système semblable pour l'ordre des formes improprement primitives, ce nouveau système jouira de la même propriété relativement à toute forme qui appartient au même ordre.

Les formes différentes qui correspondent au déterminant quelconque D, sont divisées par M. GAUSS en genres, qui sont analogues à ce que LEGENDRE appelle groupes de diviseurs quadratiques. La différence qui existe à cet égard entre les illustres géomètres que je viens de citer, tient uniquement à ce que LEGENDRE exclut les déterminants qui ont des diviseurs carrés, ce que M. GAUSS

*) On peut consulter sur cette analogie remarquable un article que M. GAUSS a inséré dans les annonces littéraires de Gottingue et dans lequel l'illustre auteur, après avoir rendu compte d'un ouvrage de M. SERBER sur les formes quadratiques à trois indéterminées, entre dans des détails très intéressants, sur la manière dont on peut représenter géométriquement les propriétés des formes du second degré qui renferment deux ou trois entiers indéterminés.[1])

[1]) Gauss' Werke, Band II, S. 188—196. K.

ne fait pas et ce que nous ne ferons pas non plus, la considération des déterminants de cette espèce étant indispensable dans différentes recherches. Voici maintenant les principes très faciles à établir, sur lesquels repose la division en genres. (Disq. arithm. art. 229 et suivants.)

I. Si l est un nombre premier impair qui divise D, les entiers m, non-divisibles par l, qui peuvent être représentés par une même forme ayant D pour déterminant, sont ou tous tels que $\left(\frac{m}{l}\right) = 1$, ou tous tels que $\left(\frac{m}{l}\right) = -1$.

II. Lorsqu'on a $D \equiv 3 \pmod 4$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = -1$.

III. Lorsqu'on a $D \equiv 2 \pmod 8$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{8}(m^2-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{8}(m^2-1)} = -1$.

IV. Lorsqu'on a $D \equiv 6 \pmod 8$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1$.

V. Lorsqu'on a $D \equiv 4 \pmod 8$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = -1$.

VI. Lorsqu'on a $D \equiv 0 \pmod 8$, les nombres impairs m susceptibles d'être représentés par la même forme, sont tous exclusivement contenus dans l'une de ces quatre formes $8u+1$, 3, 5, 7, ou ce qui revient au même, on a à la fois $(-1)^{\frac{1}{2}(m-1)} = \pm 1$, $(-1)^{\frac{1}{8}(m^2-1)} = \pm 1$, chacun des deux signes ambigus restant invariable pour la même forme.

Toute propriété de la nature de celles exprimées dans les énoncés précédents, est ce que M. GAUSS appelle un caractère particulier de la forme à laquelle cette propriété appartient. C'est ainsi que les caractères particuliers de la forme $5x^2+4xy+14y^2$, dont le déterminant est $-66 = -2.3.11$, sont contenus dans les équations:

$$\left(\frac{m}{3}\right) = -1, \quad \left(\frac{m}{11}\right) = 1, \quad (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1.$$

L'ensemble des caractères particuliers d'une forme constitue son caractère complet, et la distribution des formes en genres consiste à rapporter au

même genre les formes qui ont le même caractère complet, et à des genres différents celles dont les caractères complets sont différents. Quant au nombre des genres différents, ou ce qui est la même chose, des caractères complets différents, il est, généralement parlant, moindre que celui des combinaisons que l'on peut former avec les caractères particuliers différents, puisqu'il existe toujours, à l'exception d'un cas singulier, une relation entre les caractères particuliers qui conviennent à la même forme quadratique, relation qui dérive des théorèmes (2) du paragraphe précédent. Pour voir en quoi consiste cette relation, soit S^2 le plus grand carré qui divise D, et désignons par P ou par $2P$ le quotient $\frac{D}{S^2}$, suivant qu'il est impair ou pair. Nous aurons donc selon ces deux cas:

$$D = PS^2, \quad \text{ou} \quad D = 2PS^2,$$

et le nombre impair P étant décomposé en ses facteurs simples p, p', p'', ...:

$$P = pp'p'' \ldots,$$

ces facteurs seront tous inégaux. Si nous considérons maintenant une forme quelconque, appartenant à l'ordre proprement primitif et ayant D pour déterminant, on pourra toujours attribuer aux indéterminées x et y des valeurs premières entre elles et telles que la valeur correspondante m de la forme soit positive, impaire et première à D. Cela étant, D sera résidu quadratique relativement à m et par suite aussi à l'égard de tous les facteurs simples de m. (Disq. arithm. art. 154.) On aura donc $\left(\frac{D}{m}\right) = 1$, et par conséquent suivant les deux cas que nous venons de distinguer:

$$\left(\frac{P}{m}\right) = 1, \quad \text{ou} \quad \left(\frac{2P}{m}\right) = \left(\frac{2}{m}\right)\left(\frac{P}{m}\right) = 1.$$

D'un autre côté, m étant positif, il résulte des équations (2) §. 2:

$$\left(\frac{P}{m}\right) = \left(\frac{m}{P}\right)(-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(m-1)}.$$

Si l'on remarque maintenant que la puissance $(-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(m-1)}$ est équivalente à 1, ou à $(-1)^{\frac{1}{2}(m-1)}$, suivant que $P \equiv 1$, ou $P \equiv 3 \pmod 4$, et que l'on écrive $\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\ldots$ à la place de $\left(\frac{m}{P}\right)$, et $(-1)^{\frac{1}{8}(m^2-1)}$ à la place de $\left(\frac{2}{m}\right)$, on aura ces résultats:

$$D = PS^2, \quad \begin{cases} P \equiv 1 \pmod 4, & \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = 1, \\ P \equiv 3 \pmod 4, & (-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = 1, \end{cases}$$

$$D = 2PS^2, \quad \begin{cases} P \equiv 1 \pmod 4, & (-1)^{\frac{1}{8}(m^2-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = 1, \\ P \equiv 3 \pmod 4, & (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = 1. \end{cases}$$

Quant aux caractères particuliers qui n'entrent pas dans ces relations, il n'existe aucune condition à leur égard, ou pour parler plus exactement et pour ne pas aller au delà de ce qui a été démontré, il ne résulte aucune condition qui les concerne, des théorèmes (2) §. 2 dont nous venons de faire usage. Au moyen des résultats précédents et des théorèmes énoncés plus haut, il sera facile de former le tableau suivant qui pourra servir dans chaque cas à faire l'énumération complète des genres différents qui répondent au déterminant D, et dans lequel:

$$r, \quad r', \quad r'', \quad \ldots$$

désignent les nombres premiers impairs inégaux qui divisent D sans diviser P.

Premier cas. $D = PS^2$, $P \equiv 1 \pmod 4$.

$S \equiv 1 \pmod 2$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$			$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$
$S \equiv 2 \pmod 4$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$		$(-1)^{\frac{1}{2}(m-1)}$,	$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$
$S \equiv 0 \pmod 4$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$	$(-1)^{\frac{1}{2}(m-1)}$,	$(-1)^{\frac{1}{8}(m^2-1)}$,	$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$

Second cas. $D = PS^2$, $P \equiv 3 \pmod 4$.

$S \equiv 1 \pmod 2$,	$(-1)^{\frac{1}{2}(m-1)}$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$		$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$
$S \equiv 2 \pmod 4$,	$(-1)^{\frac{1}{2}(m-1)}$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$		$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$
$S \equiv 0 \pmod 4$,	$(-1)^{\frac{1}{2}(m-1)}$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$	$(-1)^{\frac{1}{8}(m^2-1)}$,	$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$

Troisième cas. $D = 2PS^2$, $P \equiv 1 \pmod 4$.

$S \equiv 1 \pmod 2$,	$(-1)^{\frac{1}{8}(m^2-1)}$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$		$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$
$S \equiv 0 \pmod 2$,	$(-1)^{\frac{1}{8}(m^2-1)}$,	$\left(\frac{m}{p}\right)$,	$\left(\frac{m}{p'}\right)$,	$\ldots$	$(-1)^{\frac{1}{2}(m-1)}$,	$\left(\frac{m}{r}\right)$,	$\left(\frac{m}{r'}\right)$,	$\ldots$

Quatrième cas. $D = 2PS^2$, $P \equiv 3 \pmod 4$.

$S \equiv 1 \pmod 2$,	$(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}$, $\left(\frac{m}{p}\right)$, $\left(\frac{m}{p'}\right)$, ...	$\left(\frac{m}{r}\right)$, $\left(\frac{m}{r'}\right)$, ...
$S \equiv 0 \pmod 2$,	$(-1)^{\frac{1}{2}(m-1)}$, $(-1)^{\frac{1}{8}(m^2-1)}$, $\left(\frac{m}{p}\right)$, $\left(\frac{m}{p'}\right)$, ...	$\left(\frac{m}{r}\right)$, $\left(\frac{m}{r'}\right)$, ...

Pour énumérer les caractères complets, c'est-à-dire les genres différents pouvant avoir lieu pour un déterminant donné, il faudra écrire toutes les expressions qui forment la ligne horizontale relative au déterminant donné dans ce tableau, les unes à la suite des autres, après avoir égalé chaque expression à ± 1, et varier ensuite les signes ambigus de toutes les manières possibles, en s'assujettissant toutefois à la condition que les seconds membres de celles de ces équations qui répondent à la première partie de la ligne horizontale, doivent donner 1 pour produit, cette condition coïncidant avec celle dont la nécessité a été établie plus haut. Soit, par exemple, $D = 2.3.5^2$. Ce déterminant se rapportant à la première subdivision du quatrième cas, on aura ces 4 caractères complets:

$$(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = 1, \quad \left(\frac{m}{3}\right) = 1, \quad \left(\frac{m}{5}\right) = 1; \quad (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = 1, \quad \left(\frac{m}{3}\right) = 1, \quad \left(\frac{m}{5}\right) = -1;$$

$$(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1, \left(\frac{m}{3}\right) = -1, \left(\frac{m}{5}\right) = 1; \quad (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1, \left(\frac{m}{3}\right) = -1, \left(\frac{m}{5}\right) = -1.$$

Suivant la notation de M. Gauss, ces genres seraient caractérisés comme il suit:

1 et 3, 8; $R3$; $R5$: 1 et 3, 8; $R3$; $N5$;
5 et 7, 8; $N3$; $R5$: 5 et 7, 8; $N3$; $N5$.

Il importe de remarquer que les considérations précédentes ne prouvent nullement que les genres compatibles avec la condition énoncée, existent réellement; on peut en conclure seulement qu'il ne saurait y en avoir d'autres. Quant à la question de savoir 1°. si pour chaque déterminant il y a réellement des formes qui appartiennent à chacun des genres ainsi énumérés, et 2°. de quelle manière les formes différentes se distribuent entre les genres, qui ont une existence réelle, c'est une question très difficile qui forme l'un des principaux objets de la seconde partie de la 5ième section de l'ouvrage de M. Gauss, et dont nous donnerons aussi plus bas la solution au moyen de nos principes.

Nous ferons encore observer, avant d'aller plus loin, que si l'on désigne par λ le nombre des expressions contenues dans la même ligne horizontale du tableau précédent, le nombre des genres énumérés de la manière indiquée sera

évidemment exprimé par $2^{\lambda-1}$. Il n'y a qu'une seule exception à cette règle générale, exception qui a lieu lorsque la première partie de la ligne qui est assujettie à une condition dont l'effet est de réduire le nombre des combinaisons de moitié, n'existe pas. En jetant les yeux sur le tableau, on voit de suite que cela ne peut arriver que lorsque le déterminant se trouve compris dans le premier cas, et qu'en même temps P ne contient aucun facteur premier p, p', ... Comme l'on a alors d'une part $P \equiv 1 \pmod 4$ et de l'autre $P = \pm 1$, et par suite $P = 1$, on voit que ce cas n'a lieu que lorsque le déterminant est un carré positif, et que le nombre des genres est alors égal à 2^{λ}.

Tout ce qui précède, est relatif aux formes proprement primitives. Il nous reste à considérer le cas des formes appartenant à l'ordre improprement primitif, et qui ne peuvent représenter que des nombres pairs. Ce cas ne peut avoir lieu que lorsqu'on a $D \equiv 1 \pmod 4$, et par suite $P \equiv 1 \pmod 4$, $S \equiv 1 \pmod 2$. Si l'on désigne par m un entier positif, impair et premier à D, dont le double puisse être exprimé par une pareille forme, on formera sans peine le tableau qui suit, et dont l'usage est entièrement semblable à celui du tableau donné plus haut:

$D = PS^2$, $P \equiv 1 \pmod 4$, $S \equiv 1 \pmod 2$.

$$\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \ldots \mid \left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \ldots.$$

§. 4.

Nous avons maintenant à examiner sous quelles conditions et de combien de manières différentes un nombre m que je suppose positif, impair et premier à D, ou son double, peut être représenté par les formes du déterminant D, en supposant que les valeurs positives ou négatives que l'on attribuera à cet effet aux indéterminées x et y, doivent être premières entre elles. Pour qu'une telle représentation soit possible, il faut que D soit résidu quadratique relativement à m ou à $2m$ (Disq. arithm. 154), conditions dont la seconde ne diffère pas de la première. Or, pour que D soit résidu quadratique par rapport à m, il faut et il suffit qu'on ait pour chacun des diviseurs simples f de m (art. 105):

$$\left(\frac{D}{f}\right) = 1. \tag{1}$$

En supposant f positif, et distinguant comme dans le paragraphe précédent, les

quatre cas suivants que le déterminant D peut présenter:

$$D = PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod 4, \quad D = 2PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod 4,$$

la condition dont il s'agit, pourra être remplacée, en vertu des théorèmes (2) §. 2 et selon les quatre cas, par l'une de celles-ci:

$$(2) \quad \left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1)}\left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1)}\left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1)+\frac{1}{2}(f'-1)}\left(\frac{f}{P}\right) = 1.$$

Cela posé, soit:

$$(3) \qquad ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

le système complet des formes différentes (proprement primitives) ayant pour déterminant le nombre négatif D, et voyons combien de fois le nombre m dont tout diviseur simple f est supposé satisfaire à la condition (1), peut être représenté de la manière indiquée, par la totalité de ces formes. Si nous désignons par μ le nombre des diviseurs premiers inégaux f de m, la congruence:

$$z^2 \equiv D \pmod m$$

aura autant de racines différentes qu'il y aura d'unités dans la puissance 2^μ (art. 105). Soient:

$$l, \quad l', \quad l'', \quad \ldots$$

ces racines et cherchons, d'après les préceptes de l'art. 180, les représentations qui appartiennent à chacune de ces racines. Pour obtenir celles qui se rapportent à $z = l$, il faudra voir si parmi les formes (3) il y en a une qui soit équivalente à celle-ci:

$$mx^2+2lxy+\frac{l^2-D}{m}y^2.$$

Or, m étant impair et premier à D, cette dernière sera proprement primitive, et aura donc toujours son équivalente dans le système (3), par laquelle m pourra être représenté de deux manières. Le même raisonnement pouvant s'appliquer à toutes les autres racines l', l'', ..., on voit que m peut être représenté par la totalité des formes (3) d'autant de manières différentes qu'il y a d'unités dans la puissance $2^{\mu+1}$, deux représentations étant considérées comme différentes lorsqu'elles se font par des formes différentes ou lorsqu'ayant lieu par la même forme, et désignant par x, y et par x', y' les valeurs simultanées des indéterminées, on n'a pas à la fois $x = x'$, et $y = y'$.

Si le système complet (3) est celui de l'ordre improprement primitif, et si en même temps le nombre qu'il s'agit de représenter par ces formes, est

$2m$, on arrive à la même conclusion. Il suffit de remarquer que le nombre des racines de la congruence $z^2 \equiv D \pmod{2m}$ est également 2^μ, et que l'une quelconque de ces racines étant désignée par l, la forme:

$$2mx^2+2lxy+\frac{l^2-D}{2m}y^2$$

sera improprement primitive. C'est ce qui résulte de ce que m est impair et premier à D, et de ce que, l^2 et D étant de la forme $4\nu+1$, le coefficient de y^2 est pair. Nous avons donc ce théorème dans lequel les deux cas sont réunis dans le même énoncé:

Théorème I.

Soient:

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

les formes proprement (improprement) primitives différentes, ayant l'entier négatif D pour déterminant; soit encore m un nombre positif, impair et premier à D, dont tous les diviseurs simples f satisfont à celle des conditions (2), qui se rapporte au nombre donné D, et désignons par μ le nombre des facteurs simples inégaux de m. Cela posé, je dis que, si les indéterminées x et y sont assujetties à n'avoir pas de diviseur commun, l'entier m ($2m$) sera toujours représenté par la totalité de ces formes, d'autant de manières différentes qu'il y a d'unités dans la puissance $2^{\mu+1}$.

Remarque. Le théorème précédent est sujet à deux exceptions, dont la première a lieu lorsqu'on a $D = -1$, la seconde lorsqu'on a $D = -3$, et qu'il s'agit des formes de l'ordre improprement primitif. Il résulte de l'article déjà cité de l'ouvrage de M. Gauss, que le nombre des représentations est respectivement dans ces cas $2^{\mu+2}$ ou $3.2^{\mu+1}$.

Pour établir le théorème que nous allons énoncer, et qui se rapporte au cas où D est un nombre positif (*non-carré*)*), il n'y aura rien à changer aux considérations précédentes, si ce n'est qu'au lieu de s'appuyer sur l'art. 180 des Disq. arithm., il faudra recourir à l'art. 205 du même ouvrage. Pour réunir le cas des formes proprement primitives et celui des formes improprement primitives dans un énoncé commun, nous avons fait usage de la lettre ω, par laquelle il faut entendre le nombre 1 ou 2 selon ces deux cas.

*) Les formes dont le déterminant est un carré positif, et qui se décomposent toujours en deux facteurs linéaires, ne sont pas de véritables formes quadratiques. Par cette raison nous les exclurons toujours dans ce qui va suivre.

Théorème II.

Soient:

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

les formes proprement (improprement) primitives différentes ayant l'entier positif D pour déterminant; soit encore m un nombre positif, impair et premier à D, dont tous les facteurs simples f satisfont à celle des conditions (2) qui se rapporte au nombre donné D, et désignons par μ le nombre des facteurs simples inégaux de m. Cela posé, et les indéterminées x et y étant assujetties à n'avoir pas de diviseur commun, je dis que les représentations de ωm par la totalité de ces formes pourront toujours être distribuées en 2^μ groupes distincts, en comprenant dans un même groupe deux représentations telles que:

$$ax^2+2bxy+cy^2=\omega m, \quad ax'^2+2bx'y'+cy'^2=\omega m,$$

qui se font par la même forme quadratique, et dans lesquelles les valeurs x, y et x', y' des indéterminées sont liées entre elles par les équations:

$$x=\frac{1}{\omega}(x't-(bx'+cy')u), \quad y=\frac{1}{\omega}(y't+(ax'+by')u),$$

t et u désignant des entiers quelconques positifs ou négatifs tels qu'on ait:

$$t^2-Du^2=\omega^2. \tag{4}$$

[On peut remarquer que cet énoncé, si l'on y supprimait la condition que D doit être positif, resterait exact et comprendrait alors le théorème I avec ses deux exceptions. En effet, D étant supposé négatif, l'équation (4) n'a en général que ces deux solutions $t=\pm\omega$, $u=0$, ce qui donne deux représentations pour chaque groupe, de sorte que le nombre total des représentations, fini dans ce cas, devient $2^{\mu+1}$ comme dans le théorème I. Il n'y a exception que lorsqu'on a ou $D=-1$, $\omega=1$; ou $D=-3$, $\omega=2$, auxquels cas le nombre des solutions de l'équation (4) est respectivement 4 ou 6, ce qui s'accorde avec les exceptions indiquées plus haut. Mais tout en faisant remarquer ce que le cas de D positif et celui de D négatif ont de commun, comme sous d'autres rapports ces deux cas sont très différents et doivent être traités séparément, nous avons cru devoir donner deux énoncés distincts, pour pouvoir appliquer plus facilement les résultats précédents que nous aurons souvent à employer.]

Il est facile de voir que les représentations, ou ce qui est la même chose, les solutions de l'équation:

$$ax^2+2bxy+cy^2=\omega m, \tag{5}$$

qui appartiennent au même groupe, peuvent toujours se déduire toutes de l'une quelconque d'entre elles, $x=\alpha$, $y=\gamma$, au moyen des formules:

$$x=\frac{1}{\omega}(\alpha t-(b\alpha+c\gamma)u), \quad y=\frac{1}{\omega}(\gamma t+(a\alpha+b\gamma)u), \tag{6}$$

en attribuant à t et u toutes les valeurs entières, tant positives que négatives, qui satisfont à l'équation (4).

Nous allons faire voir maintenant qu'il existe certaines limites très simples entre lesquelles se trouve toujours comprise une de ces solutions en nombre infini, et entre lesquelles il ne saurait y en avoir plus d'une. Pour éviter des distinctions inutiles à notre objet, nous supposerons que dans chacune des formes données:

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

les coefficients de x^2 et de xy sont positifs, et que celui de y^2 est négatif. On s'assure facilement de la légitimité de cette supposition; il suffit de remarquer que parmi les formes qui composent une même classe, et entre lesquelles nous pouvons en choisir une à volonté, pour construire ce que nous avons appelé le système complet des formes différentes, il y en a toujours au moins une qui satisfait aux conditions énoncées. En effet, la période des formes réduites qui appartiennent à une classe donnée de déterminant positif, contient toujours au moins deux formes (Disq. arithm. art. 187), et il est évident que sur deux formes contiguës quelconques de cette période, il y en a toujours une qui est telle que:

$$a>0, \quad b>0, \quad c<0. \tag{7}$$

Ces conditions ayant lieu, il est facile de voir que parmi les solutions de l'équation (5), il ne saurait y en avoir aucune pour laquelle x soit zéro, puisqu'il résulterait de cette supposition: $cy^2=\omega m$, ce qui est impossible, c et m ayant des signes opposés. La valeur particulière α sera donc aussi différente de zéro, et nous remarquerons que cette valeur peut toujours être supposée positive. Cela résulte de ce que la solution $x=\alpha$, $y=\gamma$, qui sert de point de départ pour obtenir toutes celles qui appartiennent à un même groupe, peut être choisie à volonté dans ce groupe, et de ce que le groupe qui contient la solution $x=\alpha$, $y=\gamma$, renferme évidemment aussi celle-ci: $x=-\alpha$, $y=-\gamma$, cette dernière se déduisant par les formules (6) de la première, en supposant $t=-\omega$, $u=0$.

Les solutions, en nombre infini, qui forment un même groupe, et qui résultent des équations (6), peuvent se distribuer en deux groupes partiels dont le premier comprend toutes celles pour lesquelles on a $x > 0$, tandis que celles du second satisfont à la condition $x < 0$.

Nous allons maintenant faire voir que dans le premier de ces groupes partiels, les valeurs de y s'étendent depuis $-\infty$ jusqu'à ∞, sans que cette indéterminée puisse obtenir la même valeur dans deux solutions différentes, et que celle de ces solutions pour laquelle y a la plus petite valeur positive, différente de zéro, satisfait à des conditions d'inégalité très simples au moyen desquelles il est facile de la séparer de toutes les autres, et de réduire chaque groupe à une représentation unique, ce qui rendra le théorème II entièrement semblable au théorème I qui se rapporte aux déterminants négatifs. Pour remplir l'objet que nous avons en vue, nous observerons qu'il résulte de l'équation:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2 = \omega m,$$

mise sous la forme:

$$(b\alpha+c\gamma)^2-Da^2 = \omega cm,$$

et de ce que ωcm est négatif, qu'on a, abstraction faite des signes:

$$a\sqrt{D} > b\alpha+c\gamma,$$

et comme on a pareillement en vertu de l'équation (4):

$$\frac{t}{\omega} > \frac{u}{\omega}\sqrt{D},$$

on conclut, en faisant toujours abstraction des signes:

$$at > (b\alpha+c\gamma)u.$$

Il suit de là et de la supposition $\alpha > 0$, que pour embrasser toutes les représentations contenues dans les équations (6) pour lesquelles x a une valeur positive, on n'aura à faire usage que de celles des solutions de l'équation (4) dans lesquelles t a le signe plus. Or, il résulte d'un théorème connu que toutes les solutions qui remplissent cette condition, sont données par les formules:

$$t_n = \frac{\omega}{2}\left\{\left(\frac{T}{\omega}+\frac{U}{\omega}\sqrt{D}\right)^n+\left(\frac{T}{\omega}-\frac{U}{\omega}\sqrt{D}\right)^n\right\},$$
$$u_n = \frac{\omega}{2\sqrt{D}}\left\{\left(\frac{T}{\omega}+\frac{U}{\omega}\sqrt{D}\right)^n-\left(\frac{T}{\omega}-\frac{U}{\omega}\sqrt{D}\right)^n\right\},$$

dans lesquelles T et U désignent les plus petits nombres positifs (autres que

ω et 0) qui satisfont à l'équation (4), n devant être égalé successivement à tous les entiers depuis $-\infty$ jusqu'à ∞. On aura donc pour le groupe partiel dans lequel x est positif, en distinguant les différentes solutions de ce groupe par l'indice n, déjà employé dans les équations précédentes:

$$x_n = \frac{1}{\omega}(at_n-(ab+\gamma c)u_n), \quad y_n = \frac{1}{\omega}(\gamma t_n+(a\alpha+\gamma b)u_n).$$

En substituant les expressions de t_n, u_n, la seconde de ces équations deviendra:

$$y_n = \left(\frac{\gamma\sqrt{D}+a\alpha+\gamma b}{2\sqrt{D}}\right)\left(\frac{T}{\omega}+\frac{U}{\omega}\sqrt{D}\right)^n+\left(\frac{\gamma\sqrt{D}-a\alpha-\gamma b}{2\sqrt{D}}\right)\left(\frac{T}{\omega}-\frac{U}{\omega}\sqrt{D}\right)^n.$$

Il est facile de voir que les quantités:

$$\gamma\sqrt{D}+a\alpha+\gamma b, \quad \gamma\sqrt{D}-a\alpha-\gamma b$$

sont la première positive, la seconde négative. Pour s'en assurer il suffira de faire voir que $a\alpha+\gamma b$ est numériquement supérieur à $\gamma\sqrt{D}$ et positif. La première de ces assertions se prouve, en mettant l'équation:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2 = \omega m$$

sous la forme:

$$(a\alpha+\gamma b)^2-D\gamma^2 = \omega am,$$

et observant que le second membre est positif. Pour justifier la seconde assertion, on remarquera que, puisque la valeur numérique de $a\alpha+\gamma b$ surpasse celle de $\gamma\sqrt{D}$, elle surpassera *a fortiori* celle de γb, b étant $< \sqrt{D}$. De là et de ce que $a\alpha$ a le signe positif, on conclut que $a\alpha+\gamma b$ est également positif.

Comme en vertu de ce qui précède, les coefficients qui entrent dans l'expression de y_n, sont le premier positif, le second négatif, et que d'un autre côté, les quantités positives:

$$\frac{T}{\omega}+\frac{U}{\omega}\sqrt{D}, \quad \frac{T}{\omega}-\frac{U}{\omega}\sqrt{D},$$

dont le produit est 1, sont évidemment la première supérieure, la seconde inférieure à l'unité, on voit sans peine que chacun des deux termes dont se compose y_n, croît avec l'indice n. On aura donc, quel que soit cet indice:

$$y_n > y_{n-1},$$

ce qui prouve, comme nous l'avons avancé plus haut, que l'indéterminée y ne saurait obtenir deux fois la même valeur dans le groupe partiel où x est positif, et l'on voit également que y doit passer du négatif au positif, car on a

évidemment $y_{-\infty} = -\infty$, $y_{\infty} = \infty$. Pour obtenir la solution que nous avons en vue, et dans laquelle y_n a la plus petite valeur positive, différente de zéro, il faudra poser ces deux conditions:

$$y_n > 0, \quad y_{n-1} \geqq 0.$$

Si l'on observe qu'en vertu des expressions de x_n, y_n, t_n, u_n, données plus haut, on a la relation:

$$y_{n-1} = \frac{1}{\omega}(y_n T - (ax_n + by_n)U),$$

la seconde de ces conditions prendra cette autre forme:

$$(T - bU)y_n \leq aUx_n.$$

Comme on a $T > U\sqrt{D}$, $b < \sqrt{D}$, et par suite $T - bU > 0$, l'inégalité précédente est équivalente à celle-ci:

$$y_n \leq \frac{aU}{T - bU} x_n.$$

Il résulte de ce qui précède, que parmi les représentations en nombre infini, formant un même groupe, et qui sont toutes données par les équations (6), il y en a toujours une qui satisfait à ces trois conditions:

$$(8) \qquad x > 0, \quad y > 0, \quad y \leqq \frac{aU}{T - bU} x.$$

Ces inégalités ont été déduites de la définition de la solution particulière que nous voulions séparer de toutes les autres contenues dans le même groupe qu'elle. D'après cette définition, la solution dont il s'agit devait appartenir au premier des deux groupes partiels, et répondre dans ce groupe à la plus petite valeur positive de y. On peut prouver réciproquement que toute solution pour laquelle les inégalités précédentes ont lieu, est nécessairement, parmi toutes les solutions formant avec elle un même groupe total, celle à laquelle s'applique la définition précédente; il suffit pour cela de répéter en sens inverse les raisonnements que nous venons de développer. Cela étant, on voit que le théorème II peut être remplacé par un autre théorème dont voici l'énoncé.

Théorème III.

Les suppositions du théorème II étant conservées, si l'on ajoute que les coefficients et les indéterminées de la forme $ax^2 + 2bxy + cy^2$, doivent satisfaire aux conditions (7) et (8), et que l'on assujettisse toutes les autres formes à des

conditions analogues, je dis que le nombre des représentations différentes de l'entier ωm, que l'on peut effectuer au moyen des formes données, sera exprimé par la puissance 2^μ.

Pour rendre plus faciles les applications que nous aurons à faire du théorème précédent, il conviendra de mettre sous une forme géométrique le résultat sur lequel ce théorème est fondé. Soient à cet effet OX, OY deux axes rectangulaires des x et des y, dirigés dans le sens des coordonnées positives, le premier horizontalement, le second verticalement et de bas en haut. Les variables x et y dans l'équation:

$$ax^2 + 2bxy + cy^2 = \omega m$$

étant considérées comme continues, cette équation sera à une hyperbole, et l'on déduira facilement des conditions $a > 0$, $b > 0$, $c < 0$, que l'axe des y sépare l'une de l'autre, les deux branches infinies de cette courbe. Si donc nous appelons première branche celle de ces deux branches infinies sur laquelle l'abscisse x est partout positive, le premier des deux groupes partiels précédemment distingués, répondra à cette première branche. Cela étant l'interprétation géométrique du résultat établi plus haut consiste en ce que, parmi les solutions en nombre infini formant le même groupe total, et qui sont toutes comprises dans les équations (6), il y en a toujours une, et qu'il ne saurait y en avoir plus d'une, qui soit représentée par un point de l'arc de la première branche, intercepté d'une part par l'axe OX, et de l'autre par la droite qui a pour équation:

$$y = \frac{aU}{T - bU} x;$$

ce à quoi il faut ajouter qu'on doit toujours exclure la solution qui répond à l'extrémité inférieure de cet arc.

§. 5.

Il nous reste une dernière question préliminaire à résoudre, avant d'en venir au véritable objet de ce mémoire. Cette question consiste à assigner toutes les valeurs simultanées des indéterminées x et y qui, étant substituées dans une forme donnée du déterminant D, rendent cette forme première à D, et en outre impaire ou impairement paire suivant qu'il s'agit d'une forme proprement ou improprement primitive. Nous désignons par D_1 la valeur numérique de D, et nous commencerons cette recherche par l'examen du cas où la forme donnée appartient à l'ordre proprement primitif. Ce cas se subdivise lui-même,

suivant que D est pair ou impair. Soit en premier lieu D impair. Les indéterminées x et y étant mises sous la forme:

$$2D_1 v+\alpha, \quad 2D_1 w+\gamma,$$

où v, w désignent des entiers quelconques positifs ou négatifs, α, γ étant des nombres pris l'un et l'autre dans la suite:

$$0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1-1,$$

on aura évidemment:

$$ax^2+2bxy+cy^2 \equiv a\alpha^2+2b\alpha\gamma+c\gamma^2 \pmod{2D_1}.$$

La question proposée revient donc à voir pour lesquelles des combinaisons α, γ, ou plutôt, pour combien de ces combinaisons (car c'est uniquement leur nombre qu'il nous importe de connaître) le second membre est premier à $2D_1$. Nous observerons d'abord qu'on peut, sans nuire en rien à la généralité de la question, supposer l'un des coefficients extrêmes, le premier a par exemple, sans diviseur commun avec $2D_1$. En effet, si cette condition n'a pas lieu dans la forme donnée, on peut toujours transformer celle-ci en une autre où elle se trouve remplie. Soit $a'x'^2+2b'x'y'+c'y'^2$ la nouvelle forme équivalente à la première, et soient:

$$x = px'+qy', \quad y = rx'+sy', \quad ps-qr = 1$$

les équations qui correspondent à cette transformation. Si maintenant dans les congruences:

$$\alpha \equiv p\alpha'+q\gamma', \quad \gamma \equiv r\alpha'+s\gamma' \pmod{2D_1}$$

on combine les nombres α', γ', pris l'un et l'autre dans la suite:

$$0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1-1,$$

de toutes les manières possibles, et que l'on détermine α, γ de manière que ces nombres se trouvent compris entre les mêmes limites, à chaque combinaison α', γ' correspondra une combinaison α, γ, et réciproquement, comme on le voit en mettant les congruences précédentes sous la forme:

$$\alpha' \equiv s\alpha-q\gamma, \quad \gamma' \equiv -r\alpha+p\gamma \pmod{2D_1}.$$

De là et de ce que l'on a évidemment:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2 \equiv a'\alpha'^2+2b'\alpha'\gamma'+c'\gamma'^2 \pmod{2D_1},$$

on conclut que les nombres des combinaisons α, γ et α', γ' pour lesquelles:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2 \quad \text{et} \quad a'\alpha'^2+2b'\alpha'\gamma'+c'\gamma'^2$$

sont premiers à $2D_1$ coïncident. Cette conclusion justifiant l'assertion avancée

plus haut, nous pouvons considérer a comme premier à $2D_1$. Cela posé, pour que le trinôme:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2$$

n'ait pas de diviseur commun avec $2D_1$, il faut et il suffit que le produit:

$$a(a\alpha^2+2b\alpha\gamma+c\gamma^2) = (a\alpha+b\gamma)^2-D\gamma^2$$

jouisse de la même propriété, et par suite, que $a\alpha+b\gamma$ soit premier à $2D_1$, lorsque γ est pair, ou que $a\alpha+b\gamma$ soit pair et premier à D_1, lorsque γ est impair. Or, γ ayant une valeur déterminée, celles de l'expression $a\alpha+b\gamma$, lorsqu'on y pose successivement:

$$\alpha = 0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1-1,$$

coïncideront, abstraction faite des multiples de $2D_1$, avec la même suite. Tout se réduit donc à voir dans le cas de γ pair, combien la suite précédente renferme de termes premiers à $2D_1$, et dans le cas de γ impair, combien il y en a dans la même suite, qui jouissent de la double propriété d'être pairs et premiers à D_1. Si l'on désigne par A le nombre des entiers positifs non-supérieurs*) à D_1, qui n'ont pas de diviseur commun avec D, le nombre des termes en question sera, pour l'un et l'autre cas, exprimé par A. Comme d'un autre côté, γ est susceptible de $2D_1$ valeurs différentes, on voit que les combinaisons α, γ qui donnent à:

$$a\alpha^2+2b\alpha\gamma+c\gamma^2$$

une valeur première à $2D_1$, sont au nombre de $2D_1A$. Une discussion toute semblable étant appliquée au cas où D est pair, fait voir que le nombre des combinaisons est alors $4D_1A$.

Considérons en dernier lieu le cas où la forme donnée:

$$ax^2+2bxy+cy^2$$

appartient à l'ordre improprement primitif. Si nous posons:

$$\tfrac{1}{2}a = a', \quad \tfrac{1}{2}c = c'$$

et comme précédemment:

$$x = 2D_1 v+\alpha, \quad y = 2D_1 w+\gamma,$$

nous aurons:

$$a'x^2+bxy+c'y^2 \equiv a'\alpha^2+b\alpha\gamma+c'\gamma^2 \pmod{2D_1},$$

*) Je dis à dessein non-supérieurs, pour que le cas de $D_1 = 1$ ne fasse pas exception.

et il s'agira de voir pour combien de combinaisons α, γ le second membre est impair et premier à D_1. Pour y parvenir de la manière la plus simple, nous supposerons, ce qui est permis, que a' n'ait pas de diviseur commun avec $2D_1$. Cela étant, il faut distinguer le cas où l'on a $D \equiv 1$, et celui où $D \equiv 5 \pmod 8$. Dans le premier de ces deux cas, b étant impair, il résulte de l'équation:

$$D = b^2 - ac = b^2 - 4a'c',$$

que c' est pair, et l'on voit de même que dans le second, c' est impair. On conclut de là que:

$$a'\alpha^2 + b\alpha\gamma + c'\gamma^2$$

ne saurait être impair dans le premier cas, à moins que les nombres α, γ ne soient le premier impair, le second pair, et dans le second, à moins que α, γ ne soient ou l'un pair, l'autre impair, ou impairs tous les deux. Pour avoir égard à l'autre condition d'après laquelle:

$$a'\alpha^2 + b\alpha\gamma + c'\gamma^2$$

doit être premier à D_1, on remarquera qu'il faut et qu'il suffit, pour qu'elle soit remplie, que le produit:

$$4a'(a'\alpha^2 + b\alpha\gamma + c'\gamma^2) = (a\alpha + b\gamma)^2 - D\gamma^2$$

jouisse de la même propriété. Cela posé, si nous supposons d'abord $D \equiv 1 \pmod 8$, il faudra, après avoir attribué à γ une valeur déterminée paire, égaler α à chaque terme de la suite:

$$1, \quad 3, \quad 5, \quad \ldots, \quad 2D_1 - 1,$$

et voir combien de fois $a\alpha + b\gamma$, ou ce qui est la même chose, le reste de cette expression, pris relativement au diviseur D_1, est premier à D_1. Or il est facile de voir que les restes de $a\alpha + b\gamma$ sont, abstraction faite de l'ordre:

$$0, \quad 1, \quad 2, \quad \ldots, \quad D_1 - 1;$$

on en conclut qu'à chaque valeur de γ correspond un nombre Δ de valeurs impaires de α, telles que:

$$a'\alpha^2 + b\alpha\gamma + c'\gamma^2$$

soit impair et premier à D. Il résulte de là et de ce que le nombre γ est lui-même susceptible de D_1 valeurs différentes, que le nombre des combinaisons α, γ qui donnent à l'expression:

$$\tfrac{1}{2}(a\alpha^2 + 2b\alpha\gamma + c\gamma^2)$$

une valeur impaire et première à D, est égal à $D_1\Delta$. Si nous considérons en

second lieu le cas où $D \equiv 5 \pmod 8$, on trouve, comme dans le cas précédent, qu'à chaque valeur paire de γ, il correspond un nombre de valeurs convenables de α, égal à Δ, puisque, γ étant pair, α doit être impair; mais il n'en est plus de même, lorsque la valeur déterminée que l'on attribue à γ, est impaire, α pouvant être alors pair ou impair. Il faut, dans cette dernière supposition, égaler α dans l'expression $a\alpha + b\gamma$ à chacun des nombres:

$$0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1 - 1.$$

Or, les valeurs de $a\alpha + b\gamma$, correspondant à ces nombres, étant diminuées des multiples de D_1 qu'elles contiennent, coïncideront évidemment avec la suite:

$$0, \quad 1, \quad 2, \quad \ldots, \quad D_1 - 1,$$

chacun des termes de cette suite étant supposé écrit deux fois. On conclut de là que les valeurs convenables de α, répondant à une valeur impaire donnée de γ, sont toujours au nombre de 2Δ. Si l'on remarque maintenant que, parmi les valeurs:

$$0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1 - 1$$

dont γ est susceptible, il y en a D_1 qui sont paires, et autant qui sont impaires, on verra que dans le cas où l'on a $D \equiv 5 \pmod 8$, le nombre des combinaisons α, γ, rendant le trinôme:

$$\tfrac{1}{2}(a\alpha^2 + 2b\alpha\gamma + c\gamma^2)$$

impair et premier à D, est égal à $3D_1\Delta$.

Nous résumerons ici les résultats qui ont été établis dans ce paragraphe. La valeur numérique du déterminant D étant désignée par D_1, et Δ exprimant le nombre de ceux des termes:

$$1, \quad 2, \quad \ldots, \quad D_1$$

qui n'ont pas de diviseur commun avec D_1, les valeurs simultanées de x et de y qui rendent une forme quelconque de ce déterminant, ou la moitié de cette forme lorsqu'elle appartient à l'ordre improprement primitif, impaire et première à D, peuvent toujours se distribuer en systèmes de la forme:

$$x = 2D_1 v + \alpha, \quad y = 2D_1 w + \gamma,$$

où v et w désignent des entiers indéterminés positifs où négatifs, et où α et γ sont l'un et l'autre compris dans la suite:

$$0, \quad 1, \quad 2, \quad \ldots, \quad 2D_1 - 1;$$

quant au nombre des systèmes qui jouissent de la propriété énoncée, il sera, lorsqu'il s'agit d'une forme proprement primitive $2D_1\Delta$ ou $4D_1\Delta$, suivant que

D est impair ou pair, et lorsque la forme est improprement primitive, $D_1 \Delta$ ou $3 D_1 \Delta$, suivant que l'on a $D \equiv 1$ ou $D \equiv 5 \pmod 8$.

Nous terminerons les préliminaires en démontrant le lemme qui suit. „Soit $K = kk'k''\ldots$ le produit des nombres premiers positifs, impairs et inégaux k, k', k'', $\ldots$, et désignons par L un entier quelconque qui divise K. Posons encore $\theta = \pm 1$, $\eta = \pm 1$, les signes ambigus étant quelconques et indépendants l'un de l'autre. Cela étant, je dis que l'expression:

$$\Sigma \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right),$$

où le signe sommatoire s'étend à tous les entiers n premiers à $2K$, et compris depuis $n = 1$ jusqu'à $n = 8K - 1$, est toujours égale à zéro, si on n'a pas simultanément $\theta = 1$, $\eta = 1$, $L = 1$."

Désignons par a l'un quelconque des nombres $1, 2, \ldots, k-1$, par a' l'un quelconque des nombres $1, 2, \ldots, k'-1$, et ainsi de suite. Soit encore b l'un quelconque des nombres 1, 3, 5, 7. Cela posé, il est facile de voir que l'on obtiendra toutes les valeurs que n doit recevoir dans la somme précédente, en déterminant, pour chacune des combinaisons $a, a', \ldots; b$, le nombre n, moindre que $8K$, qui satisfait aux congruences simultanées:

$$n \equiv a \pmod k, \quad n \equiv a' \pmod{k'}, \quad \ldots, \quad n \equiv b \pmod 8.$$

On conclut de ces congruences:

$$\left(\frac{n}{k}\right) = \left(\frac{a}{k}\right), \quad \left(\frac{n}{k'}\right) = \left(\frac{a'}{k'}\right), \quad \ldots, \quad \theta^{\frac{1}{2}(n-1)} = \theta^{\frac{1}{2}(b-1)}, \quad \eta^{\frac{1}{8}(n^2-1)} = \eta^{\frac{1}{8}(b^2-1)}.$$

Si maintenant on désigne ceux des nombres premiers $k, k', \ldots$ qui sont contenus dans L, par $k_0, k_0', \ldots$, les autres par $k_1, k_1', \ldots$, la somme du lemme:

$$\Sigma \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right) \quad \text{ou} \quad \Sigma \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{k_0}\right)\left(\frac{n}{k_0'}\right)\ldots,$$

sera exprimé par le produit*):

$$(k_1-1)(k_1'-1)\ldots \sum_a \left(\frac{a}{k_0}\right) \sum_{a'} \left(\frac{a'}{k_0'}\right) \ldots \sum_b \theta^{\frac{1}{2}(b-1)} \eta^{\frac{1}{8}(b^2-1)}$$
$$(a = 1, 2, \ldots, k_0-1; \quad a' = 1, 2, \ldots, k_0'-1; \quad \ldots; \quad b = 1, 3, 5, 7)$$

dont les facteurs:

$$\sum_a \left(\frac{a}{k_0}\right), \quad \sum_{a'} \left(\frac{a'}{k_0'}\right), \quad \ldots$$

s'évanouissent évidemment. Comme on a encore:

$$\sum_b \theta^{\frac{1}{2}(b-1)} \eta^{\frac{1}{8}(b^2-1)} = 0$$

*) Im Originaltext sind die einzelnen Factoren des Products angegeben; die Formel-Darstellung habe ich der Deutlichkeit wegen hinzugefügt und deshalb noch einige Aenderungen angebracht. K.

pour les trois cas: $\theta = 1$, $\eta = -1$; $\theta = -1$, $\eta = 1$; $\theta = -1$, $\eta = -1$, il résulte que l'expression:

$$\Sigma \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right)$$

s'évanouit toujours, à moins qu'on n'ait à la fois $\theta = 1$, $\eta = 1$, $L = 1$, ce qu'il s'agissait de prouver.

§. 6.

En passant maintenant aux questions indiquées dans le préambule de ce mémoire, nous conserverons les notations dont nous avons fait usage dans les §§. 3, 4 et 5. Nous poserons donc:

(1) $$D = PS^2, \quad \text{ou} \quad D = 2PS^2,$$

S^2 étant toujours le plus grand carré qui divise D, et:

(2) $$P = pp'p''\ldots,$$

$p, p', p'', \ldots$ étant des nombres premiers impairs, positifs ou négatifs, tous différents les uns des autres. Nous poserons aussi:

(3) $$R = rr'r''\ldots,$$

$r, r', r'', \ldots$ désignant, comme plus haut, les facteurs premiers impairs inégaux, contenus dans S, sans l'être dans P. Soit encore q un nombre premier positif impair quelconque, qui n'est contenu ni dans P ni dans R, et décomposons chacun de ces produits d'une manière quelconque en deux facteurs, sans exclure le cas où l'un de ces facteurs serait égal à l'unité, c'est-à-dire, écrivons les deux équations:

(4) $$P = P_1 P_2, \quad R = R_1 R_2.$$

Posons enfin:

(5) $$\delta = \pm 1, \quad \varepsilon = \pm 1, \quad \theta = \pm 1, \quad \eta = \pm 1,$$

les signes étant quelconques et indépendants les uns des autres. Cela étant et s désignant une variable continue positive, assujettie à rester supérieure à l'unité, nous aurons par le développement en série, et en ayant égard aux équations (2) et (3) du §. 2:

$$\frac{1}{1 - \theta^{\frac{1}{2}(q-1)} \eta^{\frac{1}{8}(q^2-1)} \left(\frac{q}{P_2 R_1}\right) \frac{1}{q^s}} = 1 + \cdots + \theta^{\frac{1}{2}(q^l-1)} \eta^{\frac{1}{8}(q^{2l}-1)} \left(\frac{q^l}{P_2 R_1}\right) \frac{1}{(q^l)^s} + \cdots,$$

où, pour abréger, on n'a écrit dans le second membre que son terme général, dans lequel il faut égaler l successivement à toutes les valeurs entières depuis $l = 0$ jusqu'à $l = \infty$.

Supposons maintenant que dans l'équation précédente, on mette pour q toutes les valeurs dont ce nombre est susceptible, c'est-à-dire tous les nombres premiers impairs positifs qui ne divisent pas D, et que l'on forme le produit de toutes ces équations. Le produit des seconds membres formera une série dont la loi est très facile à reconnaître, si l'on se rappelle que, d'après un théorème connu, un nombre composé ne peut résulter que d'une seule manière, de la multiplication de facteurs simples, et que l'on continue en même temps à avoir égard aux théorèmes cités du §. 2. On obtient ainsi l'équation:

$$(6)\qquad \Pi \frac{1}{1-\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}} = \Sigma\theta^{\frac{1}{2}(n-1)}\eta_1^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P_2R_1}\right)\frac{1}{n^s},$$

le signe de multiplication Π se rapportant à toutes les valeurs de q, précédemment définies, et le signe sommatoire s'étendant à tous les entiers, compris depuis $n=1$ jusqu'à $n=\infty$, qui remplissent la double condition d'être impairs et premiers à D, ou plus simplement, qui sont premiers à $2D$.

Avant d'aller plus loin, nous aurions à montrer la nécessité de la supposition faite plus haut, et d'après laquelle on doit avoir $s>1$. On s'en rendra facilement compte, si l'on remarque que la série précédente n'a une somme indépendante de l'arrangement de ses termes, que lorsque la condition $s>1$ a lieu, et qu'il en est de même du produit, dont la valeur n'est également indépendant de l'ordre de ses facteurs qu'autant que la même condition est remplie. Il me semble d'autant plus inutile d'entrer dans de plus grands développements à ce sujet, que je me suis déjà expliqué avec détail sur le point en question, dans la démonstration du théorème sur la progression arithmétique que j'ai citée plus haut et qui est fondée sur une équation de même nature, mais plus générale que la précédente.

Si dans l'équation (6) on remplace θ, η respectivement par $\delta\theta$, $\varepsilon\eta$, et que l'on change en même temps P_2 en P_1, elle deviendra:

$$(7)\qquad \Pi \frac{1}{1-(\delta\theta)^{\frac{1}{2}(q-1)}(\varepsilon\eta)^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1R_1}\right)\frac{1}{q^s}} = \Sigma(\delta\theta)^{\frac{1}{2}(n-1)}(\varepsilon\eta)^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P_1R_1}\right)\frac{1}{n^s}.$$

On a encore, en y faisant $\theta=1$, $\eta=1$, $P_2=1$, $R_1=1$, et remplaçant s par $2s$:

$$(8)\qquad \Pi \frac{1}{1-\frac{1}{q^{2s}}} = \Sigma\frac{1}{n^{2s}},$$

les signes de multiplication et de sommation s'étendant toujours aux valeurs de q et de n, précédemment définies. Le produit des équations (6) et (7) étant divisé par l'équation (8), le facteur général dans le premier membre sera:

$$\frac{\left(1+\frac{1}{q^s}\right)\left(1-\frac{1}{q^s}\right)}{\left(1-(\delta\theta)^{\frac{1}{2}(q-1)}(\varepsilon\eta)^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1R_1}\right)\frac{1}{q^s}\right)\left(1-\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}\right)}.$$

Comme le numérateur de cette fraction est évidemment équivalent à:

$$\left(1+\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}\right)\left(1-\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}\right),$$

elle pourra se mettre sous cette forme plus simple:

$$\frac{1+\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}}{1-(\delta\theta)^{\frac{1}{2}(q-1)}(\varepsilon\eta)^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1R_1}\right)\frac{1}{q^s}}.$$

L'expression précédente présente deux cas différents, suivant que l'on a:

$$\delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1P_2}\right) = \delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P}\right) = -1 \quad \text{ou} \quad +1.$$

Dans le premier de ces deux cas, elle est égale à l'unité et peut être omise dans le produit; dans le second, on peut lui donner cette autre forme:

$$\frac{1+\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}}{1-\theta^{\frac{1}{2}(q-1)}\eta_1^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2R_1}\right)\frac{1}{q^s}}.$$

Les doubles signes dans les valeurs $\delta=\pm1$, $\varepsilon=\pm1$, que contient l'équation (7), ont été tout à fait arbitraires jusqu'à présent. Nous supposerons désormais que suivant les quatre cas déjà distingués dans les §§. 3 et 4, et que le déterminant D peut présenter, savoir:

$$D=PS^2,\quad P\equiv1 \text{ ou } 3 \text{ (mod. 4)};\quad D=2PS^2,\quad P\equiv1 \text{ ou } 3 \text{ (mod. 4)},$$

ces signes seront respectivement:

$$(9)\qquad \delta=1,\ \varepsilon=1;\quad \delta=-1,\ \varepsilon=1;\quad \delta=1,\ \varepsilon=-1;\quad \delta=-1,\ \varepsilon=-1.$$

Cela étant, la condition:

$$\delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P}\right) = 1$$

coïncidera avec celle des quatre conditions (2) du §. 4 qui correspond à chacun des quatre cas précédents. En désignant donc les nombres premiers q positifs,

impairs et non-diviseurs de D qui y satisfont, par f, cette lettre aura la même signification que dans le §. 4, c'est-à-dire que l'on aura:

$$\vartheta^{\frac{1}{2}(f-1)}\varepsilon^{\frac{1}{2}(f^2-1)}\left(\frac{f}{P}\right)=1, \tag{10}$$

et le premier membre de l'équation dont l'origine a été indiquée plus haut, sera:

$$\Pi\frac{1+\vartheta^{\frac{1}{2}(f-1)}\eta_1^{\frac{1}{2}(f^2-1)}\left(\frac{f}{P_2R_1}\right)\frac{1}{f^s}}{1-\vartheta^{\frac{1}{2}(f-1)}\eta_1^{\frac{1}{2}(f^2-1)}\left(\frac{f}{P_2R_1}\right)\frac{1}{f^s}},$$

le signe Π s'étendant à toutes les valeurs de f. Au moyen de l'équation:

$$\frac{1+z}{1-z}=1+2z+2z^2+2z^3+\cdots$$

et en ayant égard aux équations (2) et (3) du §. 2, le facteur général du produit précédent pourra se développer en une série dont le $(l+1)^{\text{ième}}$ terme est:

$$2\vartheta^{\frac{1}{2}(f^l-1)}\eta_1^{\frac{1}{2}(f^{2l}-1)}\left(\frac{f^l}{P_2R_1}\right)\frac{1}{(f^l)^s}.$$

Le premier terme qui répond à $l=0$, fait exception à cette loi et a l'unité pour valeur. Il est facile de conclure de là, et en ayant toujours égard aux équations citées du §. 2, que le produit précédent peut lui-même prendre la forme d'une série, ayant pour terme général:

$$\vartheta^{\frac{1}{2}(m-1)}\eta_1^{\frac{1}{2}(m^2-1)}\left(\frac{m}{P_2R_1}\right)\frac{2^\mu}{m^s},$$

où m désigne généralement tous les entiers positifs, impairs et premiers à D, n'ayant que des diviseurs simples f tels que la condition (10) soit satisfaite, et où μ indique, comme dans le §. 4, le nombre des diviseurs simples inégaux de m, sans compter le diviseur 1. On peut remarquer que le terme qui répond à $m=1$, ne fait pas exception à la loi générale, l'expression précédente se réduisant à l'unité dans ce cas. Nous avons donc l'équation:

$$\left\{\begin{array}{l}\Sigma\frac{1}{n^{2s}}\cdot\Sigma\theta^{\frac{1}{2}(m-1)}\eta_1^{\frac{1}{2}(m^2-1)}\left(\frac{m}{P_2R_1}\right)\frac{2^\mu}{m^s}\\ =\Sigma(\delta\theta)^{\frac{1}{2}(n-1)}(\varepsilon\eta_1)^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P_1R_1}\right)\frac{1}{n^s}\cdot\Sigma\theta^{\frac{1}{2}(n-1)}\eta_1^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P_2R_1}\right)\frac{1}{n^s},\end{array}\right. \tag{11}$$

dans laquelle on doit étendre les sommations à tous les entiers n ou m, précédemment définis, et l'on doit se rappeler que les valeurs $\delta=\pm1$, $\varepsilon=\pm1$ sont celles que nous avons fixées par les conditions (9), tandis que les signes dans les équations $\theta=\pm1$, $\eta=\pm1$ restent arbitraires.

En faisant $\theta=1$, $\eta=1$, $P_2=1$, $R_1=1$, et par suite $P_1=P$, l'équation précédente prendra la forme:

$$\Sigma\frac{1}{n^{2s}}\cdot\Sigma\frac{2^\mu}{m^s}=\Sigma\frac{1}{n^s}\cdot\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n^s}. \tag{12}$$

C'est cette équation particulière qui nous servira à déterminer le nombre des formes différentes qui répondent à un déterminant quelconque positif ou négatif. Il faudra, dans cette recherche, traiter séparément le cas où D est positif et celui où D est négatif, et subdiviser encore chacun de ces deux cas suivant qu'il s'agira de formes proprement ou improprement primitives. Mais comme il y a néanmoins une partie commune à l'analyse de ces quatre cas, il conviendra, pour n'avoir pas à présenter deux fois les mêmes considérations, que nous nous occupions d'abord de cette partie de la discussion, dont l'objet consiste à voir quelle forme prend le second membre de l'équation (12), si l'on y suppose $s=1+\varrho$, et que l'on considère la variable positive ϱ comme devenant moindre que toute quantité donnée.

Pour commencer cet examen par le premier des deux facteurs contenus dans le second membre, soient e, e', e'', ... ceux des nombres:

$$1,\ 2,\ 3,\ \ldots,\ 2D_1-1$$

qui n'ont pas de diviseur commun avec $2D_1$. Cela posé, il est évident que la somme $\Sigma\frac{1}{n^{1+\varrho}}$, où n ne doit recevoir que des valeurs positives et premières à $2D_1$, peut être décomposée en autant de sommes partielles de la forme:

$$\frac{1}{e^{1+\varrho}}+\frac{1}{(2D_1+e)^{1+\varrho}}+\frac{1}{(4D_1+e)^{1+\varrho}}+\cdots$$

qu'il y a de termes dans la suite e, e', e'', ... Comme, d'un autre côté, on conclut facilement du résultat obtenu plus haut sur la série (1) du §. 1, que chacune de ces sommes partielles prend la forme $\frac{1}{2D_1}\cdot\frac{1}{\varrho}$, et qu'il est d'ailleurs évident que le nombre de ces sommes partielles, ou ce qui revient au même, le nombre des termes e, e', e'', ... est Δ ou 2Δ, selon que D est impair ou pair, la lettre Δ ayant la même signification que dans le §. 5, on aura selon ces deux cas:

$$\Sigma\frac{1}{n^{1+\varrho}}=\frac{\Delta}{2D_1}\cdot\frac{1}{\varrho},\quad\text{ou}\quad\Sigma\frac{1}{n^{1+\varrho}}=\frac{\Delta}{D_1}\cdot\frac{1}{\varrho}, \tag{13}$$

la variable ϱ étant toujours supposée infiniment petite. Si nous considérons

en second lieu l'autre facteur du second membre, il est facile de voir que ce facteur est un cas particulier de la série à laquelle se rapporte le troisième des lemmes du §. 1; il faudra, pour l'y comprendre, supposer dans la série générale de ce lemme:

$$c_n = \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right), \quad \text{ou} \quad c_n = 0,$$

suivant que n est ou n'est pas premier à $2D_1$. Quant aux deux conditions que ce lemme suppose, et qui consistent 1°. en ce que c_n doit être une fonction périodique de l'indice n, et 2°. en ce que la somme des termes qui composent une période, doit être zéro, on s'assure facilement qu'elles sont remplies. Cela est évident pour la première, et pour voir que la seconde a également lieu, il suffira de recourir au lemme qui termine le §. 5, et de remarquer qu'on ne saurait avoir à la fois $\delta = 1$, $\varepsilon = 1$, $P = \pm 1$. En effet, il résulte des conditions (9) que les équations précédentes ne sont compatibles entre elles que lorsqu'on a $P = 1$; ces équations se rapportent alors au cas que nous avons exclu où le déterminant est un carré positif. Il résulte de ce qui précède que la somme:

$$\Sigma \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n^{1+\varrho}},$$

lorsqu'on y considère la variable positive comme devenant infiniment petite, converge vers une limite finie donnée par l'expression:

$$\Sigma \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}, \tag{14}$$

dans laquelle il faut supposer que les valeurs de n se suivent dans l'ordre naturel, c'est-à-dire de manière à former une suite croissante.

I. Revenons maintenant à l'équation (12), et considérons en premier lieu le cas où D est négatif de sorte que $D = -D_1$. Soient

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots \tag{15}$$

les formes différentes et proprement primitives de ce déterminant D, formes dont je désignerai le nombre par h. Cela étant, on aura l'égalité:

$$\Sigma \frac{2^{\mu+1}}{m^s} = \Sigma \frac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \ldots, \tag{16}$$

où le second membre contient autant de termes qu'il y a de formes (15), et où la double sommation dans chaque terme doit s'étendre à tous les systèmes de valeurs entières de x et de y, comprises entre $-\infty$ et ∞, qui remplissent

la double condition de n'avoir pas de diviseur commun et de donner à la forme où elles sont substituées, une valeur première à $2D$. Cela résulte 1°. de ce que chacun des entiers m contenus dans le premier membre est, en vertu du théorème I du §. 4, susceptible d'être représenté de la manière indiquée et par l'ensemble des formes (15), autant de fois qu'il y a d'unités dans l'expression $2^{\mu+1}$, et 2°. de ce que réciproquement toute valeur première à $2D$, que l'une quelconque des formes (15) peut obtenir lorsqu'on y attribue à x et y des valeurs sans diviseur commun, coïncide d'après les résultats connus et que nous avons rappelés au commencement du paragraphe cité, avec l'un des entiers désignés par m. Si maintenant l'on substitue l'expression de $\Sigma \frac{2^{\mu+1}}{m^s}$, donnée par l'équation précédente, dans l'équation (12), il viendra:

$$\Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \cdots$$
$$= 2\Sigma \frac{1}{n^s} \cdot \Sigma \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n^s}.$$

Il est facile de voir que chacun des termes du premier membre peut être mis sous une forme plus simple. Le premier de ces termes est évidemment équivalent à l'expression:

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^s},$$

où les valeurs simultanées de x et de y, dans la sommation double, ne sont plus assujetties qu'à la condition unique de rendre le trinôme où elles sont substituées, impair et premier à D. En attachant donc ce sens au signe Σ', on aura:

$$\begin{cases} \Sigma' \frac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma' \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \cdots \\ \qquad = 2\Sigma \frac{1}{n^s} \cdot \Sigma \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n^s}. \end{cases} \tag{17}$$

Il faut maintenant poser $s = 1+\varrho$, la variable positive ϱ étant toujours considérée comme infiniment petite, et voir ce que les différents termes du premier membre deviendront dans cette supposition. Puisque d'après les résultats que nous avons établis dans le §. 5, les valeurs simultanées que l'on doit attribuer à x et y, dans chacune de ces sommes doubles, dans la première par exemple, peuvent être distribuées en systèmes de la forme:

$$x = 2D_1 v + \alpha, \quad y = 2D_1 w + \gamma, \tag{18}$$

on voit que la somme en question peut être décomposée en autant de sommes partielles qu'il y a de ces systèmes, telles que:

$$\Sigma \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}},$$

où il faut substituer pour x et y les expressions précédentes, et sommer ensuite relativement aux entiers v et w, depuis $-\infty$ jusqu'à ∞. Pour obtenir cette somme partielle, nous chercherons l'entier qui exprime combien de fois le trinôme $ax^2+2bxy+cy^2$, dans cette somme, obtient une valeur ne surpassant pas la quantité positive quelconque σ. Or, cette dernière question est évidemment identique à celle de savoir combien dans l'intérieur ou sur le contour de l'ellipse, déterminée par l'équation:

$$ax^2+2bxy+cy^2 = \sigma,$$

il y a de points dont les coordonnées x et y sont de la forme (18), et si l'on observe que l'aire de cette ellipse est:

$$\frac{\pi}{\sqrt{(ac-b^2)}}\sigma = \frac{\pi}{\sqrt{D_1}}\sigma,$$

où la lettre π a la signification ordinaire, on conclura immédiatement du second lemme du §. 1*) que le nombre qu'il s'agit de déterminer, peut être mis sous la forme:

$$\frac{\pi}{4\sqrt{D_1}}\sigma+\sigma^{\delta}\psi(\sigma)$$

l'exposant constant δ ayant une valeur quelconque comprise entre $\frac{1}{2}$ et 1, et la fonction $\psi(\sigma)$ restant finie quelque grande que l'on suppose la variable σ. Il résulte de là et du premier théorème du paragraphe déjà cité, que la somme partielle que nous considérons, a la valeur:

$$\frac{\pi}{4\sqrt{D_1}}\cdot\frac{1}{\varrho},$$

d'où l'on conclut, en considérant que d'après le §. 5, le nombre des systèmes (18) et par suite celui des sommes partielles dans lesquelles la somme:

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}}$$

*) Il est évident par la nature de ce lemme, que les points placés sur le contour de la courbe peuvent être considérés à volonté comme des points intérieurs ou comme des points extérieurs. On peut donc aussi et à plus forte raison, ranger ces points en partie parmi les points intérieurs et en partie parmi les points extérieurs, comme nous le ferons plus bas, lorsque nous nous occuperons des déterminants positifs.

a été partagée, est $2D_1\Delta$ ou $4D_1\Delta$, selon que D est impair ou pair, que la somme précédente est suivant ces deux cas:

$$\frac{\pi\Delta}{2\sqrt{D_1}}\cdot\frac{1}{\varrho} \quad \text{ou} \quad \frac{\pi\Delta}{\sqrt{D_1}}\cdot\frac{1}{\varrho}.$$

Comme ce résultat ne contient rien qui soit particulier à la forme $ax^2+2bxy+cy^2$, et qu'il ne renferme que le déterminant commun à toutes les formes (15), on voit que le premier membre de l'équation (17), en supposant toujours ϱ infiniment petit et en distinguant le cas de D impair et celui de D pair, est:

$$\frac{h\pi\Delta}{2\sqrt{D_1}}\cdot\frac{1}{\varrho} \quad \text{ou} \quad \frac{h\pi\Delta}{\sqrt{D_1}}\cdot\frac{1}{\varrho}.$$

Au moyen de ces expressions et des résultats (13) et (14), précédemment établis, l'équation (17) se changera pour une valeur infiniment petite de ϱ, dans l'équation remarquable qui suit et où les cas de D pair et impair sont confondus dans la même forme:

$$h = \frac{2}{\pi}\sqrt{D}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}. \tag{19}$$

Cette équation est sujette à une exception qui a lieu lorsque D est -1, et qui est une suite de l'exception que le théorème I du §. 4 souffre dans le même cas. Pour rétablir l'exactitude dans ce cas singulier, il faut doubler le second membre, comme cela résulte de l'analyse précédente, et comme on peut aussi le vérifier *à posteriori*. En effet, on a dans ce cas $h=1$, $D_1=1$, $\delta=-1$, $\varepsilon=1$, $P=-1$; l'équation modifiée, comme on vient de le dire, deviendra donc:

$$1 = \frac{4}{\pi}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots\right),$$

ce qui est exact d'après la série connue de Leibniz.

II. Le déterminant D étant toujours négatif et en outre tel que $D\equiv 1 \pmod 4$, nous supposerons que les formes (15) sont celles de l'ordre impropement primitif. On aura dans cette supposition, $\delta=1$, $\varepsilon=1$, et l'égalité (16) devra être remplacée par celle-ci:

$$\Sigma\frac{2^{\mu+1}}{(2m)^s} = \Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}+\Sigma\frac{1}{(a'x^2+2b'xy+c'y^2)^s}+\cdots,$$

où la double sommation s'étend dans chaque terme à toutes les valeurs simultanées de x et de y qui n'ont pas de diviseur commun, et qui rendent la moitié de la forme entrant dans ce terme, première à $2D$. La substitution de l'ex-

pression précédente dans l'équation (12) donne:

$$\Sigma\frac{1}{n^{2s}}\cdot\Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}+\Sigma\frac{1}{n^{2s}}\cdot\Sigma\frac{1}{(a'x^2+2b'xy+c'y^2)^s}+\cdots$$
$$=2^{1-s}\Sigma\frac{1}{n^s}\cdot\Sigma\left(\frac{n}{P}\right)\frac{1}{n^s},$$

équation de laquelle on passe, comme dans le cas déjà examiné, à cette autre:

$$(20)\qquad \begin{cases}\Sigma'\dfrac{1}{(ax^2+2bxy+cy^2)^s}+\Sigma'\dfrac{1}{(a'x^2+2b'xy+c'y^2)^s}+\cdots\\ \qquad=2^{1-s}\Sigma\dfrac{1}{n^s}\cdot\Sigma\left(\dfrac{n}{P}\right)\dfrac{1}{n^s},\end{cases}$$

le signe Σ' indiquant que dans la double sommation la moitié de la forme quadratique ne doit recevoir que des valeurs premières à $2D$. En supposant maintenant $s=1+\varrho$, ϱ étant toujours une variable infiniment petite et positive, on achèvera la solution comme dans le cas déjà traité, si l'on se rappelle que d'après ce qui a été démontré dans le §. 5, le nombre des systèmes de la forme:

$$x=2D_1v+\alpha,\quad y=2D_1w+\gamma,$$

qui rendent la moitié d'une forme improprement primitive du déterminant D première à $2D$, est $D_1\Delta$ ou $3D_1\Delta$, suivant que l'on a $D\equiv 1$ ou $D\equiv 5$ (mod. 8). On trouve ainsi pour le nombre h des formes improprement primitives:

$$(21)\qquad \begin{cases}h=\dfrac{2}{\pi}\sqrt{D_1}\,\Sigma\left(\dfrac{n}{P}\right)\dfrac{1}{n}, & D\equiv 1\ (\text{mod. }8),\\ h=\dfrac{1}{3}\dfrac{2}{\pi}\sqrt{D_1}\,\Sigma\left(\dfrac{n}{P}\right)\dfrac{1}{n}, & D\equiv 5\ (\text{mod. }8).\end{cases}$$

On doit ajouter que la seconde de ces équations est en défaut lorsqu'on a $D=-3$, comme cela résulte de l'exception à laquelle le théorème I du §. 4 est sujet dans le même cas, et que pour rétablir l'exactitude, le second membre doit être triplé.

III. Nous passons maintenant au cas des déterminants positifs, c'est-à-dire au cas où l'on a $D=D_1$, et nous supposerons d'abord que les formes différentes (15) appartiennent à l'ordre proprement primitif, et remplissent chacune les conditions (7) du §. 4. On a alors d'après le théorème III du §. 4:

$$\Sigma\frac{2^\mu}{m^s}=\Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}+\Sigma\frac{1}{(a'x^2+2b'xy+c'y^2)^s}+\cdots,$$

où la double sommation dans chacun des termes du second membre doit s'étendre

à tous les systèmes de valeurs simultanées de x et y, premières entre elles, qui donnent au trinôme où elles sont substituées, une valeur première à $2D$ et satisfont en outre aux inégalités (8) du paragraphe cité, lorsqu'il s'agit du premier terme, et à des inégalités de forme analogue pour tous les autres termes.

Comme les nombres susceptibles d'être exprimés par une forme de déterminant positif, peuvent être positifs ou négatifs, il semble d'abord que l'on doive ajouter encore la condition que les indéterminées soient choisies de manière à donner à la forme quadratique une valeur positive; mais il est aisé de voir que cette condition est déjà implicitement contenue dans les précédentes. En effet, a, b, x et y étant positifs, la condition:

$$x\geqq\frac{T-bU}{aU}y$$

entraînera évidemment celle-ci:

$$ax^2+2bxy+cy^2\geqq\frac{y^2}{aU^2}(T^2-(b^2-ac)U^2)=\frac{y^2}{aU^2}.$$

L'expression précédente de $\Sigma\frac{2^\mu}{m^s}$ étant substituée dans l'équation (12), il viendra:

$$\Sigma\frac{1}{n^{2s}}\cdot\Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}+\Sigma\frac{1}{n^{2s}}\cdot\Sigma\frac{1}{(a'x^2+2b'xy+c'y^2)^s}+\cdots$$
$$=\Sigma\frac{1}{n^s}\cdot\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n^s}.$$

On voit sans peine que le produit:

$$\Sigma\frac{1}{n^s}\cdot\Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}$$

peut être mis sous cette forme plus simple:

$$\Sigma'\frac{1}{(ax^2+2bxy+cy^2)^s},$$

où la double sommation est supposée s'étendre à toutes les valeurs simultanées de x et y, qui rendent le trinôme premier à $2D$, et en outre telles que l'on ait:

$$x>0,\quad y>0,\quad y\leqq\frac{aU}{T-bU}x.$$

Il suffit pour cela de remarquer que les conditions (8) du §. 4 conservent la même forme lorsqu'on y remplace x et y par nx et ny, n étant positif, et que si l'on écrit ensuite x et y au lieu de nx et ny, les nouvelles indéterminées x et y ne seront plus assujetties à la condition d'être premières entre elles. En

attachant donc au signe Σ' le sens que l'on vient de définir et en supposant, bien entendu, que s'il s'agit de la seconde forme, a, b dans la dernière des inégalités précédentes doivent être remplacées par a', b', et ainsi de suite, on aura l'équation:

$$(22)\qquad \begin{cases} \Sigma' \dfrac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma' \dfrac{1}{(a'x^2+2b'xy+c'y^2)^s} + \cdots \\ \qquad = \Sigma \dfrac{1}{n^s} \cdot \Sigma \delta^{\frac{1}{2}(u-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \left(\dfrac{n}{P}\right) \dfrac{1}{n^s}. \end{cases}$$

Il s'agira maintenant de voir ce que les différents termes de cette équation deviendront, lorsqu'après avoir posé $s = 1+\varrho$, la variable positive ϱ devient moindre que toute grandeur donnée. A cet effet, nous décomposerons chacun des termes du premier membre, le premier:

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}},$$

par exemple, en autant de sommes partielles qu'il y a de systèmes de la forme:

$$x = 2Dv+\alpha, \quad y = 2Dw+\gamma,$$

qui rendent le trinôme $ax^2+2bxy+cy^2$ premier à $2D$. Soit:

$$\Sigma \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}}; \quad \begin{matrix} x>0, \quad y>0, \quad y \leqq \dfrac{aU}{T-bU}x, \\ x = 2Dv+\alpha, \quad y = 2Dw+\gamma, \end{matrix}$$

l'une de ces sommes partielles, dans laquelle la sommation double relative à v et w doit s'étendre à toutes les valeurs entières depuis $-\infty$ jusqu'à ∞*). Pour obtenir l'expression de cette somme, nous désignerons par σ une variable positive quelconque, et nous chercherons le nombre qui exprime combien de fois le trinôme $ax^2+2bxy+cy^2$ dans la double sommation obtient une valeur non-supérieure à σ. Or, d'après la construction géométrique indiquée dans le §. 4, la recherche dont il s'agit, revient évidemment à la question de savoir combien dans l'intérieur ou sur le contour du secteur hyperbolique, terminé d'une part par les droites:

$$y = 0, \quad y = \frac{aU}{T-bU}x,$$

et de l'autre par l'arc de la première branche de l'hyperbole:

$$ax^2+2bxy+cy^2 = \sigma,$$

*) Compatibles avec les conditions précédentes.[1])

[1]) Anmerkung von Dirichlet's Hand in dem an Gauss gesandten Exemplar. K.

il y a de points dont les coordonnées x et y sont de la forme:

$$x = 2Dv+\alpha, \quad y = 2Dw+\gamma.$$

Ajoutons, pour être tout à fait exact, quoique cela n'influe en rien sur le résultat définitif, que l'on doit faire abstraction de ceux des points en question qui pourraient se trouver sur la partie du contour, formée par l'axe de x. Si l'on a recours aux coordonnées polaires r et φ, liées aux coordonnées rectangulaires x et y par les équations $x = r\cos\varphi$, $y = r\sin\varphi$, l'aire du secteur sera:

$$\tfrac{1}{2}\int r^2 d\varphi = \tfrac{1}{2}\sigma \int \frac{d\varphi}{a\cos^2\varphi+2b\cos\varphi\sin\varphi+c\sin^2\varphi},$$

les limites de l'intégrale étant zéro et l'angle aigu dont la tangente trigonométrique est $\frac{aU}{T-bU}$. L'intégration étant effectuée par les méthodes connues, on trouvera pour l'aire dont il s'agit, cette expression très simple:

$$\frac{\sigma}{2\sqrt{D}}\log(T+U\sqrt{D}).$$

Au moyen de ce résultat et du second lemme du §. 1, on conclura que le nombre que nous nous étions proposé de déterminer, peut être mis sous la forme:

$$\frac{\sigma}{8\sqrt{D^3}}\log(T+U\sqrt{D})+\sigma^\vartheta\psi(\sigma),$$

l'exposant constant ϑ étant compris entre $\frac{1}{2}$ et 1, et la fonction $\psi(\sigma)$ restant finie, quelque grande que l'on suppose la variable σ. Il suit de là et du premier des théorèmes du §. 1, que la somme partielle que nous considérons, est:

$$\frac{1}{8\sqrt{D^3}}\log(T+U\sqrt{D})\frac{1}{\varrho},$$

et comme d'après les résultats du §. 5, le nombre des sommes partielles contenues dans la même somme totale, est $4D\Delta$ ou $2D\Delta$, suivant que D est pair ou impair, on conclura que chacun des termes du premier membre de l'équation (22) est selon ces deux cas, et pour une valeur infiniment petite de ϱ:

$$\frac{\Delta}{2\sqrt{D^3}}\log(T+U\sqrt{D})\frac{1}{\varrho}, \quad \text{ou} \quad \frac{\Delta}{4\sqrt{D^3}}\log(T+U\sqrt{D})\frac{1}{\varrho}.$$

Si donc nous désignons par h le nombre des formes différentes du déterminant D, le premier membre sera:

$$\frac{h\Delta}{2\sqrt{D^3}}\log(T+U\sqrt{D})\frac{1}{\varrho}, \quad \text{ou} \quad \frac{h\Delta}{4\sqrt{D^3}}\log(T+U\sqrt{D})\frac{1}{\varrho},$$

selon que D est pair ou impair.

Comme, d'un autre côté et en vertu des résultats (13) et (14), le second membre est respectivement dans ces deux cas:

$$\frac{A}{D}\cdot\frac{1}{\varrho}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n} \quad \text{ou} \quad \frac{A}{2D}\cdot\frac{1}{\varrho}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n},$$

on conclura, en supprimant le facteur $\frac{1}{\varrho}$, commun aux deux membres:

$$h=\frac{2\sqrt{D}}{\log(T+U\sqrt{D})}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}, \tag{23}$$

équation qui convient à un déterminant positif (non-carré) quelconque, pair ou impair, et dans laquelle T et U sont les plus petits entiers positifs, autres que 1 et 0, qui satisfont à l'équation $t^2-Du^2=1$.

IV. Le cas où le déterminant positif D est de la forme $4\nu+1$, et où les formes de ce déterminant dont il s'agit de déterminer le nombre h, sont celles de l'ordre improprement primitif, étant entièrement semblable à celui que nous venons de traiter en détail, nous nous contenterons de rapporter le résultat qui répond à ce cas, et qui est contenu dans les équations qui suivent:

$$\begin{cases} h=\dfrac{2\sqrt{D}}{\log\frac{1}{2}(T+U\sqrt{D})}\,\Sigma\left(\dfrac{n}{P}\right)\dfrac{1}{n}, & D\equiv 1 \pmod 8,\\ h=\dfrac{1}{3}\dfrac{2\sqrt{D}}{\log\frac{1}{2}(T+U\sqrt{D})}\,\Sigma\left(\dfrac{n}{P}\right)\dfrac{1}{n}, & D\equiv 5 \pmod 8, \end{cases} \tag{24}$$

dans lesquelles T et U désignent les moindres entiers positifs, autres que 2 et 0, qui satisfont à l'équation $t^2-Du^2=4$.

V. Nous nous occuperons maintenant de la recherche déjà indiquée dans le §. 3, en prouvant que les genres énumérés d'après les principes connus et que nous avons rappelés dans le paragraphe cité, existent tous réellement et contiennent chacun le même nombre de formes. Soient à cet effet:

$$\varphi,\ \varphi',\ \varphi'',\ \ldots \quad | \quad \psi,\ \psi',\ \psi'',\ \ldots \tag{25}$$

les expressions qui servent à faire cette énumération pour un déterminant quelconque, soit qu'il s'agisse des formes proprement primitives, soit qu'il s'agisse de celles qui composent l'ordre improprement primitif, lorsque ce dernier ordre existe pour le déterminant donné. Les déterminants carrés étant exclus, la première partie de la ligne précédente contiendra au moins un terme, et il résulte de l'inspection des deux tableaux donnés dans le §. 3, que les expressions

$\varphi,\ \varphi',\ \varphi'',\ \ldots$ qui forment cette première partie, sont toujours telles qu'on ait:

$$\varphi\varphi'\varphi''\ldots=\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{m}{P}\right). \tag{26}$$

Nous désignerons généralement par χ l'une quelconque des expressions (25), ou l'un quelconque des produits que l'on peut former avec ces expressions, en les combinant 2 à 2, 3 à 3, et ainsi de suite, ou enfin le produit de toutes, en n'excluant que le seul produit (26), autrement dit, nous désignerons par χ l'un quelconque des termes de l'expression développée:

$$[(1+\varphi)(1+\varphi')(1+\varphi'')\ldots][(1+\psi)(1+\psi')(1+\psi'')\ldots]-\varphi\varphi'\varphi''\ldots-1. \tag{27}$$

Si nous conservons à la lettre λ la même signification que nous lui avons donnée dans le §. 3, le nombre des expressions χ sera $2^\lambda-2$. Cela supposé, nous allons faire voir que si l'on partage le nombre total h des formes qui répondent au déterminant donné, en deux groupes comprenant respectivement H et H' formes, en rangeant dans le premier groupe toutes celles qui satisfont à la condition $\chi=1$, et dans le second celles qui remplissent la condition opposée $\chi=-1$, on aura toujours:

$$H-H'=0.$$

Pour prouver ce dont il s'agit, il suffira d'appliquer l'analyse dont nous avons fait usage, en partant de l'équation (12), à l'équation plus générale (11), après avoir attribué dans cette dernière à θ, η, P_2 et R_1 des valeurs qui font coïncider l'expression $\theta^{\frac{1}{2}(m-1)}\eta^{\frac{1}{8}(m^2-1)}\left(\frac{m}{P_2R_1}\right)$ avec χ. Il est facile de voir qu'en remplissant cette condition, il ne peut arriver qu'on ait à la fois, soit:

$$\theta=1,\quad \eta=1,\quad P_2R_1=\pm 1,$$

soit:

$$\delta\theta=1,\quad \varepsilon\eta=1,\quad P_1R_1=\pm 1.$$

L'impossibilité du premier système de valeurs simultanées résulte de ce que χ contient au moins un facteur de l'une des formes:

$$(-1)^{\frac{1}{2}(m-1)},\quad (-1)^{\frac{1}{8}(m^2-1)},\quad \left(\frac{m}{P}\right),\quad \left(\frac{m}{r}\right);$$

et pour que le second pût avoir lieu, il faudrait que l'on eût $\theta=\delta$, $\eta=\varepsilon$, $P_2R_1=\pm P$, ce qui donnerait à χ la forme:

$$\vartheta^{\frac{1}{2}(m-1)}\varepsilon^{\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)=\varphi\varphi'\varphi''\ldots,$$

que nous avons exclue plus haut. Il résulte de là que chacun des deux facteurs du second membre de l'équation (11) est de même nature que le second facteur du second membre de l'équation (12), et que par conséquent ces deux facteurs convergent l'un et l'autre vers une limite finie de la forme (14), lorsque la variable ϱ devient infiniment petite. Pour discuter le premier membre de l'équation (11) dans la même circonstance, il faudra substituer à l'égalité (16), lorsqu'il s'agit d'un déterminant négatif et de l'ordre proprement primitif, celle-ci:

$$\Sigma\chi\frac{2^{\mu+1}}{m^s}=\pm\Sigma\frac{1}{(ax^2+2bxy+cy^2)^s}\pm\Sigma\frac{1}{(a'x^2+2b'xy+c'y^2)^s}\pm\cdots,$$

où l'on doit choisir le signe supérieur ou le signe inférieur dans chacun des termes du second membre, suivant que la forme que ce terme contient, satisfait à la condition $\chi=1$, ou à $\chi=-1$, et il faudra faire une substitution analogue dans les trois autres cas. Cela posé, on voit sans peine et sans qu'il soit nécessaire d'entrer dans aucun détail à cet égard, que le premier membre de l'équation (11), en y supposant toujours la variable ϱ infiniment petite, sera, abstraction faite d'un facteur purement numérique, et qui varie suivant les quatre cas, le produit de $(H-H')\frac{1}{\varrho}$ et d'une expression telle que:

$$\frac{\Delta}{\sqrt{D_1^3}}\pi,\quad \frac{\Delta}{\sqrt{D^3}}\log(T+U\sqrt{D})\quad\text{ou}\quad \frac{\Delta}{\sqrt{D^3}}\log\tfrac{1}{2}(T+U\sqrt{D}).$$

Or, cette dernière expression étant manifestement différente de zéro, il faut, pour que le premier membre reste fini comme le second, qu'on ait:

$$H-H'=0,$$

ce qu'il s'agissait de faire voir.

Au moyen de ce résultat, il nous sera facile de prouver que les formes sont également réparties entre les genres énumérés d'après les règles du §. 3. Soit pour abréger $2^{\lambda-1}=\varkappa$, et désignons par $h_1, h_2, h_3, \ldots, h_\varkappa$ les nombres des formes contenues dans les différents genres, rangés dans un ordre quelconque, les termes de la suite précédente qui répondraient à des genres non-existants étant supposés égaux à zéro. Si maintenant l'on remarque que les formes qui composent un même genre, satisfont tous ou à la condition $\chi=1$, ou à la condition opposée $\chi=-1$, il est évident que toute équation de la forme:

$$H-H'=0$$

peut s'écrire comme il suit:

$$h_1\pm h_2\pm h_3\pm\ldots\pm h_\varkappa=0. \tag{28}$$

Nous avons donné dans cette équation le signe + au premier terme; le signe de tout autre terme est + ou −, selon que le genre auquel ce terme correspond, satisfait à la même condition $\chi=\pm1$ que celui auquel se rapporte h_1, ou à la condition opposée. Il s'agira maintenant d'examiner combien de fois, dans l'ensemble des équations analogues à la précédente et dont le nombre est $2^\lambda-2$, comme celui des expressions χ, un terme quelconque h_ω, autre que le premier, a le signe + ou le signe −, ou autrement dit, combien de fois ce terme a un signe égal ou opposé à celui du premier terme. Soit à cet effet:

$$\varphi=\alpha,\quad \varphi'=\alpha',\quad \varphi''=\alpha'',\quad \ldots\quad |\quad \psi=\beta,\quad \psi'=\beta',\quad \psi''=\beta'',\quad \ldots$$

le caractère complet du genre pour lequel h_1 désigne le nombre des formes, $\alpha, \alpha', \alpha'', \ldots$; $\beta, \beta', \beta'', \ldots$ étant des valeurs déterminées de la forme ±1, dont les premières satisfont à la condition $\alpha\alpha'\alpha''\cdots=1$. Soit de même:

$$\varphi=\mathfrak{a},\quad \varphi'=\mathfrak{a}',\quad \varphi''=\mathfrak{a}'',\quad \ldots\quad |\quad \psi=\mathfrak{b},\quad \psi'=\mathfrak{b}',\quad \psi''=\mathfrak{b}'',\quad \ldots$$

le caractère complet du genre auquel se rapporte h_ω. Cela posé, il suffit de se reporter à l'expression (27) dont le développement donne toutes les expressions χ, pour voir que l'excès du nombre des cas où h_1 et h_ω ont le même signe, sur celui où ils sont précédés de signes opposés, sera donné par l'expression qui suit:

$$[(1+\alpha\mathfrak{a})(1+\alpha'\mathfrak{a}')\ldots][(1+\beta\mathfrak{b})(1+\beta'\mathfrak{b}')\ldots]-\alpha\mathfrak{a}\alpha'\mathfrak{a}'\ldots-1.$$

Or les deux caractères complets étant différents, on ne saurait avoir à la fois:

$$\alpha\mathfrak{a}=1,\quad \alpha'\mathfrak{a}'=1,\quad \ldots;\qquad \beta\mathfrak{b}=1,\quad \beta'\mathfrak{b}'=1,\quad \ldots;$$

la première partie de l'expression précédente a donc la valeur zéro, et comme l'on a évidemment:

$$\alpha\mathfrak{a}.\alpha'\mathfrak{a}'\cdots=1,$$

l'excès dont il s'agit a la valeur −2. Il suit de là que si l'on ajoute toutes les équations de la forme (28), dont le nombre est $2^\lambda-2$, et l'équation évidente:

$$2h_1+2h_2+2h_3+\cdots+2h_\varkappa=2h,$$

il en résultera celle-ci: $2^\lambda h_1=2h$, et par suite $h_1=\frac{h}{2^{\lambda-1}}$, ce qui prouve que la totalité des formes se partage également entre les différents genres, le genre auquel se rapporte le nombre h_1, ayant été arbitrairement choisi.

On a ainsi une démonstration nouvelle et très simple de l'un des principaux théorèmes de la théorie des formes quadratiques et qui n'avait été établi

jusqu'à présent que par le concours d'un grand nombre de considérations diverses. Voyez l'ouvrage de M. GAUSS, art. 252, 261 et 287, III.

Il nous resterait maintenant à développer les théorèmes que contiennent les équations établies dans les quatre numéros précédents de ce paragraphe et qui sont de deux espèces, les uns résultant des expressions de h telles que nous les avons obtenues dans ce qui précède, les autres exigeant au contraire que l'on effectue préalablement les sommations indiquées dans ces expressions, pour que le nombre h se présente sous une forme purement arithmétique. Comme les résultats dont il s'agit, sont très nombreux et pour la plupart entièrement nouveaux, il sera convenable de les présenter avec quelque étendue. Par cette raison j'en remettrai l'exposition à la continuation de ces recherches, et je terminerai cette première partie, en remplissant l'engagement que j'ai pris dans le mémoire déjà cité sur la progression arithmétique. D'après le §. 11 de ce mémoire*), il reste à prouver que la somme:

$$\Sigma(\pm 1)^{\alpha}(\pm 1)^{\beta}(\pm 1)^{\gamma}(\pm 1)^{\varepsilon}\ldots\frac{1}{n}$$

dans laquelle les signes supérieurs n'ont pas simultanément lieu, a une valeur différente de zéro.

Partageons les nombres premiers positifs $p, p', p'', \ldots$ auxquels se rapportent les valeurs ambiguës de la forme ± 1, à partir de la troisième, en deux groupes, en comprenant dans le premier groupe tous ceux de ces nombres premiers, auxquels le signe inférieur correspond. En continuant à représenter par $p, p', p'', \ldots$ les nombres du premier groupe, soit:

$$\pm pp'p''\ldots = P,$$

le double signe restant à fixer; soient encore $r, r', r'', \ldots$ ceux du second groupe et posons:

$$rr'r''\ldots = R.$$

Cela posé, il résulte de la signification des lettres $\alpha, \beta, \gamma, \gamma', \ldots$, expliquée dans le §. 7 du mémoire cité, que la somme précédente peut être mise sous la forme:

$$\Sigma(\pm 1)^{\frac{1}{2}(n-1)}(\pm 1)^{\frac{1}{2}(n'-1)}\left(\frac{n}{P}\right)\frac{1}{n}.$$

Si maintenant l'on suppose le signe arbitraire dans l'équation:

$$\pm pp'p''\ldots = P$$

*) S. 341 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

tellement choisi que le nombre P soit de la forme $4\mu+1$ ou de la forme $4\mu+3$, suivant que le signe donné dans l'expression $(\pm 1)^{\frac{1}{2}(n-1)}$ est le signe supérieur ou inférieur, il est évident que la somme précédente coïncidera avec celle que contient l'expression obtenue plus haut pour le nombre h des formes qui répondent au déterminant D, en supposant ce déterminant égal à PR^2 ou à $2PR^2$, suivant que le signe donné dans l'expression $(\pm 1)^{\frac{1}{2}(n'-1)}$ est le signe supérieur ou le signe inférieur. On conclut de là que la somme que nous avions à considérer, est en effet toujours différente de zéro, puisque, s'il en était autrement, le nombre h se réduirait lui-même à zéro, ce qui est impossible, comme on le voit par la forme $x^2 - Dy^2$, qui a lieu quel que soit le déterminant D.*)

§. 7.

Nous allons maintenant développer les conséquences qui dérivent des équations établies dans les 4 premiers numéros du paragraphe précédent, en commençant par celles qui s'obtiennent indépendamment de la sommation des deux séries générales contenues dans les expressions de h. Nous passerons ensuite à celles qui résultent de cette sommation, que l'on peut effectuer soit par l'intégration d'une fraction rationnelle, soit au moyen des séries connues de sinus ou de cosinus.

Reprenons l'équation (17), dans laquelle les deux sommations relatives à n doivent s'étendre à tous les entiers positifs impairs et premiers au déterminant négatif D. Si dans la première de ces deux sommes l'on écrit n' à la place de n, l'équation pourra se mettre sous la forme:

$$(1)\quad \Sigma'\frac{1}{(ax^2+2bxy+cy^2)^{\gamma}}+\Sigma'\frac{1}{(a'x^2+2b'xy+c'y^2)^{\gamma}}+\cdots=2\Sigma\delta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n'-1)}\left(\frac{n}{P}\right)\frac{1}{(nn')^{\gamma}},$$

le signe Σ indiquant une double sommation relative à n et n'. Il est facile de donner à cette série la forme d'une série simple, en réunissant en un seul tous les termes pour lesquels le produit nn' a la même valeur. On aura ainsi pour terme général $\sigma_n\frac{1}{n^{\gamma}}$, n ayant toujours la même signification que précédemment, et σ_n désignant l'excès du nombre des diviseurs k de n qui satisfont à la condition:

$$\delta^{\frac{1}{2}(k-1)}\varepsilon^{\frac{1}{2}(k'-1)}\left(\frac{k}{P}\right)=1,$$

*) Hier schliesst der erste im 19. Bande des CRELLE'schen Journals abgedruckte, vom 4. Juli 1839 datirte Theil der Abhandlung. K.

sur celui de ces diviseurs qui satisfont à la condition opposée:

$$\delta^{\frac{1}{2}(k-1)}\varepsilon^{\frac{1}{2}(k^2-1)}\left(\frac{k}{P}\right) = -1.$$

Le premier membre peut également se réduire à une série simple de forme analogue et dont le terme général a pour coefficient le nombre qui exprime combien de fois l'entier n peut être représenté par la totalité des formes quadratiques, en attribuant aux indéterminées x et y de ces formes des valeurs quelconques positives ou négatives, premières entre elles ou non. En désignant le nombre dont il s'agit par τ_n, on aura:

$$\Sigma\tau_n\frac{1}{n^s} = 2\Sigma\sigma_n\frac{1}{n^s}.$$

Cette équation ayant lieu pour toute valeur de l'indéterminée s, supérieure à l'unité, il est facile d'en conclure qu'on a $\tau_n = 2\sigma_n$.

Ce résultat et celui qui se déduit de la même manière de l'équation (20), après en avoir mis le second membre sous la forme:

$$2\Sigma\left(\frac{n}{P}\right)\frac{1}{(2nn')^s},$$

peuvent être réunis dans l'énoncé commun que voici et dans lequel nous distinguons en formes de première et de seconde espèce celles que nous avons appelées précédemment proprement et improprement primitives*).

„n étant un entier positif impair et premier au déterminant négatif D, si l'on désigne par σ l'excès du nombre des diviseurs k de n qui sont tels qu'on ait $\delta^{\frac{1}{2}(k-1)}\varepsilon^{\frac{1}{2}(k^2-1)}\left(\frac{k}{P}\right) = 1$ (où δ, ε et P ont la signification que nous avons fixée au §. 6), sur celui de ces diviseurs qui remplissent la condition opposée $\delta^{\frac{1}{2}(k-1)}\varepsilon^{\frac{1}{2}(k^2-1)}\left(\frac{k}{P}\right) = -1$, le double du nombre σ exprimera de combien de manières différentes l'entier n $(2n)$ est susceptible d'être représenté par le système complet des formes de première (seconde) espèce, dont D est le déterminant."

*) J'ai cru devoir sur ce point m'écarter de la terminologie adoptée dans les Disq. arithm., pour pouvoir conserver dans les dénominations l'analogie qui existe entre les objets qu'elles servent à désigner. Les formes quadratiques à coefficients complexes dont nous aurons à nous occuper dans la suite de ces recherches, présentent sous le rapport dont il s'agit ici, une variété plus grande que les formes ordinaires, et à laquelle les expressions employées par M. Gauss ne s'adapteraient que difficilement. En effet dans les formes de cette nature, le plus grand diviseur commun de a, $2b$, c peut être l'unité, le nombre $1+\sqrt{-1}$, ou enfin le nombre 2, en supposant toujours celui de a, b, c égal à l'unité.

Il importe de remarquer que ce résultat présente les mêmes cas d'exception que le théorème I du §. 4, et que le nombre des représentations est respectivement pour ces deux cas 4σ ou 6σ.

En attribuant à D des valeurs déterminées, on obtient des théorèmes très simples tels que ceux-ci:

„Le nombre des solutions de l'équation $x^2+y^2 = n$ est égal au quadruple de l'excès du nombre des diviseurs de n qui ont la forme $4\nu+1$, sur celui des diviseurs compris dans la forme $4\nu+3$."

„Le nombre des solutions de l'équation $x^2+2y^2 = n$ est égal au double de l'excès des diviseurs de n, qui sont de l'une des formes $8\nu+1$, 3, sur celui de ces diviseurs qui sont de l'une de celles-ci: $8\nu+5$, 7."

Et ainsi de suite.

Le premier de ces théorèmes particuliers était déjà connu. M. Jacobi qui l'avait d'abord conclu du rapprochement de deux séries qui appartiennent à la théorie des fonctions elliptiques, en a donné depuis une démonstration purement arithmétique*).

On peut, par des considérations du même genre, parvenir au résultat général énoncé ci-dessus en partant du théorème déjà cité du §. 4. C'est ce que nous allons faire voir en peu de mots en nous bornant au cas où les formes sont de la première espèce, le même raisonnement s'appliquant à l'autre cas. Supposons en premier lieu que les diviseurs simples de n soient tous de l'espèce de ceux que nous avons désignés par f, et posons $n = f_1^{\lambda_1}f_2^{\lambda_2}f_3^{\lambda_3}\ldots$, f_1, f_2, f_3, ... désignant des nombres premiers inégaux. Pour faire l'énumération complète de toutes les représentations dont n est susceptible, nous les rangerons en groupes, en comprenant dans le même groupe celles de ces représentations pour lesquelles le plus grand diviseur commun des indéterminées x et y a la même valeur l, dont le carré devra évidemment diviser n. Il est évident que le nombre des représentations contenues dans un pareil groupe, est le même que celui des représentations de l'entier $\frac{n}{l^2}$, en assujettissant les indéterminées x et y à être premières entre elles. Or il résulte de la supposition faite sur la nature de f_1, f_2, ... et du théorème déjà cité, que ce dernier nombre est exprimé par 2.2^μ, μ désignant le nombre des diviseurs simples inégaux de $\frac{n}{l^2}$.

*) Voyez le Tome XII du Journal de Crelle p. 167.

Tout se réduit donc à déterminer la somme des puissances 2^μ qui correspondent aux entiers de la forme $\frac{n}{l^2}$. Pour obtenir cette somme, considérons le polynôme:

$$F_1 = 2f_1^{\lambda_1} + 2f_1^{\lambda_1-2} + 2f_1^{\lambda_1-4} + \cdots$$

qui doit être continué tant que les exposants ne deviennent pas négatifs, et dans lequel le coefficient du dernier terme est supposé égal à 2 ou à 1, selon que l'exposant de ce terme a la valeur 1 ou 0. Le produit développé de ce polynôme et des polynômes analogues relatifs à $f_2, f_3, \ldots$ étant évidemment composé de tous les termes de la forme $2^\mu \frac{n}{l^2}$, on obtiendra la somme des puissances 2^μ, en remplaçant les nombres $f_1, f_2, \ldots$ par l'unité. Mais par ce changement $F_1, F_2, \ldots$ deviendront respectivement $\lambda_1+1, \lambda_2+1, \ldots$, d'où l'on conclut que le nombre des représentations qu'il s'agit d'obtenir, est égal au double du produit $(\lambda_1+1)(\lambda_2+1)\ldots$, qui exprime, comme l'on sait, le nombre des diviseurs de n. On voit que dans ce premier cas, le résultat est conforme à l'énoncé général, puisque dans ce cas, où les diviseurs remplissent tous la première des deux conditions exprimées dans cet énoncé, le nombre des diviseurs ne diffère pas de l'excès désigné par σ. Passons maintenant au cas général où n renferme aussi des nombres premiers g, tels qu'on ait:

$$\delta^{\frac{1}{2}(g-1)} \varepsilon^{\frac{1}{8}(g^2-1)} \left(\frac{g}{P}\right) = -1,$$

et posons:

$$n = f_1^{\lambda_1} f_2^{\lambda_2} \ldots \times g_1^{\nu_1} g_2^{\nu_2} \ldots$$

Il est facile de conclure du cas déjà examiné que dans cette supposition le nombre des représentations dont n est susceptible, sera exprimé par $2(\lambda_1+1)(\lambda_2+1)\ldots$, lorsque les exposants $\nu_1, \nu_2, \ldots$ sont tous pairs, et se réduit au contraire à zéro, lorsque cette circonstance n'a pas lieu. Nous avons donc à prouver que l'excès σ a la valeur $(\lambda_1+1)(\lambda_2+1)\ldots$ ou la valeur zéro, selon que n se trouve dans le premier ou le second de ces deux cas. Pour y parvenir, faisons le produit des expressions:

$$1+f_1+\cdots+f_1^{\lambda_1},\quad 1+f_2+\cdots f_2^{\lambda_2},\quad \ldots,\quad 1+g_1+\cdots+g_1^{\nu_1},\quad 1+g_2+\cdots g_2^{\nu_2},\quad \ldots$$

dont les différents termes donnent tous les diviseurs de n. L'un quelconque de ces diviseurs étant désigné par k, on aura $\delta^{\frac{1}{2}(k-1)} \varepsilon^{\frac{1}{8}(k^2-1)} \left(\frac{k}{P}\right) = \pm 1$, le signe supérieur ou inférieur ayant lieu, selon que le nombre des facteurs $g_1, g_2, \cdots$

contenus dans k sera pair ou impair. On conclut de là que le produit précédent se changera en σ, si l'on y fait $1 = f_1 = f_2 = \cdots$, $-1 = g_1 = g_2 = \cdots$. Le produit deviendra ainsi:

$$(\lambda_1+1)(\lambda_2+1)\ldots \times \frac{1-(-1)^{\nu_1+1}}{2} \cdot \frac{1-(-1)^{\nu_2+1}}{2} \cdots,$$

et il est évident que cette expression est en effet $(\lambda_1+1)(\lambda_2+1)\ldots$, lorsque $\nu_1, \nu_2, \ldots$ sont tous pairs, et zéro dans tout autre cas.

Les résultats précédents sont relatifs au cas où le déterminant D est un entier négatif. Il existe des propriétés analogues pour les formes dont le déterminant est positif. Pour établir ces propriétés, on peut faire usage des séries que nous avons considérées dans les Nos. III et IV du §. 6. On peut aussi y parvenir par des raisonnements purement arithmétiques entièrement semblables à ceux que nous venons d'indiquer, et en prenant pour point de départ le théorème III du §. 4.

Il serait donc inutile d'entrer dans de nouveaux détails à cet égard, et nous nous bornerons à énoncer les résultats qui se rapportent aux formes à déterminant positif. Mais il est bon de faire précéder cet énoncé d'une remarque propre à le simplifier et qui concerne les conditions auxquelles les coefficients des formes à déterminant positif ont été assujetties dans les §§. 4 et 6. On y a supposé, que les coefficients de chacune de ces formes, telle que $ax^2+2bxy+cy^2$, étaient les deux premiers positifs, le troisième négatif. Or de ces conditions la première et la troisième sont seules nécessaires, et tout ce qui a été démontré dans les paragraphes cités, subsiste également lorsque b est négatif ou zéro. Nous n'avons en effet eu nulle part égard au signe du coefficient moyen, si ce n'est dans le No. III du §. 6, pour prouver que l'expression $ax^2+2bxy+cy^2$ est positive, lorsqu'on y suppose:

$$x>0,\quad y>0,\quad y \leqq \frac{aU}{T-bU}\, x.$$

Mais il est facile de voir que ce résultat ne dépend pas non plus du signe de b. Pour s'en assurer, on remarquera que la dernière des inégalités précédentes peut se mettre sous la forme $(ax+by)U \geqq yT$, d'où l'on conclut, le second membre étant positif, $(ax+by)^2 U^2 \geqq y^2 T^2$. On a, d'un autre côté, $T^2 > DU^2$, et par suite en multipliant, $(ax+by)^2 > Dy^2$, ou ce qui revient au même, le coefficient a étant positif, $ax^2+2bxy+cy^2 > 0$; ce qu'il s'agissait de prouver.

En ayant égard à la remarque qui vient d'être faite, et désignant comme

précédemment par ω l'unité ou le nombre 2, selon qu'il s'agira de formes de première ou de seconde espèce, on pourra réunir les résultats dont il s'agit dans l'énoncé suivant.

„D étant un entier positif (non-carré) et T et U désignant les plus petites valeurs positives de t et u (autres que ω et 0) qui satisfont à l'équation $t^2 - Du^2 = \omega^2$, supposons que:

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

soient les formes différentes de première (seconde) espèce, ayant le nombre D pour déterminant, ces formes étant tellement choisies que les coefficients de x^2 soient tous positifs, et ceux de y^2 tous négatifs; supposons encore que les indéterminées x et y ne doivent recevoir que des valeurs positives, et soient de plus assujetties dans la première de ces formes à la condition $y \leq \frac{aU}{T-bU}x$, et dans les autres à des conditions analogues. Cela étant et n désignant un entier positif, impair et premier à D, je dis que le nombre des représentations différentes dont ωn est susceptible au moyen des formes données, est égal à l'excès du nombre des diviseurs k de n, pour lesquels l'expression $\vartheta^{\frac{1}{2}(k-1)}\varepsilon^{\frac{1}{8}(k^2-1)}\left(\frac{k}{P}\right)$ a la valeur 1, sur celui de ces diviseurs qui donnent à la même expression la valeur -1.“

Pour appliquer ce théorème à un cas particulier, soit $D = 2$. On a alors $\omega = 1$, $T = 3$, $U = 2$, $\vartheta = 1$, $\varepsilon = -1$, $P = 1$, et le système complet des formes se réduit à un seul terme, pour lequel nous pouvons prendre la forme $x^2 - 2y^2$. Le résultat relatif à ce cas est donc:

„Si dans l'équation $x^2 - 2y^2 = n$, où n est impair et positif, les indéterminées x et y ne sont susceptibles que de valeurs positives et en outre telles qu'on ait $3y \leq 2x$, le nombre des solutions de cette équation sera exprimé par l'excès du nombre des diviseurs de n qui ont l'une des formes $8\nu \pm 1$, sur celui de ces diviseurs qui sont de l'une de celles-ci: $8\nu \pm 5$.“

Comme dans l'équation (1) établie ci-dessus, de même que dans les trois équations analogues que pour abréger nous nous sommes dispensés d'écrire, les deux membres sont égaux par groupes de termes, en ce sens que le terme unique qui résulte de la réunion de tous les termes particuliers du second membre, pour lesquels le produit nn' a une valeur déterminée, est identique à celui qui provient dans le premier de tous les termes particuliers pour lesquels

les formes quadratiques ont cette même valeur déterminée, on voit que la vérité de ces équations est indépendante de la forme particulière de la fonction qui y entre, et que cette fonction qui, dans ces équations telles qu'elles se sont présentées d'abord, est une puissance de l'exposant $-s$, peut être remplacée par une fonction entièrement arbitraire. Il viendra ainsi, en n'écrivant toujours que l'équation qui se rapporte au premier des quatre cas généraux:

$$(2) \quad \Sigma'\varphi(ax^2+2bxy+cy^2)+\Sigma'\varphi(a'x^2+2b'xy+c'y^2)+\cdots = 2\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\varphi(nn'),$$

les signes sommatoires ayant toujours la même signification. Il faut seulement ajouter que la fonction désignée par la caractéristique φ doit être telle que les séries précédentes soient convergentes et du nombre de celles que nous avons appelées séries de première espèce. Cette condition se trouvera remplie, par exemple, si l'on suppose:

$$\varphi(z) = q^z,$$

q étant une constante réelle ou imaginaire, dont la valeur numérique ou le module soit moindre que l'unité. Ce cas est surtout remarquable, en ce qu'il permet d'effectuer l'une des sommations dans le second membre et de transformer les séries doubles contenues dans le premier, en sommes de produits de séries simples, de sorte que l'équation exprime alors un rapport entre certaines séries simples qui sont précisément celles qui se présentent dans la théorie des fonctions elliptiques. La simplification dont nous parlons, n'a toutefois lieu que pour l'équation (2) et pour l'autre équation analogue qui se rapporte à une valeur négative de D; elle ne s'étend pas au cas où le déterminant est positif. On peut bien, dans ce dernier cas, exécuter encore l'une des sommations indiquées dans le second membre, mais les conditions d'inégalité auxquelles sont assujetties celles relatives à x et y empêchent que les séries doubles en x et y ne soient transformées en produits de séries simples.

Comme les formules auxquelles on se trouve conduit par la réduction dont nous venons de parler, sont nouvelles et paraissent présenter quelque intérêt, nous indiquerons brièvement la manière dont on peut l'effectuer. L'équation (2), lorsqu'on y attribue à la fonction φ la forme exponentielle, se change en celle-ci:

$$(3) \quad \Sigma'q^{ax^2+2bxy+cy^2}+\Sigma'q^{a'x^2+2b'xy+c'y^2}+\cdots = 2\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)q^{nn'}.$$

Dans le cas particulier où les coefficients moyens b, b', ... sont tous égaux

à zéro, le premier membre se présente immédiatement comme la somme d'un nombre limité de produits de séries simples. Soit, par exemple, $D=-2$; il n'existe alors que la seule forme x^2+2y^2, et la somme $\Sigma' q^{x^2+2y^2}$, dans laquelle x^2+2y^2 ne doit recevoir que des valeurs impaires, devra s'étendre à tous les entiers impairs x, et à tous les entiers pairs ou impairs y. En réunissant les termes qui répondent à des valeurs opposées de x ou de y, le premier membre prendra la forme de ce produit:

$$2(q+q^{3^2}+q^{5^2}+\cdots)(1+2q^2+2q^{2.2^2}+2q^{2.3^2}+\cdots).$$

Quant au second membre, comme l'on a $\delta=-1$, $\varepsilon=-1$, $P=-1$, il deviendra $2\Sigma(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}q^{nn'}$, le signe Σ s'étendant à toutes les valeurs positives et impaires de n et de n'. En effectuant la sommation par rapport à n', on aura:

$$2\Sigma(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}\frac{q^n}{1-q^{2n}}.$$

On a donc dans ce cas particulier l'équation:

$$(q+q^9+q^{25}+\cdots)(1+2q^3+2q^8+2q^{18}+\cdots)=\frac{q}{1-q^2}+\frac{q^3}{1-q^6}-\frac{q^5}{1-q^{10}}-\frac{q^7}{1-q^{14}}+\cdots,$$

facile à vérifier par les formules connues de la théorie des fonctions elliptiques.

Passons à un cas plus général et qui suffira pour montrer de quelle manière la réduction dont il est question, pourra être effectuée quelle que soit la valeur négative attribuée à D. Soit $D=-p$, p désignant un nombre premier $4\nu+3$. Dans cette supposition on a $\delta=1$, $\varepsilon=1$, $P=-p$; le second membre deviendra donc, en mettant au lieu de $\left(\frac{n}{-p}\right)$ l'expression équivalente $\left(\frac{n}{p}\right)$:

$$2\Sigma\left(\frac{n}{p}\right)q^{nn'}.$$

Comme n et n' doivent recevoir toutes les valeurs positives impaires et premières à p, l'expression précédente, en y effectuant la sommation relative à n', se changera en:

$$(4)\qquad 2\Sigma\left(\frac{n}{p}\right)\frac{q^n}{1-q^{2n}}-2\Sigma\left(\frac{n}{p}\right)\frac{q^{np}}{1-q^{2np}}.$$

Considérons maintenant l'une des sommes doubles contenues dans le premier membre de l'équation (3), la première par exemple. D'après ce que nous avons vu au §. 5, les valeurs simultanées que x et y doivent obtenir dans

cette somme, peuvent être distribuées en un certain nombre de systèmes de la forme $x=2pu+\alpha$, $y=2pv+\gamma$, où α et γ sont des entiers déterminés et u et v des entiers indéterminés qui doivent prendre toutes les valeurs depuis $-\infty$ jusqu'à ∞. On aura donc, pour la somme partielle qui répond à ce système, en mettant $ax^2+2bxy+cy^2$ sous la forme $\frac{1}{a}((ax+by)^2+py^2)$:

$$\Sigma q^{\frac{1}{a}(2p(au+bv)+a\alpha+b\gamma)^2}q^{\frac{p}{a}(2pv+\gamma)^2}.$$

Décomposons maintenant cette somme partielle à son tour en d'autres sommes, en écrivant successivement av, $av+1$, ..., $av+a-1$ à la place de v. On aura ainsi pour l'une quelconque de ces nouvelles sommes partielles, dont le nombre est a, l'expression suivante qui se rapporte à la substitution de $av+\lambda$, et dans laquelle on a fait, pour abréger, $2pb\lambda+a\alpha+b\gamma=k$, $2p\lambda+\gamma=l$:

$$\Sigma q^{\frac{1}{a}(2pa(u+bv)+k)^2}q^{\frac{p}{a}(2pav+l)^2}.$$

Or, si l'on considère maintenant la sommation relative à u comme devant être effectuée la première, rien n'empêche de remplacer $u+bv$ par u, et le résultat prend la forme d'un produit de deux séries simples:

$$(5)\qquad \Sigma q^{\frac{1}{a}(2pau+k)^2}\Sigma q^{\frac{p}{a}(2pav+l)^2}.$$

Il est d'ailleurs facile de voir que ces deux séries peuvent être réduites à la fonction si remarquable que M. Jacobi a introduite dans la théorie des fonctions elliptiques et qui a pour expression:

$$1-q\cos 2x+2q^4\cos 4x-2q^9\cos 6x+\cdots.$$

D'un autre côté, on peut aussi réduire aux fonctions elliptiques les deux séries (4), en combinant les formules connues de cette théorie avec les belles expressions que M. Gauss a données pour exprimer $\left(\frac{n}{p}\right)$ par une série finie de sinus ou de cosinus.

Les formules que l'on obtient ainsi, me paraissent surtout remarquables en ce que les produits de la forme (5), qui composent le premier membre, dépendent, quant à leur nombre et quant aux constantes a, k, l qu'ils renferment, du nombre et des coefficients des formes quadratiques différentes qui ont lieu pour le déterminant correspondant, et il y a lieu d'espérer qu'en approfondissant le rapprochement que nous venons d'indiquer, on parviendra à des résultats plus importants et qui pourront jeter un nouveau jour sur la nature des formes

quadratiques à déterminant négatif. C'est du moins la considération qui me détermine à proposer cet aperçu, tout incomplet qu'il est, à l'attention des géomètres.

§. 8.

Nous nous proposons dans ce paragraphe 1°. d'établir la relation très simple qui existe entre les nombres des formes de première et de seconde espèce qui répondent au même déterminant et 2°. d'examiner de quelle manière le nombre des formes d'un déterminant quelconque dépend de celui qui se rapporte à ce déterminant, divisé par le plus grand carré qu'il contient.

I. Soient h et h' respectivement les nombres des formes de première et de seconde espèce dont le déterminant D est un entier $4\nu+1$. Si nous supposons en premier lieu D négatif, l'équation (19) §. 6 donnera, en observant qu'on a $\vartheta = 1$, $\varepsilon = 1$:

$$h = \frac{2}{\pi}\sqrt{D_1}\,\Sigma\left(\frac{n}{P}\right)\frac{1}{n}.$$

Il suffit de comparer cette expression aux équations (21), pour en conclure:

$$h = h', \quad D \equiv 1 \pmod 8; \qquad h = 3h', \quad D \equiv 5 \pmod 8.$$

Il faut seulement ajouter que la seconde de ces équations est en défaut pour $D = -3$, et qu'on a alors $h = h'$.

II. Lorsque D est positif, la relation qui existe entre h et h', résulte de la même manière de la comparaison des équations (23) et (24). Si l'on désigne par T, U et T', U', respectivement les plus petites valeurs positives qui satisfont aux équations:

$$(1)\quad t^2 - Du^2 = 1, \qquad (2)\quad t'^2 - Du'^2 = 4,$$

la relation dont il s'agit, sera exprimée comme il suit:

$$h = h'\frac{\log\frac{1}{2}(T'+U'\sqrt{D})}{\log(T+U\sqrt{D})}, \quad D \equiv 1 \pmod 8;$$

$$h = 3h'\frac{\log\frac{1}{2}(T'+U'\sqrt{D})}{\log(T+U\sqrt{D})}, \quad D \equiv 5 \pmod 8.$$

Pour réduire ce résultat à une forme plus simple, nous observerons que les solutions de l'équation (1) sont évidemment toutes comprises dans celles de l'équation (2); il suffit de considérer celles de ces dernières où t' et u' sont pairs et de poser $t = \frac{1}{2}t'$, $u = \frac{1}{2}u'$. Il résulte de là que si T' et U' sont pairs, on a $T = \frac{1}{2}T'$, $U = \frac{1}{2}U'$, et il est facile de voir que ce cas a toujours lieu

lorsque D est de la forme $8\nu+1$, puisque dans cette supposition l'équation (2) ne saurait être satisfaite par des valeurs impaires de t' et u'. Reste à considérer le cas où D a la forme $8\nu+5$, et où en même temps T' et U' sont impairs. Comme toutes les solutions positives de l'équation (2) sont données par la formule:

$$\frac{t'+u'\sqrt{D}}{2} = \left(\frac{T'+U'\sqrt{D}}{2}\right)^n,$$

où n est un entier positif, on conclut de la remarque faite plus haut que l'on obtiendra les valeurs T et U, en déterminant le plus petit exposant n pour lequel t' et u' sont pairs, et en posant ensuite $T = \frac{1}{2}t'$, $U = \frac{1}{2}u'$. Or il est facile de voir que cet exposant est le nombre 3; car en faisant $n = 2$, on trouve pour u' la valeur impaire $T'U'$, tandis que celle qui répond à $n = 3$, et qui est $\frac{1}{4}U'(3T'^2 + DU'^2)$, est évidemment paire. On a donc:

$$T + U\sqrt{D} = \left(\frac{T'+U'\sqrt{D}}{2}\right)^3.$$

En appliquant les résultats précédents aux deux équations données ci-dessus, on voit que, pour un déterminant de la forme $8\nu+1$, on a toujours $h = h'$, et que lorsque D a la forme $8\nu+5$, tout dépend des entiers T' et U'; selon que ces entiers seront pairs ou impairs, on aura $h = 3h'$ ou $h = h'$.

III. Venant à la seconde des questions énoncées ci-dessus, nous remarquerons d'abord qu'après avoir établi dans ce qui précède, le rapport qui a lieu entre les formes de première et de seconde espèce qui appartiennent au même déterminant, nous pouvons, dans la question qui nous reste à traiter, considérer les formes qu'il s'agit de comparer, quant à leur nombre, comme appartenant à la première espèce. Soient D et $D' = DS^2$ les deux déterminants, D n'ayant pas de facteur carré et S étant supposé positif, et désignons par h et h' les nombres des formes qui répondent respectivement à ces deux déterminants. Comme les quantités ϑ, ε, P sont évidemment les mêmes pour ces deux déterminants, si l'on suppose en premier lieu D négatif, on aura en vertu de l'équation (19) du §. 6:

$$h = \frac{2\sqrt{D_1}}{\pi}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}, \qquad h' = \frac{2S\sqrt{D_1}}{\pi}\,\Sigma\vartheta^{\frac{1}{2}(n-1)}\varepsilon^{\frac{1}{2}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}.$$

Quoique les termes généraux des deux séries contenues dans ces expressions soient de même forme, ces séries ont néanmoins des valeurs différentes. En effet, dans la première équation la sommation doit s'étendre à tous les entiers n impairs et premiers à D, tandis que dans la seconde n ne doit

recevoir que des valeurs impaires et premières à D'. Pour découvrir la relation qui existe entre ces deux sommes, il faut se reporter à l'équation (6) du §. 6. Si l'on suppose dans cette équation $\theta = \delta$, $\eta = \varepsilon$, $P_2 = P$, $R_1 = 1$, on voit que les séries précédentes peuvent être considérées l'une et l'autre comme la limite vers laquelle converge le produit:

$$\Pi \frac{1}{1-\delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{8}(q^2-1)}\left(\frac{q}{P}\right)\frac{1}{q^s}}$$

lorsque la variable s approche indéfiniment de l'unité; mais il y a cette différence que lorsqu'il s'agit de la première série, il faut exclure de ce produit tous les nombres premiers impairs et positifs q qui divisent D, tandis que pour obtenir la seconde série, il faut exclure tous ceux de ces nombres q qui divisent $D' = DS^2$. Il résulte de là que si l'on désigne par r, r', r'', ... les nombres premiers impairs, positifs et inégaux, contenus dans D', sans l'être dans D, le rapport de la première série à la seconde a pour expression:

$$\Pi \frac{1}{1-\delta^{\frac{1}{2}(r-1)}\varepsilon^{\frac{1}{8}(r^2-1)}\left(\frac{r}{P}\right)\frac{1}{r}},$$

le signe Π s'étendant à toutes les valeurs de r qu'on vient de définir.

Au moyen de ce résultat, la comparaison des équations en h et h' donnera celle-ci:

$$h' = hS\Pi\left(1-\delta^{\frac{1}{2}(r-1)}\varepsilon^{\frac{1}{8}(r^2-1)}\left(\frac{r}{P}\right)\frac{1}{r}\right),$$

qui exprime la relation cherchée entre h et h'. On doit ajouter que cette équation ne s'applique pas au cas où $D = -1$, et qu'il faut dans ce cas doubler son premier membre.

IV. Le cas où D et D' sont positifs, étant susceptible d'une analyse toute semblable, nous nous bornerons à énoncer le résultat qui s'y rapporte. Si l'on désigne par T, U et T', U' les plus petites valeurs positives qui satisfont aux équations $t^2 - Du^2 = 1$, $t'^2 - D'u'^2 = 1$, le résultat dont il s'agit, sera:

$$h' = hS\frac{\log(T+U\sqrt{D})}{\log(T'+U'\sqrt{D'})}\left(1-\delta^{\frac{1}{2}(r-1)}\varepsilon^{\frac{1}{8}(r^2-1)}\left(\frac{r}{P}\right)\frac{1}{r}\right),$$

où l'on peut remarquer que le facteur logarithmique équivaut évidemment a l'unité divisée par le plus petit exposant positif λ tel que le coefficient de $\sqrt{D}$ dans la puissance $(T+U\sqrt{D})^\lambda$ développée soit divisible par S.

Nous observons, en finissant ce paragraphe et avant de nous occuper de la sommation mentionnée au commencement du précédent paragraphe, que les deux questions que nous venons de traiter, ont déjà été résolues dans l'ouvrage de M. GAUSS (art. 253—256), mais par d'autres moyens. Quant aux résultats, on trouve que ceux de l'illustre auteur, identiques aux nôtres dans le cas des déterminants négatifs, en diffèrent essentiellement et se présentent sous une forme plus compliquée, lorsque la comparaison qu'il s'agit de faire, doit porter sur des formes à déterminant positif.

§. 9.

La sommation qui nous reste à effectuer, peut être opérée par deux méthodes différentes, en s'aidant des formules remarquables que M. GAUSS a établies dans le beau Mémoire ayant pour titre „*Summatio quarumdam serierum singularium.*“ *) La première de ces méthodes est fondée sur certaines séries connues ordonnées suivant les sinus ou les cosinus des arcs multiples. En l'employant dans la note**) qui a précédé le présent Mémoire, nous avons déjà remarqué qu'elle s'applique, de la même manière et avec une facilité égale, à toutes les séries qui servent à exprimer le nombre des formes pour un déterminant quelconque, c'est-à-dire aux deux séries générales (19) et (23) du §. 6. Nous avons même ajouté que les séries de cette forme sont encore susceptibles d'être sommées par le même moyen, dans plusieurs cas différents de celui où l'exposant s de la puissance $\frac{1}{n^s}$, contenue dans le terme général, est égal à l'unité, ce qui était d'ailleurs évident. En effet, la méthode dont il s'agit, consistant à remplacer le facteur qui multiplie $\frac{1}{n^s}$, au moyen des formules de M. GAUSS par un nombre limité de termes de l'une des formes $\sin nx$, $\cos nx$, on voit que la série, après cette transformation, se trouve changée en une somme de suites trigonométriques dont chacune a pour terme général une expression telle que $\frac{\sin nx}{n^s}$ ou $\frac{\cos nx}{n^s}$, et peut par conséquent être sommée pour les mêmes valeurs de s, pour lesquelles D. BERNOULLI a donné les sommes de ces dernières.

La seconde méthode est fondée sur le procédé connu de l'intégration des fractions rationnelles. Les séries déjà citées (19) et (23) §. 6, coïncident

*) Gauss' Werke, Bd. II, S. 9. K.

**) Voyez le tome XVIII du Journal de CRELLE p. 259.[1])

[1]) S. 357 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

avec celles qui forment la seconde des trois classes de suites infinies que nous avons eu à distinguer dans le Mémoire sur la progression arithmétique, et nous avons déjà observé dans le Mémoire cité §. 10, que les séries de seconde et troisième classe peuvent être sommées par la méthode qui avait été expliquée en détail dans le §. 4 du même Mémoire. Les deux méthodes que nous venons de citer, sont l'une et l'autre d'une grande simplicité. La seconde étant celle qui se présente le plus naturellement, nous allons l'employer d'abord. Mais avant d'entreprendre ce calcul, il faut rappeler les formules de M. GAUSS. Voici une démonstration de ces expressions, fondée sur les mêmes principes dont j'ai déjà fait usage dans un précédent mémoire*), mais plus simple à quelques égards.

Désignant par $f(x)$ une fonction de x, que je suppose continue entre les limites $x = 0$ et $x = \pi$, si l'on pose:

$$\int_0^\pi f(x)\cos sx\,dx = c_s,$$

on aura, comme l'on sait:

$$c_0 + 2\Sigma c_s \cos sx = \pi f(x),$$

le signe Σ s'étendant à tous les entiers depuis $s = 1$ jusqu'à $s = \infty$. Comme ce développement subsiste entre les limites $x = 0$ et $x = \pi$ inclusivement, on aura en particulier:

$$c_0 + 2\Sigma c_s = \pi f(0).$$

Il est facile de voir comment cette équation doit être modifiée, lorsque les limites de l'intégrale c_s ont des valeurs quelconques. Considérons par exemple les limites 0 et $2h\pi$, h désignant un entier positif, et posons:

$$(1) \qquad \int_0^{2h\pi} f(x)\cos sx\,dx = c_s,$$

la fonction étant toujours continue entre ces limites. L'intégrale précédente étant partagée en $2h$ intégrales partielles dont les limites sont:

$$0 \text{ et } \pi,\ \pi \text{ et } 2\pi,\ \ldots,\ (2h-1)\pi \text{ et } 2h\pi,$$

et toutes ces nouvelles intégrales étant ramenées à avoir pour limites communes 0 et π, le premier membre de l'équation (1) se changera en:

$$\int_0^\pi [f(x)+f(2\pi-x)+f(2\pi+x)+\cdots+f(2(h-1)\pi-x)+f(2(h-1)\pi+x)+f(2h\pi-x)]\cos sx\,dx.$$

*) S. 237 und S. 257 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Cette expression de c_s ayant la même forme que celle donnée ci-dessus, on aura:

$$(2) \qquad c_0 + 2\sum_{s=1}^{s=\infty} c_s = \pi(f(0)+f(2h\pi)+2\sum_{s=1}^{s=h-1} f(2s\pi)),$$

le terme général c_s du premier membre étant donné par l'équation (1). Cela posé, considérons l'intégrale:

$$\int_{-\infty}^{\infty} \cos(x^2)dx = a,$$

a étant une quantité numérique. Posons dans cette intégrale $x = \frac{z}{2}\sqrt{\frac{n}{2\pi}}$, z désignant la nouvelle variable et n étant un entier positif divisible par 4. Il viendra ainsi:

$$\int_{-\infty}^{\infty} \cos\left(\frac{n}{8\pi}z^2\right)dz = 2a\sqrt{\frac{2\pi}{n}}.$$

Cette intégrale étant décomposée en une infinité d'autres ayant pour limites deux multiples consécutifs de 2π, tels que $2s\pi$ et $2(s+1)\pi$, et ces nouvelles intégrales étant ramenées à avoir les limites communes 0 et 2π par le changement de z en $2s\pi+z$, on aura:

$$\Sigma\int_0^{2\pi} \cos\frac{n}{8\pi}(2s\pi+z)^2 dz = 2a\sqrt{\frac{2\pi}{n}},$$

le signe Σ s'étendant depuis $s = -\infty$ jusqu'à $s = \infty$.

En développant sous le signe cosinus, omettant le terme $\frac{1}{2}ns^2\pi$, multiple de 2π, et réunissant les termes de la somme qui répondent à des valeurs opposées de s, il viendra:

$$\int_0^{2\pi}\cos\left(\frac{n}{8\pi}z^2\right)dz + 2\Sigma\int_0^{2\pi}\cos\left(\frac{n}{8\pi}z^2\right)\cos\left(s\frac{nz}{2}\right)dz = 2a\sqrt{\frac{2\pi}{n}},$$

le signe Σ s'étendant depuis $s = 1$ jusqu'à $s = \infty$. Si maintenant l'on fait $nz = 2x$, on aura:

$$\int_0^{n\pi}\cos\left(\frac{x^2}{2n\pi}\right)dx + 2\Sigma\int_0^{n\pi}\cos\left(\frac{x^2}{2n\pi}\right)\cos sx\,dx = a\sqrt{2n\pi}.$$

Comme l'entier n est pair, le premier membre rentre dans la forme de celui de l'équation (2), $f(x)$ étant $\cos\left(\frac{x^2}{2n\pi}\right)$. On aura donc en vertu de cette équation:

$$\cos 0 + \cos\left(\frac{n}{2}\right)^2\frac{2\pi}{n} + 2\sum_{s=1}^{s=\frac{1}{2}n-1}\cos s^2\frac{2\pi}{n} = a\sqrt{\frac{2n}{\pi}}.$$

Si l'on observe que l'on a $\cos s^2\frac{2\pi}{n} = \cos(n-s)^2\frac{2\pi}{n}$, l'équation précédente pourra prendre cette forme plus simple:

$$\sum_{s=0}^{s=n-1} \cos s^2\frac{2\pi}{n} = a\sqrt{\frac{2n}{\pi}}.$$

Pour déterminer la quantité a indépendante de n, il suffira de donner à n une valeur particulière. Posant, par exemple, $n=4$, on trouve $a=\sqrt{\frac{1}{2}\pi}$. On a donc définitivement, quel que soit l'entier $n=4\mu$:

$$\sum_{s=0}^{s=n-1} \cos s^2\frac{2\pi}{n} = \sqrt{n}.$$

En opérant de la même manière sur l'intégrale $\int_{-\infty}^{\infty}\sin(x^2)dx$, on trouve aussi:

$$\sum_{s=0}^{s=n-1} \sin s^2\frac{2\pi}{n} = \sqrt{n}.$$

Il serait facile d'obtenir par une analyse semblable les sommes de la forme des précédentes, pour les cas où n est de l'une des trois formes $4\mu+1$, $4\mu+2$, $4\mu+3$; mais il est plus simple encore de ramener ces cas à celui ou n a la forme 4μ.

Pour y parvenir, soient n et m deux entiers quelconques dont le premier est supposé positif, et posons:

$$\sum_{s=0}^{s=n-1} e^{s^2\frac{2m\pi i}{n}} = \varphi(m, n),$$

où i désigne, pour abréger, la quantité imaginaire $\sqrt{-1}$.

La fonction $\varphi(m, n)$ jouit de plusieurs propriétés remarquables. On a d'abord évidemment, si m' désigne un troisième entier tel qu'on ait $m' \equiv m \pmod{n}$:

$$\varphi(m, n) = \varphi(m', n). \tag{3}$$

On a encore, en supposant c premier à n:

$$\varphi(m, n) = \varphi(c^2 m, n). \tag{4}$$

Cela résulte de ce que l'expression cs, en y faisant successivement:

$$s = 0,\ 1,\ \ldots,\ n-1,$$

donne les mêmes nombres pour restes lorsqu'on la divise par n.

Une troisième propriété est exprimée par l'équation:

$$\varphi(m, n)\varphi(n, m) = \varphi(1, mn), \tag{5}$$

qui suppose les entiers n et m l'un et l'autre positifs et premiers entre eux.

En effet, comme on a:

$$\sum_{s=0}^{s=n-1} e^{s^2\frac{2m\pi i}{n}} = \varphi(m, n), \qquad \sum_{t=0}^{t=m-1} e^{t^2\frac{2n\pi i}{m}} = \varphi(n, m),$$

il viendra en multipliant:

$$\Sigma\Sigma e^{(m^2s^2+n^2t^2)\frac{2\pi i}{mn}} = \varphi(m, n)\varphi(n, m),$$

ou encore, si l'on ajoute à l'exposant l'expression $2st\pi i$, multiple de $2\pi i$:

$$\Sigma\Sigma e^{(ms+nt)^2\frac{2\pi i}{mn}} = \varphi(m, n)\varphi(n, m).$$

Le binôme $ms+nt$ peut être remplacé par son reste relatif au diviseur mn. Or, m et n étant premiers entre eux, il est facile de voir que les valeurs de ce reste entre les limites de la double sommation, coïncident, abstraction faite de l'ordre, avec les termes de la suite $0, 1, 2, \ldots, mn-1$. Le résultat prend donc la forme d'une somme simple et l'on a:

$$\sum_{s=0}^{s=mn-1} e^{s^2\frac{2\pi i}{mn}} = \varphi(m, n)\varphi(n, m),$$

ce qu'il s'agissait de prouver.

Au moyen des équations qui viennent d'être établies, il est facile d'obtenir la valeur de $\varphi(1, n)$, quelle que soit la forme de l'entier n. Si l'on suppose d'abord $n=4\mu$, on aura, en vertu des sommations effectuées plus haut:

$$\varphi(1, n) = (1+i)\sqrt{n}.$$

Soit en second lieu n un entier impair. L'équation (5) donne, en y faisant $m=4$:

$$\varphi(4, n)\varphi(n, 4) = \varphi(1, 4n).$$

Le second membre est, d'après l'équation précédente, égal à $2(1+i)\sqrt{n}$. D'un autre côté, les deux expressions $\varphi(4, n)$, $\varphi(n, 4)$ peuvent, au moyen des équations (3) et (4), être remplacées, la première par $\varphi(1, n)$, la seconde par $\varphi(1, 4)$ ou par $\varphi(3, 4)$, suivant que n est de la forme $4\mu+1$ ou de $4\mu+3$. Or il est facile de voir qu'on a:

$$\varphi(1, 4) = 2(1+i), \qquad \varphi(3, 4) = 2(1-i).$$

On conclut de là:

$$\varphi(1, n) = \sqrt{n}, \quad n = 4\mu+1; \qquad \varphi(1, n) = i\sqrt{n}, \quad n = 4\mu+3.$$

Reste à considérer le cas ou n a la forme $4\mu+2$. Dans cette supposition, $\frac{n}{2}$ et 2 étant premiers entre eux, l'équation (5) donnera:

$$\varphi\left(2, \frac{n}{2}\right).\varphi\left(\frac{n}{2}, 2\right) = \varphi(1, n),$$

et comme d'un autre côté, $\varphi\left(\frac{n}{2}, 2\right) = \varphi(1, 2) = 0$, il s'ensuivra:

$$\varphi(1, n) = 0.$$

Considérons spécialement le cas où n est un nombre premier impair p, et soient a et b respectivement les résidus et les non-résidus quadratiques de p, moindres que ce nombre. On aura alors, en observant que l'expression $i^{\left(\frac{p-1}{2}\right)^2}$ se réduit à 1 ou à i, suivant que p a la forme $4\mu+1$ ou $4\mu+3$:

$$\varphi(1, p) = i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p},$$

équation qu'on peut mettre, en remplaçant s^2 par son reste, sous cette forme:

$$1+2\Sigma e^{a\frac{2\pi i}{p}} = i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p},$$

le signe Σ s'étendant à toutes les valeurs de a. Si m désigne un entier non-divisible par p, on aura pareillement, en remplaçant ms^2 par son reste:

$$\varphi(m, p) = 1+2\Sigma e^{a\frac{2\pi i}{p}} \quad \text{ou} \quad \varphi(m, p) = 1+2\Sigma e^{b\frac{2\pi i}{p}},$$

suivant que:

$$\left(\frac{m}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{m}{p}\right) = -1.$$

Puisque d'un autre côté:

$$\Sigma e^{a\frac{2\pi i}{p}} + \Sigma e^{b\frac{2\pi i}{p}} = -1,$$

on pourra réunir les deux résultats dans cette formule:

$$\varphi(m, p) = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

On donnera à l'expression $\varphi(m,p)$, en y mettant au lieu de s^2 son reste, cette forme:

$$\varphi(m, p) = 1+2\Sigma e^{a\frac{2m\pi i}{p}}$$

et la comparaison de ces deux équations fournira celle-ci:

$$1+2\Sigma e^{a\frac{2m\pi i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

Si maintenant l'on observe qu'on a évidemment $\Sigma e^{a\frac{2m\pi i}{p}} + \Sigma e^{b\frac{2m\pi i}{p}} = -1$, l'équation précédente pourra se changer en celle-ci:

$$1+2\Sigma e^{b\frac{2m\pi i}{p}} = -\left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

En soustrayant cette équation de la précédente et divisant le résultat par 2, on aura définitivement:

$$\Sigma e^{a\frac{2m\pi i}{p}} - \Sigma e^{b\frac{2m\pi i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

Cette équation subsiste quel que soit l'entier m, pourvu qu'il ne soit pas divisible par p. Lorsque m est un multiple de p, le premier membre se réduit évidemment à zéro. Nous écrirons l'équation d'une manière plus abrégée et comme il suit:

$$\Sigma\left(\frac{g}{p}\right) e^{g\frac{2m\pi i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}, \tag{6}$$

où le signe sommatoire s'étend depuis $g = 1$ jusqu'à $g = p-1$.

§. 10.

D'après les résultats obtenus dans le §. 8, où nous avons fait voir que la détermination du nombre h des formes quadratiques qui répondent à un déterminant quelconque, se réduit toujours à une question du même genre et relative au cas où le déterminant n'a pas de diviseur carré et où les formes dont il s'agit d'obtenir le nombre, appartiennent à la première espèce, nous n'aurons plus à nous occuper que des 4 déterminants:

$$P, \quad 2P, \quad -P, \quad -2P,$$

$P = pp'p'' \ldots$ désignant un entier impair et positif dont les diviseurs simples p, p', p'', ... sont tous différents les uns des autres.

Il importe de remarquer que la lettre P telle qu'on vient de la définir, a la même signification que dans les §§. 5 et 6, lorsque le déterminant que nous désignerons toujours par D, est positif, mais que dans le cas de D négatif, cette lettre telle qu'elle a été employée dans les paragraphes cités, répond à ce que nous désignons maintenant par $-P$. Cela ne change rien à l'expression $\left(\frac{n}{P}\right)$, contenue dans l'équation (19) du §. 6, et à la valeur de ε fixée par les équations (9) du même paragraphe, cette valeur devant être $+1$ ou -1, suivant que le déterminant, délivré de tout diviseur carré, est impair ou pair. Mais il n'en est pas de même de ϑ, cette valeur dépendant du reste que donne P, pris avec son signe, relativement au diviseur 4. Il résulte de là qu'en posant pour abréger:

$$V = \Sigma\vartheta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(a'-1)}\left(\frac{n}{P}\right)\frac{1}{n},$$

où le signe Σ s'étend à tous les entiers n positifs, impairs et premiers à P, les expressions $\delta = \pm 1$, $\varepsilon = \pm 1$ qui doivent entrer dans la série V contenue dans l'équation (19) ou (23), suivant qu'il s'agit d'un déterminant négatif ou positif, seront déterminées comme il suit:

$$\left.\begin{array}{ll} D = P, & P = 4\mu+1 \\ D = -P, & P = 4\mu+3 \end{array}\right\} \delta = 1, \quad \varepsilon = 1;$$

$$\left.\begin{array}{ll} D = P, & P = 4\mu+3 \\ D = -P, & P = 4\mu+1 \end{array}\right\} \delta = -1, \quad \varepsilon = 1;$$

$$\left.\begin{array}{ll} D = 2P, & P = 4\mu+1 \\ D = -2P, & P = 4\mu+3 \end{array}\right\} \delta = 1, \quad \varepsilon = -1;$$

$$\left.\begin{array}{ll} D = 2P, & P = 4\mu+3 \\ D = -2P, & P = 4\mu+1 \end{array}\right\} \delta = -1, \quad \varepsilon = -1.$$

Cela posé, nous avons successivement à considérer les quatre combinaisons que présentent les équations simultanées $\delta = \pm 1$, $\varepsilon = \pm 1$.

I. Supposons d'abord $\delta = 1$, $\varepsilon = 1$. La série V étant divisée par $\left(1-\left(\frac{2}{P}\right)\frac{1}{2}\right)$, il viendra:

$$\frac{V}{1-\left(\frac{2}{P}\right)\frac{1}{2}} = \Sigma\left(\frac{n}{P}\right)\frac{1}{n},$$

le signe Σ s'étendant à tous les entiers positifs n, premiers à P, pairs ou impairs.

En exprimant la série par une intégrale comme au §. 1, on aura:

$$\frac{V}{1-\left(\frac{2}{P}\right)\frac{1}{2}} = -\int_0^1 \frac{\frac{1}{x}f(x)dx}{x^P-1},$$

où l'on a fait, pour abréger, $f(x) = \Sigma\left(\frac{n}{P}\right)x^n$, le signe Σ s'étendant aux entiers précédemment définis moindres que P. En appliquant à cette intégrale la méthode ordinaire de décomposition, on trouve:

$$\frac{V}{1-\left(\frac{2}{P}\right)\frac{1}{2}} = -\frac{1}{P}\Sigma f\left(e^{\frac{2m\pi i}{P}}\right)\int_0^1 \frac{dx}{x-e^{\frac{2m\pi i}{P}}},$$

le signe Σ s'étendant à tous les entiers m depuis $m = 0$ jusqu'à $m = P-1$. Tout se réduit donc à obtenir la fonction $f\left(e^{\frac{2m\pi i}{P}}\right) = \Sigma\left(\frac{n}{P}\right)e^{\frac{n}{P}2m\pi i}$.

Pour y parvenir, mettons la fraction $\frac{n}{P}$, contenue dans l'exposant, sous la forme:

$$\frac{n}{P} = \mu + \frac{g}{p} + \frac{g'}{p'} + \cdots,$$

μ étant un entier positif ou négatif, et $g, g', \ldots$ désignant des entiers positifs respectivement inférieurs à $p, p', \ldots$. On sait que cela ne peut se faire que d'une seule manière (*Disq. arith.* 311), et il est manifeste, n étant premier à P, qu'aucun des entiers $g, g', \ldots$ ne saurait être zéro. Il est encore facile de voir qu'en donnant à n toutes les valeurs qu'il doit recevoir dans la sommation, $g, g', \ldots$ présenteront toutes les combinaisons que l'on peut former avec les entiers depuis $g = 1$ jusqu'à $g = p-1$, depuis $g' = 1$ jusqu'à $g' = p'-1$, etc. Quant à l'entier μ, on pourra le négliger parce qu'il est multiplié par $2m\pi i$ dans l'exposant. Si maintenant nous faisons pour un instant $\frac{P}{p} = r$, $\frac{P}{p'} = r', \ldots$, l'équation précédente donne:

$$n \equiv gr + g'r' + \cdots \pmod{P},$$

d'où l'on conclut ces égalités:

$$\left(\frac{n}{p}\right) = \left(\frac{g}{p}\right)\left(\frac{r}{p}\right), \quad \left(\frac{n}{p'}\right) = \left(\frac{g'}{p'}\right)\left(\frac{r'}{p'}\right), \quad \ldots$$

au moyen desquelles la fonction $f\left(e^{\frac{2m\pi i}{P}}\right)$ deviendra le produit $\left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right)\ldots$ multiplié par les sommes:

$$\Sigma\left(\frac{g}{p}\right)e^{g\frac{2m\pi i}{p}}, \quad \Sigma\left(\frac{g'}{p'}\right)e^{g'\frac{2m\pi i}{p'}}, \quad \ldots.$$

Remplaçant ces dernières par leurs valeurs fournies par l'équation (6) du paragraphe précédent, on aura:

$$f\left(e^{\frac{2m\pi i}{P}}\right) = \left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right)\ldots i^{\left(\frac{p-1}{2}\right)^2+\left(\frac{p'-1}{2}\right)^2+\cdots}\left(\frac{m}{P}\right)\sqrt{P}$$

en supposant m premier à P. Dans le cas contraire $f\left(e^{\frac{2m\pi i}{P}}\right)$ s'évanouira parce qu'une au moins des sommes précédentes se réduira à zéro. Quant au produit $\left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right)\cdots$, on remarquera qu'il se compose d'autant de produits partiels de la forme $\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right)$, que les nombres $p, p', \ldots$ peuvent être combinés deux

à deux. Or, comme on a:

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right)=(-1)^{\frac{p-1}{2}\frac{p'-1}{2}}=i^{2\frac{p-1}{2}\frac{p'-1}{2}},$$

on voit que l'expression qui multiplie $\left(\frac{m}{P}\right)\sqrt{P}$ dans l'équation obtenue plus haut, peut prendre la forme:

$$i^{\left(\frac{P-1}{2}+\frac{p'-1}{2}+\cdots\right)^2}=i^{\left(\frac{P-1}{2}\right)^2}.$$

Nous avons donc définitivement:

$$(1)\qquad f\left(e^{\frac{2m\pi i}{P}}\right)=0 \quad \text{ou} \quad f\left(e^{\frac{2m\pi i}{P}}\right)=i^{\left(\frac{P-1}{2}\right)^2}\left(\frac{m}{P}\right)\sqrt{P},$$

suivant que m a ou n'a pas de diviseur commun avec P. Substituant cette valeur et observant que tant que $m<P$, on a:

$$\int_0^1\frac{dx}{x-e^{\frac{2m\pi i}{P}}}=\log\left(2\sin\frac{m\pi}{P}\right)+\frac{\pi}{2}\left(1-\frac{2m}{P}\right)i,$$

il viendra:

$$\frac{V}{1-\left(\frac{2}{P}\right)\frac{1}{2}}=-\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\left\{\log\left(2\sin\frac{m\pi}{P}\right)+\frac{\pi}{2}\left(1-\frac{2m}{P}\right)i\right\},$$

le signe sommatoire s'étendant à tous les entiers m inférieurs et premiers à P. L'équation précédente se simplifie en remarquant qu'on a $\Sigma\left(\frac{m}{P}\right)=0$; elle devient ainsi:

$$\frac{V}{1-\left(\frac{2}{P}\right)\frac{1}{2}}=-\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\left(\log\sin\frac{m\pi}{P}-\frac{m\pi}{P}i\right).$$

Le premier membre étant réel, les imaginaires doivent se détruire dans le second, comme il est d'ailleurs facile de le vérifier.

Distinguons maintenant les deux formes que P peut présenter, en supposant successivement $P=4\mu+1$ et $P=4\mu+3$. Nous obtenons ainsi:

$$(a)\qquad\begin{cases}P=4\mu+1, & V=-\dfrac{1}{\sqrt{P}}\left(1-\left(\frac{2}{P}\right)\frac{1}{2}\right)\Sigma\left(\frac{m}{P}\right)\log\sin\dfrac{m\pi}{P},\\ P=4\mu+3, & V=-\dfrac{\pi}{(\sqrt{P})^3}\left(1-\left(\frac{2}{P}\right)\frac{1}{2}\right)\Sigma\left(\frac{m}{P}\right)m,\end{cases}$$

le signe Σ s'étendant toujours aux entiers m inférieurs et premiers à P.

II. Soit en second lieu $\delta=-1$, $\varepsilon=1$. Comme le facteur qui multiplie $\frac{1}{n}$ dans la série V, est le même pour des valeurs de n qui diffèrent d'un multiple de $4P$, on aura d'après ce qui a été dit dans le §. 1:

$$V=-\int_0^1\frac{\frac{1}{x}F(x)dx}{x^{4P}-1},$$

en posant pour abréger:

$$F(x)=\Sigma(-1)^{\frac{1}{2}(n-1)}\left(\frac{n}{P}\right)x^n,$$

le signe Σ s'étendant à tous les entiers n inférieurs et premiers à $4P$.

La méthode connue pour la décomposition des fractions rationnelles donne:

$$V=-\frac{1}{4P}\Sigma F\left(e^{\frac{2m\pi i}{4P}}\right)\int_0^1\frac{dx}{x-e^{\frac{2m\pi i}{4P}}},$$

où le signe Σ s'étend à tous les entiers depuis $m=0$ jusqu'à $m=4P-1$. Tout se réduit donc à déterminer l'expression $F\left(e^{\frac{2m\pi i}{4P}}\right)$.

On peut y parvenir par des considérations analogues à celles que nous avons employées dans le numéro précédent pour trouver $f\left(e^{\frac{2m\pi i}{P}}\right)$, mais il est plus simple de ramener ce cas à celui que nous avons déjà examiné. Pour cela, on décomposera la fraction $\frac{n}{4P}$, contenue dans l'exposant, comme il suit:

$$\frac{n}{4P}=\mu+\frac{\gamma}{4}+\frac{n'}{P},$$

où il est facile de voir qu'en supposant γ et n' positifs et respectivement inférieurs à 4 et à P, les valeurs de γ et de n' présenteront, dans la sommation qu'il s'agit d'effectuer relativement à n, toutes les combinaisons des nombres γ inférieurs et premiers à 4, avec tous les nombres n' inférieurs et premiers à P. De l'équation précédente mise sous la forme:

$$n\equiv P\gamma+4n' \pmod{4P},$$

on conclut facilement:

$$(-1)^{\frac{1}{2}(n-1)}=(-1)^{\frac{1}{2}(P-1)}(-1)^{\frac{1}{2}(\gamma-1)},\qquad\left(\frac{n}{P}\right)=\left(\frac{n'}{P}\right).$$

La fonction $F\left(e^{\frac{2m\pi i}{4P}}\right)$ deviendra par la substitution de ces valeurs:

$$F\left(e^{\frac{2m\pi i}{4P}}\right) = (-1)^{\frac{1}{2}(P-1)}\Sigma(-1)^{\frac{1}{2}(\gamma-1)}e^{\gamma\frac{2m\pi i}{4}}.\Sigma\left(\frac{n'}{P}\right)e^{n'\frac{2m\pi i}{P}}.$$

Quant à la seconde des deux sommes contenues dans le second membre, elle est évidemment identique à la fonction $f\left(e^{\frac{2m\pi i}{P}}\right)$, n' ayant ici la même signification que n dans le numéro précédent. La première somme pourrait se déduire des formules données dans le §. 9, mais comme elle n'a que deux termes répondant à $\gamma = 1, 3$, on voit sans peine et indépendamment de ces formules que, pour une valeur impaire de m, elle se réduit à $2i(-1)^{\frac{1}{2}(m-1)}$, et qu'elle s'évanouit dans le cas contraire. Substituant les valeurs des deux sommes et remplaçant en même temps $(-1)^{\frac{1}{2}(P-1)}$ par $(i^2)^{\frac{1}{2}(P-1)}$, on aura:

$$(2) \qquad F\left(e^{\frac{2m\pi i}{4P}}\right) = i^{\left(\frac{P+1}{2}\right)^2}(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)\sqrt{4P}$$

en supposant m premier à $4P$. Dans le cas contraire le premier membre s'évanouit parce qu'une au moins des sommes que nous venons de considérer, se réduit à zéro. Au moyen de ce résultat, on conclura:

$$V = -\frac{i^{\left(\frac{P+1}{2}\right)^2}}{\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)\left(\log 2\sin\frac{m\pi}{4P} + i\frac{\pi}{2}\left(1-\frac{m}{2P}\right)\right),$$

le signe s'étendant aux entiers m inférieurs et premiers à $4P$. Si l'on observe que pour ces valeurs on a:

$$\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right) = 0,$$

l'équation précédente prendra la forme plus simple:

$$V = -\frac{i^{\left(\frac{P+1}{2}\right)^2}}{\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)\left(\log\sin\frac{m\pi}{4P} - i\pi\frac{m}{4P}\right).$$

En distinguant maintenant les deux formes que le nombre P peut présenter lorsqu'on le divise par 4, on aura:

$$(b) \qquad \begin{cases} P = 4\mu+3, & V = -\dfrac{1}{\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\dfrac{m}{P}\right)\log\sin\dfrac{m\pi}{4P}, \\ P = 4\mu+1, & V = -\dfrac{\pi}{(\sqrt{4P})^3}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\dfrac{m}{P}\right)m, \end{cases}$$

le signe sommatoire se rapportant aux entiers m inférieurs et premiers à $4P$.

III. Les cas qui nous restent à considérer et qui répondent à $\delta = 1$, $\varepsilon = -1$; $\delta = -1$, $\varepsilon = -1$, étant entièrement semblables à ceux qui viennent d'être traités, nous indiquerons rapidement le calcul qui s'y applique. En conservant d'abord la valeur ambiguë $\delta = \pm 1$, on aura:

$$V = -\int_0^1 \frac{\frac{1}{x}\Sigma\delta^{\frac{1}{2}(n-1)}(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)x^n}{x^{8P}-1}\,dx,$$

le signe Σ s'étendant aux entiers n inférieurs et premiers à $8P$. On conclut de là:

$$V = -\frac{1}{8P}\Sigma A_m\int_0^1 \frac{dx}{x-e^{\frac{2m\pi i}{8P}}},$$

le signe Σ se rapportant aux entiers compris entre $m = 0$ et $m = 8P-1$, et A_m désignant, pour abréger, la somme:

$$\Sigma\delta^{\frac{1}{2}(n-1)}(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)e^{\frac{n}{8P}2m\pi i},$$

étendue aux entiers n définis plus haut. En faisant:

$$\frac{n}{8P} = \mu + \frac{\gamma}{8} + \frac{n'}{P},$$

il est facile de voir que n recevra toutes les valeurs auxquelles la sommation doit s'étendre, en combinant les entiers γ inférieurs et premiers à 8 avec les n' inférieurs et premiers à P. Si l'on remarque en outre qu'en vertu du §. 2, la congruence $n \equiv P\gamma + 8n' \pmod{8P}$ entraîne ces équations:

$$\delta^{\frac{1}{2}(n-1)} = \delta^{\frac{1}{2}(P-1)}\delta^{\frac{1}{2}(\gamma-1)}, \qquad (-1)^{\frac{1}{8}(n^2-1)} = (-1)^{\frac{1}{8}(P^2-1)}(-1)^{\frac{1}{8}(\gamma^2-1)},$$
$$\left(\frac{n}{P}\right) = \left(\frac{2}{P}\right)\left(\frac{n'}{P}\right) = (-1)^{\frac{1}{8}(P^2-1)}\left(\frac{n'}{P}\right),$$

l'expression A_m prendra la forme:

$$A_m = \delta^{\frac{1}{2}(P-1)}f\left(e^{\frac{2m\pi i}{P}}\right)\Sigma\delta^{\frac{1}{2}(\gamma-1)}(-1)^{\frac{1}{8}(\gamma^2-1)}e^{\gamma\frac{2m\pi i}{8}}.$$

Tout se réduit donc à avoir la somme relative à γ. On pourrait la déduire du paragraphe précédent; mais comme elle ne se compose que d'un nombre limité de termes qui répondent à $\gamma = 1, 3, 5, 7$, on voit de suite que lorsqu'on a $\delta = 1$, la somme est zéro ou $(-1)^{\frac{1}{8}(m^2-1)}\sqrt{8}$, et que lorsqu'on a $\delta = -1$,

elle est zéro ou $(-1)^{\frac{1}{8}(m-1)+\frac{1}{8}(m^2-1)}i\sqrt{8}$, suivant que m est pair ou impair. On conclut de là ces deux équations:

$$(3)\qquad \Sigma(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)e^{n\frac{2m\pi i}{8P}}=(-1)^{\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)i^{\left(\frac{P-1}{2}\right)^2}\sqrt{8P},$$

$$(4)\qquad \Sigma(-1)^{\frac{1}{8}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)e^{n\frac{2m\pi i}{8P}}=(-1)^{\frac{1}{8}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)i^{\left(\frac{P-1}{2}\right)^2}\sqrt{8P},$$

qui supposent m premier à $8P$, et dont les seconds membres, dans le cas contraire, doivent être remplacés par zéro. Au moyen de ces expressions le calcul s'achève comme dans les cas déjà examinés, et l'on trouve:

$$(c)\quad\begin{cases}\delta=1,\quad \varepsilon=-1\begin{cases}P=4\mu+1, & V=-\dfrac{1}{\sqrt{8P}}\Sigma(-1)^{\frac{1}{8}(m^2-1)}\left(\dfrac{m}{P}\right)\log\sin\dfrac{m\pi}{8P},\\ P=4\mu+3, & V=-\dfrac{\pi}{(\sqrt{8P})^3}\Sigma(-1)^{\frac{1}{8}(m^2-1)}\left(\dfrac{m}{P}\right)m,\end{cases}\\ \delta=-1,\quad \varepsilon=-1\begin{cases}P=4\mu+3, & V=-\dfrac{1}{\sqrt{8P}}\Sigma(-1)^{\frac{1}{8}(m-1)+\frac{1}{8}(m^2-1)}\left(\dfrac{m}{P}\right)\log\sin\dfrac{m\pi}{8P},\\ P=4\mu+1, & V=-\dfrac{\pi}{(\sqrt{8P})^3}\Sigma(-1)^{\frac{1}{8}(m-1)+\frac{1}{8}(m^2-1)}\left(\dfrac{m}{P}\right)m,\end{cases}\end{cases}$$

les sommations s'étendant aux entiers m inférieurs et premiers à $8P$.

IV. Nous allons maintenant résoudre la question dont nous venons de nous occuper, par la première des deux méthodes indiquées plus haut, qui est celle des séries trigonométriques, en nous bornant toutefois, pour abréger, aux séries V qui se rapportent aux déterminants négatifs.

Soit en premier lieu $\delta=1$, $\varepsilon=1$, $P=4\mu+3$; on a alors:

$$V=\Sigma\left(\frac{n}{P}\right)\frac{1}{n},$$

le signe Σ se rapportant aux entiers n impairs et premiers à P. D'après l'équation (1), on a pour un nombre P de la forme $4\mu+3$:

$$\frac{1}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\sin n\frac{2m\pi}{P}=\left(\frac{n}{P}\right)\quad\text{ou}\quad=0,$$

suivant que n est ou n'est pas premier à P, le signe Σ s'étendant aux entiers m inférieurs et premiers à P. Si l'on introduit cette expression dans la série V à la place de $\left(\frac{n}{P}\right)$, on pourra étendre la sommation relative à n à tous les entiers impairs, l'expression précédente s'évanouissant pour des valeurs de

n qui ne sont pas premières à P. Il viendra ainsi, en intervertissant l'ordre des deux sommes:

$$V=\frac{1}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\Sigma\frac{1}{n}\sin n\frac{2m\pi}{P}.$$

La première peut s'obtenir au moyen du résultat connu d'après lequel la série:

$$(5)\qquad \frac{\sin x}{1}+\frac{\sin 3x}{3}+\frac{\sin 5x}{5}+\cdots$$

a la valeur $\frac{\pi}{4}$ ou $-\frac{\pi}{4}$, suivant que x est compris entre 0 et π, ou entre π et 2π. En distinguant donc les valeurs de m inférieures à $\frac{1}{2}P$ de celles qui surpassent $\frac{1}{2}P$, et désignant ces valeurs respectivement par m' et m'', il viendra:

$$V=\frac{\pi}{4\sqrt{P}}\left(\Sigma\left(\frac{m'}{P}\right)-\Sigma\left(\frac{m''}{P}\right)\right).$$

Comme dans la seconde somme on peut évidemment remplacer m'' par $P-m'$, et qu'on a d'ailleurs, P étant de la forme $4\mu+3$:

$$\left(\frac{P-m'}{P}\right)=\left(\frac{-1}{P}\right)\left(\frac{m'}{P}\right)=-\left(\frac{m'}{P}\right),$$

on aura:

$$V=\frac{\pi}{2\sqrt{P}}\Sigma\left(\frac{m'}{P}\right),$$

expression d'une forme différente de celle que nous avons trouvée plus haut. Si, avant de sommer, on avait divisé par $\left(1-\left(\frac{2}{P}\right)\frac{1}{2}\right)$, on serait tombé sur le même résultat que nous avons obtenu par l'autre méthode.

Soit en second lieu $\delta=-1$, $\varepsilon=1$, $P=4\mu+1$. On a alors:

$$V=\Sigma(-1)^{\frac{1}{4}(n-1)}\left(\frac{n}{P}\right)\frac{1}{n},$$

où n ne doit recevoir que des valeurs premières à $4P$. L'équation (2) donne pour ce cas:

$$\frac{1}{\sqrt{4P}}\Sigma(-1)^{\frac{1}{4}(m-1)}\left(\frac{m}{P}\right)\sin n\frac{2m\pi}{4P}=(-1)^{\frac{1}{4}(n-1)}\left(\frac{n}{P}\right)\quad\text{ou}\quad=0,$$

suivant que n est ou n'est pas premier à $4P$, le signe Σ s'étendant aux entiers m inférieurs et premiers à $4P$. Introduisant cette expression dans la série V,

il viendra:

$$V = \frac{1}{\sqrt{4P}} \Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)\Sigma\frac{1}{n}\sin n\frac{2m\pi}{4P}.$$

L'expression qu'on a substituée, s'évanouissant lorsque n n'est pas premier à $4P$, on voit que l'on peut, dans la somme:

$$\Sigma\frac{1}{n}\sin n\frac{2m\pi}{4P},$$

supposer à volonté que n obtient toutes les valeurs entières ou seulement celles qui sont impaires.

Dans la première supposition on aura en vertu de l'équation:

$$\tfrac{1}{2}(\pi-x) = \frac{\sin x}{1}+\frac{\sin 2x}{2}+\frac{\sin 3x}{3}+\cdots$$

qui subsiste depuis $x=0$ jusqu'à $x=2\pi$:

$$\Sigma\frac{1}{n}\sin n\frac{2m\pi}{4P} = \tfrac{1}{2}\left(\pi-\frac{m\pi}{2P}\right),$$

et par suite:

$$V = \frac{\pi}{2\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)-\frac{\pi}{(\sqrt{4P})^2}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)m,$$

ou ce qui revient au même, la première somme étant évidemment nulle:

$$V = -\frac{\pi}{(\sqrt{4P})^2}\Sigma(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)m,$$

ce qui coïncide avec la valeur obtenue par l'autre méthode.

Si en second lieu on suppose que n ne reçoit que des valeurs impaires, on trouvera, au moyen de l'équation (5), et en désignant par m' ou m'' les valeurs de m, suivant qu'elles sont inférieures ou supérieures à $2P$:

$$V = \frac{\pi}{4\sqrt{4P}}\left(\Sigma(-1)^{\frac{1}{2}(m'-1)}\left(\frac{m'}{P}\right)-\Sigma(-1)^{\frac{1}{2}(m''-1)}\left(\frac{m''}{P}\right)\right).$$

En mettant $4P-m'$ à la place de m'', et observant qu'on a:

$$(-1)^{\frac{1}{2}(4P-m'-1)}\left(\frac{4P-m'}{P}\right) = -(-1)^{\frac{1}{2}(m'-1)}\left(\frac{m'}{P}\right),$$

on obtiendra cette nouvelle expression de V:

$$V = \frac{\pi}{2\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m'-1)}\left(\frac{m'}{P}\right).$$

En traitant les deux autres cas de la même manière, on trouvera, outre les résultats déjà obtenus par l'autre méthode, deux nouveaux résultats que nous allons réunir avec les deux précédents:

$$(d)\quad\begin{cases}\delta=1, & \varepsilon=1, & P=4\mu+3, & V=\dfrac{\pi}{2\sqrt{P}}\Sigma\left(\dfrac{m'}{P}\right),\\[2ex] \delta=-1, & \varepsilon=1, & P=4\mu+1, & V=\dfrac{\pi}{2\sqrt{4P}}\Sigma(-1)^{\frac{1}{2}(m'-1)}\left(\dfrac{m'}{P}\right),\\[2ex] \delta=1, & \varepsilon=-1, & P=4\mu+3, & V=\dfrac{\pi}{2\sqrt{8P}}\Sigma(-1)^{\frac{1}{2}(m'-1)}\left(\dfrac{m'}{P}\right),\\[2ex] \delta=-1, & \varepsilon=-1, & P=4\mu+1, & V=\dfrac{\pi}{2\sqrt{8P}}\Sigma(-1)^{\frac{1}{2}(m'-1)+\frac{1}{8}(m'^2-1)}\left(\dfrac{m'}{P}\right).\end{cases}$$

Les valeurs m' sont premières à P et en outre impaires dans les trois dernières équations. Quant aux limites des sommations, on doit ajouter que les valeurs de m' doivent être respectivement inférieures à $\frac{1}{2}P$, $2P$, $4P$, $4P$.

Les expressions de V peuvent prendre beaucoup d'autres formes encore. On obtient, par exemple, des expressions différentes des précédentes et plus simples, si dans le cas où le terme général renferme l'un des facteurs:

$$(-1)^{\frac{1}{2}(n-1)},\quad (-1)^{\frac{1}{8}(n^2-1)},$$

ou l'un et l'autre, on les conserve dans la série, en n'introduisant les formules de M. Gauss que pour remplacer l'expression $\left(\frac{n}{P}\right)$. C'est ce que nous allons faire pour les trois derniers cas du tableau précédent (d).

Dans le premier de ces trois cas, on a:

$$V = \Sigma(-1)^{\frac{1}{2}(n-1)}\left(\frac{n}{P}\right)\frac{1}{n},\qquad P=4\mu+1,$$

et l'équation (1) donne alors:

$$\Sigma\left(\frac{m}{P}\right)\cos n\frac{2m\pi}{P} = \left(\frac{n}{P}\right)\sqrt{P}\quad\text{ou}\quad =0,$$

suivant que n est ou n'est pas premier à P, m devant recevoir toutes les valeurs inférieures et premières à P. En substituant cette expression de $\left(\frac{n}{P}\right)$, on aura:

$$V = \frac{1}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\Sigma(-1)^{\frac{1}{2}(n-1)}\frac{1}{n}\cos n\frac{2m\pi}{P},$$

où la sommation relative à n, peut maintenant s'étendre à tous les entiers impairs. Or on sait que la série:

$$\frac{\cos x}{1} - \frac{\cos 3x}{3} + \frac{\cos 5x}{5} - \cdots$$

a la valeur:

$$\frac{\pi}{4}, \quad -\frac{\pi}{4}, \quad \frac{\pi}{4},$$

suivant que x est compris dans les trois intervalles:

$$0 \text{ et } \frac{\pi}{2}, \quad \frac{\pi}{2} \text{ et } \frac{3\pi}{2}, \quad \frac{3\pi}{2} \text{ et } 2\pi.$$

Désignant donc respectivement par m', m'', m''' les valeurs de m comprises dans les trois intervalles:

$$0 \text{ et } \tfrac{1}{4}P, \quad \tfrac{1}{4}P \text{ et } \tfrac{3}{4}P, \quad \tfrac{3}{4}P \text{ et } P,$$

on aura:

$$V = \frac{\pi}{4\sqrt{P}}\left[\Sigma\left(\frac{m'}{P}\right) - \Sigma\left(\frac{m''}{P}\right) + \Sigma\left(\frac{m'''}{P}\right)\right].$$

On a d'ailleurs évidemment:

$$\Sigma\left(\frac{m'}{P}\right) = \Sigma\left(\frac{m'''}{P}\right) \quad \text{et} \quad \Sigma\left(\frac{m'}{P}\right) + \Sigma\left(\frac{m''}{P}\right) + \Sigma\left(\frac{m'''}{P}\right) = 0,$$

d'où l'on conclut:

$$(e) \qquad V = \frac{\pi}{\sqrt{P}}\Sigma\left(\frac{m'}{P}\right),$$

m' désignant les valeurs premières à P, comprises entre 0 et $\frac{1}{4}P$.

Dans le second cas on a:

$$V = \Sigma(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}, \quad P = 4\mu+3.$$

En substituant la valeur de $\left(\frac{n}{P}\right)$ donnée par l'équation (1), il viendra:

$$V = \frac{1}{\sqrt{P}}\Sigma\left(\frac{m}{P}\right)\Sigma(-1)^{\frac{1}{8}(n^2-1)}\frac{1}{n}\sin n\frac{2m\pi}{P},$$

n pouvant maintenant recevoir toutes les valeurs impaires premières à P ou

non. Or la série:

$$\frac{\sin x}{1} - \frac{\sin 3x}{3} - \frac{\sin 5x}{5} + \frac{\sin 7x}{7} + \cdots$$

étant sommée par les moyens connus, on trouve que sa valeur est respectivement:

$$0, \quad \frac{\pi}{2\sqrt{2}}, \quad 0, \quad -\frac{\pi}{2\sqrt{2}}, \quad 0,$$

suivant que x est compris dans les cinq intervalles:

$$0 \text{ et } \frac{\pi}{4}, \quad \frac{\pi}{4} \text{ et } \frac{3\pi}{4}, \quad \frac{3\pi}{4} \text{ et } \frac{5\pi}{4}, \quad \frac{5\pi}{4} \text{ et } \frac{7\pi}{4}, \quad \frac{7\pi}{4} \text{ et } 2\pi.$$

En désignant donc par m' les valeurs de m comprises entre $\frac{1}{8}P$ et $\frac{3}{8}P$, et par m'' celles qui tombent entre $\frac{5}{8}P$ et $\frac{7}{8}P$, on aura:

$$V = \frac{\pi}{2\sqrt{2P}}\left[\Sigma\left(\frac{m'}{P}\right) - \Sigma\left(\frac{m''}{P}\right)\right],$$

ou plus simplement en observant qu'on peut remplacer m'' par $P-m'$, et qu'on a $\left(\frac{P-m'}{P}\right) = -\left(\frac{m'}{P}\right)$:

$$(f) \qquad V = \frac{\pi}{\sqrt{2P}}\Sigma\left(\frac{m'}{P}\right).$$

On trouve d'une manière semblable, P étant de la forme $4\mu+1$:

$$(g) \qquad V = \Sigma(-1)^{\frac{1}{8}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n} = \frac{\pi}{\sqrt{2P}}\left(\Sigma\left(\frac{m'}{P}\right) - \Sigma\left(\frac{m''}{P}\right)\right),$$

en désignant par m' et m'' les valeurs premières à P et respectivement comprises dans les deux intervalles 0 et $\frac{1}{8}P$, $\frac{3}{8}P$ et $\frac{1}{2}P$. Il importe de remarquer que les équations (e) et (g) ne s'appliquent pas au cas où $P=1$.

§. 11.

On pourrait donner beaucoup d'autres formes à l'expression de la série V, soit que cette série réponde à un déterminant négatif, soit qu'elle se rapporte à un déterminant positif. Mais comme ces détails ne présentent aucune difficulté, nous ne nous y arrêterons pas et nous passons à l'énumération des différents théorèmes, qui résultent des équations (19) et (23) du §. 6, lorsqu'on y introduit les expressions qui viennent d'être obtenues.

Déterminants positifs.

(I) $$D=P,\quad P=4\mu+1,\quad h=\frac{2-\left(\frac{2}{P}\right)}{\log(T+U\sqrt{P})}\log\frac{\Pi\sin\frac{b\pi}{P}}{\Pi\sin\frac{a\pi}{P}},$$

où les entiers m inférieurs et premiers à P sont désignés par a ou par b, suivant que l'équation $\left(\frac{m}{P}\right)=\pm 1$ a lieu avec le signe supérieur ou avec le signe inférieur.

(II) $$D=P,\quad P=4\mu+3,\quad h=\frac{1}{\log(T+U\sqrt{P})}\log\frac{\Pi\sin\frac{b\pi}{4P}}{\Pi\sin\frac{a\pi}{4P}},$$

où les entiers m inférieurs et premiers à $4P$ sont désignés par a ou par b, suivant que le signe ambigu, dans l'équation $(-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{P}\right)=\pm 1$, est le signe supérieur ou inférieur.

(III) $$D=2P,\quad P=4\mu+1,\quad h=\frac{1}{\log(T+U\sqrt{2P})}\log\frac{\Pi\sin\frac{b\pi}{8P}}{\Pi\sin\frac{a\pi}{8P}},$$

où les entiers m inférieurs et premiers à $8P$ sont désignés par a ou par b, suivant que le signe ambigu, dans l'équation $(-1)^{\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)=\pm 1$, est le signe supérieur ou inférieur.

(IV) $$D=2P,\quad P=4\mu+3,\quad h=\frac{1}{\log(T+U\sqrt{2P})}\log\frac{\Pi\sin\frac{b\pi}{8P}}{\Pi\sin\frac{a\pi}{8P}},$$

où les entiers m inférieurs et premiers à $8P$ sont désignés par a ou par b, suivant que l'on a $(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)=+1$ ou $=-1$.

Déterminants négatifs.

(V) $$D=-P,\quad P=4\mu+3,\quad h=\left(2-\left(\frac{2}{P}\right)\right)\frac{\Sigma b-\Sigma a}{P}=A-B.$$

Dans cette équation a et b ont la même signification que dans le premier cas, et A et B désignent respectivement combien il existe de valeurs a et b au-dessous de $\frac{1}{2}P$.

(VI) $$D=-P,\quad P=4\mu+1,\quad h=\frac{\Sigma b-\Sigma a}{4P}=\frac{A-B}{2}.$$

Les lettres a et b ont la même signification que dans le second cas, et A et B désignent respectivement les nombres des valeurs a et b qui sont inférieures à $2P$. On a encore dans ce sixième cas, en désignant par A' et B' les nombres des valeurs a et b au-dessous de $\frac{1}{4}P$, a et b ayant le même sens que dans le premier cas:

$$h=2(A'-B').$$

(VII) $$D=-2P,\quad P=4\mu+3,\quad h=\frac{\Sigma b-\Sigma a}{8P}=\frac{A-B}{2}.$$

Les lettres a et b ont la même signification que dans le troisième cas, et A et B désignent respectivement les nombres des valeurs a et b moindres que $4P$. On a encore dans ce septième cas, en désignant par A' et B' les nombres des valeurs a et b, comprises entre $\frac{1}{8}P$ et $\frac{3}{8}P$, a et b ayant le même sens que dans le premier cas:

$$h=2(A'-B').$$

(VIII) $$D=-2P,\quad P=4\mu+1,\quad h=\frac{\Sigma b-\Sigma a}{8P}=\frac{A-B}{2},$$

où a et b ont le même sens que dans le quatrième cas, et A et B désignent les nombres des valeurs a et b qui tombent au-dessous de $4P$. On a encore si, conservant aux lettres a et b la même signification que dans le premier cas, l'on désigne par A', B' et A'', B'' les nombres des valeurs a, b qui sont contenues dans les deux intervalles compris entre 0 et $\frac{1}{8}P$, $\frac{3}{8}P$ et $\frac{1}{2}P$:

$$h=2(A'-B'-A''+B'').$$

Il nous reste à présenter quelques remarques sur les résultats qui viennent d'être énoncés. Pour parler d'abord des quatre premiers cas, nous devons dire que les expressions qui s'y rapportent, quoique très simples, ne sont pas sous la forme qui en montre la véritable signification. Pour leur donner cette forme, nous nous occuperons spécialement du premier de ces cas. Les trois autres donnent lieu à des remarques entièrement semblables. Soit x une indéterminée et considérons les deux produits:

$$\Pi\left(x-e^{\frac{2a\pi i}{P}}\right),\quad \Pi\left(x-e^{\frac{2b\pi i}{P}}\right).$$

Il est évident qu'en posant:

$$X = \Pi\left(x - e^{\frac{2\alpha\pi i}{P}}\right)\Pi\left(x - e^{\frac{2b\pi i}{P}}\right),$$

le polynôme X ne sera autre chose que le premier membre de l'équation que l'on obtient en délivrant l'équation binôme $x^P - 1 = 0$ de ses racines non-primitives. Il est facile de conclure de là que pour $x = 1$, on a:

$$X = 1 \quad \text{ou} \quad X = P$$

suivant que le nombre des facteurs simples p, p', p'', ... de P est supérieur ou égal à l'unité. (Le cas où l'on aurait $P = 1$. est exclu, le déterminant étant un carré dans ce cas.)

On a donc suivant les deux cas qui viennent d'être distingués:

$$\Pi\left(1 - e^{\frac{2\alpha\pi i}{P}}\right)\Pi\left(1 - e^{\frac{2b\pi i}{P}}\right) = 1 \quad \text{ou} \quad = P.$$

On a aussi:

$$\Pi\left(1 - e^{\frac{2\alpha\pi i}{P}}\right) = \Pi\left(-2i\sin\frac{a\pi}{P}\right)e^{\frac{\pi i}{P}\Sigma a},$$

$$\Pi\left(1 - e^{\frac{2b\pi i}{P}}\right) = \Pi\left(-2i\sin\frac{b\pi}{P}\right)e^{\frac{\pi i}{P}\Sigma b};$$

observant donc que les valeurs a et b sont en nombre égal, que la suite des valeurs a renferme toujours avec un nombre a son complément $P - a$, et qu'il en est de même de la suite des valeurs b, on en conclura:

$$\frac{\Pi\sin\frac{b\pi}{P}}{\Pi\sin\frac{a\pi}{P}} = \frac{\Pi\left(1 - e^{\frac{2b\pi i}{P}}\right)}{\Pi\left(1 - e^{\frac{2\alpha\pi i}{P}}\right)},$$

puis, en ayant égard à une équation précédente:

$$\frac{\Pi\sin\frac{b\pi}{P}}{\Pi\sin\frac{a\pi}{P}} = \Pi\left(1 - e^{\frac{2b\pi i}{P}}\right)^2 \quad \text{ou} \quad = \frac{1}{P}\Pi\left(1 - e^{\frac{2b\pi i}{P}}\right)^2$$

suivant les deux cas déjà distingués. La détermination de h dépend donc du produit:

$$\Pi\left(1 - e^{\frac{2b\pi i}{P}}\right).$$

Or il résulte d'un théorème connu dû à M. Gauss et qu'il est facile d'étendre à un nombre composé P, que le polynôme:

$$\Pi\left(x - e^{\frac{2b\pi i}{P}}\right)$$

est toujours de la forme $\frac{1}{2}(Y + Z\sqrt{P})$, Y et Z étant des polynômes à coefficients entiers. En désignant donc par Y_1 et Z_1 les valeurs que Y et Z prennent pour $x = 1$, et passant des logarithmes aux nombres, l'équation qui détermine h, deviendra:

$$(T + U\sqrt{P})^h = \left(\frac{Y_1 + Z_1\sqrt{P}}{2}\right)^{h-2\left(\frac{2}{P}\right)} \quad \text{ou} \quad (T + U\sqrt{P})^h = \left(\frac{Y_1 + Z_1\sqrt{P}}{2\sqrt{P}}\right)^{h-2\left(\frac{2}{P}\right)},$$

suivant que le nombre des facteurs simples de P est supérieur ou égal à l'unité.

Sous cette forme les résultats qui se rapportent à un déterminant positif, paraîtront bien remarquables, s'il est vrai, comme l'a dit un illustre géomètre, que l'intérêt que présentent les recherches arithmétiques ait sa source non seulement dans la difficulté de la matière, mais surtout dans les rapports intimes que les recherches de ce genre dévoilent entre des théories entre lesquelles on ne soupçonnerait aucune connexion.

Quant au calcul des polynômes Y et Z, il peut se faire, soit par la méthode de M. Gauss, soit par un moyen dont Legendre a fait usage et qui est fondé sur les relations connues qui existent entre les coefficients d'une équation et les sommes des puissances semblables de ses racines. Il est facile de voir qu'à l'aide de ces relations on peut obtenir successivement tous les coefficients d'une équation lorsque les sommes des puissances de ses racines sont connues, comme cela arrive ici, la somme des puissances $m^{\text{ièmes}}$ des racines de l'équation:

$$\Pi\left(x - e^{\frac{2b\pi i}{P}}\right) = 0$$

résultant sans difficulté de la formule (1) du paragraphe précédent.

On trouve ainsi, en supposant par exemple $P = 3 \cdot 11$:

$$Y = 2x^{10} - x^9 + 8x^8 + 5x^7 + 2x^6 + 14x^5 + 2x^4 + 5x^3 + 8x^2 - x + 2,$$
$$Z = x^9 + x^7 + 2x^6 + 2x^4 + x^3 + x,$$

par suite:

$$Y_1 = 46, \qquad Z_1 = 8,$$

et comme on a $\left(\frac{2}{P}\right) = 1$:

$$\left(\frac{Y_1 + Z_1\sqrt{P}}{2}\right)^{h-2\left(\frac{2}{P}\right)} = (23 + 4\sqrt{33})^h.$$

On a d'un autre côté:

$$T+U\sqrt{P} = 23+4\sqrt{33},$$

d'où il suit $h = 2$, ce qui est exact, les formes qui répondent au déterminant 33, étant x^2-33y^2, $33x^2-y^2$.

Pour donner un exemple du cas où P se réduit à un nombre premier, soit $P = 17$; on trouve alors $Y_1 = 34$, $Z_1 = 8$, et l'expression:

$$\left(\frac{Y_1+Z_1\sqrt{P}}{2\sqrt{P}}\right)^{4-2\left(\frac{2}{P}\right)}$$

devient $(4+\sqrt{17})^2 = 33+8\sqrt{17}$, ce qui est la première puissance de $T+U\sqrt{P}$, comme cela doit être, puisque pour le déterminant 17 il n'existe que la seule forme x^2-17y^2.

Les expressions de h, relatives aux déterminants négatifs, n'ont besoin d'aucune explication. Nous ajouterons seulement que pour un cas particulier qui se rapporte au n°. V, le résultat avait déjà été indiqué par M. JACOBI. (Voir le Journal de CRELLE Tome IX.)

Nous terminerons ce mémoire en indiquant une application que l'on peut faire des expressions de h, dans le cas des déterminants négatifs. On sait que, lorsqu'un entier k peut être décomposé en trois carrés, ou en d'autres termes lorsque l'équation $x^2+y^2+z^2 = k$ est possible, le nombre de ses solutions dépend du nombre des formes dont le déterminant est $-k$. Les théorèmes qui fixent cette dépendance, ont d'abord été découverts par LEGENDRE dans les cas les plus simples et par voie d'induction. M. GAUSS les a ensuite démontrés d'une manière générale et très ingénieuse dans la 5ième section de son ouvrage. Il est évident qu'il suffit de comparer les théorèmes dont il s'agit avec les résultats auxquels nous sommes parvenus dans ce paragraphe et dans le §. 8, pour en conclure, par la simple élimination du nombre des formes quadratiques qui entre dans les uns et dans les autres, de nouvelles expressions pour le nombre des solutions de l'équation $x^2+y^2+z^2 = k$, expressions qui ne renfermeront plus rien qui soit relatif aux formes quadratiques. Je me bornerai ici à cette seule remarque et je n'entreprendrai pas quant à présent l'énumération de ces nouveaux théorèmes; ces détails seront mieux placés dans un autre mémoire dans lequel je chercherai à établir les résultats dont il s'agit d'une manière directe et sans y faire concourir les deux théories dont je viens de parler.

ÜBER EINE EIGENSCHAFT DER QUADRATISCHEN FORMEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1840, S. 49—52.

ÜBER
EINE EIGENSCHAFT DER QUADRATISCHEN FORMEN.

[Auszug aus einer in der Akademie der Wissenschaften am 5. März 1840 gelesenen Abhandlung.]

Die vorgelesene Abhandlung ist als die Fortsetzung einer früheren zu betrachten, welche in dem Jahrgange von 1837 gedruckt ist, und worin der erste strenge Beweis des Satzes gegeben worden ist, dass jede arithmetische Reihe, deren erstes Glied und deren Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*). In der gegenwärtigen Abhandlung wird dieser Satz auf quadratische Formen, d. h. auf Ausdrücke von der Gestalt $ax^2+2bxy+cy^2$ ausgedehnt, die jedoch der Beschränkung unterworfen werden müssen, dass die darin enthaltenen bestimmten Zahlen a, $2b$, c keinen gemeinschaftlichen Factor haben.

Die Principien, auf welchen der Beweis dieser Eigenschaft beruht, obgleich im Wesentlichen mit denjenigen übereinstimmend, von welchen in der angeführten Abhandlung Gebrauch gemacht worden ist, bedürfen zum Behufe dieser neuen Anwendung einiger Modificationen, welche wir an einem speciellen Falle anzudeuten versuchen wollen. Es ist dies der Fall, wo die Determinante eine negative Primzahl $-p$ ist, welche, abgesehen vom Zeichen, die Form $4n+3$ hat, und wo diese Determinante zugleich zu den sogenannten regelmässigen gehört *(determinans regularis, Disq. arith. art. 306, VI)*.

Es sei $h=2\lambda+1$ die Anzahl der verschiedenen Formen, welche für die Determinante $-p$ stattfinden, und welche unter der gemachten Voraussetzung sich alle aus einer derselben, φ_1, durch successives Zusammensetzen bilden lassen. Diese Formen, welche wir durch φ bezeichnen und durch Indices von einander unterscheiden wollen, lassen sich dann immer in folgende

*) S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Ordnung bringen:

$$(1) \qquad \varphi_{-\lambda},\ \varphi_{-(\lambda-1)},\ \ldots,\ \varphi_{-1},\ \varphi_0,\ \varphi_1,\ \ldots,\ \varphi_{\lambda-1},\ \varphi_\lambda,$$

welche Reihe als in sich zurückkehrend zu betrachten ist, so dass auf φ_λ wieder $\varphi_{-\lambda}$ folgt, und wo jede Form aus der vorhergehenden und der Form φ_1 zusammengesetzt ist, φ_0 die Hauptform x^2+py^2 bedeutet, und entgegengesetzten Formen:

$$ax^2+2bxy+cy^2, \quad ax^2-2bxy+cy^2,$$

entgegengesetzte Indices entsprechen.

Theilt man die Gesammtheit der positiven ungeraden Primzahlen (p ausgenommen) in zwei Classen, von welchen die erste alle diejenigen enthält, in Bezug auf welche $-p$ quadratischer Rest ist, die zweite alle übrigen umfasst, und bezeichnet die in den beiden Classen enthaltenen Zahlen allgemein respective mit f und g, so lassen sich bekanntlich die Primzahlen der ersten Classe ausschliesslich durch die Formen (1) darstellen, und zwar ist jede Primzahl f fähig, durch zwei entgegengesetzte Formen:

$$\varphi_\gamma \quad \text{und} \quad \varphi_{-\gamma},$$

und nur durch diese ausgedrückt zu werden; wobei es sich von selbst versteht, dass für $\gamma = 0$ diese beiden Formen sich auf die Hauptform reduciren. Der doppelte Werth:

$$\pm\gamma$$

soll nun der Index von f heissen.

Es sei ferner:

$$\frac{2\pi}{h} = \omega,$$

wo π die gewöhnliche Bedeutung hat, t irgend eine der Zahlen:

$$(2) \qquad 0,\ 1,\ 2,\ \ldots,\ \lambda$$

und endlich s eine positive die Einheit übertreffende Grösse. Alsdann findet folgende Gleichung statt, deren Wahrheit leicht aus den bekannten Sätzen über die Zusammensetzung der Formen folgt:

$$2\Pi\frac{1}{1-\frac{1}{g^{2s}}}\cdot\Pi\frac{1}{1-2\frac{\cos t\gamma\omega}{f^s}+\frac{1}{f^{2s}}} = \Sigma\frac{1}{\varphi_0^s}+2\cos t\omega\,\Sigma\frac{1}{\varphi_1^s}+\cdots+2\cos\lambda t\omega\,\Sigma\frac{1}{\varphi_\lambda^s}.$$

In dieser Gleichung bezieht sich das erste Multiplicationszeichen auf alle Primzahlen g, das zweite auf alle Primzahlen f, und $\pm\gamma$ ist der jedesmalige Index

von f. Was das Zeichen Σ betrifft, so bedeutet dasselbe, dass man in der quadratischen Form, vor welcher es steht, den unbestimmten Zahlen x und y alle Systeme positiver oder negativer Werthe von solcher Beschaffenheit beilegen muss, dass der entsprechende Werth der Form ungerade und nicht durch p theilbar wird. Setzt man zur Abkürzung:

$$2\Pi\frac{1}{1-\frac{1}{g^{2s}}} = G$$

und bezeichnet die rechte Seite der Gleichung mit L_t, nimmt dann die Logarithmen von beiden Seiten und entwickelt jeden der Logarithmen, welche f enthalten, nach der bekannten Formel:

$$-\tfrac{1}{2}\log(1-2z\cos\alpha+z^2) = \frac{z}{1}\cos\alpha+\frac{z^2}{2}\cos 2\alpha+\cdots,$$

so erhält man:

$$\Sigma\frac{\cos t\gamma\omega}{f^s}+\tfrac{1}{2}\Sigma\frac{\cos 2t\gamma\omega}{f^{2s}}+\cdots = -\tfrac{1}{2}\log G+\tfrac{1}{2}\log L_t.$$

Diese allgemeine Gleichung enthält, wie die frühere, $\lambda+1$ besondere Gleichungen, welche den verschiedenen Werthen (2) von t entsprechen. Addirt man diese besonderen Gleichungen, nachdem man sie der Reihe nach mit:

$$1,\ 2\cos\mu\omega,\ 2\cos 2\mu\omega,\ \ldots,\ 2\cos\lambda\mu\omega$$

multiplicirt hat, und nimmt man für μ eine der Zahlen $1, 2, \ldots, \lambda$, so kommt:

$$(3) \quad \Sigma\frac{1}{f^s}+\tfrac{1}{2}\Sigma\frac{1}{f^{2s}}+\cdots = \frac{1}{h}(\log L_0+2\cos\mu\omega\log L_1+\cdots+2\cos\lambda\mu\omega\log L_\lambda),$$

wo die erste Summation auf alle Primzahlen auszudehnen ist, deren Index $\pm\mu$ ist, die zweite auf diejenigen, deren doppelt genommener Index congruent $\pm\mu$ (mod. h) ist, u. s. w. Für $\mu = 0$ erhält man durch dasselbe Verfahren:

$$(4) \quad \Sigma\frac{1}{f^s}+\tfrac{1}{2}\Sigma\frac{1}{f^{2s}}+\cdots = -\tfrac{1}{2}\log G+\frac{1}{2h}(\log L_0+2\log L_1+\cdots+2\log L_\lambda),$$

wo die Summation sich resp. über alle Primzahlen erstreckt, deren Indices, resp. mit $1, 2, \ldots$ multiplicirt, durch h theilbar werden.

Die Gleichungen (3) und (4) gelten, wie diejenigen, aus welchen sie abgeleitet sind, für jeden Werth von s, welcher grösser als 1 ist. Setzt man daher:

$$s = 1+\varrho,$$

wo ϱ positiv angenommen ist, so kann man die Veränderliche ϱ unendlich klein werden lassen. Untersucht man nun die unter dem Logarithmenzeichen vorkommenden Ausdrücke in dieser Voraussetzung, so findet man durch sehr einfache Betrachtungen, die jedoch hier nicht ausgeführt werden können, dass L_0 unendlich wird, dass hingegen L_t, wenn t nicht den Werth 0 hat, sich einer endlichen, von der Null verschiedenen Grenze nähert, und dass dieselbe Eigenschaft dem Producte G zukommt. Aus diesem Resultate folgt sogleich, dass die zweite und also auch die erste Seite jeder von den Gleichungen (3) und (4) für ein unendlich kleines ϱ unendlich gross wird, und dann ferner, wie in der früheren Abhandlung, dass die Summe:

$$\Sigma \frac{1}{f^{1+\varrho}}$$

aus unendlich vielen Gliedern besteht, oder, was dasselbe ist, dass jede der Formen (1) eine unendliche Anzahl von Primzahlen enthält.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 190—194.

UNTERSUCHUNGEN
ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

[Auszug aus einer in der Akademie der Wissenschaften am 27. Mai 1841 gelesenen Abhandlung.]

Da sich diese Untersuchungen, sowohl hinsichtlich der darin befolgten Methode als durch ihre Resultate, an frühere Arbeiten des Verfassers anschliessen, so wird es zur leichteren Verständlichkeit der hier zu gebenden Andeutungen zweckmässig sein, wenn wir diesen eine kurze Erwähnung einiger der früher behandelten Fragen vorausschicken.

In einer Abhandlung, welche unter denen der Akademie für das Jahr 1837 gedruckt ist*), hat man sich die Aufgabe gestellt, den längst bekannten und oft als Lemma benutzten Satz, nach welchem jede arithmetische Reihe, deren erstes Glied und deren Differenz keinen gemeinschaftlichen Factor haben, eine unendliche Anzahl von Primzahlen enthält, in aller Strenge zu beweisen. Der dort entwickelte Beweis bietet das Merkwürdige dar, dass er ungeachtet der rein arithmetischen Natur des zu begründenden Satzes wesentlich auf der Betrachtung stetig veränderlicher Grössen beruht, indem derselbe von der Bildung unendlicher Reihen ausgeht, die wie die schon von EULER in der *Introd. in Anal. inf.* behandelten durch Multiplication einer unendlichen Anzahl von Factoren entstehen. Diese neuen Reihen unterscheiden sich jedoch darin von den EULER'schen, dass in die Factoren, von denen jeder ein Glied der Reihe der Primzahlen enthält, noch Potenzen von Wurzeln der Einheit eingehen, deren Exponenten mit den sogenannten Indices der Primzahlen zusammenfallen, wenn diese mit allen übrigen auf ein System primitiver Wurzeln bezogen wird. Sobald man den eben angedeuteten Weg betreten hat, scheint sich der Beweis mit der grössten Leichtigkeit

*) S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

und, so zu sagen, ganz von selbst zu gestalten; allein bei aufmerksamer Betrachtung bemerkt man eine Schwierigkeit, ohne deren Beseitigung das Verfahren ganz illusorisch werden oder doch nur auf besondere Fälle anwendbar sein würde. Diese Schwierigkeit besteht in der für den Erfolg unerlässlichen Nachweisung, dass die Summen gewisser Reihen, deren Convergenz leicht einzusehen ist, von der Null verschieden sind, und hat nicht etwa, wie man es zunächst vermuthen sollte, ihren Grund in der Unmöglichkeit die Summation auszuführen. Diese Operation ist vielmehr in allen Fällen leicht zu bewerkstelligen; allein der endliche Ausdruck, welchen man dadurch erhält, gewährt keine Erleichterung für die geforderte Nachweisung, und es ist im Allgemeinen eben so schwer aus der Summe in endlicher Form zu erkennen, dass sie von Null verschieden ist, als dies bei der ursprünglichen Reihe der Fall war.

Nach mancherlei fruchtlosen Versuchen war es zwar gelungen, die erwähnte Schwierigkeit vollständig zu überwinden; doch waren die Betrachtungen, zu welchen man seine Zuflucht zu nehmen genöthigt war, so complicirt und indirect, dass sie nur wenig befriedigen konnten und die Auffindung eines kürzeren und der Natur der Sache mehr entsprechenden Verfahrens sehr wünschenswerth machen mussten. Wiederholte auf diesen Gegenstand gerichtete Bemühungen hatten denn auch endlich den beabsichtigten Erfolg und führten zu dem unerwarteten Resultate, dass die erwähnten Reihen mit einer Aufgabe zusammenhängen, deren Lösung in einem der wichtigsten Theile der Zahlenlehre eine längst gefühlte Lücke ausfüllt. Die Theorie, von welcher wir reden, ist die der quadratischen Formen, welche zuerst von LAGRANGE begründet, später durch LEGENDRE und besonders durch GAUSS zu einem hohen Grade der Ausbildung gelangt ist. Bekanntlich sind die Eigenschaften solcher Formen hauptsächlich von einer durch ihre Coefficienten bestimmten ganzen Zahl, welche die Determinante der Form heisst, abhängig, und LAGRANGE hat gezeigt, dass jeder Determinante, sie sei positiv oder negativ, nur eine endliche Anzahl wesentlich verschiedener Formen entspricht, so wie derselbe grosse Geometer auch das Verfahren angegeben hat, nach welchem sich für jede numerisch gegebene Determinante diese wesentlich verschiedenen Formen darstellen lassen. Die Frage nach dem allgemeinen Zusammenhange zwischen der Anzahl der Formen und der Determinante wird jedoch durch die Kenntniss dieses nur in bestimmten Fällen auszuführenden Verfahrens nicht erledigt, und diese Frage ist es nun, welche in den oben erwähnten Untersuchungen ihre Lösung erhält.

Von den daraus hervorgehenden Resultaten, welche im CRELLE'schen Journal (Bd. XIX u. XXI)*) ausführlich entwickelt worden sind, ist für unseren Zweck nur zu erwähnen, dass die Abhängigkeit der Anzahl der Formen von der Determinante sich in einer ganz verschiedenen Weise darstellt, je nachdem die Determinante negativ oder positiv ist. Im ersteren Falle ist diese Abhängigkeit rein arithmetischer Natur, während der Ausdruck für die Anzahl der Formen im zweiten Falle gewisse Verbindungen der Coefficienten der Hülfsgleichungen enthält, welche bei der Kreistheilung vorkommen.

Was nun die neuen Untersuchungen betrifft, deren ersten Theil die der Akademie vorgelegte Abhandlung enthält, so haben diese den Zweck, die eben angeführten Resultate auf die Theorie der complexen Zahlen auszudehnen. Den Gedanken, complexe ganze Zahlen, d. h. Ausdrücke von der Form $t+u\sqrt{-1}$, in die höhere Arithmetik einzuführen, verdankt man dem berühmten Verfasser der *Disq. arithm.*, welcher auf diese Erweiterung durch seine Untersuchungen über die Theorie der biquadratischen Reste geführt worden ist, deren Fundamentaltheoreme nur dann in ihrer höchsten Einfachheit und ganzen Schönheit erscheinen, wenn man sie auf complexe Primzahlen bezieht. Die Wichtigkeit des so erweiterten Begriffs der ganzen Zahl ist jedoch nicht auf die eben erwähnte Anwendung beschränkt; es wird vielmehr durch dessen Einführung den Untersuchungen der höheren Arithmetik ein neues Gebiet aufgeschlossen, auf welchem fast jede Eigenschaft reeller Zahlen ihr Analogon findet, welches nicht selten der ersteren hinsichtlich der Einfachheit und Eleganz gleichkommt oder sie gar übertrifft. So gilt z. B. der angeführte Satz über die arithmetische Reihe auch noch für complexe Zahlen, d. h. der Ausdruck $an+b$ enthält unendlich viele complexe Primzahlen, wenn man darin a und b als gegebene complexe Zahlen ohne gemeinschaftlichen Factor, n dagegen als eine unbestimmte complexe Zahl betrachtet. Der Beweis bleibt dem für reelle Zahlen sehr ähnlich, und diese Ähnlichkeit erstreckt sich auch auf den hier gleichfalls vorkommenden Umstand, dass man zu zeigen hat, dass gewisse convergirende Reihen Summen haben, welche von Null verschieden sind. Die Analogie machte es im höchsten Grade wahrscheinlich, dass zwischen diesen Reihen und der Anzahl der quadratischen Formen für die entsprechende complexe Determinante ein ähnlicher Zusammenhang stattfinden müsse, wie er früher für reelle Determinanten nachgewiesen worden war.

*) S. 411 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Doch war dieser Zusammenhang in der Theorie der complexen Zahlen weit schwerer aufzufinden, nicht nur wegen der grösseren Complication des Gegenstandes, sondern hauptsächlich deshalb, weil die Theorie der quadratischen Formen auf dem Gebiete der complexen Zahlen noch ganz unausgebildet war und es also erforderlich wurde, die bekannten Sätze der Theorie der quadratischen Formen, im gewöhnlichen Sinne des Wortes, der Reihe nach durchzugehen, um zu erkennen, mit welchen Modificationen sie für complexe Zahlen gelten.

Nach dieser vorläufigen Untersuchung gelangt man in der That dahin, den vermutheten Zusammenhang nachzuweisen, und es bleibt alsdann nur noch übrig, die erwähnten Reihen zu summiren, um den Ausdruck zu erhalten, welcher die Anzahl der Formen für eine complexe Determinante als Function dieser Determinante bestimmt. Als schliessliches Resultat der Untersuchung stellt sich heraus, dass die Abhängigkeit der Anzahl der Formen von der Determinante derjenigen ganz ähnlich ist, welche in dem zweiten der oben angeführten Fälle stattfindet, nur mit dem Unterschiede, dass die Rolle, welche dort die Hülfsgleichungen für die Kreistheilung spielen, hier von den Gleichungen übernommen wird, welche sich auf die Theilung der Lemniscate oder, was dasselbe ist, auf die Theilung der elliptischen Functionen beziehen, welche dem Modul $\sqrt{\frac{1}{2}}$ entsprechen.

Merkwürdiger noch als dieses allgemeine Resultat ist ein besonderer Fall, wo die Anzahl der Formen unabhängig von der Theilung der Lemniscate bestimmt werden kann. Es ist dies der Fall einer reellen Determinante D; für eine solche ist nämlich, wenn man sie in der Theorie der complexen Zahlen betrachtet, die Anzahl der Formen ein Product von drei Factoren, von welchen der erste eine einfache algebraische Function der Determinante darstellt, während der zweite und dritte mit den Zahlen zusammenfallen, welche in der gewöhnlichen Theorie der quadratischen Formen bezeichnen, wie viel Formen für die Determinanten $+D$ und $-D$ stattfinden. Dieses Resultat enthält, wenn wir uns nicht sehr täuschen, einen der schönsten Sätze der Theorie der complexen Zahlen und muss um so mehr überraschen, als in der Theorie der reellen Zahlen zwischen den Formen, welche zwei entgegengesetzten Determinanten entsprechen, gar kein Zusammenhang zu bestehen scheint.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1841, S. 141—161.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

[Gelesen in der Akademie der Wissenschaften am 27. Mai 1841.]

Gegenwärtige Abhandlung bildet einen Theil einer grösseren Arbeit, welche den Zweck hat, mehrere der Theorie der reellen ganzen Zahlen angehörige, früher von mir gelöste Fragen auf das Gebiet der complexen Zahlen zu verpflanzen und vermittelst derselben Methode, von welcher in den erwähnten Untersuchungen Gebrauch gemacht worden ist, zu behandeln. Zu dieser Erweiterung hat mich nicht nur die Aussicht auf die neuen Resultate, welche sich von derselben erwarten liessen, sondern auch und mehr noch der Wunsch bestimmt, auf solche Weise jene frühere Behandlungsweise einer Prüfung zu unterwerfen und klar zu übersehen, ob der Erfolg derselben einer wirklichen Übereinstimmung der Methode mit der wahren Natur der gelösten Fragen oder, wie es bei mathematischen Untersuchungen nicht selten der Fall ist, mehr zufälligen Umständen zuzuschreiben sei. Diese Probe nun hat die Methode mit Glück bestanden, indem es nur geringer, sich ganz von selbst aus der veränderten Beschaffenheit des Gegenstandes ergebender Modificationen bedurfte, um sie auf die analogen, der Theorie der complexen Zahlen angehörigen Fragen anwendbar zu machen.

Der bei weitem grössere Theil der neuen Untersuchungen, deren Zweck ich im Vorhergehenden bezeichnet habe, bezieht sich auf die Lehre von den quadratischen Formen und wird nächstens an einem anderen Orte erscheinen.*) In der gegenwärtigen Abhandlung beschäftige ich mich ausschliesslich mit dem Beweise des Satzes, dass der Ausdruck $kt+l$, in welchem t eine unbestimmte complexe ganze Zahl und k, l gegebene solche Zahlen ohne gemeinschaftlichen Factor bezeichnen, immer unendlich viele Primzahlen enthält. Dieser Beweis

*) S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

setzt, wie der früher gegebene des analogen Satzes für reelle Zahlen, ausser den Fundamentaltheoremen über die complexen Zahlen gewisse Eigenschaften der quadratischen Formen voraus, weshalb ich mich, um unnütze Wiederholungen zu vermeiden, auf die eben erwähnten Untersuchungen berufen werde*).

§. 1.

Obgleich, wie schon bemerkt worden, die Elementareigenschaften der complexen Zahlen als bekannt vorausgesetzt werden, so wird es doch zweckmässig sein, einige dieser Eigenschaften, welche für das Folgende von besonderer Wichtigkeit sind, hier ganz kurz anzugeben.

Wir setzen, wie gewöhnlich, $\sqrt{-1} = i$ und nennen complexe ganze Zahl jeden Ausdruck $f+gi$, in welchem f und g reelle ganze Zahlen bedeuten. Die der complexen Zahl $f+gi$ entsprechende positive Zahl f^2+g^2 wird ihre Norm genannt und mit $N(f+gi)$ bezeichnet werden. Vier complexe Zahlen:

$$f+gi, \quad -g+fi, \quad -f-gi, \quad g-fi,$$

welche so von einander abhängen, dass irgend drei derselben aus der vierten entstehen, wenn man diese mit -1, $\pm i$ multiplicirt, sollen *zusammengehörig* heissen.

In Bezug auf einen gegebenen complexen Modul m lässt sich immer eine Zahlenreihe bilden, welche die doppelte Eigenschaft besitzt, dass sich unter ihren Gliedern eines und nur eines befindet, welches mit einer beliebigen Zahl nach dem Modul m congruent ist.

Die Anzahl der Glieder eines solchen Systems incongruenter Zahlen ist $N(m)$. Auch lässt sich allgemein bestimmen, wie viel Glieder es in einem solchen Systeme giebt, die mit m keinen gemeinschaftlichen Factor haben.

Setzt man nämlich:

$$m = i^{\mu} a^{\alpha} b^{\beta} c^{\gamma} \ldots, \tag{1}$$

wo a, b, c, ... Primzahlen bedeuten, von denen keine der anderen gleich ist

*) Diese Untersuchungen sind, seit gegenwärtige Abhandlung der Akademie vorgelegt worden ist, unter dem Titel „*Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*“ im Crelle'schen Journal Band XXIV bekannt gemacht worden.[1]) Ausser dem im Titel angegebenen Gegenstande enthält die eben angeführte Abhandlung eine kurze Darstellung der Elemente der Theorie der complexen Zahlen, wobei ich mich jedoch auf die Sätze beschränkt habe, die zum Verständniss jener Abhandlung erforderlich waren. Eine vollständigere Darstellung dieser Elemente findet man in der zweiten Abhandlung über die biquadratischen Reste von Gauss, in welcher dieser grosse Geometer den Begriff der complexen Zahl zuerst in die Wissenschaft eingeführt hat, und auf welche ich den Leser verweise.

[1]) S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

noch mit ihr zusammengehört, und setzt ferner:

$$N(a) = A, \quad N(b) = B, \quad N(c) = C, \quad \ldots,$$

so wird die verlangte Anzahl $\psi(m)$ durch die Gleichung:

$$\psi(m) = (A-1)A^{\alpha-1}.(B-1)B^{\beta-1}.(C-1)C^{\gamma-1}\ldots$$

gegeben.

Sind:

$$\mu, \quad \mu', \quad \mu'', \quad \ldots \tag{2}$$

die Glieder, deren Anzahl so eben bestimmt wurde, und bezeichnet l eine Zahl, die mit m keinen gemeinschaftlichen Factor hat, so beweist man leicht, dass die Zahlen:

$$l\mu, \quad l\mu', \quad l\mu'', \quad \ldots,$$

wenn man von ihrer Ordnung absieht, mit den Zahlen (2) nach dem Modul m congruent sind, und hieraus erschliesst man, wie in dem bekannten Beweise des Fermat'schen Satzes für reelle Zahlen, die Congruenz:

$$l^{\psi(m)} \equiv 1 \pmod{m}. \tag{3}$$

Wie man in der gewöhnlichen Zahlentheorie die positiven Zahlen als die ursprünglichen und die negativen als durch Multiplication mit dem Factor -1 aus diesen entstanden zu betrachten pflegt, so gewährt es für manche auf complexe Zahlen bezügliche Betrachtungen eine wesentliche Erleichterung, wenn man unter je vier zusammengehörigen Zahlen eine nach einem festen Princip gewählte als die ursprüngliche oder primäre und die übrigen als die Producte dieser in -1, $\pm i$ ansieht. Das Bedürfniss einer solchen Unterscheidung ist besonders bei der Betrachtung ungerader Zahlen fühlbar, und man hat bei der zu treffenden Wahl darauf zu sehen, dass, wie das Product von positiven Factoren selbst wieder positiv ist, so auch hier aus der Multiplication primärer Factoren wieder eine primäre Zahl hervorgehe. Wie leicht zu sehen, findet sich in jeder Gruppe zusammengehöriger ungerader Zahlen immer eine und nur eine Zahl $f+gi$, für welche f und g resp. die Form $4\mu+1$ und 2μ haben, so wie auch nur eine, für welche $f-1$ und g entweder beide in der Form 4μ oder beide in der Form $4\mu+2$ enthalten sind, und man überzeugt sich ohne Schwierigkeit, dass der eben ausgesprochenen Bedingung Genüge geschieht, welche dieser Zahlen man auch allgemein, d. h. für alle Gruppen zusammengehöriger Zahlen, als die primäre betrachte. In der oben citirten Abhandlung haben wir die erste Definition gewählt; doch bleibt alles dort Gesagte wörtlich

richtig, wenn die zweite Definition zu Grunde gelegt wird. Diese letztere ist für unseren gegenwärtigen Zweck vorzuziehen; wir werden deshalb in dieser Abhandlung diejenigen ungeraden Zahlen $f+gi$ als primär betrachten, für welche $f-1$ und g gleichzeitig die Form 4μ oder gleichzeitig die Form $4\mu+2$ haben, und bemerken nur noch zur leichteren Anwendung dieser Definition, dass dieselbe offenbar darauf hinauskommt, in jeder Gruppe zusammengehöriger ungerader Zahlen diejenige als primär zu bezeichnen, welche nach dem Modul $2+2i$ der positiven Einheit congruent ist.

Unter dieser Voraussetzung hat man für jede ungerade primäre Zahl m:

$$m = a^{\alpha}b^{\beta}c^{\gamma}\ldots, \tag{4}$$

wo $a, b, c, \ldots$ von einander verschiedene primäre Primzahlen bedeuten, welche so wie ihre Exponenten durch m vollständig bestimmt sind.

§. 2.

Ehe wir an die Behandlung der Frage gehen können, welche den eigentlichen Gegenstand dieser Abhandlung bildet, sind einige Eigenschaften der Potenzreste für complexe Moduln abzuleiten.

Sind k und l zwei complexe Zahlen ohne gemeinschaftlichen Factor, und ist e der kleinste von Null verschiedene Exponent, für den $l^e \equiv 1 \pmod{k}$ ist, so sagt man, l gehöre für den Modul k zum Exponenten e. Es ist leicht sich zu überzeugen, dass alsdann:

$$1,\ l,\ l^2,\ \ldots,\ l^{e-1}$$

nach dem Modul k incongruent sind, so wie auch dass, wenn man die Reihe weiter fortsetzt, dieselben Reste periodisch wiederkehren, so dass also nur diejenigen Potenzen, deren Exponenten Vielfache von e sind, der Einheit congruent werden. Da:

$$l^{\psi(k)} \equiv 1 \pmod{k}$$

ist, so wird also e immer ein Theiler von $\psi(k)$ sein. In dem speciellen Falle, wo $e = \psi(k)$ ist, bilden die Potenzen:

$$1,\ l,\ l^2,\ \ldots,\ l^{\psi(k)-1}$$

ein System, wie wir es im vorigen Paragraphen betrachtet haben, d. h. welches ein Glied, aber auch nur eines enthält, welches mit einer beliebigen Zahl, die mit k keinen gemeinschaftlichen Factor hat, nach dem Modul k congruent

ist, und l heisst dann eine primitive Wurzel von k. Kennt man den Exponenten e, zu welchem l gehört, so kann man leicht denjenigen bestimmen, zu dem irgend eine Potenz l^s von l gehört. Man sieht ohne Schwierigkeit, dass dieser Exponent gleich $\frac{e}{\delta}$ ist, wenn δ den grössten gemeinschaftlichen (positiven) Theiler von s und e bezeichnet.

I. Wir betrachten zuerst den Fall, wo der Modul eine Potenz $(a+bi)^{\nu}$ einer ungeraden zweigliedrigen Primzahl $a+bi$ ist, so dass also:

$$N(a+bi) = a^2+b^2 = p$$

eine reelle Primzahl $4\mu+1$ ist. Für diesen Fall ist es leicht, die Existenz einer primitiven Wurzel zu zeigen. Ist die reelle Zahl $\mathfrak{a}$ eine primitive Wurzel für den Modul p^{ν}, so wird sie es auch in Bezug auf den Modul $(a+bi)^{\nu}$ sein. Da nämlich nach der ausgesprochenen Voraussetzung:

$$1,\ \mathfrak{a},\ \mathfrak{a}^2,\ \ldots,\ \mathfrak{a}^{(p-1)p^{\nu-1}-1}$$

nach dem Modul p^{ν} incongruent sind, so haben sie dieselbe Eigenschaft für den Modul $(a+bi)^{\nu}$, und andererseits ist:

$$\psi((a+bi)^{\nu}) = (p-1)p^{\nu-1}.$$

Hat man eine solche primitive Wurzel $\mathfrak{a}$ gewählt, so soll der Exponent:

$$\alpha_n < (p-1)p^{\nu-1},$$

für welchen:

$$\mathfrak{a}^{\alpha_n} \equiv n \pmod{(a+bi)^{\nu}}$$

ist, der Index der beliebigen nicht durch $a+bi$ theilbaren Zahl n heissen. Es folgt unmittelbar aus dieser Definition, dass man den Index eines Productes erhält, wenn man von der Summe der Indices der Factoren das grösste darin enthaltene Vielfache von $(p-1)p^{\nu-1}$ abzieht.

Die Zahl $\mathfrak{a}$ ist immer quadratischer Nichtrest von $a+bi$, da sonst jedes n quadratischer Rest von $a+bi$ sein müsste. Hieraus folgt sogleich, dass α_n gerade oder ungerade sein wird, je nachdem n quadratischer Rest oder Nichtrest von $a+bi$ ist. Man hat daher, wenn man sich des in der oben citirten Abhandlung eingeführten Zeichens bedient:

$$\left[\frac{n}{a+bi}\right] = (-1)^{\alpha_n}. \tag{5}$$

II. Der jetzt zu behandelnde Fall ist der eines Moduls von der Form r^g, wo r eine eingliedrige Primzahl bezeichnet. Da wir r reell und positiv voraussetzen können, so ist r eine Primzahl $4\mu+3$.

Zu dieser Untersuchung ist die Congruenz:

$$(b+zr)^{\varepsilon r^{g-2}} \equiv b^{\varepsilon r^{g-2}} + \varepsilon z b^{\varepsilon r^{g-2}-1} r^{g-1} \pmod{r^g}$$

erforderlich, welche schon in den *Disq. arith.* (art. 86) benutzt worden ist. Es ist zwar dort angenommen worden, dass b und z reell sind, aber derselbe Beweis ist auch auf den Fall anwendbar, wo b und z complexe Zahlen sind. Die im Exponenten vorkommenden Zahlen ε und $g \gtrless 2$ sind, wie sich von selbst versteht, positiv.

Für den Modul r^g existirt keine primitive Wurzel, ausser wenn $g=1$ ist; denn es ist mit Hülfe der obigen Congruenz leicht einzusehen, dass der höchste Exponent, zu welchem eine Zahl für diesen Modul gehören kann, $(r^2-1)r^{g-1}$ ist, während:

$$\psi(r^g) = (r^2-1)r^{2g-2}$$

ist. Dass es aber zum Exponenten $(r^2-1)r^{g-1}$ gehörende Zahlen giebt, kann man, wie folgt, zeigen. Da die aufgestellte Behauptung für $g=1$ schon erwiesen ist (*Theor. res. biq. auct.* C. F. Gauss art. 53), so sei b eine für den Modul r zum Exponenten r^2-1 gehörige Zahl, d. h. eine primitive Wurzel von r. Unter dieser Voraussetzung wird:

$$(b+zr)^\varepsilon - 1$$

nur dann durch r theilbar sein, wenn ε ein Vielfaches von r^2-1 ist. Es folgt hieraus, dass der Exponent, zu dem $b+zr$ für den Modul r^g gehört, durch r^2-1 theilbar sein muss. Da aber andererseits auch:

$$(b+zr)^{(r^2-1)r^{g-1}} \equiv 1 \pmod{r^g}$$

ist, wie aus obiger Congruenz sogleich folgt, wenn man:

$$(b+zr)^{r^2-1} = 1+ur$$

setzt, so sieht man, dass der erwähnte Exponent ein Theiler von $(r^2-1)r^{g-1}$ sein muss. Man wird daher eine zum Exponenten $(r^2-1)r^{g-1}$ gehörige Zahl $b+zr$ finden können, wenn sich z so wählen lässt, dass nicht:

$$(b+zr)^{(r^2-1)r^{g-2}} \equiv 1 \pmod{r^g}$$

ist. Es ist aber nach obigem Lemma:

$$-1+(b+zr)^{(r^2-1)r^{g-2}} \equiv -1+b^{(r^2-1)r^{g-2}} + (r^2-1)zb^{(r^2-1)r^{g-2}-1} r^{g-1} \pmod{r^g}.$$

Berücksichtigt man nun, dass:

$$-1+b^{(r^2-1)r^{g-2}} = Br^{g-1}$$

ist, wo B eine ganze Zahl bedeutet, und setzt zur Abkürzung:

$$(r^2-1)b^{(r^2-1)r^{g-2}-1} = C,$$

so ist klar, dass die geforderte Bedingung erfüllt sein wird, sobald man z so wählt, dass die Congruenz $Cz+B \equiv 0 \pmod{r}$ nicht stattfindet; und dies kann immer geschehen, da C kein Vielfaches von r ist.

Es liesse sich das eben erhaltene Resultat leicht vervollständigen und allgemein bestimmen, wie viel verschiedene, d. h. incongruente Zahlen zum Exponenten $(r^2-1)r^{g-1}$ oder überhaupt zu irgend einem Divisor desselben gehören. Ist er^ν ein solcher, wo e in r^2-1 aufgeht, und $\nu \gtrless g-1$, so wird die fragliche Anzahl durch den Ausdruck $\varphi(e)\psi(r^\nu)$ gegeben, worin $\varphi(e)$ die Anzahl der Zahlen bezeichnet, welche in der Reihe 0, 1, 2, ..., $e-1$ keinen gemeinschaftlichen Factor mit e haben. Da aber die Kenntniss dieser Anzahl zu unserem Zwecke nicht erforderlich ist, so wollen wir uns bei deren Bestimmung nicht aufhalten. Das Einzige, was für das Folgende nöthig ist, betrifft die Form der zum Exponenten r^{g-1} gehörigen Zahlen, welche sehr leicht auszumitteln ist. Wenn $\mathfrak{c}$ zu dem genannten Exponenten gehört, so dass also $\mathfrak{c}^{r^{g-1}}-1$ durch r^g und folglich auch durch r theilbar ist, so wird r^{g-1} ein Vielfaches von dem Exponenten sein, zu dem $\mathfrak{c}$ für den Modul r gehört. Da der letztere Exponent aber auch andererseits ein Theiler von r^g-1 sein muss, so hat derselbe den Werth 1, d. h. $\mathfrak{c}$ ist von der Form $1+zr$, und es bleibt nur noch zu untersuchen, welcher Bedingung z unterworfen sein muss, damit $1+zr$ für den Modul r^g wirklich zum Exponenten r^{g-1} gehöre. Zu diesem Zwecke bemerke man, dass, da nach dem obigen Lemma:

$$(1+zr)^{g-1}-1$$

offenbar durch r^g theilbar ist, der Exponent, zu dem $1+zr$ gehört, in r^{g-1} aufgehen und also kein anderer als r^{g-1} selbst sein wird, wenn z so beschaffen ist, dass die Congruenz:

$$(1+zr)^{r^{g-2}} \equiv 1 \pmod{r^g}$$

nicht stattfindet. Giebt man dieser mit Hülfe des Lemmas die Form:

$$zr^{g-1} \equiv 0 \pmod{r^g},$$

so sieht man, dass die nöthige und ausreichende Bedingung, damit $\mathfrak{c}$ zum Ex-

ponenten r^{g-1} gehöre, darin besteht, dass $\mathfrak{c}$ in dem Ausdruck $1+zr$ enthalten und z kein Vielfaches von r sei.

Dies vorausgesetzt, wird es uns leicht sein nachzuweisen, dass, wenn $\mathfrak{b}$ eine gegebene zum Exponenten $(r^2-1)r^{g-1}$ gehörige Zahl ist, immer eine zweite zum Exponenten r^{g-1} gehörige Zahl $\mathfrak{c}=1+zr$ von solcher Beschaffenheit gefunden werden kann, dass die Congruenz:

$$\mathfrak{b}^\beta \equiv \mathfrak{c}^\gamma \pmod{r^g},$$

worin β und γ resp. in den Reihen:

$$0,\ 1,\ 2,\ \ldots,\ (r^2-1)r^{g-1}-1;\quad 0,\ 1,\ \ldots,\ r^{g-1}-1$$

enthaltene Zahlen bedeuten, nicht anders bestehen kann, als wenn man gleichzeitig $\beta=0$, $\gamma=0$ hat. Wir bemerken zunächst, dass, da offenbar von den beiden Gleichungen $\beta=0$, $\gamma=0$ die eine die andere zur Folge hat, wir nur zu zeigen haben, dass $\mathfrak{c}$ so gewählt werden kann, dass die Congruenz nicht bestehen kann, wenn β und γ beide von Null verschieden sind. Es ist ferner leicht einzusehen, dass die Möglichkeit der Congruenz die Theilbarkeit von β durch r^2-1 voraussetzt. Setzen wir daher:

$$\beta=(r^2-1)\beta',\qquad \mathfrak{b}^{r^{g-1}}=1+kr,$$

wo k eine gegebene, nicht durch r theilbare Zahl bedeutet, so wird unsere Congruenz:

$$(1+kr)^{\beta'} \equiv (1+zr)^\gamma \pmod{r^g},$$

und es ist nur noch übrig z so einzurichten, dass dieselbe nicht bestehen kann, wenn β' und γ beide in der Reihe $1,\ 2,\ \ldots,\ r^{g-1}-1$ gewählt werden. Da $1+kr$ und $1+zr$ zum Exponenten r^{g-1} und folglich $(1+kr)^{\beta'}$ und $(1+zr)^\gamma$ zu den Exponenten $r^{g-1-\lambda}$ und $r^{g-1-\mu}$ gehören, wo r^λ und r^μ die höchsten in β' und γ aufgehenden Potenzen von r bedeuten, so erfordert unsere Congruenz, dass man $\lambda=\mu$ habe, und wird, wenn man $\beta'=r^\lambda\beta''$ und $\gamma=r^\lambda\gamma'$ setzt:

$$(1+kr)^{\beta''r^\lambda} \equiv (1+zr)^{\gamma'r^\lambda} \pmod{r^g}.$$

Da $\lambda \gtrless g-2$ ist, und diese letztere Congruenz, für $\lambda<g-2$ als richtig vorausgesetzt, auch noch für $\lambda=g-2$ bestehen wird, so haben wir bloss zu zeigen, dass für ein gehörig gewähltes z die Congruenz:

$$(1+kr)^{\beta''r^{g-2}} \equiv (1+zr)^{\gamma'r^{g-2}} \pmod{r^g}$$

nicht stattfinden kann. Nach dem obigen Lemma ist diese ganz gleichbedeutend mit:

$$(\gamma'z-\beta''k)r^{g-1} \equiv 0 \pmod{r^g},$$

oder was dasselbe ist, mit:

$$\gamma'z \equiv \beta''k \pmod{r}.$$

Jetzt bemerke man, dass, da die nicht durch r theilbaren Zahlen γ' und β'' reell sind, man immer eine reelle und offenbar nicht durch r theilbare Zahl δ so bestimmen kann, dass $\beta'' \equiv \gamma'\delta \pmod{r}$ wird, wodurch die letzte Congruenz in:

$$z \equiv k\delta \pmod{r}$$

übergeht. Da δ und also auch $k\delta$ nur $r-1$ nach dem Modul r incongruente Werthe annehmen kann, während für z, welches nur die Bedingung zu erfüllen hat, nicht durch r theilbar zu sein, r^2-1 verschiedene Werthe gewählt werden können, so sieht man, dass es $r^2-1-(r-1)=r(r-1)$ incongruente Werthe von z von solcher Beschaffenheit giebt, dass die letzte Congruenz unmöglich wird, w. z. b. w.

Das eben erhaltene Resultat, nach welchem für die auf die angegebene Weise bestimmten und zu den Exponenten $(r^2-1)r^{g-1}$ und r^{g-1} gehörigen Basen $\mathfrak{b}$ und $\mathfrak{c}$ die Congruenz:

$$\mathfrak{b}^\beta \equiv \mathfrak{c}^\gamma \pmod{r^g},$$

in welcher β und γ resp. Glieder der Reihen:

$$0,\ 1,\ 2,\ \ldots,\ (r^2-1)r^{g-1}-1;\quad 0,\ 1,\ 2,\ \ldots,\ r^{g-1}-1$$

bedeuten, nur für den Fall $\beta=\gamma=0$ bestehen kann, lässt sich auf eine etwas verschiedene Weise aussprechen, und man überzeugt sich ohne Schwierigkeit, dass nach demselben der Ausdruck:

$$\mathfrak{b}^\beta\mathfrak{c}^\gamma$$

für alle Verbindungen β, γ, deren Anzahl:

$$(r^2-1)r^{g-1}.r^{g-1}=(r^2-1)r^{2g-2}=\psi(r^g)$$

ist, lauter nach dem Modul r^g incongruente Zahlen darstellt, d. h. jeder nicht durch r theilbaren Zahl n einmal und nur einmal congruent wird.

Die Werthe β, γ, für welche dies geschieht, sollen die Indices von n heissen und mit β_n, γ_n bezeichnet werden. Offenbar haben congruente Zahlen dieselben Indices, und man sieht leicht, wie die Indices eines Productes aus denen der Factoren abzuleiten sind.

Da $\mathfrak{c} \equiv 1 \pmod{r}$ ist, so folgt aus:

$$\mathfrak{b}^{\beta_n}\mathfrak{c}^{\gamma_n} \equiv n \pmod{r^\sigma}$$

sogleich:

$$\mathfrak{b}^{\beta_n} \equiv n \pmod{r},$$

und dann, da $\mathfrak{b}$ offenbar quadratischer Nichtrest von r ist, dass β_n gerade oder ungerade sein wird, je nachdem n quadratischer Rest oder Nichtrest von r ist, oder mit Anwendung des schon oben gebrauchten Zeichens:

$$\left[\frac{n}{r}\right] = (-1)^{\beta_n}. \tag{6}$$

III. Es bleibt uns noch der Fall zu untersuchen, wo der Modul eine Potenz von $1+i$ ist.

Es seien $\varkappa$ und e zwei positive Zahlen, von denen die letztere als ungerade vorausgesetzt wird, und ausserdem sei t eine beliebige complexe ungerade Zahl. Da:

$$(1+t(1+i)^\varkappa)^e = 1+et(1+i)^\varkappa+\cdots$$

ist und offenbar alle Glieder auf der rechten Seite, vom dritten an, durch $(1+i)^{\varkappa+1}$ theilbar sind, so folgt, dass $(1+t(1+i)^\varkappa)^e$ die Form $1+t'(1+i)^\varkappa$ haben wird, wo t' wieder ungerade ist. Ferner ist, wenn man $\varkappa \leqq 3$ annimmt:

$$(1+t(1+i)^\varkappa)^2 = 1+t'(1+i)^{\varkappa+2},$$

wo t' ebenfalls ungerade ist. Wenn man diese beiden Resultate mit einander verbindet, so findet man ohne Schwierigkeit, dass — immer unter der Voraussetzung $\varkappa \leqq 3$ — die Gleichung:

$$(1+t(1+i)^\varkappa)^\vartheta = 1+t'(1+i)^{\varkappa+2\varrho}$$

besteht, in welcher t' wie t ungerade ist und ϱ den Exponenten der höchsten in ϑ aufgehenden Potenz von 2 bezeichnet.

Zu unserem Zwecke reicht es hin, wenn der Exponent der als Modul zu betrachtenden Potenz von $1+i$ ungerade und $\leqq 7$ ist. Es sei daher der Modul:

$$(1+i)^{3+2h},$$

so dass $h \leqq 2$ ist. Setzt man in dem vorher erhaltenen Resultate $\varkappa = 3$ oder $\varkappa = 4$, so sieht man sogleich, dass $1+t(1+i)^\varkappa$ für den Modul $(1+i)^{3+2h}$ zum Exponenten 2^h gehört. Dies vorausgesetzt, ist es leicht sich zu überzeugen, dass die beiden zum Exponenten 2^h gehörigen Zahlen $1+t(1+i)^3$ und $1+u(1+i)^4$, in denen t und u ungerade sind, immer die Eigenschaft besitzen, dass die

Congruenz:

$$(1+t(1+i)^3)^\delta \equiv (1+u(1+i)^4)^\varepsilon \pmod{(1+i)^{3+2h}},$$

wenn man darin unter δ und ε aus der Reihe 0, 1, 2, ..., 2^h-1 zu nehmende Zahlen versteht, nur für den Fall bestehen kann, wo:

$$\delta = \varepsilon = 0$$

ist. In der That, da offenbar jede der Voraussetzungen $\delta = 0$, $\varepsilon = 0$ die andere zur Folge hat, so haben wir nur noch nachzuweisen, dass unsere Congruenz unmöglich wird, wenn δ und ε beide von der Null verschieden sind.

Bezeichnet man mit 2^ϱ und 2^σ die höchsten in δ und ε resp. aufgehenden Potenzen von 2, wo $\varrho < h$, $\sigma < h$, so werden die beiden Seiten resp. in den beiden Formen:

$$1+t'(1+i)^{3+2\varrho}, \quad 1+u'(1+i)^{4+2\sigma}$$

enthalten sein, worin t' und u' ungerade Zahlen bezeichnen. Setzt man diese Werthe ein, so kommt:

$$t'(1+i)^{3+2\varrho} \equiv u'(1+i)^{4+2\sigma} \pmod{(1+i)^{3+2h}},$$

welche Congruenz offenbar unmöglich ist, da die Exponenten $3+2\varrho$ und $4+2\sigma$ ungleich und beide kleiner als $3+2h$ sind.

Setzt man speciell $t = 1$, $u = -1$, so kann also die Congruenz:

$$(-1+2i)^\delta \equiv 5^\varepsilon \pmod{(1+i)^{3+2h}}$$

nur unter der Voraussetzung stattfinden, dass man $\delta = \varepsilon = 0$ habe, oder, was, wie man sich leicht überzeugt, auf dasselbe hinauskommt, der Ausdruck:

$$(-1+2i)^\delta 5^\varepsilon$$

stellt für alle Verbindungen δ, ε, deren Anzahl offenbar 2^{2h} beträgt, lauter nach dem Modul $(1+i)^{3+2h}$ incongruente Zahlen dar. Alle diese Zahlen sind primär, d. h. congruent 1 $\pmod{(1+i)^3}$, da $-1+2i$ und 5 selbst diese Eigenschaft besitzen. Erwägt man nun, dass offenbar für jeden durch $(1+i)^3$ theilbaren Modul zwei congruente ungerade Zahlen immer gleichzeitig primär oder nicht primär sind, und dass folglich unser Ausdruck nur primären Zahlen congruent werden kann, und bemerkt man ferner, dass für den Modul $(1+i)^{3+2h}$, wie leicht zu sehen ist, nur $\frac{1}{4}\psi((1+i)^{3+2h}) = 2^{2h}$ ungerade primäre Zahlen existiren, die unter einander incongruent sind, so sieht man, dass der obige Ausdruck

jeder ungeraden primären Zahl n einmal und nur einmal congruent wird. Die Exponenten δ_n, ε_n, für welche dies geschieht, sollen wieder die Indices von n heissen, und es leuchtet ein, dass man den ersten oder zweiten Index eines Productes findet, indem man von der Summe der ersten oder zweiten Indices der Factoren das grösste darin enthaltene Vielfache von 2^h abzieht.

Die Indices δ_n, ε_n besitzen wieder Eigenschaften, welche den am Schlusse der beiden vorhergehenden Nummern bemerkten analog sind und sich wie diese auf die Theorie der quadratischen Reste beziehen. Setzt man:

$$(-1+2i)^{\delta_n}5^{\varepsilon_n} = \lambda'+\nu' i,$$

wo λ' und ν' resp. ungerade und gerade sind, so hat man nach dem in der angeführten Abhandlung (§. 8, Gleichung (e) und (f)) Bewiesenen[1]):

$$(-1)^{\frac{\lambda'+\nu'-1}{4}} = \left[\frac{i}{\lambda'+\nu' i}\right] = \left[\frac{i}{-1+2i}\right]^{\delta_n}\left[\frac{i}{5}\right]^{\varepsilon_n},$$

$$(-1)^{\frac{(\lambda'+\nu')^2-1}{8}} = \left[\frac{1+i}{\lambda'+\nu' i}\right] = \left[\frac{1+i}{-1+2i}\right]^{\delta_n}\left[\frac{1+i}{5}\right]^{\varepsilon_n},$$

und folglich, da:

$$\left[\frac{i}{-1+2i}\right] = -1, \quad \left[\frac{i}{5}\right] = 1, \quad \left[\frac{1+i}{-1+2i}\right] = 1, \quad \left[\frac{1+i}{5}\right] = -1$$

ist:

$$(-1)^{\frac{\lambda'+\nu'-1}{4}} = (-1)^{\delta_n}, \quad (-1)^{\frac{(\lambda'+\nu')^2-1}{8}} = (-1)^{\varepsilon_n}.$$

Wird nun $n = \lambda+\nu i$ gesetzt, und bemerkt man, dass wegen:

$$\lambda+\nu i \equiv \lambda'+\nu' i \pmod{8},$$

welche letztere Congruenz daraus folgt, dass 8 ein Factor von $(1+i)^{3+2h}$ ist, λ und ν resp. von λ' und ν' um Vielfache von 8 verschieden sind, so sieht man sogleich, dass in den zuletzt erhaltenen Gleichungen λ', ν' mit λ, ν vertauscht werden können, und man erhält:

$$(7) \qquad n = \lambda+\nu i, \quad (-1)^{\frac{\lambda^2+\nu^2-1}{4}} = (-1)^{\delta_n}, \quad (-1)^{\frac{(\lambda+\nu)^2-1}{8}} = (-1)^{\varepsilon_n}.$$

IV. Wir sind jetzt im Stande, eine beliebige Zahl k als Modul zu betrachten; um jedoch jede unnütze Weitläufigkeit zu vermeiden, beschränken wir uns auf den Fall, wo k gerade ist, die höchste darin aufgehende Potenz von $1+i$ einen Exponenten der Form $3+2h$ hat und $h \gtreqless 2$ ist. Die Zahl k sei,

[1]) S. 559 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

abgesehen von dem Factor i^μ, das Product der Primzahlpotenzen:

$$(8) \qquad (a+bi)^{f}, \ (a'+b'i)^{f'}, \ \ldots; \qquad r^{g}, \ r^{g'}, \ \ldots; \qquad (1+i)^{3+2h}.$$

Die ungeraden und zweigliedrigen Primzahlen $a+bi$, $a'+b'i$, ..., welche zu grösserer Einfachheit primär vorausgesetzt werden, sind ungleich, und r, r', ... sind eingliedrige, positive, ebenfalls von einander verschiedene Primzahlen.

Wählt man nun für jeden der Moduln (8) nach den Vorschriften der drei vorhergehenden Nummern eine oder zwei Basen:

$$(9) \qquad \mathfrak{a}, \ \mathfrak{a}', \ \ldots; \qquad \mathfrak{b}, \ \mathfrak{c}, \ \mathfrak{b}', \ \mathfrak{c}', \ \ldots; \qquad -1+2i, \ 5,$$

so erhält man für jedes n, welches relative Primzahl zu k und zugleich primär ist, eine Reihe von Indices:

$$(10) \qquad \alpha_n, \ \alpha'_n, \ \ldots; \qquad \beta_n, \ \gamma_n, \ \beta'_n, \ \gamma'_n, \ \ldots; \qquad \delta_n, \ \varepsilon_n,$$

welche *das System der Indices von n* heissen soll und völlig bestimmt ist, wenn die Basen ein für allemal gewählt sind. Dass congruente Zahlen n und n' dasselbe System der Indices haben, ist klar, und dass auch der umgekehrte Satz stattfindet, geht daraus hervor, dass bei vorausgesetzter Identität der Systeme für zwei Zahlen n und n', die Congruenz $n \equiv n'$ für jeden der Moduln (8) und folglich auch für den Modul k besteht. Berücksichtigt man die Anzahl der Werthe, die den einzelnen Indices (10) zukommen können, so sieht man sogleich, dass die Anzahl der verschiedenen Systeme (10) durch das Product:

$$(p-1)p^{f-1}.(p'-1)p'^{f'-1}\ldots\times(r^2-1)r^{2g-2}.(r'^2-1)r'^{2g'-2}\ldots\times 2^{2h},$$

d. h. durch $\frac{1}{4}\psi(k)$ ausgedrückt wird, wie dies auch in der That der Fall sein muss, da $\frac{1}{4}\psi(k)$ offenbar mit der Anzahl aller nach dem Modul k incongruenten Zahlen, welche mit diesem keinen gemeinschaftlichen Factor haben und überdies primär sind, zusammenfällt.

Da wir in den folgenden Paragraphen häufig eine Reihe von Zahlen von der eben angegebenen Beschaffenheit zu betrachten haben werden, d. h. eine Reihe, die ein und nur ein Glied enthält, welches jeder primären, zu k relativen Primzahl nach dem Modul k congruent ist, so wollen wir übereinkommen, mit:

$$(11) \qquad l$$

das allgemeine Glied einer solchen aus $\frac{1}{4}\psi(k)$ Gliedern bestehenden Zahlenreihe zu bezeichnen.

§. 3.

Indem wir zu dem in der Einleitung als Gegenstand dieser Abhandlung bezeichneten Satze übergehen, nach welchem:

$$kt+l$$

immer unendlich viel Primzahlen enthält, wenn die gegebenen Zahlen k und l keinen gemeinsamen Theiler haben, bemerken wir zunächst, dass man offenbar, ohne der Allgemeinheit zu schaden, k als durch $1+i$ theilbar und den Exponenten der höchsten darin aufgehenden Potenz von $1+i$ als ungerade und $\geqq 7$ betrachten kann, so dass also k von der in §. 2, IV. vorausgesetzten Form sein wird. Erwägt man ferner, dass vier zusammengehörige Zahlen immer zugleich Primzahlen sind oder nicht sind, so leuchtet ein, dass man l als eine primäre Zahl ansehen kann, und dass daher auch dieser Buchstabe in der ihm unter (11) gegebenen Bedeutung genommen werden kann.

Dies vorausgesetzt, bilde man unter Beibehaltung aller in §. 2, IV. gebrauchten Bezeichnungen, den Basen (9) der Reihe nach entsprechend, die binomischen Gleichungen:

$$(12)\quad \begin{cases} \varphi^{(p-1)p^{f-1}}=1, \quad \varphi'^{(p'-1)p'^{f'-1}}=1, \quad \ldots, \\ \psi^{(r^2-1)r^{2g-1}}=1, \quad \chi^{r^{2g-1}}=1; \quad \psi'^{(r'^2-1)r'^{2g'-1}}=1, \quad \chi'^{r'^{2g'-1}}=1; \quad \ldots, \\ \vartheta^{2^h}=1, \quad \eta^{2^h}=1, \end{cases}$$

und setze ferner zur Abkürzung:

$$\Omega_n = \varphi^{a_n}\varphi'^{a'_n}\ldots\times\psi^{\beta_n}\chi^{\gamma_n}\psi'^{\beta'_n}\chi'^{\gamma'_n}\ldots\times\vartheta^{\delta_n}\eta^{\varepsilon_n}.$$

Das so gebildete Product besitzt mehrere sehr leicht zu beweisende und für das Folgende wichtige Eigenschaften, welche vor allen Dingen zu betrachten sind.

Denkt man sich zunächst die in Ω enthaltenen Wurzeln der Einheit als constant, so hat man offenbar:

$$(13)\qquad \Omega_{nn'} = \Omega_n\Omega_{n'},$$

und wenn $n' \equiv n \pmod{k}$ angenommen wird:

$$(13')\qquad \Omega_{n'} = \Omega_n.$$

Ferner ist, immer unter der Voraussetzung, dass man die in Ω enthaltenen Wurzeln der Einheit nicht ändert, und wenn das Zeichen Σ sich auf alle unter

(11) definirten Werthe von l erstreckt:

$$(14)\qquad \Sigma\Omega_l = 0, \quad \text{oder} \quad \Sigma\Omega_l = \tfrac{1}{4}\psi(k),$$

je nachdem unter den Wurzeln $\varphi, \varphi', \ldots, \psi, \chi, \psi', \chi', \ldots, \vartheta, \eta$ wenigstens eine von der positiven Einheit verschiedene sich befindet oder alle dieser gleich sind. In der That lässt sich unsere Summe, da allen l alle möglichen Systeme (10) entsprechen, leicht in Factoren zerlegen, von denen jeder nur eine der oben genannten Wurzeln enthält. Derjenige dieser Factoren, in welchem φ vorkommt, ist offenbar:

$$1+\varphi+\varphi^2+\cdots+\varphi^{(p-1)p^{f-1}-1}$$

und folglich gleich 0 oder gleich $(p-1)p^{f-1}$, je nachdem φ von der positiven Einheit verschieden oder derselben gleich ist, und da Ähnliches von allen übrigen gilt, so ist die ausgesprochene Behauptung bewiesen.

Wenn wir uns jetzt, wie überall im Folgenden, des Zeichens S bedienen, um eine Summation anzudeuten, welche sich über alle Combinationen der Wurzeln der Gleichungen (12) erstreckt, deren Anzahl offenbar gleich $\frac{1}{4}\psi(k)$ ist, so hat man endlich:

$$(15)\qquad S\Omega_n = \tfrac{1}{4}\psi(k), \quad \text{oder} \quad S\Omega_n = 0,$$

je nachdem $n \equiv 1$ oder nicht $\equiv 1 \pmod{k}$ ist.

Das erste Resultat folgt unmittelbar daraus, dass für $n \equiv 1$ alle Indices (10) verschwinden. Um sich von der Richtigkeit des zweiten zu überzeugen, darf man nur bemerken, dass $S\Omega_n$ in Factoren zerlegt werden kann, von denen jeder nur die Wurzeln einer der Gleichungen (12) enthält, und dass der auf die erste dieser Gleichungen sich beziehende nichts anderes ist als die Summe der a_n^{ten} Potenzen aller Wurzeln dieser Gleichung. Dieser Factor wird daher und wegen $a_n < (p-1)p^{f-1}$ immer verschwinden, ausser wenn $a_n = 0$ ist. Aus diesem und den ähnlichen Resultaten, welche für die übrigen Factoren gelten, folgt die zweite der Gleichungen (15) sogleich, wenn man berücksichtigt, dass, wenn n nicht $\equiv 1 \pmod{k}$ ist, wenigstens einer der Indices (10) von Null verschieden sein wird.

Nach den bisher getroffenen Einleitungen können wir ohne Schwierigkeit die Gleichung:

$$(16)\qquad \Pi \frac{1}{1-\Omega_{\mathfrak{q}}\frac{1}{(Nq)^s}} = \Sigma\Omega_n \frac{1}{(Nn)^s} = L$$

beweisen. In dieser Gleichung bedeutet s eine beliebige positive, die Einheit übertreffende Grösse, und was das Multiplicationszeichen Π und das Summationszeichen Σ betrifft, so erstreckt sich ersteres über alle primären Primzahlen q, welche nicht in k aufgehen, während letzteres auf alle primären Zahlen n auszudehnen ist, die mit k keinen gemeinsamen Theiler haben. Die in Ω eingehenden Wurzeln $\varphi, \varphi', \ldots$ können beliebig gewählt werden, müssen aber in jedem Ω dieselben sein, so dass also unsere allgemeine Gleichung $\frac{1}{4}\psi(k)$ besondere, den verschiedenen Wurzelverbindungen entsprechende Gleichungen darstellt.

Um sich von der Richtigkeit der Gleichung (16) zu überzeugen, entwickle man den allgemeinen Factor auf der ersten Seite mit Berücksichtigung der Gleichung (13). Man erhält so:

$$\frac{1}{1-\Omega_q \frac{1}{(Nq)^s}} = 1+\Omega_q \frac{1}{(Nq)^s}+\Omega_{q^2} \frac{1}{(Nq^2)^s}+\cdots$$

Führt man nun die auf der ersten Seite der Gleichung (16) angedeutete Multiplication aus und erinnert sich, dass nach (4) jede Zahl n nur auf eine Weise als ein Product von Potenzen primärer Primzahlen dargestellt werden kann, so wird die erste Seite unserer Gleichung in die zweite übergehen, w. z. b. w.

§. 4.

Wir müssen jetzt die allgemeine Reihe L (16), welche, wie leicht zu sehen, so lange $s > 1$ ist, einen endlichen, von der Art der Aufeinanderfolge ihrer Glieder unabhängigen Werth hat, näher betrachten und namentlich auszumitteln suchen, wie sich dieser Werth ändert, wenn man, $s = 1+\varrho$ setzend, die positive Variable ϱ unendlich klein werden lässt. Die zu untersuchende Reihe L zerfällt in $\frac{1}{4}\psi(k)$ Partialreihen, von denen jede alle diejenigen Glieder enthält, für welche n derselben Zahl l (11) nach dem Modul k congruent ist. Irgend eine solche Partialreihe ist, wenn man von dem allen ihren Gliedern gemeinsamen Factor Ω_l abstrahirt:

$$W = \Sigma \frac{1}{N(kt+l)^{1+\varrho}},$$

wo sich das Zeichen Σ auf alle complexen ganzen Zahlen t bezieht. Nun ist in der Abhandlung[1]) *Recherches sur les formes quadratiques à coefficients et à*

[1]) S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

indéterminées complexes (§. 18, II.) gezeigt worden, dass letztere Reihe für ein unendlich kleines ϱ dem Ausdruck $\frac{\pi}{N(k)}\frac{1}{\varrho}$ gleich wird. Dieses Resultat lässt sich mit Hülfe der am angeführten Orte entwickelten Betrachtungen vervollständigen, und man beweist leicht, dass:

$$W = \frac{\pi}{N(k)}\frac{1}{\varrho}+A+\varrho F(\varrho)$$

ist, wo A eine reelle Constante und $F(\varrho)$ eine reelle Function von ϱ bezeichnet, die sich für ein unendlich klein werdendes ϱ einer endlichen Grenze nähert. Hieraus folgt sogleich mit Berücksichtigung von (14), dass:

$$(17)\quad L = \frac{\pi\psi(k)}{4N(k)}\frac{1}{\varrho}+F(\varrho), \quad \text{oder} \quad L = A+A'i+\varrho(\Phi(\varrho)+i\Phi'(\varrho))$$

ist, je nachdem die in L enthaltenen Wurzeln der Einheit alle der positiven Einheit gleich sind oder wenigstens eine derselben von dieser verschieden ist. A und A' sind reelle Constanten und $F(\varrho)$, $\Phi(\varrho)$, $\Phi'(\varrho)$ reelle Functionen von ϱ, die für einen unendlich kleinen Werth der positiven Veränderlichen ϱ sich endlichen Grenzen nähern.

Die Reihen L zerfallen nach den verschiedenen in ihnen enthaltenen Wurzelcombinationen in folgende drei Classen. Die erste dieser Classen besteht aus der einzigen Reihe, in welcher alle Wurzeln der Einheit den Werth 1 haben, und auf welche sich die erste der Gleichungen (17) bezieht. Die zweite Classe umfasst alle übrigen Reihen, in denen nur reelle Wurzeln vorkommen. Bemerkt man nun, dass nur in denjenigen der Gleichungen (12), deren Wurzeln mit $\chi, \chi', \ldots$ bezeichnet sind, die Exponenten ungerade sind, so sieht man, dass zur Darstellung aller Reihen der zweiten Classe die doppelten Zeichen in:

$\varphi = \pm 1,\ \varphi' = \pm 1, \ldots;\ \psi = \pm 1,\ \chi = 1,\ \psi' = \pm 1,\ \chi' = 1, \ldots;\ \vartheta = \pm 1,\ \eta = \pm 1$

auf jede mögliche Weise combinirt werden müssen, wobei nur die eine aus allen oberen Zeichen bestehende Verbindung als der ersten Classe entsprechend ausgeschlossen bleiben muss. Die dritte Classe endlich wird alle Reihen in sich begreifen, in denen wenigstens eine imaginäre Wurzel der Einheit vorkommt, und man sieht ohne Schwierigkeit, dass die Reihen dieser Classe immer paarweise einander zugeordnet sind, indem, unter der ausgesprochenen Voraussetzung, die beiden Wurzelcombinationen:

$$\varphi, \varphi', \ldots;\ \psi, \chi, \psi', \chi', \ldots;\ \vartheta, \eta \quad \text{und} \quad \frac{1}{\varphi}, \frac{1}{\varphi'}, \ldots;\ \frac{1}{\psi}, \frac{1}{\chi}, \frac{1}{\psi'}, \frac{1}{\chi'}, \ldots;\ \frac{1}{\vartheta}, \frac{1}{\eta}$$

offenbar von einander verschieden sind. Bei diesen Reihen findet der Übergang von einer derselben zu der ihr zugeordneten statt, wenn man in der zweiten Gleichung (17) i mit $-i$ vertauscht, während für die Reihen der zweiten Classe, für welche die erwähnte Gleichung ebenfalls gilt, die in dieser Gleichung vorkommenden imaginären Glieder verschwinden.

Wird ϱ unendlich klein, so wächst der Werth der die erste Classe L constituirenden Reihe über jede positive Grenze hinaus, während die Werthe aller übrigen sich endlichen Grenzen nähern, wie aus (17) ersichtlich. Dies ist jedoch zu unserem Zwecke nicht ausreichend, und wir müssen nachweisen, dass alle diese Grenzen von Null verschieden sind, d. h. dass in der zweiten der Gleichungen (17) nie gleichzeitig $A = 0$, $A' = 0$ ist. Wir wollen für einen Augenblick annehmen, dieser Nachweis sei für alle Reihen der zweiten Classe geführt. Unter dieser Voraussetzung soll im folgenden Paragraphen die Richtigkeit derselben Behauptung für die dritte Classe gezeigt und zugleich der am Anfang des §. 3 aufgestellte Satz abgeleitet werden, so dass uns dann nur noch übrig bleiben wird, am Schlusse der Abhandlung die hinsichtlich der Reihen der zweiten Classe vorausgesetzte Eigenschaft zu beweisen.

§. 5.

Nimmt man von beiden Seiten der Gleichung (16) die NEPER'schen Logarithmen und entwickelt, so kommt:

$$\cdots + \frac{1}{\mu} \Sigma \Omega_{q^\mu} \frac{1}{(Nq)^{\mu+\mu\varrho}} + \cdots = \log L,$$

wo wir zur Abkürzung nur das allgemeine Glied geschrieben haben, in welchem für μ successive alle Werthe von $\mu = 1$ bis $\mu = \infty$ zu setzen sind, und wo sich das Summenzeichen auf alle q erstreckt.

Es sei nun l irgend eine bestimmte der unter (11) definirten Zahlen, und man setze $ll' \equiv 1 \pmod{k}$, wo l', wie l, primär und Primzahl zu k ist. Multiplicirt man unsere Gleichung mit Ω_r und summirt nach allen Wurzelverbindungen, so erhält man:

$$\cdots + \frac{1}{\mu} \Sigma (S\Omega_{r\varrho^\mu}) \frac{1}{(Nq)^{\mu+\mu\varrho}} + \cdots = S\Omega_r \log L.$$

Nun ist, nach (15):

$$S\Omega_{r\varrho^\mu} = 0,$$

ausser wenn $l'q^\mu \equiv 1$ oder, was dasselbe ist, ausser wenn $q^\mu \equiv l \pmod{k}$ ist, für welchen Fall:

$$S\Omega_{r\varrho^\mu} = \tfrac{1}{4}\psi(k)$$

ist. Die Gleichung wird daher:

$$(18) \qquad \Sigma' \frac{1}{(Nq)^{1+\varrho}} + \tfrac{1}{2}\Sigma' \frac{1}{(Nq)^{2+2\varrho}} + \cdots = \frac{4}{\psi(k)} S\Omega_r \log L,$$

wo sich das Zeichen Σ' im ersten, zweiten, ... Gliede resp. auf die Primzahlen q erstreckt, deren erste, zweite, ... Potenzen congruent $l \pmod{k}$ sind. Setzt man speciell $l \equiv 1$, so ist:

$$l' \equiv 1 \pmod{k}, \qquad \Omega_r = 1,$$

und das allgemeine Resultat geht über in:

$$\Sigma' \frac{1}{(Nq)^{1+\varrho}} + \tfrac{1}{2}\Sigma' \frac{1}{(Nq)^{2+2\varrho}} + \cdots = \frac{4}{\psi(k)} S\log L.$$

Wir betrachten jetzt die Summe $S\log L$ für den Fall, wo ϱ unendlich klein wird. Was zunächst die den Reihen der zweiten Classe entsprechenden Glieder betrifft, so werden sich diese sämmtlich endlichen Grenzen nähern, wogegen das der ersten Classe entsprechende Glied einen unendlich grossen positiven Werth annimmt, indem dasselbe nach (17) in die Form:

$$\log\left(\frac{1}{\varrho}\right) + \log\left(\frac{\pi\psi(k)}{4N(k)} + \varrho F(\varrho)\right)$$

gebracht werden kann, wo der erste Theil unendlich wird, während der zweite sich einer endlichen Grenze nähert. Wäre nun der endliche Grenzwerth einer Reihe der dritten Classe der Null gleich, d. h. wäre in (17) $A = 0$, $A' = 0$, so würde sich aus der Vereinigung der zwei Glieder, welche in unserer Summe dieser und der ihr zugeordneten Reihe entsprechen, der Ausdruck:

$$-2\log\left(\frac{1}{\varrho}\right) + \log(\Phi(\varrho)^2 + \Phi'(\varrho)^2)$$

ergeben, nach dessen Verbindung mit dem eben betrachteten die Summe das Glied:

$$-\log\left(\frac{1}{\varrho}\right)$$

darbieten würde, welches einen unendlich grossen negativen Werth annimmt

und nicht etwa durch $\log(\Phi(\varrho)^2+\Psi(\varrho)^2)$ aufgehoben werden kann, indem dieser letztere Logarithmus sich entweder einer endlichen Grenze nähert oder selbst einen unendlich grossen negativen Werth erhält. Dies widerspricht unserer obigen Gleichung, deren linke Seite nur positive Glieder enthält, und der hier hervortretende Widerspruch würde offenbar noch verstärkt werden, wenn man die Grenzwerthe für mehr als ein Paar zugeordneter Reihen der dritten Classe als verschwindend betrachten wollte. Es ist somit, unter Vorbehalt des noch zu leistenden Nachweises für die Reihen der zweiten Classe, bewiesen, dass $\log L$ sich immer einer endlichen Grenze nähert, den einzigen Fall ausgenommen, wenn L die Reihe der ersten Classe bezeichnet, da für diesen Fall unser Logarithmus über jede positive noch so grosse Zahl hinaus wächst.

Kehren wir jetzt zur allgemeinen Gleichung (18) zurück, so sehen wir, dass die rechte und also auch die linke Seite derselben für ein unendlich klein werdendes ϱ unendlich wird. Nun bleibt aber die Summe aller auf der linken Seite vorkommenden Reihen, von der zweiten ab, endlich, da, wie leicht zu sehen:

$$\tfrac{1}{2}\Sigma\frac{1}{(Nq)^\varrho}+\tfrac{1}{3}\Sigma\frac{1}{(Nq)^\varrho}+\cdots$$

noch endlich ist, wenn man die Summationen nicht, wie es hier geschieht, auf gewisse Primzahlen q beschränkt, sondern auf alle ganzen Zahlen, deren Norm die Einheit übertrifft, ausdehnt. Es muss daher die Summe:

$$\Sigma\frac{1}{(Nq)^{1+\varrho}}$$

über jede endliche Grenze hinaus wachsen, was nicht anders geschehen kann, als wenn die Gliederzahl derselben unendlich ist, d. h. als wenn es eine unendliche Anzahl von Primzahlen giebt, die in der Form $kt+l$ enthalten sind, w. z. b. w.

§. 6.

Zur Vervollständigung des eben gegebenen Beweises ist noch zu zeigen, dass der einem unendlich kleinen ϱ entsprechende Grenzwerth jeder Reihe der zweiten Classe von Null verschieden ist. Eine solche Reihe enthält eine Wurzelverbindung der Form:

$$\varphi=\pm1,\ \varphi'=\pm1,\ \ldots;\ \psi=\pm1,\ \chi=1,\ \psi'=\pm1,\ \chi'=1,\ \ldots;\ \vartheta=\pm1,\ \eta=\pm1.$$

Bildet man das Product aller derjenigen der Primzahlen $a+bi$, $a'+b'i$, $\ldots$,

r, r', $\ldots$, denen in dieser Wurzelcombination eine der negativen Einheit gleiche Wurzel φ, φ', $\ldots$, ψ, ψ', $\ldots$ entspricht, und bezeichnet das Product dieser Primzahlen mit Q, so wie das aller übrigen mit V (wobei es sich von selbst versteht, dass, wenn in einer dieser Gruppen keine Primzahl vorkommen sollte, man für Q oder V die Einheit zu wählen hat), so wird der im allgemeinen Gliede der Reihe enthaltene Ausdruck Ω_n nach den unter (5) und (6) erhaltenen Resultaten folgende Gestalt annehmen können:

$$\Omega_n=\left[\frac{n}{Q}\right]\vartheta^{\vartheta_n}\eta^{\varepsilon_n}.$$

Setzt man ferner, wie oben, $n=\lambda+\nu i$, so hat man:

$$\vartheta^{\vartheta_n}=\vartheta^{\frac{\lambda^2+\nu^2-1}{4}},\qquad \eta^{\varepsilon_n}=\eta^{\frac{(\lambda+\nu)^2-1}{8}}.$$

Ist $\vartheta=1$, so ist die erste dieser Gleichungen evident; ist dagegen $\vartheta=-1$, so fällt sie mit einer der unter (7) bewiesenen zusammen, und mit der zweiten verhält es sich ebenso. Der Grenzwerth irgend einer Reihe der zweiten Classe ist folglich:

$$\Sigma\vartheta^{\frac{\lambda^2+\nu^2-1}{4}}\eta^{\frac{(\lambda+\nu)^2-1}{8}}\left[\frac{\lambda+\nu i}{Q}\right]\frac{1}{(\lambda^2+\nu^2)^{1+\varrho}},$$

wo ϱ unendlich klein vorausgesetzt ist, das Zeichen Σ sich über alle ungeraden primären Zahlen $\lambda+\nu i$ erstreckt, die mit k oder, was dasselbe ist, mit QV keinen Factor gemein haben, und noch zu bemerken ist, dass nicht gleichzeitig $Q=1$, $\vartheta=1$, $\eta=1$ sein kann, da unter dieser Voraussetzung die oben betrachtete Wurzelcombination der Reihe L der ersten Classe entsprechen würde. Nun ist aber unsere Reihe mit der eben angegebenen Beschränkung immer in der allgemeinen Reihe enthalten, welche, wie wir in der schon oft citirten Abhandlung[1]) gezeigt haben, von einem endlichen Factor abgesehen, die Anzahl der Classen ausdrückt, in welche sich alle quadratischen Formen für eine beliebige, keinem Quadrat gleiche, Determinante vertheilen. Vergleicht man die in jener Abhandlung (§. 18, IV. Gleichung (18)) zur Bestimmung dieser Anzahl gefundene Reihe mit der obigen, so sieht man, dass letztere sich nach den vier Wurzelverbindungen:

$$\vartheta=1,\ \eta=1;\qquad \vartheta=-1,\ \eta=1;\qquad \vartheta=1,\ \eta=-1;\qquad \vartheta=-1,\ \eta=-1,$$

[1]) S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

welche darin vorkommen können, resp. auf die vier Determinanten:

$$QV^2,\quad iQV^2,\quad (1+i)QV^2,\quad i(1+i)QV^2$$

bezieht.

Hieraus folgt die zu beweisende Eigenschaft sogleich; denn wenn unsere Reihe sich auf Null reducirte, so würde auch die Anzahl der Classen der quadratischen Formen für die entsprechende Determinante verschwinden, was nicht möglich ist, indem diese Anzahl immer wenigstens der Einheit gleich ist.

Wir schliessen mit einer die vorher erwähnte Vergleichung erleichternden Bemerkung, welche darin besteht, dass man in der am angeführten Orte gefundenen Reihe, ohne den Werth derselben zu ändern, die Summation auf diejenigen ungeraden, mit der Determinante keinen gemeinschaftlichen Factor darbietenden, primären Zahlen $\lambda+\nu i$ beziehen kann, denen diese Benennung in dem in gegenwärtiger Abhandlung angenommenen Sinne zukommt. Dies ergiebt sich unmittelbar daraus, dass für irgend eine Gruppe ungerader zusammengehöriger Zahlen, die nach der einen Definition als primär zu betrachtende Zahl derjenigen, welche der anderen Definition entspricht, offenbar gleich oder entgegengesetzt ist, und dann ferner daraus, dass irgend ein Glied der Reihe ungeändert bleibt, wenn man darin $\lambda+\nu i$ mit $-\lambda-\nu i$ vertauscht.

RECHERCHES SUR LES FORMES QUADRATIQUES A COEFFICIENTS ET A INDÉTERMINÉES COMPLEXES.

PAR

M. G. LEJEUNE DIRICHLET.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 24 p. 291—371.

RECHERCHES
SUR LES FORMES QUADRATIQUES
A COEFFICIENTS ET A INDÉTERMINÉES COMPLEXES.

Première partie.

Comme les recherches que nous aurons à exposer dans ce Mémoire, présentent, par leur objet et par les résultats auxquels elles conduisent, beaucoup d'analogie avec d'autres recherches déjà publiées*), il convient, avant d'en donner une idée générale, de rappeler en peu de mots la question qui a été traitée dans le Mémoire que nous venons de citer. Le Mémoire dont il s'agit, se rapporte à la théorie des *formes quadratiques*, théorie qui, préparée par quelques énoncés de FERMAT et par les ingénieuses recherches d'EULER et définitivement fondée par LAGRANGE, a reçu plus tard de notables accroissements par les travaux de LEGENDRE et surtout par ceux de M. GAUSS, qui y a consacré la plus grande partie de ses „*Disquisitiones arithmeticae*“, en sorte qu'elle constitue aujourd'hui l'une des branches principales de la science des nombres. On sait que les propriétés d'une telle expression dépendent surtout d'un entier qui est une fonction très simple de ses coefficients et que, pour cette raison, on nomme le *déterminant* de la forme quadratique. Quoique le nombre des formes qui ont un même déterminant donné quelconque, positif ou négatif, soit infini, ces formes se réduisent toujours à un nombre limité d'expressions distinctes, c'est-à-dire non-transformables les unes dans les autres. Cette propriété, capitale dans la matière, a été établie par LAGRANGE qui a aussi fait connaître les opérations arithmétiques, au moyen desquelles ces formes non-équivalentes peuvent être assignées, lorsque le déterminant est numériquement donné. Mais si ce procédé suffisait pour l'objet auquel son illustre auteur l'avait destiné, il ne donnait aucune lumière sur la liaison générale qui doit exister

*) Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres. Tome XIX et XXI du Journal de CRELLE [1]).

[1]) S. 411 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

entre le déterminant et le nombre des formes distinctes qui y répondent. La loi qui exprime cette dépendance et dont la connaissance, outre qu'elle devait présenter beaucoup d'intérêt par elle-même, était indispensable pour d'autres recherches, restait donc entièrement inconnue. Or tel est précisément l'objet de la question qu'on s'est proposée dans le Mémoire cité et qu'on y a résolue au moyen d'une analyse dont le principe fondamental consiste à exprimer les propriétés caractéristiques du système des formes non-équivalentes répondant à un déterminant quelconque, à l'aide d'une équation dont l'un des membres ne contient rien qui soit relatif à ces formes, tandis que l'autre se compose de suites infinies doubles dont le nombre est égal à celui des formes et dont chacune présente dans son terme général l'une des expressions quadratiques dont il s'agit. L'équation ainsi formée renfermant une variable assujettie à la seule condition de rester supérieure à l'unité, si l'on passe au cas-limite, où cette variable approche indéfiniment de l'unité, les séries doubles tendent toutes vers une limite commune facile à assigner, et l'égalité se transforme de manière à exprimer le nombre des formes par une suite infinie d'une loi très simple et dont la somme s'obtient aisément avec le secours des formules connues. En effectuant cette dernière opération, on reconnaît que l'expression du nombre des formes qui répondent à un déterminant quelconque, présente deux cas très distincts suivant que ce déterminant est un nombre négatif ou positif. Dans le premier de ces cas, l'expression de la loi dont il s'agit a un caractère purement arithmétique, tandis que pour un déterminant positif elle est d'une nature plus composée et en quelque sorte mixte, puisque, outre les éléments arithmétiques dont elle dépend, elle en renferme d'autres qui ont leur origine dans certaines équations auxiliaires qui se présentent dans la théorie des équations binômes, et appartiennent par conséquent à l'Algèbre. Ce dernier résultat est surtout remarquable et offre un nouvel exemple de ces rapports cachés que l'étude approfondie de l'Analyse mathématique nous fait découvrir entre les questions en apparence les plus disparates.

La solution dont nous venons de rappeler l'idée fondamentale, n'empruntant de la théorie des formes quadratiques que leurs propriétés les plus élémentaires et s'achevant sans difficulté, lorsque ces propriétés ont été une fois reconnues et mises en équation, il était naturel de chercher à étendre les applications de ce genre d'analyse et à résoudre par son moyen d'autres questions analogues mais d'un ordre plus élevé. Les questions que l'on doit considérer

comme telles, sont assez nombreuses; on peut, dans les recherches de cette nature, remplacer les formes quadratiques par des fonctions homogènes d'un degré plus élevé; sans sortir du second degré, et c'est là le cas dont nous nous sommes occupé d'abord et que nous traiterons exclusivement dans ce Mémoire, on peut aussi modifier la nature des formes quadratiques et supposer par exemple que leurs coefficients sont des entiers complexes. On doit à M. Gauss l'idée de considérer de pareils entiers*), et l'on sait qu'il y a été conduit par ses recherches sur les résidus biquadratiques, qui lui ont fait reconnaître que la théorie de ces résidus qui paraît très compliquée tant qu'on la rapporte aux entiers réels, se présente sous une face bien différente, lorsqu'on l'envisage sous ce nouveau point de vue, et se résume alors dans une loi de réciprocité d'une simplicité et d'une élégance extrêmes et d'ailleurs parfaitement analogue à celle que l'on connaissait depuis longtemps pour les résidus quadratiques. L'importance de l'idée si profonde que nous venons de rappeler ne consiste pas seulement à amener de pareilles simplifications; elle est d'un usage beaucoup plus étendu et l'on doit la considérer comme ouvrant un nouveau champ aux spéculations arithmétiques.

Avant de transporter, dans la théorie des nombres ainsi généralisée, la question qui avait été traitée précédemment, il fallait se livrer à un travail préliminaire indispensable et ayant pour objet de se rendre compte des modifications que les propositions fondamentales de la théorie des formes quadratiques doivent subir pour être applicables aux entiers complexes. Ce travail achevé, on a pu reconnaître que les principes dont on avait fait usage dans le Mémoire cité, s'appliquent avec le même succès à la nouvelle question. Seulement, comme cette dernière est d'une nature plus compliquée, les discussions que la solution exige, prennent plus d'étendue et l'on trouve par exemple que pour passer à ce que nous avons nommé plus haut le cas-limite, il faut ici évaluer une intégrale définie quadruple, tandis que précédemment on n'avait eu à considérer que des intégrales doubles, se réduisant d'ailleurs sur-le-champ à la quadrature de l'ellipse ou de l'hyperbole.

Mais sans entrer ici dans d'autres détails sur la marche de la solution, nous nous bornerons à dire que le résultat définitif est entièrement semblable à celui qui répond au second des deux cas que nous avons distingués plus haut.

*) Theoria residuorum biquadraticorum. Commentatio secunda.

On reconnaît en effet que, pour un déterminant complexe, le nombre des formes se rattache généralement à la division de la fonction elliptique complète de première espèce dont le module est $\sqrt{\frac{1}{2}}$, ou ce qui revient au même, à la division de la lemniscate en parties égales, le diviseur ou le nombre de ces parties étant un entier complexe.

Outre le résultat dont nous venons d'indiquer la nature, la question présente deux résultats particuliers très singuliers et tout-à-fait inattendus. Ces résultats sont relatifs aux cas où le déterminant est un entier réel ou le produit d'un tel entier par $\sqrt{-1}$, le nombre des formes pouvant alors être assigné sans le secours des équations qui se rapportent à la division des fonctions elliptiques. Pour ne parler ici que du premier de ces deux cas dont le second ne diffère pas au fond, le résultat consiste en ce que, relativement à un entier réel D, considéré comme le déterminant de formes quadratiques à coefficients complexes, le nombre des formes distinctes est égal au produit ou au double produit des deux nombres qui expriment combien il existe de formes pour les deux déterminants opposés D et $-D$, considérés sous le point de vue ordinaire, ces deux cas étant d'ailleurs distingués par un critérium très simple.

Comme les recherches dont nous venons de présenter l'analyse, exigent des développements assez étendus, nous avons dû diviser notre travail en deux parties, dont la première que nous publions aujourd'hui, contient, outre les discussions préliminaires, la solution de la question principale conduite jusqu'au point où elle se trouve dépendre de la sommation d'une série double. Nous terminons cette première partie par l'examen des deux cas particuliers mentionnés plus haut, et qui peuvent être traités complètement, sans qu'il soit nécessaire d'effectuer la double sommation. Dans la seconde partie nous achèverons la solution générale et nous discuterons en outre quelques questions accessoires telles que celles qui concernent la distribution des formes quadratiques en genres, et que nous avons dû laisser de côté dans cette première partie, pour ne pas interrompre la marche des considérations qui se rapportent à la question principale.

Quoique les propositions élémentaires de la théorie des entiers complexes aient déjà été exposées par l'illustre géomètre que nous avons cité plus haut, nous avons pensé qu'il pourrait être commode pour le lecteur de trouver dans une courte introduction celles de ces propositions dont nous aurons à faire usage plus tard.

Définitions et théorèmes préliminaires.

§. 1.

On appelle *nombre complexe* toute expression de la forme:

$$a+bi,$$

i désignant la quantité imaginaire $\sqrt{-1}$, et a et b ayant des valeurs réelles quelconques. Comme il est souvent nécessaire de distinguer le cas où l'une des valeurs réelles a et b s'évanouit, de celui où ces valeurs sont l'une et l'autre différentes de zéro, nous nommerons l'expression précédente *monôme* ou *binôme* suivant ces deux cas.

Le nombre réel et toujours positif:

$$a^2+b^2,$$

le seul cas excepté où l'on a à la fois $a=0$, $b=0$, sera dit la *norme* du nombre complexe $a+bi$. Cette norme n'est donc autre chose que ce que l'on appelle communément le carré du module de l'expression imaginaire $a+bi$. Mais comme ce carré se présentera beaucoup plus souvent dans nos recherches que le module lui-même, il convient de lui consacrer une dénomination spéciale telle que la précédente déjà proposée par M. Gauss, d'autant plus que l'emploi du mot module pourrait donner lieu à des équivoques.

Nous conviendrons de désigner la norme en plaçant la caractéristique N devant le nombre complexe dont il s'agit, et d'écrire:

$$N(a+bi).$$

Au moyen de ce signe on aura les équations évidentes et qu'on a souvent occasion d'employer:

$$N(kl)=N(k)N(l), \quad N\left(\frac{k}{l}\right)=\frac{N(k)}{N(l)}.$$

Dans la théorie des nombres complexes on a à considérer les quatre unités:

$$1, \quad i, \quad -1, \quad -i,$$

dont l'une quelconque peut être désignée par i^ϱ, en supposant $\varrho=0, 1, 2, 3$.

On appelle nombres complexes associés quatre nombres:

$$a+bi, \quad -b+ai, \quad -a-bi, \quad b-ai,$$

dont chacun produit les trois autres, lorsqu'on le multiplie par i, -1 et $-i$. Ces quatre nombres sont toujours inégaux à moins qu'on n'ait simultanément $a=0$, $b=0$.

Deux nombres complexes:

$$a+bi, \quad a-bi$$

sont dits conjugués, l'un se changeant dans l'autre, en remplaçant i par $-i$. De pareils nombres sont toujours inégaux, excepté lorsque $b=0$.

Des nombres associés ont une norme commune et la même chose a lieu pour deux nombres conjugués.

Ce qui précède s'applique à des nombres complexes quelconques.

Les nombres complexes $a+bi$ portent différents noms, suivant la nature des nombres réels a et b, qu'on en doit considérer comme leurs éléments. Un nombre complexe $a+bi$ s'appelle entier lorsque a et b sont l'un et l'autre des entiers, rationnel lorsque a et b sont l'un et l'autre rationnels, et irrationnel dans tout autre cas. Comme les nombres que nous aurons à considérer, seront presque toujours des nombres complexes entiers, nous supprimerons généralement les adjectifs à moins que cette suppression ne puisse donner lieu à des équivoques.

Lorsque relativement à un entier complexe k on a $N(k)=1$, on peut en conclure: $k=i^e$. On voit encore par l'équation $N(kl)=N(k)N(l)$, que la norme d'un entier kl, multiple d'un autre l, est elle-même un multiple de celle de ce dernier. Il résulte de là que les diviseurs d'un entier quelconque m ont toujours des normes inférieures ou tout au plus égales à celle de m, et que ce dernier cas ne peut avoir lieu que lorsque le diviseur coïncide avec le nombre dont il s'agit ou avec l'un de ses trois associés.

Si donc, pour abréger, on nomme plus grand qu'un autre un nombre complexe dont la norme surpasse celle de ce dernier, on peut dire que les plus grands diviseurs d'un entier complexe sont cet entier lui-même et ses associés.

Un entier complexe $a+bi$ autre que i^e, est dit composé lorsqu'il peut se décomposer en deux facteurs qui ne sont ni l'un ni l'autre de la forme i^e. Dans le cas contraire il s'appelle premier.

Il est facile de voir que des nombres associés sont toujours simultanément des nombres premiers ou simultanément des nombres composés, et qu'il en est de même pour deux nombres conjugués.

§. 2.

Si m et m_1 désignent deux entiers complexes quelconques, on pourra toujours trouver un entier complexe q tel que l'on ait:

$$N(m-m_1q) \leqq \tfrac{1}{2}N(m_1).$$

Il suffit, pour s'en assurer, de remarquer qu'on a:

$$N(m-m_1q) = N(m_1)N\left(\frac{m}{m_1}-q\right),$$

et que les deux entiers réels qui entrent dans q, peuvent toujours être choisis de manière à différer de la partie réelle de $\frac{m}{m_1}$ et du coefficient de i dans cette même expression, de quantités réelles dont les valeurs numériques ne surpassent pas le nombre $\frac{1}{2}$. Il est facile de fonder là-dessus un procédé propre à faire découvrir le plus grand diviseur commun de deux entiers complexes m et m_1 quelconques. On formera les équations:

$$m=m_1q+m_2, \quad m_1=m_2q_1+m_3, \quad \ldots, \quad m_h=m_{h+1}q_h,$$

où les entiers q, q_1, ... sont choisis de manière que l'on ait:

$$N(m_2) \leqq \tfrac{1}{2}N(m_1), \quad N(m_3) \leqq \tfrac{1}{2}N(m_2), \quad \ldots,$$

ce qui aura nécessairement pour effet de conduire à une dernière équation où $m_{h+2}=0$. Cela fait, il suffit de parcourir les équations précédentes, pour voir que tout diviseur commun de m et m_1 divise aussi les entiers m_2, m_3, ..., m_{h+1}. Si l'on considère ensuite les mêmes équations en sens inverse, on voit sur le champ que réciproquement tout diviseur de m_{h+1} est aussi diviseur commun de m et m_1, d'où l'on conclut que le plus grand diviseur commun cherché est l'entier m_{h+1} ou l'un de ses associés, et que dans le cas particulier où m et m_1 sont premiers entre eux, m_{h+1} sera toujours de la forme i^e.

Le procédé précédent conduit à la démonstration du théorème suivant:

„Si, m et m_1 étant premiers entre eux, le produit mn est divisible par m_1, n sera nécessairement un multiple de m_1."

En effet d'après ce qui précède, on aura nécessairement $m_{h+1}=i^e$. D'un autre côté, comme mn est supposé divisible par m_1, on conclut des équations précédentes multipliées par n, que les produits m_2n, m_3n, ..., $m_{h+1}n$ sont également des multiples de m_1, conclusions dont la dernière coïncide avec le résultat qu'il s'agit d'établir.

Le théorème que nous venons de démontrer, étant entièrement semblable à celui qui dans la théorie ordinaire sert de base à toutes les recherches sur les nombres en tant qu'ils sont divisibles les uns par les autres, décomposables en facteurs simples etc., on en tirera les mêmes conséquences pour la théorie des nombres complexes.

En considérant en particulier m_1 comme un nombre premier absolu, on en conclut qu'un pareil nombre, pour diviser le produit de deux ou d'un plus grand nombre de facteurs, doit diviser au moins l'un de ces facteurs. De là suit encore qu'un entier premier à plusieurs autres l'est aussi à leur produit, qu'un entier divisible par plusieurs autres qui n'ont pas de diviseur commun, pris deux à deux, l'est de même par le produit de ces derniers, et ainsi de suite.

Le théorème connu d'après lequel un nombre réel ne peut se décomposer que d'une seule manière en facteurs simples réels, a aussi son analogue dans la théorie des nombres complexes. Mais de même que dans le théorème énoncé on considère tacitement les facteurs simples comme positifs ou du moins pris chacun avec un signe déterminé, il faut agir ici d'une manière analogue. Supposons pour cela que dans chaque groupe de nombres associés, on distingue l'un d'entre eux, d'ailleurs arbitrairement choisi, en l'appelant nombre primaire. Dans cette hypothèse, un entier quelconque m pourra toujours se mettre sous la forme:

$$m = i^v abc \ldots,$$

a, b, c étant des nombres premiers primaires, égaux ou inégaux, et il est facile de s'assurer que la décomposition précédente est toujours unique. En effet si l'on suppose encore:

$$m = i^{v'} a' b' c' \ldots,$$

a', b', c' étant pareillement des nombres premiers primaires, il faudra nécessairement, pour que ces deux équations s'accordent, que a divise l'un des nombres a', b', c', ... Or ces derniers étant premiers et primaires, a devra coïncider avec l'un d'entre eux, avec a' par exemple. Divisant les deux équations par a et continuant de procéder toujours de la même manière, l'identité des deux décompositions se trouvera établie. Si, comme on le fait dans la théorie ordinaire, on réunit les facteurs simples égaux sous forme de puissances, on aura donc d'une manière unique:

$$m = i^v a^\alpha b^\beta c^\gamma \ldots,$$

a, b, c, ... désignant des nombres premiers primaires inégaux et les exposants α, β, ... étant tous au moins égaux à l'unité, c'est-à-dire que les bases et leurs exposants, de même que le facteur i^v, seront complètement déterminés dès que le nombre m sera donné.

§. 3.

Avant d'aller plus loin, il convient de rechercher les conditions propres à faire reconnaître si un entier complexe est premier ou composé.

I. Considérons d'abord un nombre binôme $a+bi$, et soit $N(a+bi) = p$. Cela posé, il est facile de prouver que $a+bi$ est un nombre premier ou non suivant que sa norme, considérée au point de vue ordinaire, est elle-même un nombre premier ou composé. Observons d'abord que, si $a+bi$ est composé, en sorte qu'on puisse supposer:

$$a+bi = (c+di)(f+gi), \quad N(c+di) > 1, \quad N(f+gi) > 1,$$

on aura:

$$N(a+bi) = N(c+di)N(f+gi),$$

c'est-à-dire $N(a+bi)$ égal à un nombre composé. Ce premier point établi, il ne reste évidemment qu'à prouver que si $N(a+bi) = a^2+b^2$ est un nombre composé, $a+bi$ sera aussi composé, pour que la proposition se trouve démontrée. Soit:

$$a^2+b^2 = mn,$$

m et n étant deux entiers réels l'un et l'autre différents de l'unité. Si maintenant $a+bi$, et par suite aussi $a-bi$, était supposé premier, l'équation précédente mise sous la forme $(a+bi)(a-bi) = mn$, exigerait d'après le théorème démontré à la fin du paragraphe précédent, que m et n fussent également des nombres premiers, sans quoi le second membre renfermerait plus de facteurs simples que le premier, et il faudrait de plus que m, abstraction faite d'un facteur de la forme i^v, coïncidât avec l'un des nombres $a+bi$, $a-bi$, ce qui est impossible, ces derniers étant binômes, tandis que m est monôme.

II. D'après ce qu'on vient de prouver, on voit que pour assigner tous les nombres premiers binômes, tout revient à découvrir quels sont, parmi les nombres premiers réels et positifs, ceux qui peuvent se décomposer en deux carrés. Pour ceux de la forme $4n+3$, une pareille décomposition est impossible, la somme de deux carrés étant toujours de l'une des formes:

$$4n, \quad 4n+1, \quad 4n+2.$$

Il ne reste donc que les nombres premiers $4n+1$ et le nombre 2.

Soit p un nombre premier $4n+1$, il sera facile de prouver, qu'il existe toujours deux groupes de nombres premiers binômes associés ayant p pour norme commune. Cela résulte immédiatement du théorème connu, d'après lequel un nombre premier $4n+1$ est toujours la somme de deux carrés, et ne l'est que d'une seule manière. Mais nous n'avons pas besoin de ce théorème, qui peut être considéré au contraire comme un corollaire de la théorie des nombres complexes. Nous supposerons seulement qu'on sache que l'entier réel ξ peut

toujours être choisi de manière à rendre la formule ξ^2+1 divisible par p, comme cela résulte entr'autres du théorème de WILSON, en vertu duquel on peut poser:

$$\xi = 1.2\ldots\tfrac{1}{2}(p-1).$$

Le produit $(\xi+i)(\xi-i)$ étant ainsi divisible par le nombre p, qui ne divise évidemment ni l'un ni l'autre de ces deux facteurs, on en conclut que p est un nombre composé. Soit en conséquence:

$$p = (a+bi)(c+di), \quad a^2+b^2>1, \quad c^2+d^2>1,$$

on aura $p^2 = (a^2+b^2)(c^2+d^2)$, d'où l'on conclut, le nombre réel p^2 ne comportant que la seule décomposition $p\times p$ en facteurs positifs différents de l'unité:

$$p = a^2+b^2 = (a+bi)(a-bi),$$

où les deux facteurs évidemment binômes $a+bi$, $a-bi$, dont la norme commune est un nombre premier réel, seront premiers.

Remarquons encore que les nombres premiers $a+bi$ et $a-bi$ sont toujours distincts, c'est-à-dire qu'ils ne sont ni égaux ni associés. En effet, comme a, b sont évidemment l'un pair, l'autre impair, la supposition:

$$a-bi = i^e(a+bi)$$

exigerait d'abord $i^e = \pm 1$, et par suite l'une de celles-ci: $a=0$, $b=0$, dont l'impossibilité est manifeste.

On voit donc qu'il existe toujours deux groupes distincts de nombres premiers binômes ayant pour norme commune un nombre premier positif $4n+1$ quelconque, et l'on peut ajouter qu'il n'en existe que deux, car il résulte du théorème déjà cité que, si l'on suppose:

$$(a'+b'i)(a'-b'i) = (a+bi)(a-bi),$$

chacun des facteurs du premier membre est nécessairement égal ou associé à l'un des facteurs du second.

Le nombre 2 qui est également décomposable en deux carrés, ne donne lieu qu'à un seul groupe de nombres premiers binômes, les deux nombres conjugués $1+i$, $1-i$ appartenant pour ce cas au même groupe.

III. Il ne reste qu'à examiner quels sont les nombres monômes qui jouent le rôle de nombres premiers dans la théorie des entiers complexes. Comme sous le rapport dont il s'agit, un nombre quelconque se trouve dans la même catégorie que ses associés, nous n'aurons qu'à considérer des nombres monômes positifs, et comme, parmi ces derniers, ceux qui sont composés au point de vue ordinaire, le sont également dans la théorie des entiers complexes,

il n'est plus question que des nombres premiers positifs. Or, les nombres premiers $4n+1$ et le nombre 2 ayant déjà été reconnus comme nombres composés, il ne reste en définitif qu'à considérer les nombres premiers $4n+3$, par rapport auxquels il est facile de s'assurer qu'ils sont ici des nombres premiers, comme ils le sont au point de vue ordinaire. En effet, si pour un nombre q de cette espèce on avait:

$$q = (a+bi)(c+di), \quad N(a+bi)>1, \quad N(c+di)>1,$$

et par suite $q^2 = (a^2+b^2)(c^2+d^2)$, il faudrait, q^2 n'étant susceptible que d'une seule décomposition en facteurs positifs différents de l'unité, qu'on eût $q = a^2+b^2$, ce qui est impossible, comme nous l'avons déjà remarqué.

IV. Les nombres complexes considérés relativement au diviseur $1+i$ et à sa seconde puissance $(1+i)^2 = 2i$, forment trois classes, pour la désignation desquelles il est utile d'introduire des dénominations spéciales.

Un nombre sera dit *impair* lorsqu'il n'est pas divisible par $1+i$, *semi-pair* lorsqu'il est divisible par $1+i$ sans l'être par $(1+i)^2$ ou, ce qui revient au même, par 2, et *pair* enfin lorsqu'il peut être divisé par 2. Il est évident qu'un entier complexe $a+bi$ présentera le premier cas lorsque les deux entiers réels a et b sont l'un pair, l'autre impair, le second lorsque ces deux entiers sont l'un et l'autre impairs, et enfin le troisième lorsque a et b sont tous deux pairs.

V. Nous avons déjà eu occasion de remarquer qu'il peut être utile de distinguer l'un des quatre nombres associés qui forment un même groupe, pour le considérer en quelque sorte comme le nombre primitif ou primaire de ce groupe, les trois autres étant censés dérivés de celui-là en le multipliant par -1, $\pm i$. Le besoin d'une telle distinction réglée sur un principe invariable, se fera surtout sentir en tant qu'il s'agira de nombres impairs, et nous conviendrons donc de considérer comme le nombre *primaire* dans un groupe d'entiers complexes impairs, celui évidemment unique $a+bi$ pour lequel on a simultanément:

$$a \equiv 1 \pmod 4, \qquad b \equiv 0 \pmod 2.$$

Il est facile de conclure de cette définition que le produit de deux et par suite d'un nombre quelconque d'entiers impairs primaires, est lui-même un entier primaire.

Cette convention embrasse déjà tous les nombres premiers, à l'exception de ceux qui dérivent du nombre 2, et qui sont $1+i$, $-1+i$, $-1-i$, $1-i$. Quoique, relativement à ces derniers, le choix d'un nombre primaire soit peu utile, nous conviendrons pour plus d'uniformité de regarder comme tel le nombre $1+i$.

§. 4.

Étant donné un entier complexe quelconque m, on peut toujours concevoir la série complète des entiers complexes, distribuée en séries partielles, deux entiers étant rangés dans la même série ou dans des séries distinctes, suivant que leur différence est un multiple de m ou non. Si ensuite on choisit dans chacune de ces séries partielles l'un quelconque des termes qui la composent, on aura ce que nous appellerons *un système de résidus* pour le module donné m. Un pareil système jouit donc de la double propriété de contenir un terme et de n'en contenir qu'un, qui soit congru à un entier quelconque suivant le module auquel il répond. Pour construire un système de résidus, tout se réduit à découvrir quelque condition qui soit satisfaite par l'un des termes de toute série partielle et ne le soit que par ce seul terme, et à assigner ensuite tous les entiers distincts qui remplissent la condition dont il s'agit. On parviendra, par exemple, à une condition de ce genre, si l'on cherche d'abord, $x+yi$ désignant le terme général d'une série partielle donnée, pour quels termes de cette dernière y a la plus petite valeur non-négative, et si l'on choisit ensuite, parmi ces termes en nombre infini, celui nécessairement unique où x, supposé pareillement non-négatif, est à son tour un minimum. Pour découvrir la nature d'un pareil terme, soit $m = a+bi$, et désignons par $\alpha+\beta i$ un entier complexe arbitrairement choisi. On aura alors pour le terme général de la série partielle à laquelle cet entier appartient:

$$x+yi = (a+bi)(t+ui)+\alpha+\beta i, \quad x = at-bu+\alpha, \quad y = bt+au+\beta,$$

où t et u désignent tous les entiers réels depuis $-\infty$ jusqu'à ∞. On voit, par la dernière de ces équations, que les valeurs dont y est susceptible, sont toutes telles qu'on ait $y \equiv \beta \pmod{h}$, h désignant le plus grand diviseur commun (positif) de a et b. Il résulte de là que y peut toujours être égal à l'un des entiers $0, 1, 2, \ldots, h-1$, et ne peut être égal qu'à l'un d'entre eux. Soit donc y_0 celui de ces entiers qui satisfait à la congruence précédente. Pour que y obtienne cette valeur particulière, on aura à satisfaire à l'équation:

$$bt+au = y_0-\beta,$$

toujours résoluble et dont la solution complète, exprimée en fonction d'une solution particulière t_0, u_0, est:

$$t = t_0+\frac{a}{h}z, \quad u = u_0-\frac{b}{h}z,$$

z désignant un entier réel arbitraire. Au moyen de ces expressions, l'équation en x deviendra:

$$x = at_0-bu_0+\frac{p}{h}z,$$

où l'on suppose $a^2+b^2 = p$. Comme il reste l'indéterminée z dont nous pouvons disposer à volonté, on voit que la plus petite valeur dont x soit susceptible, est l'une de celles-ci:

$$0, \ 1, \ 2, \ \ldots, \ \frac{p}{h}-1,$$

et il est également manifeste que parmi ces dernières il n'en existe qu'une seule que x puisse comporter. Ayant ainsi reconnu que dans toute série partielle il existe toujours un terme unique pour lequel x et y soient respectivement compris dans les suites:

$$x = 0, \ 1, \ 2, \ \ldots, \ \frac{p}{h}-1, \quad y = 0, \ 1, \ 2, \ \ldots, \ h-1,$$

on voit que pour obtenir un système de résidus pour le module $a+bi$, on n'a qu'à introduire, dans l'expression $x+yi$, les valeurs précédentes combinées entre elles de toutes les manières.

Il y a un cas particulier qui mérite une attention particulière; c'est celui où a et b sont premiers entre eux, le système à former se réduisant alors simplement à la suite:

$$0, \ 1, \ 2, \ \ldots, \ p-1,$$

de sorte que pour un module m de cette nature, on peut toujours satisfaire par un entier réel ξ à la congruence:

$$\xi \equiv k \pmod{m},$$

où k désigne un entier complexe quelconque.

§. 5.

Le résultat auquel nous venons de parvenir, donne lieu à plusieurs conséquences importantes que nous allons rapidement indiquer.

I. On voit d'abord que le système des résidus qui répond à un module quelconque m, contient toujours un nombre de termes exprimé par:

$$N(m),$$

car on a $\frac{p}{h}h = p = N(m)$.

II. On peut encore assigner séparément combien parmi ces termes il y en a de divisibles par un facteur k de m. Il est en effet facile de

voir que ces derniers, étant divisés par k, constitueront un système de résidus pour le module $\frac{m}{k}$, en sorte que le nombre qu'il s'agit d'obtenir, est exprimé par:

$$N\left(\frac{m}{k}\right).$$

III. Connaissant, par ce qui précède, le nombre des termes dont tout système de résidus pour le module m doit se composer, on peut en conclure que si l'on a $N(m)$ entiers tels que la différence de deux quelconques d'entre eux ne soit pas un multiple de m, on est dès lors assuré que ces entiers forment un système de résidus relativement au module m.

Pour faire une application de ce principe, soit μ le terme général d'un système de résidus pour le module m, et désignons par n et l deux entiers déterminés dont le premier n'ait pas de diviseur commun avec m. Cela posé, je dis que l'expression $n\mu+l$ représentera également un pareil système. En effet, les valeurs de cette expression étant en nombre convenable, il ne reste plus qu'à s'assurer que deux quelconques d'entre elles ne sauraient présenter une différence multiple de m. Or cela est évident, puisque, μ' et μ'' désignant deux des valeurs dont μ est susceptible, la différence $n\mu'+l-(n\mu''+l)$ est égale au produit $n(\mu'-\mu'')$, dont le premier facteur n'a pas de diviseur commun avec m, et dont le second n'est pas un multiple de cet entier.

L'expression $n\mu+l$ représentant un système de résidus, on voit que parmi les valeurs que μ comporte, il y a toujours une valeur unique telle que cette expression soit divisible par m, ou en d'autres termes, que la congruence:

$$nx+l \equiv 0 \pmod{m},$$

lorsque n n'a pas de diviseur commun avec m, est toujours possible, et que sa solution générale est de la forme:

$$x \equiv x_0 \pmod{m},$$

x_0 désignant une solution particulière, de sorte que cette congruence a une racine unique, en considérant à l'ordinaire comme ne constituant qu'une seule racine, toutes les valeurs qui diffèrent les unes des autres de multiples du module. La congruence en question étant équivalente à l'équation:

$$nx+my+l = 0,$$

on voit encore que la solution générale de celle-ci est donnée par les formules:

$$x = x_0+mz, \quad y = y_0-nz,$$

x_0, y_0 désignant une solution particulière quelconque, et z étant un entier complexe arbitraire. Quant à la résolution effective de cette équation ou de la congruence équivalente, elle peut s'effectuer au moyen de l'algorithme employé plus haut pour découvrir le plus grand diviseur commun de deux entiers complexes; mais comme nous n'aurons pas à en faire usage, nous ne nous arrêterons pas sur cette résolution, d'ailleurs entièrement semblable à celle qui concerne les entiers réels.

IV. Soient maintenant a, b, c, ... des entiers complexes en nombre quelconque et premiers entre eux. Construisons des systèmes de résidus pour chacun de ces entiers ainsi que pour leur produit $m = abc\ldots$, et désignons par α, β, γ, ... et μ les termes généraux de ces systèmes. Cela posé, si relativement à chacun des entiers μ, nous déterminons les nombres α, β, γ, ... qui en diffèrent respectivement d'un multiple de a, b, c, ..., à tout entier μ se trouvera correspondre une combinaison unique de la forme α, β, γ, ... Prouvons réciproquement que toute combinaison de cette espèce provient toujours de l'un des entiers μ, et ne saurait provenir que de l'un d'entre eux. Cette dernière assertion est facile à justifier; en effet si la même combinaison répondait à deux entiers μ distincts, leur différence serait divisible par a, b, c, ... et par suite aussi par m, ce qui est contraire à la nature du système dont μ désigne le terme général. Ayant ainsi reconnu que les combinaisons qui proviennent des entiers μ, sont toutes différentes entre elles, il suffit de remarquer que le nombre de toutes les combinaisons possibles est évidemment:

$$N(a)N(b)N(c)\ldots = N(m),$$

c'est-à-dire égal à celui des entiers μ, pour que la proposition énoncée se trouve établie.

V. Il est facile de voir que si μ est premier à m, les entiers correspondants α, β, γ, ... seront *tous* respectivement premiers à a, b, c, ... et réciproquement. Si donc, relativement à un entier quelconque l, on désigne par $\psi(l)$ le nombre de ceux des termes formant un système de résidus pour le module l qui n'ont pas de diviseur commun avec ce dernier, on aura pour un module m décomposé en facteurs a, b, c, ... premiers entre eux:

$$\psi(m) = \psi(a)\psi(b)\psi(c)\ldots.$$

VI. Nous pouvons, au moyen de la remarque qui vient d'être faite, déterminer la fonction $\psi(m)$ pour un module m quelconque. Soit d'abord $m = a^\alpha$, a désignant un nombre premier et l'exposant α étant au moins égal

à l'unité. Pour ce cas on obtiendra évidemment le nombre de ceux des termes formant le système des résidus pour le module m qui sont premiers à m, si du nombre total des termes du système on retranche le nombre de ses termes divisibles par a. Ces nombres étant le premier égal à $N(a^\alpha)$ et le second égal à $N(a^{\alpha-1})$ (voyez plus haut I. et II.), on obtiendra pour la différence cherchée:

$$N(a^\alpha)-N(a^{\alpha-1}) = (A-1)A^{\alpha-1},$$

en supposant $A = N(a)$.

Après cela il est facile de voir que relativement à un nombre quelconque:

$$m = i^\varepsilon a^\alpha b^\beta c^\gamma \ldots,$$

a, b, c, ... étant des nombres premiers primaires inégaux et les exposants α, β, γ, ... étant tous différents de zéro, on aura:

$$\psi(m) = (A-1)A^{\alpha-1}.(B-1)B^{\beta-1}.(C-1)C^{\gamma-1}\ldots,$$

en posant pour abréger:

$$N(a) = A, \quad N(b) = B, \quad N(c) = C, \quad \ldots,$$

et l'on doit ajouter que, lorsque m est de la forme i^ε, la fonction $\psi(m)$ se réduit à l'unité positive.

Théorie des résidus quadratiques.

§. 6.

Étant donnés deux entiers complexes quelconques k et m, le premier est dit *résidu* ou *non-résidu quadratique* par rapport au second, suivant que la congruence:

$$x^2 \equiv k \pmod{m},$$

dont l'inconnue x est aussi considérée comme complexe, est ou n'est pas possible.

Pour procéder du simple au composé, dans la recherche des conditions propres à distinguer l'un de l'autre ces deux cas, nous considérons en premier lieu m comme un nombre premier impair*) non-diviseur de k qui reste quelconque. Soit:

$$(M) \qquad \mu_1, \quad \mu_2, \quad \mu_3, \quad \ldots$$

le système des résidus relatif au module m, à l'exclusion de celui des termes

*) Le cas où le module se réduit à la forme i^ε, ne donne lieu à aucune question, un entier quelconque étant toujours résidu quadratique d'un tel module. Il est néanmoins bon d'observer que les formules qu'on va établir, lorsqu'on y suppose m de cette forme, ne donnent rien d'inexact, pour être dispensé dans les recherches générales d'avoir égard à ce cas singulier.

de ce système qui est un multiple de m. Cela étant, la congruence:

$$\mu x \equiv k \pmod{m},$$

où μ désigne l'un quelconque des entiers du système (M), sera toujours satisfaite par une valeur unique x comprise dans la suite (M). Distinguons maintenant les deux cas différents que la relation de k à m peut présenter, et supposons d'abord que k soit non-résidu quadratique relativement à m. Dans cette hypothèse, x sera toujours différent de μ, d'où il suit que les entiers (M) peuvent être distribués en groupes composés chacun de deux termes dont le produit soit congru à k (mod. m). Or, le nombre de ces groupes étant évidemment $\frac{1}{2}(p-1)$, où l'on suppose $p = N(m)$, on aura en multipliant:

$$\mu_1\mu_2\mu_3\cdots \equiv k^{\frac{1}{2}(p-1)} \pmod{m}.$$

Dans la seconde hypothèse qui est celle de k résidu quadratique par rapport à m, la distribution en groupes peut encore s'effectuer sur la suite (M), après en avoir retranché les termes μ tels que $\mu^2 \equiv k \pmod{m}$. Mais comme les termes qui satisfont à cette dernière condition, évidemment toujours au nombre de deux, et tels que l'un est congru à l'autre pris avec le signe moins, donnent un produit congru à $-k \pmod{m}$, on voit qu'en multipliant ce produit par tous les autres termes rangés en groupes, il viendra:

$$\mu_1\mu_2\mu_3\cdots \equiv -k^{\frac{1}{2}(p-1)} \pmod{m}.$$

Comme le produit $\mu_1\mu_2\mu_3\ldots$ est indépendant de l'entier k, nous pouvons le déterminer en attribuant à k une valeur particulière. Si l'on suppose à cet effet $k = 1$, ce qui se rapporte évidemment au second cas, on trouve le résultat:

$$\mu_1\mu_2\mu_3\cdots \equiv -1 \pmod{m},$$

qui est analogue au théorème connu de Wilson et au moyen duquel les congruences précédentes, réunies en une seule, prennent cette forme plus simple:

$$k^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{m},$$

où il faut prendre le signe supérieur ou le signe inférieur, suivant que k est ou n'est pas résidu quadratique relativement à m.

Nous conviendrons de désigner désormais par $\left[\frac{k}{m}\right]$ le nombre ± 1 qui entre dans la congruence précédente, de sorte qu'on aura:

$$k^{\frac{1}{2}(p-1)} \equiv \left[\frac{k}{m}\right] \pmod{m}.$$

Le symbole $\left[\frac{k}{m}\right]$ est analogue à celui que Legendre a introduit, et dont l'usage est aujourd'hui généralement adopté; mais il importe de ne pas confondre

ces deux genres de notations dont la seconde, restreinte aux entiers réels, n'exprime pas toujours la même valeur que celle que nous venons de proposer désigne pour ce cas particulier. C'est ce qu'on voit par exemple, en supposant $k=2$, $m=3$, puisqu'on a alors:

$$\left[\frac{2}{3}\right]=1, \quad \left(\frac{2}{3}\right)=-1.$$

Cette circonstance n'a d'ailleurs rien qui puisse étonner, une congruence telle que $x^2\equiv 2 \pmod 3$, qui n'est pas possible tant que l'inconnue est supposée réelle, pouvant admettre des solutions, lorsque cette inconnue est considérée comme susceptible de valeurs imaginaires.

Relativement à la notation que nous venons d'adopter, on a les deux équations évidentes:

$$(a) \qquad \left[\frac{k}{m}\right]=\left[\frac{l}{m}\right], \quad \left[\frac{k}{m}\right]\left[\frac{k'}{m}\right]\left[\frac{k''}{m}\right]\ldots=\left[\frac{kk'k''\ldots}{m}\right],$$

où l'on suppose $k\equiv l \pmod m$, et où k, k', k'', ... sont des entiers quelconques non-divisibles par m.

Nous allons maintenant faire voir que la question de savoir si k est ou n'est pas résidu quadratique par rapport à m, peut toujours se ramener à une question analogue, mais qui ne porte que sur des entiers réels; en d'autres termes, nous démontrerons qu'une expression telle que $\left[\frac{k}{m}\right]$ est toujours réductible à une autre de la forme $\left(\ \right)$.

Avant de montrer comment cette réduction peut être effectuée, nous remarquerons que, l'expression $\left[\frac{k}{m}\right]$ restant évidemment invariable lorsque le nombre m est remplacé par l'un de ses associés, il sera permis de supposer désormais $m=a+bi$, a et b étant respectivement impair et pair. Cela posé, nous traiterons successivement le cas où $b=0$ et celui où b est différent de zéro.

1. Dans le premier de ces deux cas, on a $m=a$, a désignant, abstraction faite du signe, un nombre premier réel $4n+3$. Posons de plus $k=\alpha+\beta i$. Pour obtenir la valeur de $\left[\frac{\alpha+\beta i}{a}\right]$, tout se réduit à voir si la congruence:

$$(1) \qquad x^2\equiv \alpha+\beta i \pmod a$$

est ou n'est pas possible. Si l'on y suppose $x=\varphi+\psi i$, cette congruence se décomposera en ces deux congruences simultanées équivalentes qui ne contiennent

que des entiers réels:

$$(2) \qquad \varphi^2-\psi^2\equiv\alpha, \quad 2\varphi\psi\equiv\beta \pmod a.$$

Ces dernières étant élevées au carré et ajoutées donnent:

$$(\varphi^2+\psi^2)^2\equiv\alpha^2+\beta^2 \pmod a,$$

ou ce qui revient au même, $\alpha^2+\beta^2$ n'étant pas divisible par a:

$$(3) \qquad \left(\frac{\alpha^2+\beta^2}{a}\right)=1,$$

de sorte que la possibilité de la congruence (1) suppose la condition (3). Je dis réciproquement que si cette dernière est satisfaite, la possibilité de la congruence (1), ou ce qui revient au même, celle des deux congruences simultanées (2) s'ensuit. Considérons d'abord le cas où $\alpha\equiv 0 \pmod a$ et dans lequel la condition (3) a évidemment lieu. On voit qu'on satisfait alors à la première des congruences (2), en posant $\psi=\pm\varphi$, ce qui change la seconde en celle-ci: $2\varphi^2\equiv\pm\beta \pmod a$, évidemment possible si le signe est convenablement choisi. Reste à considérer le cas où α n'est pas divisible par a. En vertu de la condition (3) supposée satisfaite, il existera un entier réel s tel qu'on ait $s^2\equiv\alpha^2+\beta^2$, et par suite $(s+\beta)(s-\beta)\equiv\alpha^2 \pmod a$. Or, α n'étant pas divisible par a, on conclut de cette dernière congruence:

$$\left(\frac{s+\beta}{a}\right)=\left(\frac{s-\beta}{a}\right)=\pm 1,$$

et nous observerons qu'on peut toujours faire en sorte que le signe supérieur ait lieu. En effet la congruence en s, d'où nous sommes parti, ne contenant que le carré s^2, nous pouvons, lorsque le signe inférieur a lieu, remplacer s par $-s$, ce qui changera les expressions $\left(\frac{s+\beta}{a}\right)$, $\left(\frac{s-\beta}{a}\right)$ respectivement en $-\left(\frac{s-\beta}{a}\right)$, $-\left(\frac{s+\beta}{a}\right)$. On voit donc que, si s est convenablement choisi, on a:

$$\left(\frac{s+\beta}{a}\right)=\left(\frac{s-\beta}{a}\right)=1.$$

Cela supposé, on pourra trouver deux entiers réels t et u tels qu'on ait:

$$t^2\equiv s+\beta, \quad u^2\equiv s-\beta \pmod a,$$

et par suite:

$$(tu)^2\equiv s^2-\beta^2\equiv\alpha^2, \quad tu\equiv\pm\alpha \pmod a,$$

le signe ambigu dépendant du choix de t et u. Ajoutons que, les entiers t et u pouvant être pairs ou impairs à volonté, il sera toujours possible de les

choisir de même espèce, c'est-à-dire tous les deux pairs ou tous les deux impairs. Cela fait, il est facile de voir qu'on satisfera aux congruences (2) au moyen de ces expressions entières:

$$\varphi = \tfrac{1}{2}(t \pm u), \quad \psi = \tfrac{1}{2}(t \mp u),$$

où nous supposons que les signes soient choisis conformément à celui qui a lieu dans la congruence $tu \equiv \pm\alpha$. C'est ce dont on s'assure sans difficulté, en faisant la substitution et en ayant égard aux conditions auxquelles s, t, u sont supposés satisfaire.

Il résulte de ce qui précède que si l'on a $\left[\frac{\alpha+\beta i}{a}\right] = 1$, il s'ensuit $\left(\frac{\alpha^2+\beta^2}{a}\right) = 1$, et que la réciproque a également lieu. On conclut de là et de ce que chacune des expressions précédentes est toujours de la forme ± 1, que quel que soit l'entier $\alpha+\beta i$ non-divisible par le nombre premier a, on a toujours:

$$(b) \qquad \left[\frac{\alpha+\beta i}{a}\right] = \left(\frac{\alpha^2+\beta^2}{a}\right).$$

On peut remarquer que dans le cas particulier où l'un des entiers α, β s'évanouit, on a:

$$\left[\frac{\alpha+\beta i}{a}\right] = 1.$$

II. Considérons maintenant le cas où la partie imaginaire de $m = a+bi$ n'est pas nulle. Pour décider dans ce cas si la congruence $x^2 \equiv \alpha+\beta i \pmod{m}$ est ou n'est pas possible, nous observerons que d'après ce qui a été prouvé plus haut sur les résidus d'un module $a+bi$, pour lequel a et b sont premiers entre eux, nous pouvons considérer x comme réel. Cela étant, la congruence précédente est équivalente à l'équation:

$$x^2 - \alpha - \beta i = (\varphi+\psi i)(a+bi),$$

ou à ces équations simultanées qui ne contiennent que des entiers réels:

$$(4) \qquad x^2 - \alpha = a\varphi - b\psi, \quad -\beta = b\varphi + a\psi.$$

En les ajoutant, après les avoir multipliées par a et b, on trouve:

$$(5) \qquad ax^2 - a\alpha - b\beta = p\varphi.$$

Observons maintenant que $a\alpha+b\beta$ ne saurait être divisible par p. En effet, si cela était, p diviserait aussi x, ce qui est impossible en vertu de la congruence $x^2 \equiv \alpha+\beta i \pmod{a+bi}$, dont le premier membre est, comme le second, premier à $a+bi$ et par conséquent aussi à p, x étant réel. Cela étant, l'équation (5)

donne:

$$(6) \qquad \left(\frac{a}{p}\right) = \left(\frac{a\alpha+b\beta}{p}\right).$$

Je dis maintenant que, cette équation qui est une conséquence très simple de la congruence $x^2 \equiv \alpha+\beta i \pmod{m}$ étant supposée satisfaite, la possibilité de la congruence ou, ce qui revient au même, celle des équations (4) s'ensuit. En effet, la condition (6) entraîne immédiatement l'équation (5), qui, en y substituant pour p sa valeur a^2+b^2, se change en:

$$a(x^2 - \alpha - a\varphi) = b(\beta + b\varphi).$$

Or, a et b n'ayant pas de diviseur commun, il faut qu'on ait $\beta + b\varphi = -a\psi$, ψ étant un entier, et par suite $x^2 - \alpha - a\varphi = -b\psi$, équations qui coïncident avec celles dont il s'agit de prouver la possibilité.

L'équation (6) pouvant se mettre sous la forme:

$$\left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right) = 1,$$

on voit que chacune des deux équations:

$$\left[\frac{\alpha+\beta i}{a+bi}\right] = 1, \quad \left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right) = 1$$

est toujours une conséquence nécessaire de l'autre. De là et de ce que les expressions qui forment leurs premiers membres, sont toujours de la forme ± 1, on conclut:

$$\left[\frac{\alpha+\beta i}{a+bi}\right] = \left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right).$$

Cette dernière égalité peut prendre une forme plus simple, car on a toujours:

$$\left(\frac{a}{p}\right) = 1.$$

En effet, l'équation $a^2+b^2 = p$ donne sur le champ $\left(\frac{p}{a}\right) = 1$, si l'on fait usage du signe de LEGENDRE étendu, comme l'a proposé M. JACOBI, aux nombres composés[1]), et par suite $\left(\frac{a}{p}\right) = 1$, p étant positif et de la forme $4n+1$.

[1]) Les théorèmes qui constituent la théorie des résidus quadratiques, en tant qu'il s'agit de nombres réels, étant généralement connus, nous nous dispenserons d'en rappeler les énoncés, lorsque nous aurons à faire usage de ces théorèmes. Quant à l'usage du signe de LEGENDRE, étendu aux nombres composés, qui est moins connu, on peut sur ce point consulter le compte rendu de l'Académie de Berlin, Oct. 1837, ou le §. 2 du Mémoire déjà cité: „Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres.“*)

*) S. 422 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Nous avons donc, quel que soit l'entier $\alpha+\beta i$ non-divisible par le nombre premier $a+bi$, dans lequel b est pair, mais différent de zéro:

$$(c) \qquad \left[\frac{\alpha+\beta i}{a+bi}\right] = \left(\frac{a\alpha+b\beta}{p}\right).$$

Il importe de remarquer que l'équation (b) est tout-à-fait distincte de celle que nous venons d'établir, et ne se déduit nullement de cette dernière, en y faisant $b=0$.

§. 7.

Nous pouvons maintenant nous occuper de la question que l'on doit regarder comme la plus importante parmi celles que la théorie des résidus quadratiques présente, et qui a pour objet, étant donné un entier complexe quelconque k, d'assigner les caractères propres à distinguer les nombres premiers impairs m dont k est résidu quadratique, de ceux auxquels cet entier a la relation opposée. Comme d'après l'équation (a), démontrée plus haut, la question proposée, lorsque k est un nombre composé, se réduit sur-le-champ à des questions analogues relatives aux facteurs de k, on voit que nous n'aurons à considérer que les quatre hypothèses:

$$k = \pm 1, \quad i, \quad 1+i, \quad \alpha+\beta i,$$

$\alpha+\beta i$ étant un nombre premier impair que nous pourrions considérer comme primaire, mais dans lequel nous supposerons simplement que β, qui peut d'ailleurs s'évanouir, est pair.

Le premier cas ne donne lieu à aucune question, ± 1 étant un carré. Les trois autres sont résolus par les équations qui suivent et dans lesquelles le nombre premier impair $a+bi$ est pareillement tel que b, qui peut d'ailleurs se réduire à zéro, soit pair, et où l'on a posé pour abréger, $a^2+b^2=p$:

$$(d) \qquad \left[\frac{i}{a+bi}\right] = (-1)^{\frac{1}{4}(p-1)}, \quad \left[\frac{1+i}{a+bi}\right] = (-1)^{\frac{1}{4}(a+b)^2-1)}, \quad \left[\frac{\alpha+\beta i}{a+bi}\right] = \left[\frac{a+bi}{\alpha+\beta i}\right].$$

La première de ces équations se déduit sans difficulté, soit de la formule $k^{\frac{1}{2}(p-1)} \equiv \left[\frac{k}{m}\right] \pmod{m}$ obtenue plus haut, soit des deux équations (b) et (c), si, en suivant cette dernière voie, on suppose successivement $b=0$ et b différent de zéro.

Pour démontrer la seconde des équations (d), soit d'abord $b=0$. On a alors, au moyen de l'équation (b) et d'un théorème connu:

$$\left[\frac{1+i}{a}\right] = \left(\frac{2}{a}\right) = (-1)^{\frac{1}{4}(a^2-1)},$$

conformément à l'équation qu'il s'agit d'établir. Supposons, en second lieu, b différent de zéro. L'équation (c) donne alors:

$$\left[\frac{1+i}{a+bi}\right] = \left(\frac{a+b}{p}\right).$$

Pour obtenir la valeur du second membre, nous aurons recours à l'équation identique $2p=(a+b)^2+(a-b)^2$, de laquelle on conclut successivement au moyen de théorèmes connus:

$$\left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right), \quad \left(\frac{a+b}{p}\right) = \left(\frac{2}{a+b}\right) = (-1)^{\frac{1}{4}((a+b)^2-1)},$$

ce qui s'accorde également avec l'équation que nous nous proposions de vérifier.

La démonstration de la troisième des équations (d), à laquelle nous arrivons maintenant et qui exprime une loi de réciprocité entre deux nombres premiers impairs différents, c'est-à-dire ni égaux ni opposés, donne lieu à distinguer trois cas. Le premier de ces cas est celui où b et β sont tous les deux égaux à zéro. Dans ce premier cas, la vérité de l'équation est évidente, puisque d'après la formule (b) on a à la fois:

$$\left[\frac{a}{a}\right] = 1, \quad \left[\frac{a}{a}\right] = 1.$$

Considérons, en second lieu, le cas où l'un des entiers b et β se réduit à zéro, et soit β cet entier évanouissant, ce que la forme symétrique de notre équation permet évidemment de supposer. On a alors, en vertu des équations (c) et (b) et d'après une remarque déjà faite*):

$$\left[\frac{\alpha}{a+bi}\right] = \left(\frac{a\alpha}{p}\right) = \left(\frac{\alpha}{p}\right), \quad \left[\frac{a+bi}{\alpha}\right] = \left(\frac{p}{\alpha}\right),$$

de sorte que la vérification à effectuer résulte de l'équation connue:

$$\left(\frac{\alpha}{p}\right) = \left(\frac{p}{\alpha}\right).$$

Passant enfin au troisième cas où b et β sont l'un et l'autre différents de zéro, on appliquera la formule (c) à chacun des deux membres de l'équation qu'il

*) 8. 555: $\left(\frac{a}{p}\right)=1$. K.

s'agit de prouver et qui deviendra ainsi:

$$\left(\frac{a\alpha+b\beta}{p}\right)=\left(\frac{a\alpha+b\beta}{\varpi}\right),$$

en posant, pour un instant, $\alpha^2+\beta^2=\varpi$. Pour s'assurer de la vérité de cette dernière équation, il suffit de recourir à l'identité:

$$(a\alpha+b\beta)^2+(b\alpha-a\beta)^2=p\varpi,$$

d'où résulte successivement, $a\alpha+b\beta$ étant impair:

$$\left(\frac{p}{a\alpha+b\beta}\right)=\left(\frac{\varpi}{a\alpha+b\beta}\right),\quad \left(\frac{a\alpha+b\beta}{p}\right)=\left(\frac{a\alpha+b\beta}{\varpi}\right),\quad \text{c. q. f. d.}$$

Nous ne terminerons pas ce paragraphe sans observer que les équations (d) sont dues à M. Gauss qui les a données sans démonstration, du moins la dernière, dans le Mémoire cité plus haut. La démonstration que nous venons de développer, déjà indiquée dans une Note insérée dans le Journal de Crelle[1]), est comme on voit, une application très simple des théorèmes (b) et (c), qui indépendamment de l'usage que nous en faisons ici, nous seront indispensables pour la solution de la question qui fait le principal sujet du présent Mémoire.

§. 8.

Le symbole $\left[\frac{k}{m}\right]$, tel que nous l'avons employé jusqu'à présent, suppose que m est un nombre premier impair. Il arrive souvent qu'on a à considérer des produits de la forme:

$$\left[\frac{k}{m}\right]\left[\frac{k}{m'}\right]\left[\frac{k}{m''}\right]\cdots,$$

où m, m', m'', ... sont des nombres premiers impairs non-diviseurs de k, mais d'ailleurs égaux ou inégaux. Soit $M=mm'm''\ldots$ et convenons de désigner désormais le produit précédent simplement par:

$$\left[\frac{k}{M}\right],$$

de sorte que la valeur de notre symbole ainsi généralisé, toujours égale soit à $+1$ soit à -1, n'indiquera plus, suivant ces deux cas, si k est ou n'est pas résidu quadratique par rapport à M, et fera seulement connaître, si parmi les facteurs simples égaux ou inégaux de M, il y en a un nombre pair ou impair,

[1]) S. 173 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

auxquels k présente la dernière de ces deux relations. L'extension que nous venons d'indiquer, entièrement semblable à celle que M. Jacobi a proposée relativement au signe de Legendre et dont nous avons déjà fait un fréquent usage dans ce qui précède, donne lieu à plusieurs théorèmes analogues à ceux qui ont été démontrés dans le paragraphe précédent et faciles à déduire de ces derniers. On a d'abord évidemment les équations:

$$(e)\qquad \left[\frac{k}{M}\right]=\left[\frac{l}{M}\right],\quad \left[\frac{kk'}{M}\right]=\left[\frac{k}{M}\right]\left[\frac{k'}{M}\right],\quad \left[\frac{k}{MM'}\right]=\left[\frac{k}{M}\right]\left[\frac{k}{M'}\right],$$

qui supposent, la première, que k, toujours sans diviseur commun avec l'entier impair M, est tel qu'on ait $k\equiv l\,(\text{mod. } M)$, la seconde que k et k' sont premiers à M, et la troisième que k est premier aux entiers impairs M et M'.

Voici maintenant les équations analogues aux équations (d), ou pour mieux dire, d'une forme tout identique avec ces dernières:

$$(f)\quad \left[\frac{i}{A+Bi}\right]=(-1)^{\frac{1}{2}(P-1)},\quad \left[\frac{1+i}{A+Bi}\right]=(-1)^{\frac{1}{8}(A+B)^2-1)},\quad \left[\frac{\alpha+\beta i}{A+Bi}\right]=\left[\frac{A+Bi}{\alpha+\beta i}\right].$$

Dans ces équations $A+Bi$ et $\alpha+\beta i$ sont deux entiers complexes impairs quelconques premiers entre eux et pour lesquels les coefficients B et β, toujours considérés comme pairs, peuvent se réduire à zéro. On a d'ailleurs $P=A^2+B^2$.

La première de ces équations coïncidant avec la première des équations (d) déjà établies, lorsque $A+Bi$ se réduit au nombre premier $a+bi$, on voit que pour s'assurer qu'elle a généralement lieu, tout se réduit à faire voir que, si on la suppose exacte pour un nombre quelconque $A+Bi$, elle ne cessera pas de subsister lorsque ce dernier vient à être remplacé par le produit:

$$(a+bi)(A+Bi)$$

que nous désignerons par $A'+B'i$. Nous avons donc à montrer que la troisième des équations:

$$\left[\frac{i}{a+bi}\right]=(-1)^{\frac{1}{2}(p-1)},\quad \left[\frac{i}{A+Bi}\right]=(-1)^{\frac{1}{2}(P-1)},\quad \left[\frac{i}{A'+B'i}\right]=(-1)^{\frac{1}{2}(P'-1)},$$

où l'on suppose $p=a^2+b^2$, $P'=A'^2+B'^2$, est une conséquence des deux premières. Il suffit évidemment pour cela de prouver que les deux entiers réels:

$$\tfrac{1}{4}(p-1)+\tfrac{1}{4}(P-1),\quad \tfrac{1}{4}(P'-1)$$

sont toujours de même espèce, c'est-à-dire tous les deux pairs ou tous les deux impairs. C'est ce qui résulte sur-le-champ de l'équation identique:

$$\tfrac{1}{4}(Pp-1)-\tfrac{1}{4}(p-1)-\tfrac{1}{4}(P-1)=\tfrac{1}{4}(P-1)(p-1)$$

dont le second membre est pair et même divisible par 4, P et p étant de la forme $4n+1$.

Le même moyen de démonstration peut s'appliquer à la seconde des équations (f), et l'on voit qu'il s'agira ainsi de démontrer que les deux nombres:

$$\tfrac{1}{8}((a+b)^2-1)+\tfrac{1}{8}((A+B)^2-1), \quad \tfrac{1}{8}((A'+B')^2-1)$$

sont toujours de même espèce. Observons pour cela qu'en vertu de l'équation identique:

$$\tfrac{1}{8}((rs)^2-1)-\tfrac{1}{8}(r^2-1)-\tfrac{1}{8}(s^2-1) = \tfrac{1}{8}(r^2-1)(s^2-1),$$

dont le second membre est pair, si r et s sont des entiers impairs, le premier des deux entiers que nous avons à considérer, est de même espèce que $\frac{1}{8}|(a+b)(A+B))^2-1|$. Mais, comme d'un autre côté deux carrés dont les racines diffèrent d'un multiple de 8, diffèrent eux-mêmes d'un multiple de 16, ce dernier est à son tour de même espèce que:

$$\tfrac{1}{8}|(a+b)(A+B)-2Bb)^2-1| = \tfrac{1}{8}|(A'+B')^2-1|,$$

et l'assertion avancée se trouve établie.

La troisième des équations (f) est également très facile à obtenir. En effet, d'après l'hypothèse faite sur les entiers $A+Bi$, $\alpha+\beta i$, on peut les décomposer l'un et l'autre en facteurs simples ayant leurs parties réelles impaires. Soit n l'un des facteurs de $A+Bi$, et m l'un de ceux de $\alpha+\beta i$, on pourra, par l'emploi répété des deux dernières des équations (e), remplacer l'expression $\left[\frac{\alpha+\beta i}{A+Bi}\right]$ par un produit d'expressions de la forme $\left[\frac{m}{n}\right]$, où tout facteur m doit être combiné avec tout facteur n. Si maintenant on remplace tout symbole $\left[\frac{m}{n}\right]$ par celui-ci: $\left[\frac{n}{m}\right]$ qui lui est équivalent en vertu de la troisième des équations (d), et que l'on effectue la multiplication au moyen des équations déjà citées, le premier membre de l'équation qu'il s'agit de vérifier, se trouvera identique au second.

Il reste à opérer d'une manière générale la réduction qui pour le cas particulier d'un nombre premier $a+bi$, peut s'obtenir au moyen des équations (b) et (c) du paragraphe précédent. Soit $A+Bi$ un entier impair quelconque (B étant pair et pouvant se réduire à zéro) et $\alpha+\beta i$ un second entier, assujetti à la condition unique d'être premier à $A+Bi$; il s'agira de remplacer l'expression $\left[\frac{\alpha+\beta i}{A+Bi}\right]$ par des expressions analogues ne contenant que des entiers réels.

Considérons d'abord le cas où B s'évanouit, et celui où A et B n'ont pas de diviseur commun; nous verrons ensuite que le cas le plus général se réduit immédiatement à ceux-là. Relativement aux deux cas qui viennent d'être indiqués, on a respectivement:

$$(g) \qquad \left[\frac{\alpha+\beta i}{A}\right] = \left(\frac{\alpha^2+\beta^2}{A}\right), \quad \left[\frac{\alpha+\beta i}{A+Bi}\right] = \left(\frac{A\alpha+B\beta}{P}\right),$$

P désignant pour abréger, dans la seconde de ces équations, le binôme A^2+B^2.

Pour démontrer la première, observons qu'on peut y considérer A comme positif, les deux membres ne changeant pas lorsqu'on y remplace A par $-A$. Cela posé, soit:

$$A = \mathrm{a}\mathrm{a}' \ldots \times pp' \ldots,$$

a, a', ..., p, p', ... désignant des nombres premiers réels et positifs, les premiers, a, a', ..., de la forme $4n+3$, les seconds, p, p', ..., de la forme $4n+1$. D'après l'équation (b), chacun des premiers donne une équation telle que:

$$\left[\frac{\alpha+\beta i}{\mathrm{a}}\right] = \left(\frac{\alpha^2+\beta^2}{\mathrm{a}}\right),$$

tandis que pour chacun des derniers, p par exemple, qui peut se décomposer en deux facteurs premiers binômes $(a+bi)(a-bi)$, où b est supposé pair, on a en vertu de l'équation (c):

$$\left[\frac{\alpha+\beta i}{p}\right] = \left[\frac{\alpha+\beta i}{a+bi}\right]\left[\frac{\alpha+\beta i}{a-bi}\right] = \left(\frac{a\alpha+b\beta}{p}\right)\left(\frac{a\alpha-b\beta}{p}\right) = \left(\frac{a^2\alpha^2-b^2\beta^2}{p}\right),$$

et par suite, puisque $-b^2 \equiv a^2 \pmod{p}$:

$$\left[\frac{\alpha+\beta i}{p}\right] = \left(\frac{a^2}{p}\right)\left(\frac{\alpha^2+\beta^2}{p}\right) = \left(\frac{\alpha^2+\beta^2}{p}\right).$$

Ces deux systèmes de relations étant multipliés entre eux, donnent la formule qu'il s'agissait d'établir.

Passons à la vérification de la seconde des équations précédentes (g).

Nous supposerons d'abord $\beta = 0$, cas auquel celui où β n'est pas zéro, se ramène facilement. Comme, par hypothèse, A et B n'ont pas de diviseur commun, on pourra poser:

$$A+Bi = (a+bi)(a'+b'i)\ldots,$$

où les facteurs du second membre désignent des nombres premiers binômes, dans lesquels b, b', ... sont supposés pairs. L'équation (c) donne relativement au facteur $a+bi$:

$$\left[\frac{\alpha}{a+bi}\right] = \left(\frac{a\alpha}{p}\right) = \left(\frac{\alpha}{p}\right),$$

en posant pour abréger $a^2+b^2=p$. En faisant le produit de cette équation et des équations analogues, il viendra:

$$\left[\frac{\alpha}{A+Bi}\right]=\left(\frac{\alpha}{pp'\ldots}\right)=\left(\frac{\alpha}{P}\right).$$

Or, l'équation qu'il s'agit de prouver se réduisant, par la supposition $\beta=0$, à celle-ci:

$$\left[\frac{\alpha}{A+Bi}\right]=\left(\frac{A\alpha}{P}\right)=\left(\frac{A}{P}\right)\left(\frac{\alpha}{P}\right),$$

nous n'avons plus qu'à démontrer qu'on a $\left(\frac{A}{P}\right)=1$. Mais, comme A et B sont premiers entre eux, il résulte de l'équation $A^2+B^2=P$ que A et P sont pareillement sans diviseur commun, de sorte que $\left(\frac{P}{A}\right)=1$, et par suite $\left(\frac{A}{P}\right)=1$.

Reste à considérer le cas où β a une valeur différente de zéro. On cherchera alors un entier réel s tel qu'on ait:

$$s\equiv\alpha+\beta i \pmod{A+Bi},$$

dont l'existence suit de l'hypothèse admise sur les nombres A et B. Cela fait, on aura:

$$\left[\frac{\alpha+\beta i}{A+Bi}\right]=\left[\frac{s}{A+Bi}\right]$$

et par suite, en vertu du cas déjà démontré:

$$\left[\frac{\alpha+\beta i}{A+Bi}\right]=\left(\frac{As}{P}\right).$$

D'un autre côté, si l'on remplace la congruence précédente par deux équations équivalentes, on reconnaît sur-le-champ que s satisfait à la condition:

$$As\equiv A\alpha+B\beta \pmod{P}.$$

Cela étant, cette dernière congruence conduit à l'équation:

$$\left(\frac{As}{P}\right)=\left(\frac{A\alpha+B\beta}{P}\right),$$

dont la comparaison avec celle que nous avons obtenue plus haut, donne un résultat qui s'accorde avec la seconde des formules (g).

Il nous reste enfin à supposer l'entier impair $A+Bi$ tout-à-fait arbitraire, si ce n'est que nous considérons toujours B comme pair, ce qui ne nuit en

rien à la généralité. Soit L le plus grand diviseur commun (réel) de A et B, et posons:

$$A=A'L,\quad B=B'L,\quad A'^2+B'^2=P'.$$

L'expression $\left[\frac{\alpha+\beta i}{A+Bi}\right]$ dans laquelle $\alpha+\beta i$ n'est assujetti qu'à la seule condition d'être premier à $A+Bi$, se décomposera alors en deux facteurs:

$$\left[\frac{\alpha+\beta i}{L}\right],\quad \left[\frac{\alpha+\beta i}{A'+B'i}\right]$$

respectivement de même forme que les premiers membres des équations (g), et l'on aura en conséquence:

$$(h)\qquad \left[\frac{\alpha+\beta i}{A+Bi}\right]=\left(\frac{\alpha^2+\beta^2}{L}\right)\left(\frac{A'\alpha+B'\beta}{P'}\right).$$

§. 9.

Nous terminerons ce que nous avons à dire sur les résidus quadratiques, en considérant la congruence:

$$(1)\qquad x^2\equiv k \pmod{m},$$

où k et m sont des entiers complexes quelconques premiers entre eux, le second impair. Pour que cette congruence soit possible, il faut évidemment qu'elle puisse subsister par rapport à chacun des facteurs simples de m. Soient:

$$f,\ f',\ f'',\ \ldots$$

les nombres premiers primaires inégaux qui divisent m et soit μ leur nombre. Il faudra donc qu'on ait:

$$(2)\qquad \left[\frac{k}{f}\right]=1,\quad \left[\frac{k}{f'}\right]=1,\quad \left[\frac{k}{f''}\right]=1,\quad \ldots.$$

Je dis de plus que, ces conditions ayant lieu, la possibilité de la congruence s'ensuit et que le nombre de ses racines sera 2^μ, en considérant à l'ordinaire comme ne constituant qu'une seule racine, les entiers en nombre infini qui diffèrent les uns des autres de multiples du module m. Considérons d'abord la congruence $x^2\equiv k \pmod{f^n}$, l'exposant étant un nombre positif quelconque. Si l'on y satisfait par la supposition de $x=\alpha$, et par suite par l'hypothèse plus générale de $x=\alpha+tf^n$, t étant un entier arbitraire, il est facile d'en déduire une solution pour la congruence de même forme, mais relative au module

f^{h+l} où l'on suppose $l \leqq h$. En effet, la substitution de l'expression de x donnant:

$$\frac{x^2-k}{f^h} = \frac{a^2-k}{f^h} + 2at + t^2 f^h,$$

où le premier terme du second membre est par hypothèse un entier, on voit que pour satisfaire à la congruence $x^2 \equiv k \pmod{f^{h+l}}$, il reste à faire en sorte qu'on ait $2at \equiv -\frac{a^2-k}{f^h} \pmod{f^l}$, ce qui est toujours possible, a et par suite $2a$ étant évidemment premier au module. Comme on peut, par ce procédé, s'élever à des exposants de plus en plus grands, en partant de l'exposant $h = 1$, on voit que la condition de possibilité de la congruence:

$$x^2 \equiv k \pmod{f^h},$$

quel que soit h, est celle qui se rapporte à $h = 1$, consistant en ce que l'on doit avoir:

$$\left[\frac{k}{f}\right] = 1.$$

Voyons maintenant quel est le nombre des racines de la congruence précédente. En considérant toujours a comme une de ses racines, on pourra lui donner la forme:

$$x^2 - a^2 = (x+a)(x-a) \equiv 0 \pmod{f^h}.$$

Or, $x+a$ et $x-a$ ne pouvant être simultanément divisibles par f, on voit qu'on ne peut satisfaire à cette dernière qu'en supposant:

$$x \equiv a \quad \text{ou} \quad x \equiv -a \pmod{f^h},$$

ce qui ne donne que deux racines, qui seront toujours distinctes, leur différence $2a$ n'étant pas divisible par f.

Si maintenant l'on observe qu'en posant $m = i^e f^h f'^{h'} \ldots$, la congruence (1) est évidemment équivalente à ces congruences simultanées:

$$x^2 \equiv k \pmod{f^h}, \quad x^2 \equiv k \pmod{f'^{h'}}, \quad \ldots,$$

dont chacune, en vertu de ce qui précède, admet deux racines distinctes de la forme $\pm a$, on conclura facilement, d'après la remarque faite plus haut (§. 5, IV.) que la congruence (1) admet elle-même 2^μ racines distinctes, lorsque les conditions (2), nécessaires pour sa possibilité, sont toutes remplies. Il est bon d'ajouter que dans le cas où m est de la forme i^e, et où il n'y a aucune condition à remplir, le nombre des solutions de la congruence (1) est toujours exprimé par la formule 2^μ, car on a dans ce cas $\mu = 0$.

Théorèmes fondamentaux sur les formes quadratiques.

§. 10.

Avant d'entrer dans le sujet indiqué par le titre, il convient de faire une remarque nécessaire pour que l'exposition qu'on va lire, soit considérée sous son véritable point de vue. L'objet du présent Mémoire étant purement théorique, nous avons cherché à résoudre les questions que nous avions à traiter, par les considérations qui, théoriquement parlant, nous ont paru les plus simples, sans nous attacher à rendre les solutions propres au calcul numérique. Pour satisfaire à cette dernière condition, il faudrait entrer dans des développements assez étendus, qui ne présenteraient que très peu d'intérêt et ne seraient d'ailleurs d'aucune utilité pour l'objet de pure théorie que nous avons en vue. Limités comme nous venons de l'indiquer, les éléments de la théorie des formes quadratiques à coefficients et à indéterminées complexes peuvent être présentés dans un petit nombre de pages, si aux moyens déjà employés par les illustres géomètres qui ont fondé ou perfectionné la théorie analogue relative aux entiers réels, on ajoute quelques principes nouveaux, qui nous paraissent mériter l'attention des géomètres. Leur extrême fécondité ne sera toutefois mise dans tout son jour que par des recherches ultérieures que nous avons entreprises sur les formes des degrés supérieurs et que nous aurons à exposer plus tard.

Toute expression:

$$(1) \qquad ax^2 + 2bxy + cy^2,$$

où a, b, c sont des entiers complexes déterminés, et x, y de pareils entiers indéterminés, est ce que nous appellerons une *forme quadratique binaire* ou simplement une *forme*, cette abréviation ne pouvant donner lieu ici à aucune ambiguïté. Il est essentiel de suivre un ordre fixe tant par rapport aux indéterminées x et y, qui seront respectivement nommées la première et la seconde, que par rapport aux coefficients a, b, c, dont la désignation indiquera toujours la place que ces coefficients occupent dans l'expression que nous venons d'écrire.

Les propriétés de la forme (1) dépendant principalement du nombre D, donné par l'équation $D = b^2 - ac$, ce nombre sera dit le *déterminant* de la forme en question. Dans le cas particulier où D est un carré, ce qui comprend la supposition de $D = 0$, la forme se décompose évidemment en deux facteurs

linéaires à coefficients rationnels, en sorte que ses propriétés se déduisent facilement de celles bien connues des expressions de ce genre. C'est pourquoi nous ferons toujours abstraction de ce cas particulier. Sous cette restriction, les coefficients extrêmes a et c sont l'un et l'autre différents de zéro, d'où il suit que l'un d'entre eux, c par exemple, peut se déduire sans indétermination de l'autre a, du coefficient moyen b et du déterminant D, supposés connus, au moyen de la formule:

$$c = \frac{b^2 - D}{a}.$$

Si dans la forme (1) on remplace les indéterminées x et y par de nouvelles indéterminées x' et y', liées aux premières par les équations:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y', \tag{2}$$

où α, β, γ, δ sont des entiers donnés, elle se changera en cette autre:

$$a'x'^2 + 2b'x'y' + c'y'^2, \tag{3}$$

où l'on a:

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \quad c' = a\beta^2 + 2b\beta\delta + c\delta^2, \tag{4}$$

et l'on dit alors que la nouvelle forme (3) est *contenue* sous la forme primitive (1). En substituant les coefficients a', b', c' de la forme (3) dans l'expression de son déterminant D', il viendra:

$$D' = (\alpha\delta - \beta\gamma)^2 D. \tag{5}$$

On voit ainsi qu'une forme contenue sous une autre a toujours un déterminant multiple de celui de cette dernière, et que le quotient de ces déterminants est un carré, d'où il suit que, pour que deux formes puissent se contenir mutuellement, il faut nécessairement que leurs déterminants soient ou égaux ou opposés.

Réciproquement, si les déterminants de deux formes telles que (1) et (3) sont égaux ou opposés, et qu'en outre la première contienne la seconde, je dis que celle-ci contiendra la première. Pour le prouver, remarquons que l'hypothèse $D' = \pm D$, comparée à l'équation (5), donne celle-ci:

$$\alpha\delta - \beta\gamma = i^\nu, \tag{6}$$

les déterminants égaux à zéro étant toujours exclus. Si maintenant l'on résout les équations (2) par rapport à x' et y', on obtiendra les expressions:

$$x' = \frac{\delta}{i^\nu}x - \frac{\beta}{i^\nu}y, \quad y' = -\frac{\gamma}{i^\nu}x + \frac{\alpha}{i^\nu}y, \tag{7}$$

dont les quatre coefficients sont entiers, et qui, étant introduites dans la forme (3), la feront évidemment coïncider avec la forme (1), ce qu'il s'agissait de prouver.

Deux formes dont chacune contient l'autre, sont dites *équivalentes*. Quoique la relation mutuelle de deux formes, exprimée par cette désignation, puisse subsister aussi bien entre deux formes à déterminants opposés qu'entre deux formes dont les déterminants sont égaux, nous nous bornerons à considérer le dernier de ces deux cas. Il est en effet facile de voir que ces deux cas ne sont pas essentiellement différents, puisque, étant données deux formes qui répondent au premier, il suffit évidemment de multiplier les trois coefficients de l'une d'entre elles respectivement par 1, i, -1, pour que le groupe des deux formes rentre dans le second de ces deux cas.

La définition de l'équivalence ainsi restreinte, donne encore lieu à une nouvelle subdivision qu'il est essentiel de prendre en considération. Comme on a $D' = D$, et par suite en vertu de l'équation (5):

$$\alpha\delta - \beta\gamma = \pm 1 = \varepsilon, \tag{8}$$

nous pouvons avoir égard au signe dont l'unité est précédée dans cette équation. Nous dirons désormais que la substitution donnée par les formules (2), et qui change la forme (1) dans la forme équivalente (3), est *propre* ou *impropre*, suivant que le signe supérieur ou le signe inférieur a lieu dans l'équation (8). Observons d'abord que la substitution inverse (7) qui sert à revenir de la forme (3) à la forme (1) et qui, pour le cas qui nous occupe, se réduit à poser:

$$x' = \frac{\delta}{\varepsilon}x - \frac{\beta}{\varepsilon}y, \quad y' = -\frac{\gamma}{\varepsilon}x + \frac{\alpha}{\varepsilon}y,$$

sera toujours de même nom que la substitution directe (2). Il suffit, pour s'en assurer, de remplacer dans l'expression (8) les entiers α, β, γ, δ respectivement par $\frac{\delta}{\varepsilon}$, $-\frac{\beta}{\varepsilon}$, $-\frac{\gamma}{\varepsilon}$, $\frac{\alpha}{\varepsilon}$, ce qui changera cette expression en:

$$\frac{\alpha\delta - \beta\gamma}{\varepsilon^2} = \varepsilon.$$

Les deux substitutions étant de même nature quant à la distinction que nous venons de faire, on peut transporter la dénomination précédente au groupe des deux formes et appeler l'équivalence de ces formes propre ou impropre suivant que la valeur de ε, commune aux deux substitutions en question, est

$+1$ ou -1. Il n'est pas nécessaire pour notre objet de considérer l'équivalence impropre qui au reste se change toujours en équivalence propre, si dans l'une des formes on change le signe du coefficient moyen. En disant donc désormais que deux formes sont équivalentes, nous entendrons toujours qu'il s'agit de l'équivalence propre, ou autrement dit, qu'on peut passer de chacune de ces formes à l'autre, par une substitution telle que (2), où l'on a $\alpha\delta-\beta\gamma=1$. Pareillement, quand nous nous proposerons de découvrir toutes les transformations qui changent ces formes l'une dans l'autre, nous n'aurons en vue que celles qui satisfont à la condition précédente, et nous rejetterons toutes les transformations pour lesquelles on aurait $\alpha\delta-\beta\gamma=-1$. Comme dans ce qui va suivre, il sera le plus souvent inutile de désigner les indéterminées par des lettres particulières, nous conviendrons d'indiquer une forme telle que (1), ou une substitution telle que (2), par ces notations abrégées:

$$(a,\ b,\ c),\quad \begin{pmatrix}\alpha,&\beta\\ \gamma,&\delta\end{pmatrix}.$$

La notion de l'équivalence ainsi que nous venons de la fixer, donne lieu à ces théorèmes très simples:

I. Toute forme est équivalente à elle-même, puisqu'il est évident qu'elle ne varie pas, si on lui applique la substitution $\begin{pmatrix}1,&0\\ 0,&1\end{pmatrix}$.

II. Deux formes qui équivalent à une troisième, sont équivalentes entre elles. En effet, si la forme f, supposée équivalente à f', se transforme en celle-ci au moyen de la substitution $\begin{pmatrix}\alpha,&\beta\\ \gamma,&\delta\end{pmatrix}$, et si f' devient à son tour identique avec f'', au moyen de la substitution $\begin{pmatrix}\alpha',&\beta'\\ \gamma',&\delta'\end{pmatrix}$, on passera évidemment de f à f'', en faisant usage de la substitution unique $\begin{pmatrix}\alpha'',&\beta''\\ \gamma'',&\delta''\end{pmatrix}$, où l'on a:

$$\alpha''=\alpha\alpha'+\beta\gamma',\quad \beta''=\alpha\beta'+\beta\delta',$$
$$\gamma''=\gamma\alpha'+\delta\gamma',\quad \delta''=\gamma\beta'+\delta\delta',$$

et il ne reste plus qu'à prouver qu'on a $\alpha''\delta''-\beta''\gamma''=1$. Mais cette équation résulte sur-le-champ de l'équation identique:

$$\alpha''\delta''-\beta''\gamma''=(\alpha\delta-\beta\gamma)(\alpha'\delta'-\beta'\gamma'),$$

où l'on a par hypothèse, $\alpha\delta-\beta\gamma=1$ et $\alpha'\delta'-\beta'\gamma'=1$.

La substitution $\begin{pmatrix}\alpha'',&\beta''\\ \gamma'',&\delta''\end{pmatrix}$, qui produit le même effet que les deux substitutions $\begin{pmatrix}\alpha,&\beta\\ \gamma,&\delta\end{pmatrix}$, $\begin{pmatrix}\alpha',&\beta'\\ \gamma',&\delta'\end{pmatrix}$, employées l'une après l'autre, peut s'appeler convenablement une *substitution composée*, où il importe de remarquer que l'ordre des substitutions composantes ne peut pas être interverti.

III. Deux formes (a, b, c) et (a', b', c') étant supposées équivalentes, le plus grand diviseur commun des entiers a, b, c est le même que celui des entiers a', b', c', et la même égalité subsiste entre les deux groupes a, $2b$, c et a', $2b'$, c'.

En effet l'équivalence admise supposant une transformation telle que (2), et par suite les équations (4), on voit immédiatement que tout diviseur commun de a, b, c divise aussi a', b', c', et l'on arrive à un résultat semblable relativement aux groupes a, $2b$, c et a', $2b'$, c', si préalablement on suppose les deux membres de la seconde des équations (4) multipliés par 2. Un raisonnement analogue pouvant se faire en sens inverse, la proposition énoncée se trouve établie.

Nous observerons qu'il serait inutile de considérer des formes (a, b, c) pour lesquelles le plus grand diviseur commun σ de leurs coefficients a, b, c différerait de l'unité, puisque de pareilles formes ne sont évidemment que des formes du déterminant $\frac{D}{\sigma^2}$, affectées du facteur entier σ. Nous supposerons donc toujours a, b, c libres de tout diviseur commun; cela étant, le plus grand diviseur commun de a, $2b$, c, que nous désignerons constamment par ω, ne peut avoir que l'une des trois valeurs 1, $1+i$ ou 2, ce qui donne lieu à diviser les formes quadratiques en trois *espèces* appelées, suivant l'ordre des cas énoncés, la *première*, la *seconde* ou la *troisième*, de sorte que des formes équivalentes sont toujours de même espèce.

§. 11.

Relativement à l'équivalence des formes, il se présente deux questions principales à résoudre. Étant données deux formes ayant le même déterminant et appartenant à la même espèce, on peut demander 1° si ces formes sont équivalentes ou non, et l'équivalence supposée reconnue, on peut se proposer 2° d'assigner toutes les substitutions par lesquelles ces formes se transforment

l'une dans l'autre. Nous ne sommes pas pour le moment en mesure d'aborder la première de ces deux questions; mais nous pouvons traiter dès à présent la seconde, en la posant comme il suit:

„Étant données deux formes équivalentes ainsi qu'une transformation de la première dans la seconde, trouver toutes les transformations qui produisent le même effet."

I. La question énoncée peut se réduire à une autre plus simple et qui n'est au fond qu'une question particulière, mais de même nature que la proposée. Cette question particulière consiste à assigner toutes les substitutions par lesquelles une forme donnée se change en elle-même ou, autrement dit, reste invariable quant à ses coefficients. Pour le prouver, soit:

$$(1) \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

la substitution donnée par laquelle la première f des formes données se change dans la seconde f'. Si maintenant l'on désigne par:

$$(2) \qquad \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$$

une substitution quelconque qui change en elle-même la forme f, il résulte du paragraphe précédent (II.), que par la substitution composée des précédentes, rangées dans l'ordre (2), (1):

$$(3) \qquad \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$$

où l'on a:

$$(4) \qquad \begin{cases} \alpha' = \alpha\lambda+\gamma\mu, & \beta' = \beta\lambda+\delta\mu, \\ \gamma' = \alpha\nu+\gamma\varrho, & \delta' = \beta\nu+\delta\varrho, \end{cases}$$

f se change en f'. Cela posé, je dis que, si dans les équations (4) on introduit successivement toutes les substitutions (2), on obtiendra toutes les transformations possibles de f en f', et de plus que chacune d'entre elles ne se présentera ainsi qu'une seule fois. Pour prouver d'abord ce dernier point, il suffit d'observer que les équations (4), en y considérant λ, μ, ν, ϱ comme des inconnues, donnent ces valeurs complètement déterminées:

$$\lambda = \delta\alpha'-\gamma\beta', \quad \mu = \alpha\beta'-\beta\alpha',$$
$$\nu = \delta\gamma'-\gamma\delta', \quad \varrho = \alpha\delta'-\beta\gamma'.$$

Reste à faire voir qu'il n'existe aucune transformation $\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$ de f en f', qui

ne soit contenue dans les formules (4), en y considérant λ, μ, ν, ϱ généralement comme les coefficients des substitutions (2) définies plus haut.

Comme la résolution des équations en question a donné des valeurs entières, et que d'un autre côté, on conclut de l'équation identique:

$$(\lambda\varrho-\mu\nu)(\alpha\delta-\beta\gamma) = \alpha'\delta'-\beta'\gamma',$$

combinée avec celles-ci:

$$\alpha\delta-\beta\gamma = 1, \quad \alpha'\delta'-\beta'\gamma' = 1,$$

que l'on a aussi $\lambda\varrho-\mu\nu = 1$, tout revient évidemment à s'assurer que la substitution $\begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$ formée avec les entiers λ, μ, ν, ϱ, donnés par la résolution effectuée, est en effet l'une de celles qui changent la forme f en elle-même. Désignant pour un instant par χ la forme encore inconnue dans laquelle f se transforme par la substitution dont il s'agit, on voit d'abord que χ devient f' au moyen de la substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, et que par suite f' se change en χ au moyen de la substitution inverse $\begin{pmatrix} \delta, & -\beta \\ -\gamma, & \alpha \end{pmatrix}$. Mais d'un autre côté, cette dernière change aussi f' en f, d'où il suit qu'on a $f = \chi$, ce qu'il s'agissait de prouver.

II. Tout se réduit donc à découvrir toutes les substitutions $\begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$ par lesquelles la forme donnée $f = (a, b, c)$ se change en elle-même. Pour résoudre cette question, il s'agira d'assigner toutes les valeurs entières λ, μ, ν, ϱ telles qu'en remplaçant dans l'expression:

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

ou ce qui revient au même, a différant de zéro, dans celle-ci:

$$a(ax^2+2bxy+cy^2),$$

x et y respectivement par $\lambda x+\mu y$ et $\nu x+\varrho y$, cette expression reste identiquement la même. Nous ferons d'abord abstraction de la condition $\lambda\varrho-\mu\nu = 1$, toujours exigée dans les transformations que nous employons, et de plus nous considérerons λ, μ, ν, ϱ comme susceptibles de valeurs rationnelles quelconques. La question ainsi généralisée une fois résolue, il sera facile d'avoir égard aux conditions jusque-là négligées.

L'expression dont il s'agit, se décompose en ces deux facteurs linéaires:

$$(ax+(b+\sqrt{D})y), \quad (ax+(b-\sqrt{D})y),$$

où nous entendons par $\sqrt{D}$ une valeur déterminée, mais qui peut être arbitrairement choisie parmi les deux valeurs opposées que comporte généralement un radical carré. La substitution indiquée change le produit précédent en celui-ci:

$$[(a\lambda+bv+v\sqrt{D})x+(a\mu+b\varrho+\varrho\sqrt{D})y][(a\lambda+bv-v\sqrt{D})x+(a\mu+b\varrho-\varrho\sqrt{D})y].$$

Désignant pour un instant les huit coefficients de x et y par des lettres particulières, en posant:

$$p=a,\quad q=b+\sqrt{D},\quad \ldots,\quad p'=a\lambda+bv+v\sqrt{D},\quad q'=a\mu+b\varrho+\varrho\sqrt{D},\quad \ldots$$

l'égalité qu'il s'agit d'établir entre ces deux produits, s'écrira ainsi:

$$(px+qy)(rx+sy)=(p'x+q'y)(r'x+s'y).$$

Or, les quatre constantes p, q, r, s données étant évidemment toutes différentes de zéro, les conditions nécessaires et suffisantes pour l'identité de ces deux expressions exigent évidemment qu'on ait 1° $\frac{p'r'}{pr}=1$, et en outre 2° l'un ou l'autre de ces deux systèmes d'équations:

$$\frac{p'}{p}=\frac{q'}{q},\quad \frac{r'}{r}=\frac{s'}{s};\quad \frac{r'}{p}=\frac{s'}{q},\quad \frac{p'}{r}=\frac{q'}{s}.$$

Si maintenant, suivant qu'il s'agit du premier ou du second cas, on pose:

$$\frac{p'}{p}=\varphi+\psi\sqrt{D},\quad \text{ou}\quad \frac{r'}{p}=\varphi+\psi\sqrt{D},$$

où nous supposons φ et ψ rationnels, ce qui est permis, les coefficients p, q, ... ne renfermant que la seule irrationnelle $\sqrt{D}$, on aura respectivement:

$$\frac{r'}{r}=\varphi-\psi\sqrt{D},\quad \text{ou}\quad \frac{p'}{r}=\varphi-\psi\sqrt{D},$$

et l'équation $\frac{p'r'}{pr}=1$, commune aux deux cas, prendra la forme:

$$\varphi^2-D\psi^2=1. \tag{5}$$

Quant à l'autre condition, exprimée par deux équations, il suffit d'écrire pour l'un et l'autre cas, la première de ces deux équations, celle-ci comprenant virtuellement la seconde qui n'en diffère que par le signe du radical.

On aura donc suivant les deux cas:

$$\frac{a\lambda+bv+v\sqrt{D}}{a}=\frac{a\mu+b\varrho+\varrho\sqrt{D}}{b+\sqrt{D}}=\varphi+\psi\sqrt{D},$$

ou:

$$\frac{a\lambda+bv-v\sqrt{D}}{a}=\frac{a\mu+b\varrho-\varrho\sqrt{D}}{b+\sqrt{D}}=\varphi+\psi\sqrt{D}.$$

En égalant séparément dans ces formules les parties rationnelles et les coefficients de $\sqrt{D}$, et résolvant ensuite les équations que l'on obtient ainsi, par rapport à λ, μ, ν, ϱ, on trouve sans indétermination et suivant les deux cas:

$$\lambda=\varphi-b\psi,\quad \mu=-c\psi,\quad v=a\psi,\quad \varrho=\varphi+b\psi,$$

$$\lambda=\varphi+b\psi,\quad \mu=\frac{2b}{a}\varphi+\frac{b^2+D}{a}\psi,\quad v=-a\psi,\quad \varrho=-\varphi-b\psi.$$

On voit donc que toutes les valeurs rationnelles λ, μ, ν, ϱ qui satisfont à la condition d'invariabilité exigée, sont données par ces deux systèmes de formules très simples, où φ et ψ désignent généralement toutes les valeurs rationnelles simultanées compatibles avec l'équation (5).

Il s'agit maintenant d'avoir égard aux conditions que nous avons négligées, et dont l'une est exprimée par l'équation $\lambda\varrho-\mu\nu=1$. La substitution des expressions précédentes montre, par un calcul très simple, que le premier système y satisfait, tandis que relativement au second, on trouve $\lambda\varrho-\mu\nu=-1$. Ce dernier devant ainsi être rejeté, il ne reste plus qu'à examiner sous quelles conditions les expressions de λ, μ, ν, ϱ, données par le premier système, sont entières. Il est facile de voir que cela exige que les produits $\omega\varphi$, $\omega\psi$ (ω désignant toujours le plus grand diviseur commun de a, $2b$, c) soient des entiers. En effet, comme des équations précédentes on conclut facilement:

$$v=\frac{a}{\omega}\omega\psi,\quad \varrho-\lambda=\frac{2b}{\omega}\omega\psi,\quad -\mu=\frac{c}{\omega}\omega\psi,$$

on voit que, si le produit $\omega\psi$, réduit à sa plus simple expression, avait un dénominateur autre que l'unité, ce dénominateur serait diviseur commun des entiers $\frac{a}{\omega}$, $\frac{2b}{\omega}$, $\frac{c}{\omega}$, qui n'admettent pas de pareil diviseur. La conclusion obtenue pour $\omega\psi$, s'étend à $\omega\varphi$, au moyen de l'équation $\omega\varphi=\omega\lambda+b\omega\psi$. Mais la réciproque a également lieu, et il est facile de s'assurer que, si l'on fait usage de valeurs de φ et ψ, telles que $\varphi=\frac{t}{\omega}$, $\psi=\frac{u}{\omega}$, où t et u sont des entiers, et satisfaisant à l'équation (5), il en résultera des valeurs entières pour λ, μ, ν, ϱ. Pour le voir, substituons ces expressions dans les équations obtenues plus haut; il viendra ainsi:

$$t^2-Du^2=\omega^2, \tag{6}$$

$$\lambda=\frac{t-bu}{\omega},\quad \mu=-\frac{cu}{\omega},\quad \nu=\frac{au}{\omega},\quad \varrho=\frac{t+bu}{\omega}. \tag{7}$$

Relativement à μ et ν il n'y a rien à prouver, a et c étant divisibles par ω. Quant à λ et ϱ, comme leur différence $\varrho-\lambda=\frac{2bu}{\omega}$ est évidemment un entier, tout revient à faire voir que l'une des expressions $\frac{t+bu}{\omega}$, $\frac{t-bu}{\omega}$ est pareillement un entier. Mais de l'équation à laquelle t et u sont supposés satisfaire, mise sous la forme:

$$\frac{(t+bu)(t-bu)}{\omega^2}=1-\frac{ac}{\omega^2}u^2,$$

on conclut que le produit des deux facteurs $t+bu$ et $t-bu$ est un multiple de ω^2, d'où et de ce que ω ne renferme pas plusieurs nombres premiers différents, il suit que l'un au moins des deux facteurs est divisible par ω, ce qu'il s'agissait de faire voir. Les formules (7), en y substituant successivement toutes les solutions entières de l'équation (6), donneront donc toutes les transformations $\begin{pmatrix}\lambda, & \mu\\ \nu, & \varrho\end{pmatrix}$ de la forme (a, b, c) en elle-même, et il est d'ailleurs évident que chacune de ces transformations ne se présentera qu'une seule fois, car on voit par les deux premières des formules en question qu'à des valeurs déterminées λ et μ répondent toujours des valeurs également déterminées pour t et u.

Remarque. L'analyse qui vient de nous conduire de la manière la plus simple à la solution de la question proposée, a en outre l'avantage de montrer clairement ce qui distingue les transformations propres, les seules que nous ayons à considérer, de celles qu'on appelle impropres. On voit en effet que, s'il s'agit des transformations d'une forme en elle-même, les premières sont celles pour lesquelles les deux expressions linéaires dont la forme donnée peut être considérée comme le produit, restent l'une et l'autre invariables, abstraction faite des facteurs constants qu'elles acquièrent; tandis que les transformations impropres qui n'existent toutefois que pour des formes d'une nature particulière et répondent alors au second des deux systèmes d'équations obtenus plus haut, ont pour effet d'échanger entre elles les deux expressions linéaires dont il s'agit. La même remarque s'étend aux substitutions qui ne reproduisent pas la forme donnée, et la changent au contraire en une autre équivalente, mais distincte. En combinant ce qui précède avec le résultat du numéro précédent, il est facile de s'assurer que, si après avoir décomposé en facteurs linéaires la forme primitive et celle qui en dérive, on considère comme correspondants ceux de leurs facteurs qui contiennent le radical $\sqrt{D}$ avec le même signe, toute transformation

de la première dans la seconde sera propre ou impropre, suivant que les facteurs linéaires se changent en leurs correspondants ou non.

III. Si maintenant nous substituons les expressions (7) dans les équations (4), ces dernières prendront la forme:

$$\alpha'=\frac{\alpha t-(b\alpha+c\gamma)u}{\omega},\quad \beta'=\frac{\beta t-(b\beta+c\delta)u}{\omega},$$
$$\gamma'=\frac{\gamma t+(a\alpha+b\gamma)u}{\omega},\quad \delta'=\frac{\delta t+(a\beta+b\delta)u}{\omega}.$$

Au moyen de ces équations, on pourra donc, une première transformation $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ d'une forme (a, b, c) en une autre (a', b', c') équivalente étant donnée, en déduire toutes les transformations possibles, en supposant d'ailleurs que la solution complète de l'équation (6) soit également connue.

§. 12.

Lorsque la forme:

(1) $$ax^2+2bxy+cy^2,$$

dont nous désignerons le déterminant par D, et dont nous considérerons d'abord les coefficients a, b, c comme susceptibles d'un diviseur commun quelconque, obtient une valeur déterminée m, en y attribuant des valeurs particulières r et s aux indéterminées x et y, nous dirons que l'entier m est *représenté* par la forme donnée. Nous supposerons toujours, si nous n'avertissons expressément du contraire, que les entiers déterminés r et s sont premiers entre eux. Sous cette restriction, m diffère toujours de zéro; car il est facile de voir que l'hypothèse de $m=0$ suppose $r=0$, $s=0$, valeurs dont un nombre quelconque est diviseur commun. Il s'agit maintenant de déduire les conséquences qui résultent d'une représentation telle que nous venons de la définir. On voit tout d'abord que, si l'on choisit deux entiers ϱ et σ qui satisfassent à l'équation:

(2) $$r\sigma-s\varrho=1,$$

évidemment résoluble, et que l'on applique ensuite la substitution $\begin{pmatrix}r, & \varrho\\ s, & \sigma\end{pmatrix}$ à la forme (1), elle se changera en cette autre équivalente:

(3) $$\left(m, n, \frac{n^2-D}{m}\right),$$

où:

$$(4) \qquad m = ar^2+2brs+cs^2, \qquad (5) \qquad n = ar\varrho+b(r\sigma+s\varrho)+cs\sigma.$$

Le troisième coefficient de la forme (3) étant entier, on conclut que n satisfait à la congruence:

$$(6) \qquad z^2 \equiv D \pmod{m}.$$

On voit donc qu'une condition nécessaire, quoique nullement suffisante, pour que m puisse être représenté par la forme (1), consiste en ce que D doit être résidu quadratique relativement au module m, et que d'une représentation supposée connue, on peut toujours déduire une racine n de la congruence (6), en substituant une solution quelconque de l'équation (2) dans la formule (5). Comme l'équation (2) admet toujours une infinité de solutions, il est naturel de rechercher comment n varie, lorsqu'on passe d'une de ces solutions à une autre. Pour y parvenir, soit ϱ_0, σ_0 une solution particulière et soit n_0 la valeur correspondante de n; si maintenant l'on introduit dans la formule (5) la solution générale $\varrho = \varrho_0+r\xi$, $\sigma = \sigma_0+s\xi$, où ξ désigne un entier complexe arbitraire, on aura pour la valeur générale de n:

$$n = n_0+m\xi,$$

d'où l'on conclut que les valeurs en nombre infini dont n est susceptible, forment une racine unique de la congruence (6), puisqu'elles sont toutes congrues entre elles suivant le module m, et l'on doit ajouter que l'arbitraire ξ peut toujours être choisie de manière à faire coïncider n avec l'une quelconque des valeurs en nombre infini, que l'on peut considérer comme autant d'expressions différentes d'une même racine de la congruence en question.

Cela étant, nous dirons désormais d'une manière abrégée, que la représentation de l'entier m par la forme (1), pour laquelle on a $x = r$, $y = s$, *appartient à la valeur n de l'expression* $\sqrt{D}$ (mod. m), que l'on déduit de l'équation (5), en y substituant deux quelconques des entiers ϱ et σ qui satisfont à l'équation (2).

La conclusion que nous venons d'obtenir et qui consiste en ce que la représentation $x = r$, $y = s$, appartenant à la valeur n de $\sqrt{D}$ (mod. m), a toujours pour conséquence l'équivalence des formes (1) et (3), a également lieu en sens inverse. En effet si, supposant l'équivalence de ces dernières, nous

désignons par $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ l'une quelconque des substitutions par lesquelles la première se change dans la seconde, nous aurons évidemment les équations (2), (4) et (5), dont la seconde fournit une représentation qui, en vertu des deux autres, appartient évidemment à la valeur n de $\sqrt{D}$ (mod. m). Je dis de plus qu'il n'y a aucune représentation satisfaisant à la condition exigée, qui ne puisse s'obtenir ainsi au moyen d'une transformation de la forme (1) en (3), et que chaque représentation se présentera une seule fois, c'est-à-dire qu'elle proviendra toujours d'une transformation unique et déterminée. Pour prouver d'abord le premier point, remarquons qu'en vertu de la définition même de la valeur n à laquelle une représentation est dite appartenir, supposer l'existence d'une telle représentation pour l'entier m, c'est supposer les équations (4), (2) et (5), desquelles il résulte sur-le-champ que la forme (1), au moyen de la substitution $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$, se change en une autre du même déterminant D, et dont les deux premiers coefficients sont m et n. On conclut de là que le troisième coefficient est $\frac{n^2-D}{m}$, et que la substitution indiquée est en effet l'une de celles par lesquelles la forme (1) se change en (3). Quant au second point, il est évident que pour l'établir, on n'a qu'à faire voir que les deux équations (2) et (5), en y considérant r et s comme donnés, ne sauraient être satisfaites par plus d'un couple de valeurs de ϱ et de σ. Mais cela est manifeste, puisque les équations dont il s'agit, étant résolues, donnent ces valeurs complètement déterminées:

$$\varrho = \frac{(n-b)r-cs}{m}, \qquad \sigma = \frac{ar+(n+b)s}{m}.$$

On voit par ce qui précède, que pour que l'entier m puisse être représenté par la forme (1) de manière que ces représentations appartiennent à une valeur donnée n de l'expression $\sqrt{D}$ (mod. m), il faut et il suffit que les formes (1) et (3) soient équivalentes entre elles. Cette condition supposée remplie, on n'aura plus qu'à chercher toutes les substitutions $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ par lesquelles la forme (1) se change en (3), et l'on posera $x = r$, $y = s$. Or, les substitutions dont il s'agit ayant été exprimées dans le paragraphe précédent en fonction de l'une quelconque d'entre elles, on en conclut, si nous revenons maintenant à l'hypothèse que les coefficients de la forme (1) n'ont pas de di-

viseur commun, que les représentations cherchées sont toutes comprises dans ces deux équations:

$$x = \frac{at-(b\alpha+c\gamma)u}{\omega}, \quad y = \frac{\gamma t+(a\alpha+b\gamma)u}{\omega},$$

où α, γ appartiennent à une substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ arbitrairement choisie parmi celles qui transforment la forme (1) en (3), et où t et u satisfont généralement à l'équation $t^2-Du^2=\omega^2$. Il est bon de remarquer que le résultat est maintenant tout-à-fait indépendant de la forme (3) que nous avons eu à considérer pour l'obtenir. En effet, comme $x=\alpha$, $y=\gamma$ est évidemment une représentation particulière comprise dans les formules précédentes et qui s'en déduit en supposant $t=\omega$, $u=0$, on peut l'énoncer en disant que les équations que nous venons d'obtenir, expriment toutes les représentations appartenant à une même valeur de $\sqrt{D}$ (mod. m), en fonction de l'une quelconque d'entre elles.

§. 13.

Les questions que nous avons traitées dans les paragraphes précédents, s'étant trouvées dépendre de la solution de l'équation indéterminée:

$$t^2-Du^2=\omega^2,$$

il est temps de nous occuper de cette dernière. Mais pour ne pas donner une étendue démesurée au présent Mémoire, nous considérerons exclusivement le cas où $\omega=1$, cas qui est celui des formes de première espèce; et nous laisserons au lecteur qui voudrait s'exercer sur ces matières, le soin de chercher les modifications assez légères qu'il faudrait apporter aux recherches suivantes pour les rendre applicables aux formes des deux autres espèces.

La théorie de l'équation:

$$t^2-Du^2=1$$

peut se déduire d'un lemme dont voici l'énoncé:

„a désignant un nombre complexe irrationnel donné, on pourra toujours trouver une infinité d'entiers complexes simultanés x et y, tels qu'on ait:

$$N(x-ay)<\frac{4}{N(y)}.“$$

Observons d'abord que, si l'on satisfait à la condition du lemme par le système

x, y, on y satisfera aussi par $i^\varepsilon x$, $i^\varepsilon y$. Comme dans l'application que nous aurons à faire du lemme, il importe de ne pas employer simultanément des systèmes dérivant ainsi l'un de l'autre, nous éviterons cet inconvénient, en ne considérant deux systèmes comme distincts qu'autant que les valeurs de $N(x-ay)$ qui s'y rapportent, sont différentes entre elles. Il est en effet évident que pour deux systèmes comme ceux dont il vient d'être question, l'expression $N(x-ay)$ a toujours la même valeur. On voit encore que la condition du lemme se trouve remplie lorsque, x étant quelconque, on a $y=0$; mais nous ferons pareillement abstraction de ce cas, de sorte que $x-ay$ aura toujours une valeur irrationnelle et par conséquent différente de zéro.

Pour démontrer notre lemme, commençons par faire voir qu'on peut toujours trouver deux entiers x et y, qui satisfaisant à l'inégalité proposée, soient en outre tels que l'on ait:

$$N(x-ay)<A,$$

A désignant une quantité positive arbitrairement choisie. Soit à cet effet n un entier positif pour lequel on ait $A>\frac{1}{2n^2}$, et désignons par η l'un quelconque des entiers complexes dont les deux parties, et j'entends par là la partie réelle et le coefficient de i qui entrent dans une expression complexe quelconque, soient comprises dans la suite:

$$-n,\ -(n-1),\ \ldots,\ -1,\ 0,\ +1,\ \ldots,\ n-1,\ n.$$

Relativement à chacun des entiers η dont le nombre est évidemment égal à $(2n+1)^2$, déterminons l'entier correspondant ξ tel que les deux parties de l'expression:

$$\xi-a\eta$$

obtiennent des valeurs non-négatives et inférieures à l'unité. Cela supposé, il est évident que, si l'on désigne par:

$$p\frac{1}{2n},\quad q\frac{1}{2n}$$

les plus grands multiples de $\frac{1}{2n}$, respectivement contenus dans les deux parties dont il s'agit, les entiers réels p et q seront l'un et l'autre compris dans la suite:

$$0,\ 1,\ 2,\ \ldots,\ 2n-1.$$

Or, comme avec de pareils entiers on ne peut former qu'un nombre de combinaisons distinctes, exprimé par $(2n)^2$, tandis que celui des expressions $\xi - a\eta$ est $(2n+1)^2$, on voit que l'une au moins des combinaisons p, q devra se reproduire. Soient donc:

$$\xi - a\eta, \quad \xi' - a\eta'$$

les deux expressions ou deux des expressions pour lesquelles cette circonstance se présente; il est évident qu'en formant la différence de ces expressions, on obtiendra, en posant:

$$\xi - \xi' = x, \quad \eta - \eta' = y,$$

une nouvelle expression:

$$x - ay,$$

dans laquelle l'entier y sera évidemment différent de zéro, et dont les deux parties seront, abstraction faite du signe, inférieures à $\frac{1}{2n}$, de sorte qu'on aura:

$$N(x-ay) < \frac{1}{2n^2}, \quad \text{et par suite} \quad N(x-ay) < A,$$

ce qui coïncide avec la seconde des conditions posées plus haut. Pour prouver que l'expression $N(x-ay)$ satisfait aussi à l'autre condition qui est celle du lemme, observons que, les deux parties de $y = \eta - \eta'$ ayant évidemment des valeurs numériques non-supérieures à $2n$, on a l'inégalité $N(y) \leqq 8n^2$, dont la comparaison avec celle que nous venons d'obtenir, donne:

$$N(x-ay) < \frac{4}{N(y)},$$

conformément à l'énoncé.

Ayant ainsi prouvé qu'on peut toujours trouver un couple x, y qui, en même temps qu'il s'accorde avec la condition de l'énoncé, satisfasse à l'inégalité $N(x-ay) < A$, où A est d'une petitesse arbitraire, il est facile d'en conclure la vérité du lemme. Il suffit pour cela d'observer que, quel que soit le nombre des systèmes qu'on suppose déjà connus, on trouvera un nouveau système distinct des premiers si, appliquant le procédé que nous venons d'exposer, on y suppose A égal à la plus petite des valeurs que l'expression $N(x-ay)$ présente dans les systèmes antérieurement obtenus.

Remarquons maintenant que, relativement à deux quantités complexes quelconques r et s, on a l'inégalité connue et d'ailleurs facile à vérifier:

$$\sqrt{N(r+s)} \leqq \sqrt{N(r)} + \sqrt{N(s)},$$

les radicaux étant supposés pris positivement. Supposant $r = x - ay$, $s = 2ay$, il viendra:

$$\sqrt{N(x+ay)} \leqq \sqrt{N(x-ay)} + \sqrt{N(2ay)},$$

inégalité qui au moyen de celle du lemme, mise sous la forme:

$$\sqrt{N(x-ay)} < \frac{2}{\sqrt{N(y)}},$$

se change en:

$$\sqrt{N(x+ay)} < 2\sqrt{N(ay)} + \frac{2}{\sqrt{N(y)}}.$$

Ces deux dernières étant multipliées entre elles, donnent:

$$\sqrt{N(x^2-a^2y^2)} < 4\sqrt{N(a)} + \frac{4}{N(y)}$$

et par suite, y étant un entier complexe différent de zéro de sorte que $N(y) \geqq 1$:

$$\sqrt{N(x^2-a^2y^2)} < 4(\sqrt{N(a)}+1).$$

On voit donc que pour tous les couples d'entiers qui satisfont au lemme et dont le nombre est infini, $N(x^2-a^2y^2)$ reste au-dessous d'une limite invariable. Appliquons ce résultat au cas où $a = \sqrt{D}$, D étant un entier complexe non-carré et le radical désignant une racine déterminée qui restera toujours la même dans ce qui va suivre. Comme dans cette hypothèse, $x^2 - a^2y^2 = x^2 - Dy^2$ est un entier complexe et qu'il n'y a qu'un nombre fini d'entiers dont la norme soit inférieure à une limite donnée, il faudra nécessairement que l'expression $x^2 - Dy^2$ obtienne une infinité de fois une même valeur l qui sera évidemment différente de zéro, y n'étant pas nul. L'équation $x^2 - Dy^2 = l$ étant ainsi satisfaite par un nombre infini de systèmes x, y, on voit encore que parmi ces systèmes il s'en trouvera nécessairement un nombre illimité, pour lesquels les valeurs tant de x que de y présentent des différences multiples de l. Soient:

$$x^2 - Dy^2 = l, \quad x'^2 - Dy'^2 = l$$

deux équations pour lesquelles cela arrive, de sorte qu'on ait simultanément $x \equiv x'$, $y \equiv y'$ (mod. l). Le produit de ces équations étant:

$$(xx' - Dyy')^2 - D(xy' - yx')^2 = l^2,$$

et $xy' - yx'$ étant divisible par l en vertu des conditions supposées, $xx' - Dyy'$ sera aussi un multiple de l, de sorte qu'en divisant par l^2, on aura:

$$t^2 - Du^2 = 1,$$

les entiers t et u étant donnés par les formules:

$$t = \frac{xx' - Dyy'}{l}, \quad u = \frac{xy' - yx'}{l}.$$

Nous ajouterons qu'il ne saurait arriver qu'on eût $u = 0$, car il est facile de se convaincre que cela supposerait $x' = \pm x$, $y' = \pm y$, de sorte que les systèmes x, y et x', y' ne seraient pas distincts.

Étant ainsi assuré que l'équation $t^2 - Du^2 = 1$ est toujours résoluble sans qu'on suppose $u = 0$, on parviendra nécessairement à une solution si l'on attribue successivement à u toutes les valeurs entières dont les normes forment la suite croissante des entiers positifs susceptibles d'être décomposés en deux carrés, jusqu'à ce que l'on tombe sur une valeur de u pour laquelle Du^2+1 soit égal à un carré. Cette simple possibilité suffit pour notre objet. Il existe un algorithme assez expéditif et analogue à celui des fractions continues, au moyen duquel on peut obtenir toutes les solutions de l'équation proposée ou plutôt celle de ces solutions, que l'on doit considérer comme fondamentale et dont les autres se déduisent facilement; mais comme l'exposition de cet algorithme exigerait de longs détails qui ne sont nullement nécessaires pour le but que nous avons en vue, nous ne nous en occuperons pas ici.

§. 14.

La possibilité de l'équation:

$$t^2 - Du^2 = 1 \tag{1}$$

ayant été établie dans le paragraphe précédent, il s'agira maintenant de découvrir le lien qui existe entre ses solutions en nombre infini. C'est à quoi nous parviendrons par les considérations suivantes.

I. Observons d'abord que la double solution évidente $t = \pm 1$, $u = 0$ est la seule pour laquelle l'une des indéterminées soit égale à zéro. Car il est manifeste que l'hypothèse $t = 0$ est inadmissible, D n'étant pas un carré. Pour cette solution on a $N(t+u\sqrt{D}) = 1$, et je dis de plus qu'elle est la seule pour laquelle cette équation ait lieu. En effet, comme les expressions $N(t+u\sqrt{D})$, $N(t-u\sqrt{D})$ ont toujours des valeurs réciproques l'une de l'autre, puisque l'on a:

$$N(t+u\sqrt{D})N(t-u\sqrt{D}) = N(t^2 - Du^2) = 1,$$

la condition précédente est équivalente à celle-ci:

$$N(t+u\sqrt{D}) + N(t-u\sqrt{D}) = 2.$$

Si maintenant l'on remarque que, r et s étant des quantités complexes quelconques, on a identiquement:

$$N(r+s) + N(r-s) = 2N(r) + 2N(s),$$

cette dernière pourra prendre la forme:

$$N(t) + N(u)N(\sqrt{D}) = 1.$$

Or, $N(\sqrt{D})$ étant une quantité égale ou supérieure à l'unité, cette équation exige évidemment que l'on ait $u = 0$, ou $t = 0$ lorsque $N(D) = 1$; mais la dernière hypothèse ne pouvant avoir lieu, l'assertion avancée se trouve justifiée.

II. Je dis en second lieu que, si pour deux solutions t, u et t', u' on a $N(t'+u'\sqrt{D}) = N(t+u\sqrt{D})$, ces deux solutions sont ou identiques ou opposées, de sorte que $t' = \pm t$, $u' = \pm u$, les signes se correspondant. En effet il est clair que de deux solutions quelconques t, u et t', u' on peut en déduire une troisième au moyen de l'équation:

$$\frac{t'+u'\sqrt{D}}{t+u\sqrt{D}} = \tau + v\sqrt{D},$$

dans laquelle il faut égaler séparément les parties rationnelles et les coefficients de $\sqrt{D}$, ce qui donne:

$$\tau = tt' - Duu', \qquad v = tu' - ut'.$$

Comme, relativement à cette nouvelle solution, on a:

$$N(\tau + v\sqrt{D}) = \frac{N(t'+u'\sqrt{D})}{N(t+u\sqrt{D})} = 1,$$

et par suite $\tau = \pm 1$, $v = 0$, on conclut $t' = \pm t$, $u' = \pm u$, ce qu'il s'agissait de prouver.

III. Si l'on excepte la double solution $t = \pm 1$, $u = 0$, les solutions de l'équation (1) existent toujours par groupes de quatre, les indéterminées pouvant être prises avec un signe arbitraire. Il est évident que relativement à un pareil groupe, l'expression $t+u\sqrt{D}$ a quatre valeurs distinctes exprimées par $\pm\chi$, $\pm\frac{1}{\chi}$, χ désignant l'une quelconque d'entre elles, tandis que

$N(t+u\sqrt{D})$ ne présente que ces deux valeurs distinctes: $N(\chi)$, $N\left(\frac{1}{\chi}\right)$, réciproques l'une de l'autre. L'expression $N(t+u\sqrt{D})$ n'ayant qu'une valeur unique supérieure à l'unité pour chaque groupe, cette valeur pourra servir à caractériser ce groupe et à le distinguer de tous les autres, comme cela résulte du numéro précédent où l'on a vu que la supposition $N(t+u\sqrt{D}) = N(t'+u'\sqrt{D})$ ne peut avoir lieu que pour des solutions identiques ou opposées, c'est-à-dire appartenant au même groupe. Cela posé, nous appellerons *groupe fondamental* celui pour lequel la valeur de $N(t+u\sqrt{D})$, toujours supposée supérieure à l'unité, est moindre que la valeur analogue relative à tout autre groupe. Si maintenant l'on remarque que, la variable positive ϱ étant supposée croître à partir de $\varrho = 1$, la fonction $\varrho + \frac{1}{\varrho}$ croîtra également à partir de la valeur 2, on voit que la définition précédente revient à dire que le groupe fondamental est celui pour lequel l'expression:

$$N(t+u\sqrt{D}) + \frac{1}{N(t+u\sqrt{D})} = N(t+u\sqrt{D}) + N(t-u\sqrt{D}) = 2N(t) + 2N(u)N(\sqrt{D})$$

a la plus petite valeur supérieure à 2. Sous cette forme, la définition, quoique la même au fond, a l'avantage d'être indépendante de la supposition $N(t+u\sqrt{D}) > 1$, l'expression précédente ayant évidemment la même valeur pour chacune des quatre solutions formant un même groupe. Il est actuellement facile d'indiquer une méthode propre à faire découvrir le groupe fondamental, en supposant toujours qu'il s'agisse de simples possibilités et nullement d'une opération commode sous le rapport du calcul pratique. Ayant trouvé une première solution t, u, et déterminé la valeur correspondante de $N(t+u\sqrt{D})$, désignée par b, tout revient à voir quels sont parmi les couples d'entiers t et u, tels qu'on ait:

$$1 < N(t) + N(u)N(\sqrt{D}) \leqq \tfrac{1}{2}\left(b + \frac{1}{b}\right),$$

et qui sont évidemment en nombre fini, ceux qui, satisfaisant à l'équation (1), donnent la plus petite valeur à l'expression qui vient d'être écrite. Les quatre couples qui remplissent ces conditions, coïncident avec les quatre solutions du groupe cherché.

Il nous reste à faire voir comment de l'une des solutions de ce groupe l'on peut déduire toutes les solutions de la proposée. Quoique cela puisse se

faire au moyen de l'une quelconque d'entre elles, nous conviendrons, pour éviter des distinctions tout-à-fait inutiles, de nous servir constamment de l'une des deux solutions opposées pour lesquelles on a $N(t+u\sqrt{D}) > 1$. Nous désignerons par T, U celle des solutions fondamentales que nous emploierons et nous poserons:

$$N(T+U\sqrt{D}) = \sigma,$$

la quantité $\sigma > 1$ devant se présenter souvent dans ce qui suivra.

IV. Cela posé, je dis que toutes les solutions de l'équation (1) sont données par la formule:

$$t+u\sqrt{D} = \pm(T+U\sqrt{D})^n, \tag{2}$$

où il faut employer successivement chacun des deux signes et attribuer à l'exposant n toutes les valeurs entières depuis $-\infty$ jusqu'à ∞, et de plus, que chaque solution est contenue d'une seule manière dans cette équation, c'est-à-dire qu'elle répond toujours à un signe et à un exposant déterminés. Il est sans doute inutile d'ajouter que pour faire usage de la formule (2), il faut égaler séparément les parties rationnelles et les coefficients de $\sqrt{D}$, après avoir développé le second membre, mis préalablement sous la forme $\pm(T-U\sqrt{D})^{-n}$, lorsque n est négatif.

1°. Il est d'abord facile de prouver que les entiers t, u donnés par la formule (2), satisfont en effet à l'équation (1). Il suffit pour cela de remarquer que l'équation (2) subsiste également lorsqu'on y remplace $\sqrt{D}$ par $-\sqrt{D}$, et que l'équation ainsi modifiée, étant multipliée par l'équation primitive, donne précisément l'équation (1).

2°. Pour faire voir en second lieu qu'il n'y a aucune solution de l'équation qui ne soit comprise dans la formule (2), posons pour un instant:

$$t_n + u_n\sqrt{D} = (T+U\sqrt{D})^n.$$

L'équation (2) est alors équivalente à ces deux équations simultanées:

$$t = \pm t_n, \quad u = \pm u_n,$$

les signes étant arbitraires, mais égaux dans les deux équations. Observons maintenant que, comme la puissance $(N(T+U\sqrt{D}))^n = \sigma^n$ croît constamment depuis la valeur zéro jusqu'à une valeur infinie, lorsque l'exposant n croît lui-même depuis $-\infty$ jusqu'à ∞, il faut nécessairement que relativement à une

solution donnée τ, v quelconque, on ait:

$$N(\tau+v\sqrt{D}) = \sigma^n, \quad \text{ou} \quad \sigma^n < N(\tau+v\sqrt{D}) < \sigma^{n+1},$$

l'exposant n ayant une valeur unique et déterminée. Dans le premier cas, où l'on a $N(\tau+v\sqrt{D}) = N(t_n+u_n\sqrt{D})$, on conclura, en vertu du numéro II:

$$\tau = \pm t_n, \quad v = \pm u_n,$$

où le signe qui doit être le même pour les deux équations, est complètement déterminé, l'entier donné τ ne pouvant se réduire à zéro. On voit donc que pour ce premier cas, la solution donnée τ, v est comprise dans l'équation (2) et répond à un exposant et à un signe entièrement déterminés. Reste à considérer la seconde hypothèse; la double inégalité qui s'y rapporte, étant divisée par σ^n, se change en celle-ci:

$$1 < \frac{N(\tau+v\sqrt{D})}{N(t_n+u_n\sqrt{D})} < N(T+U\sqrt{D}),$$

en vertu de laquelle la nouvelle solution τ', v' donnée par la formule:

$$\tau'+v'\sqrt{D} = \frac{\tau+v\sqrt{D}}{t_n+u_n\sqrt{D}},$$

satisferait à la condition:

$$1 < N(\tau'+v'\sqrt{D}) < N(T+U\sqrt{D}),$$

ce qui est impossible, cette dernière inégalité étant en contradiction avec la définition du groupe fondamental. La seconde hypothèse ne pouvant avoir lieu, la proposition se trouve établie.

V. L'équation (1) présente deux cas particuliers qui méritent une mention spéciale comme devant donner lieu plus tard à une application très remarquable: ces cas sont ceux où D est un entier réel ou le produit d'un tel entier par i. Comme dans la théorie des nombres complexes, l'équation (1) ne diffère pas essentiellement de celle où D est remplacé par la valeur opposée, nous pouvons toujours considérer comme positif l'entier réel dont il vient d'être question.

1°. Considérons en premier lieu le cas où D est réel et positif et supposons le radical $\sqrt{D}$ également positif. Il est évident que, si l'on satisfait alors à l'équation (1) par les valeurs $t = \alpha+\beta i$, $u = \gamma+\delta i$, on y satisfera aussi par celles-ci: $t = \alpha-\beta i$, $u = \gamma-\delta i$. Or, ces deux solutions donnant évidemment la même valeur pour l'expression $N(t+u\sqrt{D})$ sont nécessairement identiques

ou opposées, de sorte qu'on aura:

$$\alpha-\beta i = \pm(\alpha+\beta i), \quad \gamma-\delta i = \pm(\gamma+\delta i)$$

et par suite ou $\beta = 0$, $\delta = 0$ ou $\alpha = 0$, $\gamma = 0$. On voit donc que t et u sont ou l'un et l'autre des entiers réels ou l'un et l'autre de tels entiers affectés du facteur i. Il résulte de là, et en ayant égard à la formule (2), que si la solution fondamentale se trouve dans le premier cas, l'équation (1) n'a que des solutions réelles, tandis que pour une solution fondamentale imaginaire, les solutions de l'équation (1) sont en partie réelles, en partie imaginaires, les premières répondant à des valeurs paires et les dernières à des valeurs impaires de l'exposant. Si l'on observe ensuite que toute solution imaginaire de l'équation (1) donne sur-le-champ une solution réelle de $t^2-Du^2 = -1$, et réciproquement, on peut dire que la solution fondamentale présentera le second ou le premier des deux cas indiqués, suivant que l'équation $t^2-Du^2 = -1$ admet des solutions réelles ou non. Remarquons encore qu'en vertu de la condition $N(T+U\sqrt{D}) > 1$ à laquelle la solution fondamentale est toujours supposée satisfaire, il est évident que dans le premier cas T, U et dans le second T_1, U_1 (en supposant $T = T_1 i$, $U = U_1 i$) sont toujours de même signe, de sorte que nous pourrons toujours considérer ces entiers comme positifs, l'inégalité précédente laissant le choix entre deux solutions fondamentales opposées. Cela posé, on voit que si dans le premier cas on n'a en vue que les solutions positives de l'équation (1), il faudra, dans la formule (2), adopter le signe supérieur et n'attribuer à n que des valeurs pareillement positives. La formule (2) ainsi restreinte donne évidemment des valeurs d'autant plus grandes pour le binôme $t+u\sqrt{D}$, et par suite pour chacun des entiers t et u, qui en vertu de l'équation (1) croissent toujours simultanément, que l'exposant n est lui-même plus grand, d'où il suit que les deux termes de la solution fondamentale T, U sont les plus petits entiers positifs qui résolvent l'équation (1).

Il serait également facile de faire voir que dans le second cas T_1, U_1 sont les plus petits entiers positifs qui satisfont à l'équation $t^2-Du^2 = -1$, mais il sera plus commode pour notre objet de n'employer que l'équation (1). Observons donc que pour obtenir toutes les solutions positives de cette dernière, il faudra, après avoir posé dans la formule (2) $T = T_1 i$, $U = U_1 i$, remplacer n par $2n$ et supprimer ensuite le facteur $\pm(-1)^n$. On obtient ainsi:

$$t+u\sqrt{D} = (T_1+U_1\sqrt{D})^{2n},$$

et l'on voit alors que la plus petite solution positive de l'équation (1) est donnée par $(T_1+U_1\sqrt{D})^2$.

En désignant donc généralement par τ, v les plus petits entiers positifs qui résolvent l'équation (1), on aura suivant les deux cas:

$$\tau+v\sqrt{D}=T+U\sqrt{D}, \quad \tau+v\sqrt{D}=\left(\frac{T+U\sqrt{D}}{i}\right)^2.$$

Ces deux formules peuvent être réunies dans cette formule unique:

$$\sigma=N(T+U\sqrt{D})=(\tau+v\sqrt{D})^{\varkappa}, \tag{3}$$

dans laquelle $\varkappa$ désigne le nombre 1 ou le nombre 2, suivant que l'équation $t^2-Du^2=-1$ admet des solutions réelles ou n'en admet pas.

2°. Pour traiter l'autre cas, soit $D=D'i$, D' étant positif. Il est facile de voir que si l'on satisfait alors à l'équation (1), en posant:

$$t=\alpha+\beta i, \quad u=\gamma+\delta i,$$

on y satisfera pareillement en posant:

$$t=\alpha-\beta i, \quad u=\delta+\gamma i.$$

Or, ces deux solutions donnant évidemment la même valeur pour l'expression $N(t)+N(u)N(\sqrt{D})$ qui, d'après ce qu'on a vu plus haut, peut servir à caractériser les différents groupes de solutions, on voit que les solutions précédentes appartiennent au même groupe. On a donc:

$$\delta+\gamma i=\pm(\gamma+\delta i)$$

et par conséquent $\delta=\pm\gamma$. Comme en vertu de ce résultat, u est toujours divisible par $1-i$, si nous posons dans l'équation (1):

$$u=(1-i)u', \quad t=t',$$

elle prendra la forme:

$$t'^2-2D'u'^2=1,$$

et nous retombons sur le cas déjà traité. Il est facile de conclure de là que l'expression $\sigma=N(T+U\sqrt{D})$, toujours supposée supérieure à l'unité, est pour le cas dont nous nous occupons, donnée par l'équation:

$$\sigma=N(T+U\sqrt{D})=(\tau+v\sqrt{2D'})^{\varkappa}, \tag{4}$$

τ et v désignant les plus petits entiers positifs qui résolvent l'équation:

$$t'^2-2D'u'^2=1,$$

et $\varkappa$ ayant la valeur 1 ou la valeur 2, suivant que l'équation $t'^2-2D'u'^2=-1$ admet des solutions réelles ou non.

§. 15.

La théorie de l'équation $t^2-Du^2=1$ étant maintenant connue, nous pouvons reprendre les questions déjà traitées plus haut et en achever la solution en nous bornant, comme nous en avons déjà averti, à considérer des formes quadratiques qui appartiennent à la première espèce.

I. Nous nous occuperons en premier lieu de celle de ces questions qui concerne les représentations d'un entier donné m par une forme (a, b, c) également donnée. Supposons que m soit susceptible d'être représenté par la forme dont il s'agit, et soient $x=\alpha$, $y=\gamma$ des valeurs particulières et premières entre elles, telles que la valeur correspondante de la forme soit égale à m. Cela posé, il résulte du §. 12 que toutes les représentations appartenant à la même valeur de l'expression $\sqrt{D}$ (mod. m), à laquelle appartient la représentation particulière dont il s'agit, sont données par les deux équations:

$$x=\alpha t-(b\alpha+c\gamma)u, \quad y=\gamma t+(a\alpha+b\gamma)u,$$

où il faut substituer toutes les solutions de l'équation $t^2-Du^2=1$. Les équations précédentes, étant respectivement multipliées par a et $b+\sqrt{D}$, et ensuite ajoutées, donnent le résultat très simple:

$$ax+(b+\sqrt{D})y=(a\alpha+(b+\sqrt{D})\gamma)(t+u\sqrt{D}),$$

qui, au moyen de l'équation (2) du §. 14, se change en:

$$ax+(b+\sqrt{D})y=\pm(a\alpha+(b+\sqrt{D})\gamma)(T+U\sqrt{D})^{\varkappa}.$$

Soit pour abréger $N(a\alpha+(b+\sqrt{D})\gamma)=A$, et comme dans le paragraphe cité. $N(T+U\sqrt{D})=\sigma>1$. Cela posé, si l'on prend les normes des deux membres de l'équation précédente, on en conclura:

$$N(ax+(b+\sqrt{D})y)=A\sigma^{n},$$

où il importe de remarquer que chaque valeur de $N(ax+(b+\sqrt{D})y)$, donnée par cette dernière équation, se présentera deux fois dans la totalité des représentations que nous considérons et que pour abréger, nous nommerons désormais un *groupe* de représentations, comme cela résulte évidemment du double signe contenu dans l'équation précédente, et que le passage des nombres à leurs normes a fait disparaître. Observons encore que si k désigne une constante positive arbitrairement choisie, l'entier réel n qui doit croître depuis $-\infty$

jusqu'à ∞, obtiendra évidemment une valeur et n'en obtiendra qu'une seule qui satisfasse à la double condition:

$$k < A\sigma^n \leqq k\sigma.$$

On conclut de là que dans tout groupe de représentations, ou en d'autres termes, que parmi toutes les représentations qui appartiennent à une même valeur de l'expression $\sqrt{D}$ (mod. m), il en existe toujours deux et qu'il n'en existe que deux pour lesquelles on ait:

$$k < N(ax+(b+\sqrt{D})y) \leqq k\sigma,$$

et il est d'ailleurs manifeste que les deux représentations particulières dont il s'agit et qui varient avec la constante k, sont toujours telles que, l'une étant exprimée par les formules: $x = r$, $y = s$, l'autre le sera par celles-ci: $x = -r$, $y = -s$.

Le résultat que nous venons d'obtenir, va nous fournir un moyen très simple de décider 1° si un entier donné m peut être représenté par une forme également donnée (a, b, c) ou non, et 2° d'assigner dans le premier de ces deux cas, toutes les représentations dont m est susceptible au moyen de la forme dont il s'agit. On voit d'abord que la question proposée revient à examiner si l'on peut satisfaire à ces deux conditions simultanées:

$$ax^2+2bxy+cy^2 = m, \tag{1}$$

$$k < N(ax+(b+\sqrt{D})y) \leqq k\sigma, \tag{2}$$

par des entiers x et y premiers entre eux. Si cela n'est pas possible, on sera assuré que m n'est pas susceptible d'être représenté par la forme donnée. Dans le cas contraire on trouvera une ou plusieurs doubles représentations telles que $x = \pm r$, $y = \pm s$; $x = \pm r'$, $y = \pm s'$; ..., qui appartiendront à autant de groupes distincts, et l'on obtiendra toutes les représentations cherchées, si dans les deux équations rappelées au commencement de ce paragraphe, on pose successivement $\alpha = r$, $\gamma = s$; $\alpha = r'$, $\gamma = s'$; ....

Réduite à ce point, la question ne présente plus aucune difficulté, car il est facile de se convaincre que, pour que les entiers x et y puissent satisfaire aux conditions simultanées (1) et (2), leurs normes doivent être comprises entre certaines limites faciles à assigner, de sorte que l'examen qu'il s'agit de faire, ne doit porter que sur un nombre limité de combinaisons x, y. En effet, si après avoir multiplié par a l'équation (1), on prend les normes de ses deux

membres, il viendra:

$$N(ax+(b+\sqrt{D})y)N(ax+(b-\sqrt{D})y) = N(am).$$

Cette équation étant comparée avec la double inégalité (2), on en conclura celle-ci:

$$\frac{N(am)}{k\sigma} \leqq N(ax+(b-\sqrt{D})y) < \frac{N(am)}{k},$$

et par suite en ajoutant cette dernière et l'inégalité (2):

$$k+\frac{N(am)}{k\sigma} < 2N(ax+by)+2N(\sqrt{D})N(y) < k\sigma+\frac{N(am)}{k}.$$

Il est facile de voir que les entiers x et y, et à plus forte raison les entiers x et y, premiers entre eux qui satisfont à cette double inégalité qui est une conséquence nécessaire des deux conditions (1) et (2), ne présentent qu'un nombre limité de combinaisons faciles à former; on pourra donc toujours décider si parmi ces entiers simultanés il en existe qui remplissent les deux conditions dont il s'agit, ce que nous nous étions proposé de faire voir.

La condition (2) qui, étant jointe à l'équation (1), a pour effet de réduire chaque groupe de représentations de l'entier m par la forme (a, b, c) à deux représentations particulières qu'elle sépare ainsi de toutes les autres, prend une forme remarquable lorsqu'on fait un choix convenable de la constante arbitraire k qu'elle contient.

Soit $k = N(\sqrt{am})$. La condition dont nous parlons, deviendra ainsi:

$$N(\sqrt{am}) < N(ax+(b+\sqrt{D})y) \leqq \sigma N(\sqrt{am}).$$

Observons que, comme il ne s'agit que de quantités positives, cette double inégalité est tout-à-fait équivalente à celle-ci:

$$N(am) < (N(ax+(b+\sqrt{D})y))^2 \leqq \sigma^2 N(am)$$

qui, à son tour, peut être remplacée par celle qu'on en déduit en divisant par $N(ax+(b+\sqrt{D})y)$, et en observant qu'on a:

$$N(am) = N(ax+(b+\sqrt{D})y)N(ax+(b-\sqrt{D})y).$$

On trouve ainsi:

$$N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leqq \sigma^2 N(ax+(b-\sqrt{D})y). \tag{3}$$

C'est sous cette dernière forme que nous emploierons dorénavant la condition qui sert à réduire tout groupe de représentations à deux de ses termes.

II. Quant aux deux questions que nous nous étions proposées sur l'équivalence des formes, comme celle d'entre elles qui a pour objet de déduire toutes les transformations d'une forme en une autre équivalente, d'une première transformation supposée donnée, s'est trouvée dépendre de l'équation $t^2 - Du^2 = 1$, dont nous avons donné la solution générale, nous n'avons plus à traiter que la première des questions énoncées au commencement du §. 11. Il s'agit donc de faire voir comment, étant données deux formes (a, b, c) et (a', b', c') ayant un déterminant commun D, on peut décider si ces formes sont équivalentes ou non, et obtenir, dans le premier de ces deux cas, l'une des substitutions au moyen desquelles la première se change dans la seconde. Pour résoudre cette question, on se rappellera que, d'après ce qu'on a démontré dans le §. 12, tout revient à voir s'il existe des représentations de l'entier a' par la forme (a, b, c), qui appartiennent à la valeur b' de l'expression $\sqrt{D}$ (mod. a'). Si l'on trouve qu'il n'y a aucune représentation pour laquelle la condition énoncée soit satisfaite, on sera assuré que les deux formes ne sont pas équivalentes; dans le cas contraire, l'une quelconque des représentations obtenues donnera sur-le-champ la transformation cherchée. La question proposée se trouvant ainsi réduite à celle dont nous avons donné la solution dans le numéro précédent de ce paragraphe, doit elle-même être considérée comme résolue.

III. Avant d'en venir à la question qui forme le principal sujet de ce Mémoire, nous avons encore à indiquer comment, étant donnée une forme $ax^2+2bxy+cy^2$ du déterminant D, on peut assigner d'une manière générale les valeurs simultanées x et y, pour lesquelles la valeur de cette forme soit impaire et première à D, ou plus simplement, soit première à $(1+i)D = \Delta$. Comme, en posant $x \equiv \alpha$, $y \equiv \gamma$ (mod. Δ), où α et γ peuvent être choisis dans un système de résidus relatif au module Δ, on a:

$$ax^2+2bxy+cy^2 \equiv a\alpha^2+2b\alpha\gamma+c\gamma^2 \pmod{\Delta},$$

on voit que la question proposée se réduit à examiner pour lesquelles des combinaisons α, γ ou plutôt pour combien de ces combinaisons, car c'est uniquement leur nombre qu'il nous importe de connaître, le second membre est premier à Δ. J'observe maintenant que sans nuire en rien à la généralité de la question, il est permis de considérer le coefficient a comme premier à Δ. En effet, comme la forme donnée est supposée de première espèce, on peut toujours, si elle ne satisfait pas à la condition énoncée, la transformer en une

autre où cette dernière se trouve remplie; et l'on prouve facilement que relativement à la nouvelle forme, le nombre des combinaisons dont il s'agit, est le même que pour la forme donnée. Le raisonnement par lequel cette dernière assertion peut être justifiée, étant très simple et d'ailleurs entièrement semblable à celui dont nous avons déjà fait usage dans la question analogue, relative aux entiers réels*), nous nous dispenserons de le répéter ici.

Cela posé, il est évident que, pour que l'expression $a\alpha^2+2b\alpha\gamma+c\gamma^2$ soit première à $\Delta = (1+i)D$, il faut et il suffit qu'il en soit de même du produit:

$$a(a\alpha^2+2b\alpha\gamma+c\gamma^2) = (a\alpha+b\gamma)^2 - D\gamma^2.$$

Distinguons maintenant le cas où D est impair et celui où D est divisible par $1+i$. Dans le premier de ces deux cas, il faudra, si γ est divisible par $1+i$, que $a\alpha+b\gamma$ soit premier à Δ, et si γ est impair, que $a\alpha+b\gamma$ soit divisible par $1+i$ et premier à D. Or comme, γ ayant une valeur déterminée, l'expression $a\alpha+b\gamma$, dans laquelle α est le terme général d'un système de résidus pour le module Δ, représente elle-même un semblable système (§. 5, III.), il s'agira de déterminer combien, dans un système de résidus pour le module Δ, il existe de termes premiers à Δ ou de termes premiers à D et en outre divisibles par $1+i$, selon que γ sera ou ne sera pas divisible par $1+i$. Le premier de ces deux nombres est $\psi(\Delta)$; pour obtenir le second, on se rappellera que, si l'on divise par $1+i$ ceux des termes du système en question qui renferment le facteur $1+i$, les quotients formeront un système de résidus pour le module D (§. 5, II.), d'où l'on conclut que le nombre que nous avons à déterminer, est exprimé par $\psi(D)$. J'ajoute que cette dernière expression peut être remplacée par $\psi(\Delta)$ puisque, D et $1+i$ étant premiers entre eux, on a (§. 5, V.):

$$\psi(\Delta) = \psi((1+i)D) = \psi(1+i)\psi(D) = \psi(D).$$

Ayant ainsi reconnu qu'à toute valeur déterminée γ il répond $\psi(\Delta)$ valeurs α qui satisfont aux conditions exigées, et sachant d'un autre côté que γ est susceptible d'un nombre de valeurs exprimé par $N(\Delta)$, on en conclura que les combinaisons α, γ qui rendent $a\alpha^2+2b\alpha\gamma+c\gamma^2$ premier à Δ, sont au nombre de $N(\Delta)\psi(\Delta)$.

Le cas où D est supposé divisible par $1+i$, donne le même résultat. En effet, comme le terme $D\gamma^2$ est dans ce cas divisible par $1+i$, tout se ré-

*) Recherches sur diverses applications de l'Analyse infinitésimale à la théorie des Nombres, §. 5 [1]).

[1]) S. 437 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

duit à faire en sorte que $\alpha\alpha+b\gamma$ soit premier à Δ, et l'on voit facilement que les valeurs α qui, répondant à une valeur déterminée γ, satisfont à cette condition, sont toujours au nombre de $\psi(\Delta)$, d'où l'on conclut que celui des combinaisons dont il s'agit, est égal à $N(\Delta)\psi(\Delta)$, comme dans le premier cas.

On voit ainsi que les valeurs simultanées de x et de y qui, étant substituées dans l'expression $ax^2+2bxy+cy^2$, la rendent première à $(1+i)D=\Delta$, peuvent toujours être distribuées en systèmes de la forme:

$$x=\Delta v+\alpha, \quad y=\Delta w+\gamma,$$

où v et w sont des entiers indéterminés, et α et γ des entiers déterminés, et que le nombre de ces systèmes est toujours exprimé par $N(\Delta)\psi(\Delta)$.

Classification des formes et théorèmes qui s'y rapportent.

§. 16.

La classification dont il s'agit, consiste à rapporter deux quelconques des formes qui ont un déterminant commun D, à la même classe ou à des classes distinctes, suivant que ces formes sont équivalentes ou non. Nous démontrerons d'abord que les classes ainsi définies sont toujours en nombre limité, quel que soit le déterminant donné. C'est à quoi nous parviendrons en faisant voir que dans chaque classe il existe au moins une forme (a, b, c) telle qu'on ait à la fois $\frac{1}{2}N(a)\geqq N(b)$, $N(a)\leqq N(c)$, et en prouvant ensuite que les formes de cette nature, qu'on appelle des formes *réduites*, sont toujours en nombre fini.

Pour établir le premier de ces deux points, il s'agira de montrer qu'une forme quelconque (a, b, a') peut toujours se transformer en une forme réduite équivalente. Considérons à cet effet la substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, où nous n'avons que cette seule condition $\alpha\delta-\beta\gamma=1$, et observons que cette dernière sera satisfaite si, δ restant quelconque, nous supposons $\alpha=0$, $\beta=1$, $\gamma=-1$. Au moyen de la substitution ainsi particularisée, la forme (a, b, a') se changera en une autre (a', b', a''), où l'on aura $b'=-b-a'\delta$. D'après ce que nous avons remarqué au commencement du §. 2, nous pouvons toujours disposer de l'indéterminée δ de manière que l'on ait $\frac{1}{2}N(a')\geqq N(b')$. La nouvelle forme (a', b', a'') satisfaisant alors à la première des deux conditions qui définissent les formes réduites, si l'on a en outre $N(a')\leqq N(a'')$, cette forme aura toutes les propriétés requises; si non, on en déduira par le même procédé une troisième

forme (a'', b'', a'''), où l'on aura $\frac{1}{2}N(a'')\geqq N(b'')$, et qui par conséquent sera une forme réduite si l'on a en outre $N(a'')\leqq N(a''')$. Il est manifeste que si l'on continue à opérer toujours de la même manière, on finira nécessairement par tomber sur une forme réduite équivalente à la proposée; car pour qu'il en fût autrement, il faudrait que la suite $N(a')>N(a'')>N(a''')>\cdots$ pût être indéfiniment prolongée, ce qui évidemment est impossible, les entiers a', a'', a''', ... étant tous différents de zéro si, comme on le suppose toujours, D n'est pas un carré.

Le premier point se trouvant ainsi établi, il nous reste à faire voir que les formes réduites (a, b, c) qui ont un déterminant donné D, sont en nombre limité et peuvent toujours être assignées facilement. Les deux conditions $\frac{1}{2}N(a)\geqq N(b)$, $N(a)\leqq N(c)$ donnent d'abord $N(ac)\geqq 4N(b^2)$, et par suite $\sqrt{N(ac)}\geqq 2N(b)$. Si d'un autre côté, on applique à l'équation $ac=b^2-D$ le théorème déjà employé dans le §. 13, on en conclura:

$$\sqrt{N(ac)}\leqq\sqrt{N(b^2)}+\sqrt{N(-D)},$$

ou ce qui revient au même:

$$\sqrt{N(ac)}\leqq N(b)+\sqrt{N(D)},$$

inégalité qu'il suffit de comparer à celle déjà obtenue, pour voir qu'on a:

$$N(b)\leqq\sqrt{N(D)}.$$

Comme $N(b)$ et par conséquent aussi b n'est ainsi susceptible que d'un nombre limité de valeurs faciles à assigner, pour obtenir toutes les formes réduites du déterminant D, il suffira de décomposer chacune des valeurs correspondantes de b^2-D de toutes les manières possibles en deux facteurs a et c, en supposant $N(a)\leqq N(c)$, et de ne conserver que celles des combinaisons a, b, c pour lesquelles on a $\frac{1}{2}N(a)\geqq N(b)$ *).

Ayant ainsi obtenu toutes les formes réduites (a, b, c) qui répondent à un déterminant donné, si comme nous le supposons, on n'a en vue que les formes qui appartiennent à la première espèce, il ne restera plus qu'à effacer celles des formes trouvées, pour lesquelles a, b, c ou a, $2b$, c auraient un diviseur commun.

---

*) On voit que la méthode dont nous venons de faire usage pour obtenir les formes réduites, est entièrement analogue à celle qui sert pour le même objet dans la théorie des entiers réels. Nous ajouterons que la possibilité d'appliquer cette dernière aux entiers complexes, avait déjà été remarquée par M. Jacobi (Tome XIX, p. 314 du Journal de Crelle.) [1]).

[1]) Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften, Jahrgang 1839, S. 86 K.

Il s'agit maintenant de faire l'énumération complète des classes qui répondent au déterminant D, en choisissant dans chacune de ces classes l'une quelconque des formes dont elle se compose. Des formes choisies d'après cette règle constitueront ce que nous appellerons un système complet de formes non-équivalentes ou plus simplement, *un système de formes* pour le déterminant dont il s'agit. Un tel système jouira évidemment de la double propriété de présenter une forme et de n'en présenter qu'une seule qui soit équivalente à une forme quelconque, pourvu que cette dernière ait l'entier D pour déterminant et soit d'ailleurs de première espèce. Pour construire un système de cette nature, on peut se servir des formes réduites que nous avons appris à déterminer dans ce qui précède. En effet, comme parmi les formes réduites il s'en trouve toujours au moins une, qui appartienne à une classe arbitrairement choisie, tout reviendra à éliminer les formes surabondantes. Après avoir rangé à cet effet les formes réduites dans un ordre quelconque, on commencera par comparer la première d'entre elles à chacune des suivantes et l'on effacera toutes celles de ces dernières, que l'on reconnaîtra lui être équivalentes. Cela fait, on comparera la seconde des formes que cette première opération aura laissées subsister, à chacune des suivantes pour effacer encore les formes qu'on trouvera lui être équivalentes, et ainsi de suite.

Le procédé que nous venons d'indiquer, suffit pour assigner le nombre des classes, ou ce qui revient au même, celui des termes composant un système de formes pour un déterminant quelconque, lorsque ce dernier est numériquement donné. Mais tel n'est pas l'objet principal que nous nous sommes proposé dans ce Mémoire, et qui consiste plutôt à découvrir la loi générale par laquelle le nombre des classes se trouve lié au déterminant auquel ces classes se rapportent. Pour résoudre cette dernière question, il faut pénétrer plus avant dans la nature de ce que nous avons nommé un système de formes, et se rendre compte des rapports qui existent entre un tel assemblage et la totalité des entiers que ces formes peuvent servir à représenter.

§. 17.

Soit:

$$(1) \qquad ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \ldots$$

un système de formes (de première espèce) pour le déterminant D, et proposons-nous de rechercher sous quelles conditions un entier m que nous supposerons impair et premier à D, ou réunissant ces deux conditions en une seule, que nous supposerons premier à $\Delta = (1+i)D$, peut être représenté par une ou par plusieurs de ces formes, et de déterminer, lorsque de telles représentations existent, le nombre des groupes dans lesquels leur totalité se distribue. Il est bien entendu que, comme dans ce qui précède, il n'est toujours question que de représentations pour lesquelles les indéterminées x et y soient premières entre elles. D'après le §. 12, il y a une première condition à remplir, consistant en ce que D doit être résidu quadratique à l'égard de m, et il résulte d'un autre côté du §. 9 que, pour qu'elle soit satisfaite, il faut et il suffit que pour chacun des diviseurs simples f de m, on ait:

$$(2) \qquad \left[\frac{D}{f}\right] = 1.$$

Ces conditions particulières étant supposées remplies, si l'on désigne par μ le nombre des facteurs simples primaires inégaux que l'entier m contient, la congruence $z^2 \equiv D \pmod{m}$ aura 2^μ racines, et il s'agira de chercher quels sont les groupes de représentations qui puissent répondre à ces diverses racines. Soit l l'une quelconque de ces racines, et proposons-nous de déterminer les représentations qui lui appartiennent. D'après ce qui a été démontré dans le §. 12, nous avons à examiner si parmi les formes (1) il y en a une qui soit équivalente à celle-ci:

$$\left(m, l, \frac{l^2-D}{m}\right).$$

Observons d'abord que les coefficients de cette dernière sont évidemment sans diviseur commun, puisqu'un tel diviseur diviserait aussi le déterminant D, ce qui serait contraire à l'hypothèse admise d'après laquelle m est premier à D. Comme d'un autre côté, m est supposé impair, on voit que la forme précédente appartient à la première espèce, d'où il suit que la forme dont il s'agit, a son équivalente dans le système (1). Il résulte de là et du paragraphe déjà cité, qu'il existe toujours un groupe de représentations appartenant à une racine déterminée l, et qu'il n'en existe qu'un seul, d'où l'on conclut que les représentations dont l'entier m est susceptible au moyen des expressions (1), forment toujours un nombre de groupes distincts, égal à la puissance 2^μ.

Nous pouvons maintenant réduire chacun des groupes dont il s'agit, à deux représentations individuelles, si dans chacune des formes (1), nous limitons

les indéterminées x et y, au moyen de la condition d'inégalité déjà donnée dans le §. 15, cette condition étant pour la première des expressions (1):

$$(3) \qquad N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leqq \sigma^2 N(ax+(b-\sqrt{D})y),$$

et se déduisant pour les autres de celle que nous venons d'écrire, en y accentuant les lettres a, b, c. Ces conditions étant jointes aux formes (1), on voit que le nombre des représentations dont m est susceptible au moyen des formes dont il s'agit, sera fini et exprimé par 2^{u+1}.

Au moyen du résultat que nous venons d'obtenir, il est facile de former l'équation générale que nous allons écrire:

$$(4) \qquad \Sigma 2^{u+1}F(m) = \Sigma F(ax^2+2bxy+cy^2)+\Sigma F(a'x^2+2b'xy+c'y^2)+\cdots\cdots$$

La sommation indiquée dans le premier membre est supposée embrasser la totalité des entiers m premiers à Δ dont tous les diviseurs simples f satisfont à la condition (2), μ désignant, pour chacun de ces entiers m, le nombre de ses facteurs simples primaires inégaux. Quant aux sommes contenues dans le second membre, elles sont en même nombre que les formes (1), et répondent chacune à l'une des formes en question. Dans chacune de ces sommes le signe Σ doit s'étendre à tous les systèmes de valeurs simultanées x et y qui remplissent la triple condition de n'avoir pas de diviseur commun, de donner à la forme où elles sont substituées, une valeur première à Δ, et enfin de satisfaire à la double inégalité (3) lorsqu'il s'agit de la première somme, et à des inégalités de même forme pour chacune des autres. La fonction désignée par la caractéristique F est arbitraire et doit seulement être choisie de manière que les séries contenues dans l'équation, soient convergentes et aient des sommes indépendantes de l'ordre de succession de leurs termes. La vérité de l'équation ainsi formée est évidente, et l'on voit que cette équation n'est que la traduction de la double propriété remarquée plus haut et consistant en ce que d'une part tout entier supposé premier à Δ, pour être susceptible d'être représenté par les formes (1), doit être compris parmi ceux que nous venons de désigner par m, et en ce que d'autre part chacun de ces derniers admet en effet 2^{u+1} représentations au moyen des expressions (1), si à chacune de ces expressions l'on suppose jointe une condition d'inégalité comme celle de (3). D'après la manière dont l'équation précédente subsiste, il est manifeste qu'elle ne cessera pas d'avoir lieu si l'on y remplace partout les entiers complexes qui se trouvent

sous le signe F, par leurs normes, de sorte qu'on aura aussi:

$$\Sigma 2^{u+1}F(N(m)) = \Sigma F(N(ax^2+2bxy+cy^2))+\Sigma F(N(a'x^2+2b'xy+c'y^2))+\cdots\cdots,$$

les signes sommatoires ayant toujours la même signification.

Particularisons la fonction arbitraire contenue dans l'équation, et supposons que cette fonction soit une puissance de l'exposant $-s$, où s est une quantité positive supérieure à l'unité. Il viendra ainsi:

$$\Sigma\frac{2^{u+1}}{(N(m))^s} = \Sigma\frac{1}{(N(ax^2+2bxy+cy^2))^s}+\Sigma\frac{1}{(N(a'x^2+2b'xy+c'y^2))^s}+\cdots\cdot$$

Comme d'après la définition des entiers m, quatre nombres associés se trouvent évidemment toujours simultanément compris ou non parmi ces entiers m, on voit que nous pouvons considérer la sommation indiquée dans le premier membre, comme ne devant plus s'étendre qu'aux entiers m qui satisfaisant aux conditions énoncées plus haut, soient en outre primaires, c'est-à-dire tels qu'en posant $m=\alpha+\beta i$, on ait $\alpha\equiv 1 \pmod 4$, $\beta\equiv 0 \pmod 2$, pourvu qu'en même temps nous quadruplions le premier membre. On aura ainsi:

$$(5) \qquad 8\Sigma\frac{2^{\mu}}{(N(m))^s} = \Sigma\frac{1}{(N(ax^2+2bxy+cy^2))^s}+\Sigma\frac{1}{(N(a'x^2+2b'xy+c'y^2))^s}+\cdots\cdot$$

L'entier m étant primaire, on aura toujours, d'une manière unique (§§. 2 et 3, V.), $m=f'^{h'}f''^{h''}\ldots$, les exposants h', h'', $\ldots$ étant tous différents de zéro, et f', f'', $\ldots$ désignant des nombres premiers primaires inégaux qui satisfont à la condition (2), et dont le nombre est exprimé par μ. Cela étant, il est facile de se convaincre qu'on a:

$$(6) \qquad \Sigma\frac{2^{\mu}}{(N(m))^s} = \Pi\frac{1+\frac{1}{(N(f))^s}}{1-\frac{1}{(N(f))^s}},$$

le signe Π s'étendant à tous les nombres premiers impairs et primaires f, qui ne divisent pas le déterminant D et remplissent la condition (2). Il suffit de développer le facteur général comme il suit:

$$\frac{1+\frac{1}{(N(f))^s}}{1-\frac{1}{(N(f))^s}} = 1+\frac{2}{(N(f))^s}+\frac{2}{(N(f^2))^s}+\frac{2}{(N(f^3))^s}+\cdots$$

et d'effectuer ensuite la multiplication pour reconnaître, au moyen de la remarque que nous venons de faire, que l'équation (6) est en effet exacte.

Afin de transformer ultérieurement le second membre de cette équation, soit q le terme général de la suite des nombres premiers impairs et primaires, à l'exclusion de ceux qui divisent D, et considérons le produit:

$$\Pi \frac{1}{1-\frac{1}{(N(q))^s}},$$

où le signe de multiplication est supposé s'étendre à toutes les valeurs q que nous venons de définir. Comme l'on a:

$$\frac{1}{1-\frac{1}{(N(q))^s}} = 1+\frac{1}{(N(q))^s}+\frac{1}{(N(q^2))^s}+\frac{1}{(N(q^3))^s}+\cdots$$

et qu'on sait d'un autre côté, que tout entier impair et primaire n'est susceptible que d'une seule décomposition en facteurs simples primaires, on voit que le produit précédent équivaut à une série d'une loi très simple, et que l'on a:

$$\Pi \frac{1}{1-\frac{1}{(N(q))^s}} = \Sigma \frac{1}{(N(n))^s}, \tag{7}$$

le signe Σ se rapportant à tous les entiers impairs n, primaires et premiers à D. Si au lieu du produit précédent, l'on considère le suivant:

$$\Pi \frac{1}{1-\left[\frac{D}{q}\right]\frac{1}{(N(q))^s}},$$

on reconnaîtra que ce nouveau produit, traité de la même manière, se transforme en une série ayant pour terme général $\chi \frac{1}{(N(n))^s}$, où le coefficient χ sera donné par la formule:

$$\chi = \left[\frac{D}{q'}\right]^k \left[\frac{D}{q''}\right]^{k'} \cdots,$$

si l'on suppose $n = q'^k q''^{k'} \ldots$, les exposants étant positifs, et q', q'', $\ldots$ désignant les nombres premiers inégaux q que l'entier n contient. Si maintenant l'on observe qu'en vertu de la troisième des équations (e) du §. 8, l'expression χ peut être remplacée par:

$$\left[\frac{D}{q'^k}\right]\left[\frac{D}{q''^{k'}}\right]\cdots = \left[\frac{D}{q'^k q''^{k'}\ldots}\right] = \left[\frac{D}{n}\right],$$

on aura l'équation:

$$\Pi \frac{1}{1-\left[\frac{D}{q}\right]\frac{1}{(N(q))^s}} = \Sigma \left[\frac{D}{n}\right]\frac{1}{(N(n))^s}, \tag{8}$$

dans laquelle les signes Π et Σ ont la même signification que dans l'équation (7). Cela posé, faisons le produit des équations (7) et (8), et divisons ensuite ce produit par l'équation (7), après avoir remplacé dans cette dernière s par $2s$. Le facteur général du premier membre de l'équation que l'on obtient ainsi, sera évidemment:

$$\frac{1-\frac{1}{(N(q))^{2s}}}{\left(1-\frac{1}{(N(q))^s}\right)\left(1-\left[\frac{D}{q}\right]\frac{1}{(N(q))^s}\right)} = \frac{1+\frac{1}{(N(q))^s}}{1-\left[\frac{D}{q}\right]\frac{1}{(N(q))^s}}.$$

Ce facteur présente deux cas différents selon que l'on a:

$$\left[\frac{D}{q}\right] = 1, \quad \text{ou} \quad \left[\frac{D}{q}\right] = -1.$$

Dans le second il se réduit à l'unité et peut être omis, tandis que pour le premier il prend la forme:

$$\frac{1+\frac{1}{(N(q))^s}}{1-\frac{1}{(N(q))^s}}.$$

Or, les nombres premiers q pour lesquels on a $\left[\frac{D}{q}\right] = 1$, coïncidant avec ceux que nous avons précédemment désignés par f, on voit que l'équation qu'il s'agit de former, est:

$$\Pi \frac{1+\frac{1}{(N(f))^s}}{1-\frac{1}{(N(f))^s}} = \frac{\Sigma \frac{1}{(N(n))^s}\cdot\Sigma\left[\frac{D}{n}\right]\frac{1}{(N(n))^s}}{\Sigma \frac{1}{(N(n))^{2s}}}.$$

Au moyen de ce résultat et de l'équation (6), l'équation (5) peut prendre la forme:

$$8\Sigma \frac{1}{(N(n))^s}\cdot\Sigma\left[\frac{D}{n}\right]\frac{1}{(N(n))^s} = \Sigma \frac{1}{(N(n^2))^s}\cdot\Sigma \frac{1}{(N(ax^2+2bxy+cy^2))^s}+\cdots,$$

où les signes sommatoires qui se rapportent à n, s'étendent à tous les entiers primaires et premiers à D, tandis que ceux qui sont relatifs aux valeurs simultanées x et y, conservent la signification indiquée plus haut. Il est facile de se convaincre que les produits de séries, contenus dans le second membre, sont susceptibles d'une forme beaucoup plus simple, qu'ils prennent lorsque la multi-

plication indiquée est effectuée. Pour leur donner cette nouvelle forme, nous considérerons particulièrement le premier de ces produits, la même transformation s'appliquant à tous les autres. En faisant le produit des termes généraux des deux sommes qu'il s'agit de multiplier entre elles, on aura:

$$\frac{1}{(N(n^2))^s (N(ax^2+2bxy+cy^2))^s} = \frac{1}{(N(ax'^2+2bx'y'+cy'^2))^s},$$

où l'on a posé $x' = nx$, $y' = ny$. Voyons quelle est la nature des systèmes x', y' auxquels la nouvelle sommation doit se rapporter. Comme on a:

$$n^2(ax^2+2bxy+cy^2) = ax'^2+2bx'y'+cy'^2,$$

on voit d'abord, en ayant égard aux conditions que x, y, n sont supposés remplir, 1° que pour chacun des systèmes en question, $ax'^2+2bx'y'+cy'^2$ est premier à Δ, et 2° que les entiers x', y' satisfont à la double inégalité:

$$N(ax'+(b-\sqrt{D})y') < N(ax'+(b+\sqrt{D})y') \leq \sigma^2 N(ax'+(b-\sqrt{D})y')$$

de même forme que (3), et qui résulte de cette dernière en multipliant par $N(n)$. Il est facile de prouver réciproquement que tout système x', y' qui satisfait à ces deux conditions, est en effet compris parmi ceux auxquels la nouvelle sommation doit s'étendre, et ne s'y présente qu'une fois. C'est à quoi l'on parvient, en assignant l'entier n et le système x, y, l'un et l'autre entièrement déterminés, dont la combinaison fournit le système donné x', y'. Soit à cet effet $x' = nx$, $y' = ny$, où n désigne le plus grand diviseur commun primaire de x et y, qui sera complètement déterminé ainsi que les entiers x et y. Cela étant, il est évident que n est premier à Δ, et l'on voit également sans difficulté que les entiers x et y, premiers entre eux, satisfont aussi aux deux autres conditions auxquelles les systèmes x, y sont assujettis. Cela est manifeste pour celle de ces conditions qui consiste en ce que $ax^2+2bxy+cy^2$ doit être premier à Δ, et pour prouver que la double inégalité (3) a pareillement lieu, il suffit de diviser par $N(n)$ celle que nous avons écrite plus haut et à laquelle x' et y' sont supposés satisfaire.

Après avoir ainsi reconnu la nature des systèmes x', y' que la nouvelle sommation doit embrasser, nous pouvons supprimer les accents des indéterminées x' et y'. L'équation qu'il s'agissait de transformer, deviendra ainsi:

$$(9) \qquad 8\Sigma\frac{1}{(N(n))^s}\cdot\Sigma\left[\frac{D}{n}\right]\frac{1}{(N(n))^s} = \Sigma\frac{1}{(N(ax^2+2bxy+cy^2))^s}+\cdots,$$

où la double sommation indiquée dans le premier terme du second membre est supposée s'étendre aux valeurs simultanées x et y telles que $ax^2+2bxy+cy^2$ soit premier à Δ, et satisfaisant en outre à la condition (3). Quant aux autres termes, comme ils sont de même nature que celui dont nous venons de parler, et résultent de ce dernier en accentuant les lettres a, b, c, nous continuerons à ne pas les écrire. Il s'agit maintenant de transformer l'équation que nous venons d'obtenir, de manière qu'elle exprime le nombre des formes non-équivalentes qui répondent au déterminant D. Ce sera là l'objet du paragraphe suivant.

Expression du nombre des classes au moyen d'une suite infinie double.

§. 18.

Pour parvenir au but que nous avons en vue, nous aurons à examiner ce que les différents termes de l'équation (9) du paragraphe précédent deviennent, lorsque la variable s que cette équation contient, converge vers sa limite qui est l'unité.

I. Occupons-nous d'abord du second membre, en nous bornant toujours à considérer la première des sommes dont ce membre se compose. Comme indépendamment de la double condition d'inégalité à laquelle x et y sont supposés satisfaire, ces indéterminées doivent être telles que la valeur du trinôme $ax^2+2bxy+cy^2$ soit première à Δ, on conclut du §. 15, III que les valeurs simultanées de x et y que la sommation embrasse, peuvent être distribuées en systèmes de la forme:

$$(1) \qquad x = v\Delta+\alpha, \quad y = w\Delta+\gamma,$$

où v, w et α, γ désignent des entiers complexes, les deux premiers indéterminés et les deux derniers déterminés, et que le nombre de ces systèmes est toujours $N(\Delta)\psi(\Delta)$. La somme dont il s'agit se décompose ainsi en $N(\Delta)\psi(\Delta)$ sommes partielles, telles que la suivante:

$$(2) \qquad \Sigma\frac{1}{(N(ax^2+2bxy+cy^2))^s},$$

où le signe sommatoire doit s'étendre à toutes les valeurs de x et y, données par les formules (1), et en outre telles que l'on ait:

$$(3) \qquad N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leq \sigma^2 N(ax+(b-\sqrt{D})y).$$

Pour évaluer la somme partielle (2), soit z une variable positive, et proposons-nous de déterminer l'entier positif Z qui exprime combien de fois dans la somme dont il s'agit, l'expression $N(ax^2+2bxy+cy^2)$ obtient une valeur non-supérieure à z. On sent que Z est une fonction discontinue très compliquée de la variable z; mais il ne s'agira pas d'obtenir cette fonction avec une exactitude absolue, et il suffira de connaître son expression-limite, c'est-à-dire une expression dont le rapport à Z converge vers l'unité, lorsque la variable z devient infinie. D'après ce qui précède, l'entier Z désigne le nombre des combinaisons v, w pour lesquelles on a, outre la condition (3), celle que nous allons écrire:

$$N(ax^2+2bxy+cy^2) \leqq z,$$

ou ce qui revient au même, celle-ci:

$$N(ax+(b+\sqrt{D})y)\,N(ax+(b-\sqrt{D})y) \leqq zN(a), \tag{4}$$

x et y étant supposés remplacés dans les conditions (3) et (4) par les expressions (1).

Observons maintenant que, comme il ne s'agit que d'obtenir le nombre des combinaisons v, w qui satisfont aux inégalités précédentes, nous pouvons remplacer les entiers v, w par d'autres indéterminées v', w', entières ou non, mais tellement liées à v et w qu'à toute combinaison v, w réponde une combinaison unique v', w', et réciproquement. Soit, pour abréger, $z=\frac{1}{\zeta^4}$, où ζ est supposé positif; il est facile de voir que nous remplirons la condition énoncée en posant les équations linéaires:

$$v'=\left(v+\frac{\alpha}{\Delta}\right)\zeta, \quad w'=\left(w+\frac{\gamma}{\Delta}\right)\zeta,$$

en vertu desquelles, ζ étant réel et v, w désignant des entiers complexes indéterminés, v' et w' exprimeront l'un et l'autre des nombres complexes, dont les deux parties sont les termes généraux de progressions arithmétiques réelles, ayant la quantité ζ pour raison commune. Au moyen de ces expressions les formules (1) que nous avons à substituer dans les conditions (3) et (4), deviennent:

$$x=\frac{v'\Delta}{\zeta}, \quad y=\frac{w'\Delta}{\zeta}.$$

Si maintenant l'on effectue la substitution dont il s'agit, et que l'on multiplie ensuite les inégalités (3) et (4) respectivement par $\frac{\zeta^2}{N(\Delta)}$ et $\frac{\zeta^4}{N(\Delta^2)}$, il viendra

simplement:

$$\begin{cases} N(av'+(b-\sqrt{D})w') < N(av'+(b+\sqrt{D})w') \leqq \sigma^2 N(av'+(b-\sqrt{D})w'), \\ N(av'+(b+\sqrt{D})w')\,N(av'+(b-\sqrt{D})w') \leqq N\left(\frac{a}{\Delta^2}\right), \end{cases} \tag{5}$$

de sorte que le nombre Z qu'il s'agit de déterminer, coïncide maintenant avec celui des combinaisons v', w' qui satisfont à ces dernières inégalités, dans lesquelles v' et w' ont la signification indiquée plus haut.

Il faut maintenant remplacer les nombres complexes, contenus dans ces inégalités, par leurs éléments réels. Posons pour cela:

$$v'=x+x'i, \quad w'=y+y'i, \tag{6}$$

où les quatre quantités réelles x, x', y, y' sont les termes généraux d'autant de progressions arithmétiques, indéfiniment prolongées dans les deux sens et dont la raison commune est ζ. Posons encore:

$$a=\alpha+\alpha'i, \quad b=\beta+\beta'i, \quad \sqrt{D}=\delta+\delta'i, \tag{7}$$

α, α', β, β', δ, δ' étant des constantes réelles, et soit enfin, pour abréger:

$$\begin{cases} p=\alpha x-\alpha' x', \quad q=\beta y-\beta' y', \quad r=\delta y-\delta' y', \\ p'=\alpha' x+\alpha x', \quad q'=\beta' y+\beta y', \quad r'=\delta' y+\delta y'. \end{cases} \tag{8}$$

En substituant les expressions (6) et (7), les inégalités (5) prendront la forme:

$$\begin{cases} (p+q-r)^2+(p'+q'-r')^2<(p+q+r)^2+(p'+q'+r')^2 \\ \qquad \leqq \sigma^2((p+q-r)^2+(p'+q'-r')^2), \\ ((p+q+r)^2+(p'+q'+r')^2)((p+q-r)^2+(p'+q'-r')^2) \leqq N\left(\frac{a}{\Delta^2}\right). \end{cases} \tag{9}$$

Il est maintenant facile de reconnaître que l'entier Z, lorsque la variable ζ dont il est fonction, devient infiniment petite, dépend de l'intégrale suivante:

$$\iiiint dx\,dx'\,dy\,dy' = A, \tag{10}$$

dans laquelle les différentielles dx, dx', dy, dy' sont considérées comme positives, et qui est supposée s'étendre à toutes les valeurs des variables x, x', y, y' compatibles avec les conditions (9). En effet, si dans l'intégrale précédente l'on considère les quatre différentielles comme constantes et égales à ζ, tous les éléments de cette intégrale auront la valeur commune ζ^4, de sorte que l'intégrale sera égale au produit de ζ^4 par le nombre des combinaisons x, x', y, y' qui satisfont aux conditions (9), et dans lesquelles les variables sont supposées

croître de la différence constante ζ. Or, ce dernier nombre étant précisément l'entier Z, on aura pour une valeur infiniment petite de ζ:

$$Z\zeta^4 = A,$$

ou ce qui revient au même:

$$Z = Az, \tag{11}$$

z étant supposé infini. Il est encore facile de s'assurer qu'en même temps que le rapport des deux membres de cette dernière équation tend vers la limite 1, leur différence croît moins rapidement qu'une puissance de z, dont l'exposant constant serait tant soit peu supérieur à $\frac{3}{4}$, et généralement à $\frac{m-1}{m}$, s'il s'agissait d'une intégrale de l'ordre m*).

Tout se réduit donc maintenant à obtenir la valeur A de l'intégrale (10). Pour y parvenir, on pourrait faire usage d'une substitution unique, mais le calcul devient beaucoup plus simple, si l'on emploie plusieurs substitutions successives. Observons que, l'ordre des intégrations étant arbitraire, nous pouvons considérer les intégrations relatives à x et x' comme devant être effectuées les premières, et que rien ne s'oppose alors à ce que nous remplacions les variables x et x' par de nouvelles variables t et t', liées aux premières par des équations qui contiennent y et y', pourvu que dans ces équations l'on traite y et y' comme des constantes. Posons donc:

$$t = p+q, \quad t' = p'+q',$$

p, q, p', q' désignant les expressions linéaires (8). Si l'on applique la formule connue qui sert à la transformation des intégrales doubles, on trouvera que le produit $dxdx'$ devra être remplacé par:

$$\frac{1}{a^2+a'^2}\,dtdt' = \frac{1}{N(a)}\,dtdt'.$$

*) Le principe dont nous faisons usage dans le texte, est évident et résulte immédiatement de la notion même d'une intégrale multiple, considérée comme une somme d'éléments infiniment petits, lorsque, comme il arrive ici, les variables ne doivent pas obtenir des valeurs infinies dans les intégrations qu'il s'agit d'effectuer; mais il est bon d'ajouter que si, l'intégrale elle-même restant toujours finie, cette dernière circonstance n'avait plus lieu, l'application du même principe pourrait conduire à des résultats entièrement erronés, ce dont il est facile de voir la raison, et comme on peut d'ailleurs s'en assurer par des exemples, en considérant une intégrale double exprimant une aire finie, comprise entre une courbe et son asymptote. Quant à l'assertion que nous venons d'avancer et d'après laquelle les variables x, x', y, y' ne sauraient être infinies dans notre cas, elle résulte trop simplement des conditions (9), pour qu'il soit nécessaire de nous y arrêter.

En substituant cette dernière expression dans l'intégrale et les nouvelles variables dans les conditions (9), qui définissent l'étendue des intégrations, on aura:

$$\iiiint dtdt'dydy' = AN(a),$$
$$(t-r)^2+(t'-r')^2 < (t+r)^2+(t'+r')^2 < \sigma^2((t-r)^2+(t'-r')^2),$$
$$((t+r)^2+(t'+r')^2)((t-r)^2+(t'-r')^2) < N\left(\frac{a}{A^2}\right),$$

où nous avons supprimé les signes d'égalité qui accompagnaient ceux d'inégalité et qui sont désormais inutiles, les conditions précédentes se rapportant maintenant à des variables continues. Si en second lieu, t et t' étant considérés comme constants, nous remplaçons les variables y et y' à leur tour par de nouvelles variables r et r', liées à y et y' par les deux dernières des formules (8), l'intégrale deviendra:

$$\iiiint dtdt'drdr' = AN(a)\sqrt{D},$$

les conditions qui en définissent l'étendue, étant toujours celles que nous venons d'écrire. Distribuons actuellement les quatre variables en ces deux groupes: t, r; t', r', et remplaçons-les respectivement par ces deux nouveaux groupes: x, x'; y, y', liés aux précédents par les équations:

$$x = t-r, \quad x' = t+r; \quad y = t'-r', \quad y' = t'+r',$$

en vertu desquelles il faudra mettre $\frac{1}{2}dxdx'$, $\frac{1}{2}dydy'$ respectivement à la place de $dtdr$, $dt'dr'$. L'intégrale et les conditions qui s'y rapportent, se changeront ainsi en:

$$\iiiint dxdydx'dy' = 4AN(a)\sqrt{D},$$
$$x^2+y^2 < x'^2+y'^2 < \sigma^2(x^2+y^2), \quad (x^2+y^2)(x'^2+y'^2) < N\left(\frac{a}{A^2}\right).$$

Remplaçons maintenant les variables de chacun des groupes x, y et x', y' par des coordonnées polaires, en posant:

$$x = \varrho\cos\theta, \quad y = \varrho\sin\theta; \quad x' = \varrho'\cos\theta', \quad y' = \varrho'\sin\theta',$$

où il importe de remarquer qu'indépendamment des conditions auxquelles les nouvelles variables doivent satisfaire en vertu des inégalités précédentes, il faudra regarder ϱ comme positif et θ comme étant compris entre les limites 0 et 2π, pour qu'à une même combinaison x, y ne réponde pas plus d'une combinaison ϱ, θ, et que ϱ', θ' doivent être assujettis à la même limitation. Par l'intro-

duction de ces nouvelles variables, il viendra:

$$\iiiint \varrho\varrho' d\varrho d\varrho' d\theta d\theta' = 4AN(a\sqrt{D}), \quad \varrho^2 < \varrho'^2 < \sigma^2\varrho^2, \quad \varrho^2\varrho'^2 < N\left(\frac{a}{\Delta^2}\right).$$

Les conditions d'inégalité ne contenant pas les variables θ et θ', les intégrations qui s'y rapportent, devront s'étendre depuis 0 jusqu'à 2π; en effectuant ces deux intégrations et remplaçant en outre ϱ^2, ϱ'^2 respectivement par ϱ, ϱ', de sorte que ces nouvelles variables devront être considérées comme positives, on trouvera:

$$\iint d\varrho d\varrho' = \frac{4}{\pi^2} AN(a\sqrt{D}), \quad \varrho < \varrho' < \sigma^2\varrho, \quad \varrho\varrho' < N\left(\frac{a}{\Delta^2}\right).$$

Si maintenant, ϱ étant regardé comme constant, nous remplaçons ϱ' par une nouvelle variable ν, déterminée par l'équation $\varrho' = \nu\varrho$, et qui en vertu de ce qui précède, doit être considérée comme positive, nous aurons d'abord:

$$\iint \varrho d\varrho d\nu = \frac{4}{\pi^2} AN(a\sqrt{D}), \quad 1 < \nu < \sigma^2, \quad \varrho^2 < \frac{1}{\nu} N\left(\frac{a}{\Delta^2}\right),$$

et par suite, en effectuant l'intégration relative à ϱ, et qui doit s'étendre depuis $\varrho^2 = 0$ jusqu'à $\varrho^2 = \frac{1}{\nu} N\left(\frac{a}{\Delta^2}\right)$:

$$\int \frac{d\nu}{\nu} = \frac{8}{\pi^2} AN(\Delta^2\sqrt{D}), \quad 1 < \nu < \sigma^2,$$

d'où l'on conclut enfin:

$$A = \frac{\pi^2 \log\sigma}{4N(\Delta^2\sqrt{D})}.$$

Après avoir ainsi déterminé le coefficient A, contenu dans l'équation (11), il sera facile de voir ce que la somme partielle (2) devient, lorsque l'exposant s converge vers l'unité, ou ce qui revient au même, lorsque la variable positive ϱ, supposée liée à s par l'équation $s = 1 + \varrho$, est considérée comme infiniment petite. En effet, comme la fonction Z qui exprime combien de fois dans la somme en question, l'expression $N(ax^2 + 2bxy + cy^2)$ obtient une valeur qui ne surpasse pas celle de z, est telle que les deux rapports:

$$\frac{Z}{Az^\gamma}, \quad \frac{Z - Az}{z^\gamma},$$

où γ désigne une constante supérieure à la fraction $\frac{3}{4}$, convergent le premier vers une limite égale à l'unité, le second vers la limite zéro, lorsque la variable z devient plus grande que toute grandeur donnée, on conclut sur-le-champ, du

lemme démontré dans le §. 1 du Mémoire déjà plusieurs fois cité[1]), que pour une valeur infiniment petite de ϱ, la somme (2) prend cette forme très simple:

$$\frac{A}{\varrho} = \frac{\pi^2 \log\sigma}{4N(\Delta^2\sqrt{D})} \frac{1}{\varrho}\ ^*).$$

Cette expression ne présente rien qui soit particulier à la somme partielle que nous avons considérée, ni même rien qui soit particulier à la somme totale dont cette somme partielle fait partie, puisqu'elle n'est fonction que du seul déterminant D, commun à toutes les formes quadratiques contenues dans le second membre de l'équation (9) du §. 17. On voit donc qu'il suffit de la multiplier par le nombre $N(\Delta)\psi(\Delta)$ des sommes partielles contenues dans une même somme totale, et par celui des formes qui constituent un système complet relativement au déterminant D, pour en conclure la valeur du second membre de l'équation dont il s'agit, lorsqu'on y considère ϱ comme infiniment petit. Il viendra ainsi:

$$(12) \qquad H \frac{\pi^2 \psi(\Delta) \log\sigma}{4N(\Delta\sqrt{D})} \frac{1}{\varrho},$$

H désignant le nombre des classes qui répondent au déterminant D.

II. Il s'agit maintenant de considérer le premier membre de l'équation citée. Ce membre pouvant se mettre sous la forme:

$$4\Sigma \frac{1}{(N(n))^s} \cdot 2\Sigma\left[\frac{D}{n}\right] \frac{1}{(N(n))^s},$$

occupons-nous d'abord du premier de ces deux facteurs. Comme la somme dont il s'agit, doit s'étendre à tous les entiers n, premiers à Δ et en outre primaires, il est évident que nous pouvons faire abstraction de la dernière de ces deux conditions, pourvu qu'en même temps nous omettions le facteur 4. Les valeurs que n doit recevoir, peuvent se distribuer en systèmes de la forme

*) Quoique les deux propriétés dont nous venons de faire usage, ressortent l'une et l'autre avec évidence des considérations indiquées plus haut, il peut être bon de faire remarquer que la première de ces propriétés suffit à elle seule pour en tirer la conclusion que nous venons d'énoncer. C'est ce qui résulte d'une remarque déjà faite dans le Mémoire précédent, et d'après laquelle le lemme dont il s'agit, comporte plus d'étendue qu'il n'a été nécessaire de lui donner à l'endroit cité. Il est en effet facile de reconnaitre que la vérité de ce lemme ne suppose qu'une seule condition, consistant en ce que la fonction, désignée par $f(t)$ dans son énoncé, doit être telle que l'on ait $\frac{f(t)}{t} = c$, lorsque t obtient une valeur infinie. Pour s'en assurer, on n'aura qu'à apporter une modification assez légère et qui se présente facilement, à la démonstration qui a été exposée dans le Mémoire précédent.

[1]) S. 415 und 416 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

$n = v\Delta + \alpha$, v et α désignant des entiers complexes, le premier indéterminé, le second déterminé pour chaque système, et devant être égalé successivement à tous ceux des termes d'un système de résidus pour le module Δ qui n'ont pas de diviseur commun avec ce module. Considérons la somme partielle, répondant à l'un quelconque de ces termes, et qui est:

$$\Sigma \frac{1}{(N(v\Delta+\alpha))^{1+\varrho}}.$$

Pour en obtenir la valeur, soit z une variable positive et Z la fonction discontinue de z qui exprime le nombre des entiers v pour lesquels on a:

$$N(v\Delta+\alpha) \leqq z.$$

Si nous posons, pour abréger, $z = \frac{1}{\zeta^2}$, ζ étant positif, et que nous remplacions v par une nouvelle indéterminée v' telle qu'on ait:

$$v' = \left(v + \frac{\alpha}{\Delta}\right)\zeta,$$

l'inégalité précédente se changera en celle-ci:

$$N(v') \leq \frac{1}{N(\Delta)},$$

et Z désignera alors le nombre des valeurs v' qui satisfont à cette condition. Or, en posant $v' = x + x'i$, x et x' seront évidemment les termes généraux de deux suites dont la première différence est constante et égale à ζ; on voit donc, comme plus haut, que pour une valeur infinie de z, on aura $Z = Bz$, B désignant l'intégrale:

$$\iint dx\,dx', \quad x^2 + x'^2 < \frac{1}{N(\Delta)}.$$

Mais cette intégrale étant évidemment égale à $\frac{\pi}{N(\Delta)}$, on conclura du lemme déjà employé dans le numéro précédent que la somme partielle que nous considérons, se réduit simplement à $\frac{\pi}{N(\Delta)}\frac{1}{\varrho}$ lorsque la variable ϱ est supposée devenir moindre que toute grandeur donnée; d'où il suit enfin:

$$4\Sigma \frac{1}{(N(n))^{1+\varrho}} = \frac{\pi\psi(\Delta)}{N(\Delta)}\frac{1}{\varrho}, \tag{13}$$

le signe sommatoire s'étendant, comme dans l'équation (9) du §. 17, à tous les entiers n premiers à Δ et en outre primaires.

III. Pour mettre enfin la seconde des deux sommes, rappelées au commencement du numéro précédent, sous la forme appropriée à notre but, il faut distinguer plusieurs cas différents que le déterminant D peut présenter. Observons pour cela que, si nous réunissons en un seul carré tous les facteurs doubles de D, nous pourrons toujours mettre cet entier sous la forme:

$$D = \chi Q V^2, \tag{14}$$

χ ayant l'une de ces quatre valeurs:

$$\chi = 1, \quad \chi = i, \quad \chi = 1+i, \quad \chi = i(1+i), \tag{15}$$

et Q ou $-Q$ désignant un produit de facteurs simples impairs et primaires, tous inégaux, sans exclure le cas où l'on aurait $Q = \pm 1$, qui ne peut toutefois avoir lieu qu'autant qu'on n'a pas $\chi = 1$, les déterminants carrés étant toujours exclus. Nous ajouterons que si les entiers χ, Q, V doivent être tels que nous venons de les définir, ils seront complètement déterminés pour tout déterminant donné, si ce n'est que Q, V^2 peuvent être simultanément remplacés par $-Q$, $(Vi)^2$.

Cela posé, nous allons transformer l'expression $\left[\frac{D}{n}\right]$ au moyen des équations (e) et (f) du §. 8. On a d'abord évidemment en vertu des équations citées:

$$\left[\frac{D}{n}\right] = \left[\frac{\chi Q V^2}{n}\right] = \left[\frac{\chi}{n}\right]\left[\frac{Q}{n}\right] = \left[\frac{\chi}{n}\right]\left[\frac{n}{Q}\right].$$

Pour transformer le facteur $\left[\frac{\chi}{n}\right]$, il devient nécessaire d'introduire explicitement les deux entiers réels contenus dans n; posons donc $n = \lambda + \nu i$, λ et ν étant respectivement des formes $4k+1$, $2k$. Il viendra alors suivant les quatre cas déjà distingués (15), et en ayant égard aux deux premières des équations (f) citées:

$$\left[\frac{\chi}{n}\right] = 1, \quad \left[\frac{\chi}{n}\right] = (-1)^{\frac{1}{4}(\lambda^2+\nu^2-1)},$$

$$\left[\frac{\chi}{n}\right] = (-1)^{\frac{1}{4}((\lambda+\nu)^2-1)}, \quad \left[\frac{\chi}{n}\right] = (-1)^{\frac{1}{4}(\lambda^2+\nu^2-1)+\frac{1}{4}((\lambda+\nu)^2-1)}.$$

Pour réunir ces quatre expressions en une seule formule, nous poserons $\delta = \pm 1$, $\varepsilon = \pm 1$, les signes ambigus étant choisis suivant les quatre cas que χ peut présenter en vertu des équations (15), comme il suit:

$$\delta = 1, \quad \varepsilon = 1; \quad \delta = -1, \quad \varepsilon = 1; \quad \delta = 1, \quad \varepsilon = -1; \quad \delta = -1, \quad \varepsilon = -1. \tag{16}$$

Cette convention admise, nous aurons pour tous les cas:

$$\left[\frac{\chi}{n}\right] = \delta^{\frac{1}{4}(\lambda^2+\nu^2-1)}\varepsilon^{\frac{1}{4}((\lambda+\nu)^2-1)}.$$

Au moyen de cette dernière expression et de celles déjà obtenues, le facteur du premier membre de l'équation (9) du §. 17, qu'il s'agissait de transformer, prendra la forme:

$$(17)\quad 2\Sigma\left[\frac{D}{n}\right]\frac{1}{(N(n))^{1+\varrho}} = 2\Sigma\vartheta^{\frac{1}{4}(\lambda^2+\nu^2-1)}\varepsilon^{\frac{1}{4}((\lambda+\nu)^2-1)}\left[\frac{\lambda+\nu i}{Q}\right]\frac{1}{(\lambda^2+\nu^2)^{1+\varrho}}.$$

IV. Si maintenant nous substituons les expressions (12), (13) et (17) dans l'équation citée, et que nous effacions le facteur $\frac{1}{\varrho}$ et les autres facteurs communs aux deux membres, l'équation dont il s'agit, prendra la forme:

$$(18)\quad H = \frac{8N(\sqrt{D})}{\pi\log\sigma}\,\Sigma\vartheta^{\frac{1}{4}(\lambda^2+\nu^2-1)}\varepsilon^{\frac{1}{4}((\lambda+\nu)^2-1)}\left[\frac{\lambda+\nu i}{Q}\right]\frac{1}{(\lambda^2+\nu^2)^{1+\varrho}}.$$

Telle est la suite infinie double qui exprime le nombre des classes pour un déterminant quelconque non-carré D, et dans laquelle nous avons conservé la quantité infiniment petite ϱ, qui ne doit être annulée qu'après que l'on aura fixé l'ordre dans lequel les termes de la double somme doivent se suivre, pour que cette somme soit en effet la limite de celle qui répond à une valeur infiniment petite de la variable positive ϱ. La signification des lettres qui entrent dans l'équation, a été fixée dans ce qui précède, et l'on devra se rappeler que la double sommation doit s'étendre à tous les couples d'entiers réels λ et ν, respectivement des formes $4k+1$, $2k$, et tels que l'entier complexe correspondant $\lambda+\nu i$ soit premier à D.

Pour effectuer la double sommation, il faudra d'abord transformer le facteur $\left[\frac{\lambda+\nu i}{Q}\right]$ au moyen de l'équation (h) du §. 8, et remplacer ensuite les nouveaux symboles ainsi introduits par une suite finie de sinus ou de cosinus, en se servant pour cet objet des formules connues dues à M. Gauss. Après ces deux substitutions, l'une des deux sommations pourra être exécutée au moyen d'une suite trigonométrique, dont la somme a été donnée par Euler, et la suite infinie double, réduite par-là à une série simple, se décomposera alors en plusieurs séries partielles qui rentrent dans celles par lesquelles Abel et M. Jacobi ont développé les fonctions trigonométriques de l'amplitude d'une fonction elliptique de première espèce. Mais si avec le secours des formules dont les illustres géomètres que nous venons de citer, ont enrichi l'Analyse, la sommation en elle-même ne présente pas de difficulté réelle et n'exige que peu d'espace, il n'en est pas de même de la discussion à laquelle il faut soumettre

le résultat qui s'en déduit, pour en reconnaître la véritable nature. Comme le résultat dont il s'agit, se trouve dépendre de la division en parties égales de la fonction elliptique complète de première espèce, pour le cas où le module a la valeur $\sqrt{\frac{1}{2}}$, et où le nombre de ces parties égales est un entier complexe, et que la théorie des équations algébriques qui se rapportent à une telle division, n'a été qu'ébauchée jusqu'à présent*), il sera nécessaire d'entrer à cet égard dans de nouveaux développements dont l'étendue excéderait de beaucoup les bornes que nous avons dû imposer à cette première partie de notre travail. C'est pourquoi et comme nous en avons déjà averti, nous réserverons ces détails pour la seconde partie, et nous terminerons celle-ci par l'examen des deux cas particuliers, déjà mentionnés dans le préambule du présent Mémoire.

Examen de deux cas particuliers.

§. 19.

Les deux cas qu'il s'agit de considérer, sont ceux où le déterminant D est un entier réel ou le produit d'un tel entier par i. Comme en vertu de l'équation (18) du paragraphe précédent, le nombre des classes est évidemment le même pour deux déterminants opposés, nous pourrons toujours considérer comme positif, l'entier dont il vient d'être question.

I. Soit en premier lieu D un entier positif non-carré, et soit S^2 le plus grand carré réel qui divise D. Nous aurons alors l'un de ces deux cas:

$$(1)\qquad D = PS^2,\quad D = 2PS^2,$$

P désignant un produit de nombres premiers positifs, impairs et tous inégaux, produit qui peut d'ailleurs se réduire à l'unité dans le second cas. Comme, en considérant P comme complexe, cet entier ou son opposé est primaire et n'a que des facteurs simples inégaux, il suffit de mettre la seconde des équations (1) sous la forme $D = iP((1-i)S)^2$, pour reconnaître que les équations (14), (15) et (16) du §. 18, qui se rapportent à un déterminant quelconque, donnent relativement au cas particulier qui nous occupe, $Q = P$, $\varepsilon = 1$, $\vartheta = \pm 1$, où il faut choisir le signe supérieur ou le signe inférieur dans la dernière de ces équations, selon que D présente le premier ou le second des deux cas (1). En substituant

*) Voir un Mémoire d'Abel, inséré dans le Journal de Crelle, Tome III, p. 160[2]).

[2]) Oeuvres complètes de N. H. Abel, Édition de 1839, T. I, p. 221; Édition de 1881, T. I, p. 352. K.

ces valeurs dans l'expression générale de H, et remplaçant en même temps σ par sa valeur, donnée par la formule (3) du §. 14, ainsi que $\left[\frac{\lambda+\nu i}{P}\right]$ par l'expression équivalente, fournie par la première des équations (g) du §. 8, il viendra:

$$(2) \qquad H = \frac{8D}{\pi\varkappa\log(\tau+v\sqrt{D})} \Sigma\delta^{\frac{1}{2}(\lambda^2+\nu^2-1)}\left(\frac{\lambda^2+\nu^2}{P}\right)\frac{1}{(\lambda^2+\nu^2)^{1+\varrho}},$$

de sorte que la somme double ne contient plus l'entier complexe $\lambda+\nu i$, mais seulement sa norme $\lambda^2+\nu^2$. Il est vrai que cet entier semble y entrer encore implicitement par la condition que $\lambda+\nu i$ doit être premier à D; mais ce dernier entier étant réel, on voit que la condition dont il s'agit, revient à celle que D et $\lambda^2+\nu^2$ doivent être sans diviseur commun.

II. Considérons en second lieu un déterminant de la forme $D = D'i$, D' étant un entier positif qu'il faudra seulement supposer tel que $2D'$ ne soit pas un carré, sans quoi D serait lui-même un carré. Si nous désignons par S'^2 le plus grand carré réel qui divise $2D'$, nous aurons l'une ou l'autre de ces deux équations:

$$(3) \qquad 2D' = P'S'^2, \quad 2D' = 2P'S'^2,$$

dans lesquelles P' est un produit de nombres premiers positifs, impairs et inégaux, S' étant pair dans la première de ces deux équations. Ces équations donnent respectivement celles-ci:

$$D = P'((1+i)\tfrac{1}{2}S')^2, \quad D = P'iS'^2,$$

qu'il suffit de comparer aux équations déjà citées du §. 18, pour voir que nous avons $Q = P'$, $\varepsilon = 1$, $\delta = \pm 1$, le signe supérieur ou le signe inférieur devant être choisi, selon que $2D'$ présente le premier ou le second des deux cas (3). Au moyen de ces valeurs et par des transformations analogues à celles que nous avons opérées dans le numéro précédent, l'on trouvera:

$$(4) \qquad H = \frac{8D'}{\pi\varkappa\log(\tau+v\sqrt{2D'})} \Sigma\delta^{\frac{1}{2}(\lambda^2+\nu^2-1)}\left(\frac{\lambda^2+\nu^2}{P'}\right)\frac{1}{(\lambda^2+\nu^2)^{1+\varrho}},$$

$\varkappa$, τ, v ayant la même signification que dans l'équation (4) du §. 14, et la double sommation devant s'étendre à tous les couples d'entiers réels λ, ν, respectivement compris dans les formes $4k+1$, $2k$, et tels que $\lambda^2+\nu^2$ soit premier à D'.

III. Nous allons maintenant faire voir que les sommes doubles (2) et (4) peuvent être remplacées chacune par un produit de deux séries simples. La

transformation qu'il s'agit d'effectuer, n'est qu'une application très particulière de certaines équations générales dont nous avons eu à faire usage dans le Mémoire précédent (§. 6, V.)[1]; mais, pour mieux faire sentir le principe sur lequel cette transformation repose, il nous paraît préférable de la rattacher à un théorème arithmétique très simple et susceptible d'une démonstration tout élémentaire. Voici en quoi consiste ce théorème:

„m désignant un entier positif et impair donné, le nombre des solutions de l'équation $m = x^2+y^2$, dans laquelle x et y sont des entiers réels indéterminés, est égal au quadruple excès du nombre des diviseurs (positifs) de m, qui sont compris dans la forme $4k+1$, sur celui de ces diviseurs qui ont la forme $4k+3$.“ *)

Comme les entiers x et y qui satisfont à l'équation précédente, sont toujours l'un pair, l'autre impair, on voit que si l'on considère l'un de ces entiers, le second par exemple, comme devant être pair, le nombre des solutions se réduira de moitié, et l'on voit également que si l'on suppose en outre x, pris avec son signe, de la forme $4k+1$, le nombre des solutions éprouvera une seconde réduction de même étendue, et deviendra simplement égal à l'excès défini dans l'énoncé, puisqu'à une même valeur de y répondent toujours deux valeurs opposées de x, qui sont l'une de la forme $4k+1$, l'autre de la forme $4k+3$. Au moyen de ce résultat, il est facile de former l'équation générale que nous allons écrire:

$$\Sigma F(x^2+y^2) = \Sigma(-1)^{\frac{1}{2}(n-1)}F(nn'),$$

et dans laquelle la double sommation, indiquée dans le premier membre, doit s'étendre à tous les entiers positifs ou négatifs x et y, respectivement compris dans les formes $4k+1$, $2k$, tandis que celle du second membre est supposée embrasser tous les entiers impairs et positifs n et n'. D'après la manière dont cette équation subsiste, il est encore évident qu'elle ne cessera pas d'avoir lieu, si aux conditions énoncées nous ajoutons celles que x^2+y^2 soit premier à un entier réel donné K, et qu'il en soit de même du produit nn', ces nouvelles conditions n'ayant d'autre effet que de supprimer les mêmes termes de part et d'autre. Ainsi restreintes, les indéterminées x et y auront la même signification

[1] S. 456 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

*) Voyez pour la démonstration de ce théorème, dû à M. Jacobi, le Tome XII du Journal de Crelle, p. 167, ou le Mémoire cité, §. 7.[2]

[2] S. 463 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

que celles désignées par λ et ν dans les sommes (2) et (4), en supposant respectivement $K = D$ ou $K = D'$, tandis que n et n' devront être respectivement supposés premiers à D ou à D'. Cela posé, si dans les deux sommes (2) et (4) nous remplaçons l'exposant de δ, par le produit:

$$\tfrac{1}{4}(\lambda^2+\nu^2-1)\cdot\tfrac{1}{4}(\lambda^2+\nu^2+1) = \tfrac{1}{8}((\lambda^2+\nu^2)^2-1),$$

ce qui est permis, le facteur ajouté étant impair, il suffira de supposer la fonction arbitraire $F(z)$ de la forme:

$$\vartheta^{\frac{1}{8}(z^2-1)}\left(\frac{z}{P}\right)\frac{1}{z^{1+\varepsilon}},$$

pour conclure de l'équation en question que la somme double (2) est équivalente à celle-ci:

$$\Sigma(-1)^{\frac{1}{2}(n-1)}\,\vartheta^{\frac{1}{8}((nn')^2-1)}\left(\frac{nn'}{P}\right)\frac{1}{(nn')^{1+\varepsilon}},$$

où le signe Σ se rapporte à tous les entiers positifs n et n', impairs et premiers à D. Observons maintenant que, l'exposant de ϑ étant toujours pair ou impair en même temps que le nombre $\frac{1}{8}(n^2-1)+\frac{1}{8}(n'^2-1)$, comme nous avons déjà eu occasion de le remarquer dans le §. 8, nous pouvons le remplacer par ce dernier. Par cette substitution, le terme général de la somme précédente se changera en un produit de deux facteurs qui ne contiennent chacun qu'un seul des entiers n et n', de sorte que la somme elle-même prendra la forme d'un produit de deux séries simples. On obtient ainsi et en substituant dans l'équation (2), celle que nous allons écrire:

$$(2')\qquad H = \frac{8D}{\pi\varkappa\log(\tau+v\sqrt{D})}\,\Sigma\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}\cdot\Sigma(-1)^{\frac{1}{2}(n-1)}\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n},$$

chacune des deux sommations indiquées s'étendant à tous les entiers positifs n, impairs et premiers à D. Pour plus de simplicité, nous avons remplacé n' par n, ce qui est permis, ces deux lettres ayant la même signification et ne se trouvant plus maintenant mêlées dans une même sommation. Nous avons en outre réduit à zéro la variable infiniment petite ϱ, les sommes précédentes étant en effet les limites de celles où l'on aurait conservé la quantité ϱ, pourvu que dans ces sommes l'on considère les entiers n comme formant une suite croissante, comme il est facile de s'en assurer, et comme on l'a d'ailleurs prouvé, en établissant les résultats qu'il sera nécessaire de rappeler dans le numéro suivant.

L'équation (4) étant soumise aux mêmes transformations, se changera en celle-ci:

$$(4')\qquad H = \frac{8D'}{\pi\varkappa\log(\tau+v\sqrt{2D'})}\,\Sigma\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P'}\right)\frac{1}{n}\cdot\Sigma(-1)^{\frac{1}{2}(n-1)}\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P'}\right)\frac{1}{n}.$$

IV. Il faut maintenant rappeler les résultats qui se rapportent aux formes quadratiques à coefficients réels, pour les comparer à ceux que nous venons d'établir. C'est ce que nous allons faire, en choisissant les notations de manière à faciliter la comparaison dont il s'agit. Dans le Mémoire précédent (§. 6, éq. 23)[1]), on a démontré que relativement à un déterminant positif non-carré D, le nombre des classes que nous désignerons par h_1, est donné par l'équation:

$$(5)\qquad h_1 = \frac{2\sqrt{D}}{\log(\tau+v\sqrt{D})}\,\Sigma\theta^{\frac{1}{2}(n-1)}\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n}.$$

Dans cette équation la signification des lettres τ, v, ϑ, P et n est la même que dans les équations précédentes (1), (2) et (2'), et la sommation a la même étendue que dans la dernière de ces équations. Quant à la lettre θ, elle désigne l'unité positive ou négative, selon que P est de la forme $4k+1$ ou $4k+3$. Si nous considérons en second lieu le déterminant opposé $-D$, et que nous dénotions par h_2 le nombre des classes qui y répondent, il résulte de l'équation (19)[2]) du paragraphe déjà cité, qu'on aura:

$$(6)\qquad h_2 = \frac{2\sqrt{D}}{\pi}\,\Sigma(-\theta)^{\frac{1}{2}(n-1)}\vartheta^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right)\frac{1}{n},$$

la signification de toutes les lettres et l'étendue de la sommation restant toujours les mêmes. Or, θ étant toujours de la forme ± 1, on voit que les deux séries contenues dans les équations (5) et (6), coïncident avec celles de l'équation (2'), de sorte qu'en divisant cette dernière par le produit des deux autres (5) et (6), on trouvera ce résultat très simple:

$$H = \frac{2}{\varkappa}h_1h_2.$$

L'autre cas qui est celui d'un déterminant de la forme $D'i$, conduit à un résultat analogue; il suffit pour l'obtenir, de remplacer dans ce qui précède, les équations (5) et (6), par celles qui expriment les nombres h_1 et h_2 des classes

[1]) S. 456 dieser Ausgabe von G. Lejeune Dirichlet's Werken. [2]) S. 451 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

réelles répondant aux déterminants $2D'$ et $-2D'$. On trouve alors:

$$H = \frac{1}{x} h_1 h_2.$$

Nous avons donc ces deux théorèmes très remarquables:

„D désignant un entier positif non-carré, soit H le nombre des classes dans lesquelles se distribuent les formes à coefficients complexes et au déterminant D, soient encore h_1 et h_2 les nombres des classes pour les formes à coefficients réels, répondant respectivement aux deux déterminants D et $-D$; toutes ces formes étant supposées telles que les coefficients extrêmes et le double coefficient moyen ne présentent pas de diviseur commun. Cela étant, on aura toujours:

$$H = 2h_1h_2 \quad \text{ou} \quad H = h_1h_2,$$

selon que l'équation indéterminée $t^2 - Du^2 = -1$ admettra des solutions réelles ou non."

„D désignant un entier positif dont le double ne soit pas un carré, si l'on suppose que les lettres H, h_1, h_2, en conservant une signification analogue à celle de l'énoncé précédent, se rapportent maintenant aux déterminants Di, $2D$, $-2D$, on aura:

$$H = h_1h_2 \quad \text{ou} \quad 2H = h_1h_2,$$

selon que l'équation $t^2 - 2Du^2 = -1$ admettra des solutions réelles ou non." *)

Quoique les théorèmes précédents ne contiennent aucun élément qui ne soit relatif aux nombres entiers, il paraît difficile de les établir par des considérations purement arithmétiques, tandis que la méthode mixte dont nous venons de faire usage, et qui est fondée en partie sur l'emploi de quantités variant par degrés insensibles, nous y a conduit de la manière la plus naturelle et, pour ainsi dire, sans effort.

*) On suppose tacitement dans ces énoncés, comme on le fait ordinairement, que pour un déterminant négatif on n'admette que des formes réelles dont les coefficients extrêmes soient positifs. Si l'on n'adoptait pas cet usage, le nombre h_2 aurait une valeur double de celle que nous lui supposons, et les deux énoncés seraient à modifier en conséquence.

SUR LA THÉORIE DES NOMBRES.

PAR

G. LEJEUNE DIRICHLET.

Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Tome X, p. 285—288.