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

SCHERING

# Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres

*Journal de mathématiques pures et appliquées 2^e série*, tome 4 (1859), p. 253-270.
<http://www.numdam.org/item?id=JMPA_1859_2_4__253_0>

# THÉORÈMES

RELATIFS

# AUX FORMES BINAIRES QUADRATIQUES QUI REPRÉSENTENT LES MÊMES NOMBRES;

PAR M. SCHERING,
Astronome à l'observatoire de Gottingue.

Les deux théorèmes de M. Dirichlet, l'un d'après lequel toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers (*Mémoires de l'Académie de Berlin,* année 1837, et Journal de M. Liouville, 1re série, t. IV, p. 393), et l'autre, qui concerne la possibilité d'exprimer des nombres premiers par toute forme binaire quadratique proprement primitive (*Comptes rendus de l'Académie de Berlin,* année 1840, p. 49, et Journal de Crelle, t. XXI, p. 98), sont d'une grande utilité dans l'arithmétique supérieure. Au moyen de ces propositions, on peut prouver le théorème remarqué, mais non démontré, par Legendre (dans sa *Théorie des nombres,* 3e édition, t. I, p. 237), d'après lequel une forme, qui représente tous les nombres représentés par une autre forme, contient cette dernière. La démonstration du théorème que je viens d'énoncer et qui n'éprouve des exceptions que dans des cas particuliers, fera le sujet du présent Mémoire.

THÉORÈME I. — *Si la forme* $axx + 2bxy + cyy$ *de l'ordre* o, *de déterminant* $d$ *et de la* $e^{ième}$ *espèce, représente tous les nombres qui peuvent être représentés par la forme* $AXX + 2BXY + CYY$ *de l'ordre* O, *de déterminant* D *et de la* $E^{ième}$ *espèce,* $\frac{EO}{eo}$ *sera entier et* $\frac{EED}{eed}$ *sera un nombre carré entier.*

1°. *On a* $\frac{EO}{eo}$ *entier.*

Pour abréger, nous désignerons une forme

$$AXX + 2BXY + CYY, \quad axx + 2bxy + cyy$$

par (A, B, C), $(a, b, c)$, quand nous ne parlerons pas des valeurs des indéterminées X, Y, $x$, $y$. D'après la définition de l'ordre O et de la E$^{\text{ième}}$ espèce d'une forme (A, B, C), le nombre O est le plus grand diviseur commun de A, B et C; mais EO est celui de A, 2B et C de manière que E est égal à 1 ou 2 suivant que la forme $\left(\frac{A}{O}, \frac{B}{O}, \frac{C}{O}\right)$ est proprement ou improprement primitive. Dans l'article 228 des *Disquisitiones Arithmeticæ auctore Gauss*, il est démontré qu'on peut représenter par une forme primitive $\left(\frac{A}{O}, \frac{B}{O}, \frac{C}{O}\right)$ un nombre impair ou pair [suivant que la forme est proprement (E = 1) ou improprement (E = 2) primitive] qui n'ait d'autre diviseur commun avec un nombre donné $eo$ que E. Soit E$n$ un tel nombre représenté par $\left(\frac{A}{O}, \frac{B}{O}, \frac{C}{O}\right)$, on pourra représenter le nombre EO$n$ par la forme (A, B, C), et comme nous avons supposé que tous les nombres qui peuvent être représentés par la forme (A, B, C) peuvent l'être aussi par $(a, b, c)$, le nombre EO$n$ sera représenté aussi par cette dernière forme. Tous les nombres représentés par $(a, b, c)$ étant divisibles par $eo$, le nombre EO$n$ le sera aussi, mais comme $n$ n'a pas de diviseur commun avec $eo$, celui-ci doit être diviseur de EO.

Les formes $\left(\frac{Ea}{o}, \frac{Eb}{o}, \frac{Ec}{o}\right)$ et $\left(\frac{EA}{o}, \frac{EB}{o}, \frac{EC}{o}\right)$ ayant entre eux le même rapport que $(a, b, c)$ et (A, B, C), nous ne considérerons que les premières, ou plutôt nous supposerons que pour la forme $(a, b, c)$, les nombres $e$ et $o$ soient tels, qu'on ait

$$eo = 1 \quad \text{ou} \quad eo = E.$$

2°. *Les deux déterminants d et* D *sont entre eux comme des nombres carrés.*

Pour prouver cela, nous nous appuyons sur ce lemme :

Si deux nombres $d$ et D ne sont pas entre eux comme des nombres carrés et qu'aucun des deux ne soit carré, il y aura des nombres par rapport auxquels l'un D est résidu, l'autre $d$ non résidu quadratique.

Soient $q$ et Q les plus grands carrés qui divisent $d$ et D, $\theta$ le plus

grand diviseur commun des nombres $\frac{d}{q}$ et $\frac{D}{Q}$, et enfin

$$d = q\theta\theta', \qquad D = Q\theta\theta'',$$

en prenant $\theta$ positif si l'un des nombres $d$, D est positif, et $\theta$ négatif si tous deux sont négatifs. Les nombres $\theta$, $\theta'$, $\theta''$ seront premiers entre eux, aucun ne sera divisible par un carré et deux parmi eux ne seront pas ensemble égaux à $+1$ ou à $-1$ et non plus négatifs.

Si $\theta'$ diffère de $\pm 1$ et de $\pm 2$, il y aura un nombre premier $p$ qui ne divise ni $q$ ni Q et remplit les conditions $\theta' \mathrm{N}p$, $\theta \mathrm{R}p$, $\theta'' \mathrm{R}p$ et par conséquent aussi celles-ci $d\mathrm{N}p$, $\mathrm{DR}p$, où les caractères R et N indiquent que le nombre précédent est résidu ou non résidu quadratique par rapport au suivant $p$. En effet, d'après la loi de réciprocité, tous les nombres premiers de la forme $8n+1$ et congrus à certains nombres par rapport au module $\theta'$ sont non diviseurs quadratiques de $\theta'$, et tous les nombres premiers de la forme $8n+1$ et congrus à certains nombres par rapport au module $\theta$ sont diviseurs quadratiques de $\theta$. Donc $\theta$ et $\theta'$ n'ayant aucun diviseur commun, tous les nombres premiers $p$ de la forme $8n+1$ qui sont congrus à certains nombres par rapport au module $\theta\theta'$, rempliront les conditions $\theta' \mathrm{N}p$, $\theta \mathrm{R}p$. De même on trouve que tous les nombres premiers $p$ congrus à certains nombres par rapport au module $8\theta\theta'\theta''$ remplissent les conditions $\theta' \mathrm{N}p$, $\theta \mathrm{R}p$, $\theta'' \mathrm{R}p$. Mais il y a, comme M. Dirichlet l'a démontré, une infinité de nombres premiers qui sont congrus à un nombre donné par rapport à un module donné, si le module et le nombre donné sont premiers entre eux. Cette condition étant remplie dans notre cas, il y aura une infinité de nombres premiers $p$ pour lesquels on a $\theta \mathrm{R}p$, $\theta' \mathrm{N}p$, $\theta'' \mathrm{R}p$. Parmi eux il y en a qui sont plus grands que $q$ et Q et ainsi ne divisent pas $d$ et D : ils seront diviseurs quadratiques de D, mais non pas de $d$. De même manière, on démontre que, si $\theta'$ est égal à $-1$ ou à $\pm 2$, il y a des nombres premiers respectivement de la forme $8n+7$ ou $8n+5$ qui remplissent les conditions mentionnées.

Si $\theta'$ est égal à $+1$, on peut démontrer d'une manière analogue qu'il y a des nombres premiers qui sont plus grands que $q$ et Q et pour lesquels on a $\theta \mathrm{N}p$, $\theta' \mathrm{R}p$, $\theta'' \mathrm{N}p$ et par suite $d\mathrm{N}p$, $\mathrm{DR}p$.

En revenant à notre théorème, supposons que les déterminants $d$ et D

ne sont pas entre eux comme des nombres carrés et que le nombre premier impair $p$ soit diviseur quadratique de D et non diviseur quadratique de $d$, en excluant de nos recherches les déterminants qui sont carrés. En désignant par $r$ et $s$ deux nombres entiers qui satisfassent à l'équation

$$rr = \mathrm{D} + ps,$$

nous aurons une forme $(p, r, s)$ de déterminant D par laquelle nous pourrons représenter le nombre premier $p$. La composition de la forme $(p, -r, s)$ et de (A, B, C) produit une autre forme $\varphi$ qui sera de l'ordre O et de la E$^{\text{ième}}$ espèce (article 245 des *Disquisitiones Arithmeticæ*), et par laquelle on peut représenter un nombre $n$ qui n'est pas divisible par $p$, comme nous avons supposé que $p$ ne divise pas 2D et conséquemment non plus EO. Cela résulte immédiatement de l'article 228 des *Disquisitiones Arithmeticæ*, d'après lequel une forme primitive représente aussi des nombres non divisibles par un nombre donné premier impair. La composition des deux formes proprement primitives et opposée l'une à l'autre $(p, r, s)$ et $(p, -r, s)$ donnant la forme principale $(1, 0, -\mathrm{D})$ d'après l'article 243 des *Disquisitiones Arithmeticæ*, la forme (A, B, C) sera composée des trois formes $(p, r, s)$, $(p, -r, s)$, (A, B, C) et par suite la composée de $(p, r, s)$ et de $\varphi$. D'après l'article 242 des *Disquisitiones Arithmeticæ*, on peut représenter par une forme le produit des nombres qui peuvent être représentés par d'autres formes dont la première est composée. La forme (A, B, C) représentera ainsi le produit $pn$, dont le premier facteur $p$ peut être représenté par $(p, r, s)$ et le second $n$ par $\varphi$. Mais $n$ n'étant pas divisible par $p$, et $p$ étant non-diviseur quadratique de $d$, le nombre $pn$ ne pourra être représenté par aucune forme de déterminant $d$ et ainsi non plus par $(a, b, c)$. En effet, supposons que cette forme représente $pn$ et désignons par $m$ le plus grand diviseur commun des indéterminées $x$, $y$, dans cette représentation, le produit $pn$ sera divisible par $mm$, et comme $p$ ne divise pas $n$, ce dernier doit être divisible par $mm$; donc

$$\frac{n}{mm} = n' \text{ un nombre entier.}$$

De la représentation de $pn$, on déduit immédiatement une représen-

tation de $pn'$ dans laquelle les valeurs des indéterminées n'ont pas de diviseur commun, mais une telle représentation n'est pas possible d'après l'article 154 des *Disquisitiones Arithmeticæ*, parce que $pn'$ est non diviseur quadratique de $d$. Donc le nombre $pn$ ne peut pas être représenté par la forme $(a, b, c)$, et c'est pourquoi notre supposition que $d$ et D ne sont pas entre eux comme des carrés n'est pas admissible.

3°. *Si le déterminant* D *est divisible par le nombre premier impair* $p$ *et que l'exposant de sa puissance la plus élevée qui divise l'ordre* O *ou l'exposant de celle qui divise le déterminant* D *soit impair, le déterminant* $d$ *ne sera pas divisible par une puissance plus élevée de* $p$ *que celle qui divise le déterminant* D.

Désignons par $p^\nu$ la puissance la plus élevée de $p$ qui divise l'ordre O. La forme $\left(\frac{A}{p^\nu}, \frac{B}{p^\nu}, \frac{C}{p^\nu}\right)$ dont les coefficients ne sont pas tous divisibles par $p$ représente aussi un nombre $n$ qui ne contient pas le nombre $p$ comme diviseur; ainsi la forme (A, B, C) représente le nombre $np^\nu$. Si $\nu$ est impair, cela suffira pour notre but; mais si $\nu$ est pair, nous chercherons un autre nombre représenté par (A, B, C). En désignant par $p^{2\nu+\mu}$ la puissance la plus élevée qui divise D, nous décomposerons la forme $\left(\frac{A}{p^\nu}, \frac{B}{p^\nu}, \frac{C}{p^\nu}\right)$ dans la forme proprement primitive

$$\left(p^\mu,\ 0,\ \frac{-D}{p^{2\nu+\mu}}\right),$$

et dans une autre (A', B', C') dont les coefficients ne seront pas tous divisibles par $p$, ce qui est toujours possible d'après l'article 249 des *Disquisitiones Arithmeticæ*. Cette dernière forme représentant aussi un nombre $m$ non divisible par $p$, la forme $\left(\frac{A}{p^\nu}, \frac{B}{p^\nu}, \frac{C}{p^\nu}\right)$ représentera $mp^\mu$, et la forme (A, B, C) le nombre $mp^{\nu+\mu}$. Comme nous avons supposé $2\nu + \mu$ impair et $\nu$ pair, l'exposant $\nu + \mu$ sera impair. Dans ces deux cas ($\nu$ impair ou pair), on peut donc représenter par (A, B, C) un nombre $lp^\lambda$ qui n'est pas divisible par une plus grande puissance de $p$ que $p^\lambda$, dont l'exposant $\lambda$ est impair et $\leq 2\nu + \mu$.

Comme $lp^\lambda$ doit être représenté aussi par la forme $(a, b, c)$, il y aura

des nombres entiers $x$, $y$ qui satisfont à l'équation

$$lp^{\lambda} = a\,xx + 2b\,xy + c\,yy.$$

L'ordre $o$ de la forme $(a, b, c)$ étant égal à 1 ou à 2, il sera permis de supposer $a$ non divisible par $p$, car cette forme représentant aussi des nombres non divisibles par $p$ (d'après l'article 228 des *Disquisitiones Arithmeticæ*), il y aura nécessairement, parmi les formes proprement équivalentes à $(a, b, c)$ des formes dont le premier coefficient n'est pas divisible par $p$; mais les formes équivalentes représentent les mêmes nombres, ainsi l'une peut être remplacée par l'autre. En multipliant l'équation par $a$ nous aurons,

$$a\,lp^{\lambda} = (ax + by)^2 - d\,yy.$$

Comme $\lambda$ est impair et $al$ non divisible par $p$, cette équation ne peut avoir lieu, si $d$ est divisible par $p^{\lambda+1}$; mais D est divisible par $p^{2\nu+\mu}$ et $\lambda \leqq 2\nu + \mu$, donc $d$ n'est pas divisible par une puissance plus élevée de $p$ que celle qui divise le déterminant D.

4°. *Si le nombre premier impair p divise le déterminant* D, *et que les exposants des plus grandes puissances qui divisent* D *et* O *soient zéro ou pairs, le déterminant d ne sera pas divisible par une puissance plus élevée de p que celle qui divise le déterminant* D.

Discutons d'abord le cas $a \mathrm{N} p$.

Si nous désignons par $p^{2\nu}$ la plus grande puissance qui divise l'ordre O, dans la forme $\left(\frac{\mathrm{A}}{p^{2\nu}}, \frac{\mathrm{B}}{p^{2\nu}}, \frac{\mathrm{C}}{p^{2\nu}}\right)$, ainsi que dans $(a, b, c)$, nous pourrons supposer les premiers coefficients $\frac{\mathrm{A}}{p^{2\nu}}$, $a$ non divisibles par $p$ (articles 228 et 154 des *Disquisitiones Arithmeticæ*). Le déterminant D contiendra le facteur $p^{4\nu}$, soit $p^{4\nu+2\mu}$ la puissance la plus élevée de $p$ contenue comme diviseur dans D; soit de plus

$$\mathrm{A}' = \frac{\mathrm{A}}{p^{2\nu}},$$

B' un nombre qui satisfait à la congruence

$$\mathrm{B}'\,p^{\mu} \equiv \frac{\mathrm{B}}{p^{2\nu}} \pmod{\mathrm{A}'},$$

et enfin

$$C' = \frac{B'B'p^{4\nu+2\mu} - D}{A'p^{4\nu+2\mu}},$$

nous aurons une forme $(A'p^{2\nu}, B'p^{2\nu+\mu}, C'p^{2\nu+2\mu})$, équivalente à (A, B, C).

La forme (A', B', C'), dont le déterminant $\frac{D}{p^{4\nu+2\mu}}$ ne contient pas $p$ comme diviseur représentera nécessairement aussi des résidus quadratiques de $p$. En effet, si l'on supposait que (A', B', C') ne représente aucun résidu quadratique, le coefficient A' et tous les nombres $m$, pour lesquels on a

$$m = A'XX + 2B'XY + C'YY$$

seraient N$p$. Soit

$$-\sigma\frac{D}{p^{4\nu+2\mu}} \equiv 1 \pmod{p};$$

on aurait donc, d'après la dernière équation,

$$\sigma A'm \equiv \sigma(A'X + B'Y)^2 + YY \pmod{p}.$$

Si $\sigma$ est N$p$, le produit $\sigma A'm$ le sera aussi, comme A' et $m$ sont supposés N$p$, de même $\sigma(A'm + B'Y)^2$ sera toujours N$p$. En posant pour Y l'unité et pour X tous les nombres incongrus entre eux par rapport au module $p$, on obtiendra dans la congruence

$$\sigma A'm \equiv \sigma(A'X + B')^2 + 1 \pmod{p}$$

pour $\sigma(A'X + B')^2$ tous les non résidus quadratiques de $p$ (art. 98, *Disquisitiones Arithmeticæ*). Donc, comme toutes les valeurs $m$ de l'expression $A'XX + 2B'XY + YY$ pour toutes les valeurs en nombres entiers des indéterminées X, Y sont supposées non résidus, tout non résidu augmenté de l'unité serait aussi non résidu, et par conséquent tous les nombres plus grands qu'un non résidu seraient aussi non résidus.

Si $\sigma$ est R$p$, il résulterait que tous les nombres plus grands que l'unité, qui est R$p$, seraient résidus quadratiques de $p$. Résultats absurdes auxquels nous a conduit la supposition que tous les nombres représentés par (A', B', C') soient N$p$.

En désignant par $g$ un résidu quadratique de $p$ représenté par la forme $(A', B', C')$, il y aura des nombres entiers $X'$, $Y'$ qui satisfont à l'équation

$$g = A'X'X' + 2B'X'Y' + C'Y'Y';$$

en multipliant celle-ci par $p^{2\nu+2\mu}$ et faisant

$$X = X'p^{\mu}, \quad Y = Y',$$

nous aurons

$$gp^{2\nu+2\mu} = A'p^{2\nu}XX + 2B'p^{2\nu+\mu}XY + C'p^{2\nu+2\mu}YY.$$

Ainsi le nombre $gp^{2\nu+2\mu}$ peut être représenté par la forme $(A'p^{2\nu}, B'p^{2\nu+\mu}, C'p^{2\nu+2\mu})$, et comme celle-ci est équivalente à $(A, B, C)$, le nombre $gp^{2\nu+2\mu}$ peut donc aussi être représenté par cette dernière.

Si le déterminant $d$ était divisible par $p^{2\nu+2\mu+1}$, le nombre $gp^{2\nu+2\mu}$ ne pourrait être représenté par la forme $(a, b, c)$, car l'équation

$$gp^{2\nu+2\mu} = axx + 2bxy + cyy,$$

ou

$$agp^{2\nu+2\mu} = (ax + by)^2 - dyy,$$

exigerait $ag \mathrm{R}p$ contre notre supposition $a \mathrm{N}p$ et $g \mathrm{R}p$.

Pour l'autre cas $a \mathrm{R}p$ on trouve, d'une manière analogue, que la supposition $d$ divisible par $p^{2\nu+2\mu+1}$ ne peut avoir lieu. Ainsi comme D est divisible par $p^{4\nu+2\mu}$, $d$ ne sera pas divisible par une plus grande puissance de $p$ que celle qui divise D.

5°. *Si* $d \equiv 2 \pmod 4$, *donc* $e = 1 = o$, D *sera aussi pair, parce que les déterminants* D *et* $d$ *sont entre eux comme des nombres carrés.*

6°. *Si* $d$ *est divisible par* 4 *et que les formes* $(a, b, c)$, $\left(\frac{A}{O}, \frac{B}{O}, \frac{C}{O}\right)$ *soient proprement primitives, de sorte que* $e = o = E = 1$, *on peut démontrer, de la manière appliquée aux nombres premiers impairs* $p$, *que* $d$ *ou eed n'est pas divisible par une puissance plus élevée de* 2 *que celle qui divise* D *ou* EED.

7°. *Si* $d$ *est divisible par* 4 *et* $e = 1$, $E = 2$, *nous démontrerons que* $d$

*ou e ed n'est pas divisible par une puissance plus élevée de* 2 *que celle qui divise* 4D *ou* EED.

Désignons par $2^\nu$ la puissance la plus élevée de 2 qui divise O, supposons, ce qui est toujours permis, $\frac{A}{E2^\nu}$ et $\frac{a}{o}$ impairs. En considérant le cas $\frac{a}{o} \equiv 1 \pmod 4$, nous représenterons par la forme $\left(\frac{A}{2^\nu}, \frac{B}{2^\nu}, \frac{C}{2^\nu}\right)$ un nombre $\equiv 6 \pmod 8$. Si le nombre $\frac{A}{2^\nu}$, qui peut être représenté par cette forme, n'est pas lui-même $\equiv 6 \pmod 8$, il sera $\equiv 2 \pmod 8$. Le coefficient $\frac{B}{2^\nu}$ étant impair, on peut supposer $\frac{B}{2^\nu} \equiv 1 \pmod 4$, car si cela n'a pas lieu, la forme $\left(\frac{A}{2^\nu}, \frac{B'}{2^\nu}, \frac{C'}{2^\nu}\right)$, où l'on a $B' = B + A$ et $C' = \frac{B'B' - D}{A}$, remplira cette condition et sera équivalente à la forme précédente qu'elle pourra donc remplacer dans nos recherches. En supposant ainsi $\frac{A}{2^\nu} \equiv 2 \pmod 8$, $\frac{B}{2^\nu} \equiv 1 \pmod 4$, et faisant $X \equiv 1 \pmod 2$, $Y \equiv 2 \pmod 4$, on représente par $\frac{A}{2^\nu} XX + 2\frac{B}{2^\nu} XY + \frac{C}{2^\nu} YY$ un nombre $2n$ congru à $6 \pmod 8$; et par $AXX + 2BXY + CYY$ le produit $2n2^\nu$.

Soit

$$axx + 2bxy + cyy = 2n2^\nu,$$

la représentation de $2n2^\nu$ par la forme $(a, b, c)$.

L'ordre $o$ étant égal à 1 ou à 2, le produit $2o$ sera égal à $2^o$, et la dernière équation, multipliée par $a$, deviendra

$$(ax + by)^2 - dyy = \frac{a}{o} n 2^{\nu+o}.$$

Donc $d$ ne peut être divisible par $2^{\nu+o+2}$, car autrement nous aurions $\frac{a}{o} n \mathrm{R} 4$, contre notre supposition $\frac{a}{o} \equiv 1 \pmod 4$, et $n \equiv 3 \pmod 4$.

Si $\frac{a}{o}$ est $\equiv 3 \pmod 4$, on prouve d'une manière analogue que $d$ n'est pas divisible par $2^{\nu+o+2}$.

Pour $\nu \geqq 1$ on a $\nu + o + 2 \leqq 2\nu + 2$; mais pour $\nu$ égal à zéro, on a $2\nu + 2 = 2$ et $\nu + o + 2$ peut devenir égal à 4. Dans ce cas D est impair; ainsi, parce que D et $d$ sont entre eux comme des carrés, l'exposant de la plus grande puissance de 2 qui divise $d$ sera pair, et $d$ n'étant pas divisible par $2^{\nu+o+2} = 2^4$, il ne sera donc non plus divisible par $2^3 = 2^{2\nu+2+1}$. Il résulte de là que $d$ n'est pas divisible par une plus grande puissance de 2 que $2^{2\nu+2}$, qui est la plus grande puissance de 2 qui divise EED.

8°. *Si eed est divisible par* 4, *et que les formes* $(a, b, c)$, $\left(\frac{A}{O}, \frac{B}{O}, \frac{C}{O}\right)$ *soient improprement primitives, e sera* $= 2$, $o = 1$, $d \equiv 1 \pmod 4$; *ainsi eed contiendra le nombre* 4 *comme diviseur, mais non pas* 8. *Le nombre* EO *étant divisible par eo,* D *par* OO, EED *sera divisible par eeoo, c'est-à-dire par* 4.

Nous avons donc prouvé, pour tout nombre premier pair ou impair, que sa plus grande puissance, qui divise $eed$, doit diviser aussi EED; par conséquent, $\frac{EED}{eed}$ sera un nombre entier. Mais D et $d$ sont entre eux comme des nombres carrés; ainsi, $\frac{EED}{eed}$ doit être un carré entier.

THÉORÈME II. — *Pour que la forme* $\left(2a, \frac{2}{e}b, 2c\right)$ *de déterminant d, de l'ordre* $\frac{2}{e}$ *et de la* $e^{\text{ième}}$ *espèce représente tous les nombres qui peuvent être représentés par* $\left(2A, \frac{2}{E}B, 2C\right)$ *de déterminant* D *de l'ordre* $\frac{2}{E}$ *et de la* $E^{\text{ième}}$ *espèce, il est nécessaire et suffisant que la première forme contienne la seconde si* E *ne surpasse pas* $e$; *mais si* $e$ *est* $= 1$, $E = 2$, *il faut que la forme* $\left(2a, b, \frac{c}{2}\right)$, *où* $a$ *et* $b$ *sont supposés impairs, et, par suite,* $\frac{c}{2}$ *pair (ce qui n'est pas une restriction de la généralité), contienne* $\left(2A, \frac{2}{E}B, 2C\right)$, *que le nombre des classes proprement primitives de déterminant* $\frac{d}{4}$ *ne surpasse pas celui des classes improprement primitives de même déterminant, et que* D *ne soit pas congru à* $1 \pmod 8$.

1°. Si $e$ est $= E$ ou $e = 2$, $E = 1$, le nombre $\frac{EED}{eed}$ étant carré entier, $\frac{D}{d}$ le sera aussi, nous désignerons $\frac{D}{d}$ par $\partial\partial$.

Comme nous avons supposé que l'ordre de la forme $\left(2A, \frac{2}{E}B, 2C\right)$ est $\frac{2}{E}$, les nombres A, B, C ne peuvent être tous pairs. Si A ou C est impair, on représentera par $2AXX + 2\frac{2}{E}BXY + 2CYY$ un nombre pair non divisible par 4, quand on prend un nombre impair pour X et pair pour Y, ou un nombre pair pour X et impair pour Y. Si A et C sont pairs, E sera égal à 2, car autrement (pour $E = 1$), la forme serait de la seconde espèce, contre notre supposition qu'elle est de la $E^{ième}$ espèce. En prenant des nombres impairs pour X et Y, on représente aussi dans ce cas un nombre pair non divisible par 4.

Désignons par $2A'$ un nombre qui peut être représenté par la forme $\left(2A, \frac{2}{E}B, 2C\right)$ et qui n'est pas divisible par 4; il y aura, d'après l'article 168 des *Disquisitiones Arithmeticæ*, une forme $\left(2A', \frac{2}{E}B', 2C'\right)$, qui est équivalente à la précédente, et de la même espèce et du même ordre que celle-là. Si B' est pair, E sera l'unité, car autrement la forme serait de l'ordre 2 contre notre supposition, qu'elle est de l'ordre $\frac{2}{E}$; il résulte de là que $B' + EA' = B''$ est impair, en désignant $\frac{4B''B'' - EED}{2EEA'}$ par C'', nous aurons une forme $\left(2A', \frac{2}{E}B'', 2C''\right)$, équivalente à $\left(2A', \frac{2}{E}B', 2C\right)$ et à $\left(2A, \frac{2}{E}B, C\right)$; dans la première forme A', B'' sont impairs; il est donc permis de supposer que A et B dans la forme $\left(2A, \frac{2}{E}B, 2C'\right)$ soient impairs. De même nous supposerons $a$ et $b$ dans $\left(2a, \frac{2}{e}b, 2c\right)$ impairs.

On déduit la forme $\left(2A, \frac{2}{E}B, 2C\right)$ de celle (EA, B, EC), en multi-

pliant les coefficients de la dernière par $\frac{2}{E}$. D'après l'article 243, 1°, des *Disquisitiones Arithmeticæ*, la forme (EA, B, EC) est la composée de (A, B, EEC) et de (E, B, EAC), et, d'après le théorème de M. Dirichlet, la forme proprement primitive (A, B, EEC) représente une infinité de nombres premiers : soit $p$ un de ces nombres qui ne divise pas 2D. Le nombre E peut être représenté par (E, B, EAC); donc E$p$ par (EA, B, EC) et $\frac{2}{E}$E$p$ ou $2p$ par $\left(\frac{2}{E}EA, \frac{2}{E}B, \frac{2}{E}EC\right)$, c'est-à-dire par $\left(2A, \frac{2}{E}B, 2C\right)$. Comme $\left(2a, \frac{2}{e}b, 2c\right)$ représente tous les nombres qui peuvent être représentés par $\left(2A, \frac{2}{E}B, 2C\right)$, elle représentera aussi $2p$. La congruence

$$rr \equiv d \pmod{2p}$$

n'a que deux racines $+r$ et $-r$, et la congruence

$$RR \equiv D \pmod{2p},$$

n'a que ces deux $R \equiv +r\delta$, $R \equiv -r\delta \pmod{2p}$.

Désignons $\frac{rr-d}{2p}$ par $s$, l'une des deux formes $(2p, r, s)$, $(2p, -r, s)$ sera proprement équivalente à $\left(2a, \frac{2}{e}b, 2c\right)$, et l'une des deux formes $(2p, r\delta, s\delta\delta)$, $(2p, -r\delta, s\delta\delta)$ proprement équivalente à $\left(2A, \frac{2}{E}B, 2C\right)$. Cela résulte immédiatement de l'article 168 des *Disquisitiones Arithmeticæ*, d'après lequel il y a toujours un nombre $n$ qui fait la forme $\left(m, n, \frac{nn-\Delta}{m}\right)$ équivalente à une forme donnée, si celle-ci a le déterminant $\Delta$ et représente le nombre $m$. La forme $(2p, \pm r, s)$ se change en $(2p, \pm r\delta, s\delta\delta)$ par la substitution $\begin{pmatrix} 1, & 0 \\ 0, & \pm\delta \end{pmatrix}$, ainsi la forme $\left(2A, \frac{2}{E}B, 2C\right)$ sera contenue proprement ou improprement sous $\left(2a, \frac{2}{e}b, 2c\right)$ (article 159, *Disquisitiones Arithmeticæ*).

2°. Par les éléments on sait, que la condition de $\left(2A, \frac{2}{E}B, 2C\right)$ con-

tenue sous $\left(2a, \frac{2}{e}b, 2c\right)$ suffit pour que cette dernière forme représente tous les nombres qui peuvent être représentés par la première.

3°. Si $e$ est $=1$, $E=2$, le déterminant D ne peut être $\equiv 1 \pmod 8$.

Supposons $D \equiv 1 \pmod 8$, la forme $\left(4, 1, \frac{1-D}{4}\right)$ sera improprement primitive, et il y aura une forme proprement primitive (A', B', C') dont la composition avec $\left(4, 1, \frac{1-D}{4}\right)$ a pour résultante la forme improprement primitive (2A, B, 2C) (article 251, *Disq. Arith.*). La forme (A', B', C') représente aussi un nombre impair $m$, et la forme $\left(4, 1, \frac{1-D}{4}\right)$ le nombre 4; ainsi la composée (2A, B, 2C) des deux formes représente le produit $4m$. Si ce produit était représenté par $(2a, 2b, 2c)$, il y aurait des nombres $2l, 2n$ tels, que la forme $(4m, 2l, 2n)$ serait équivalente à $(2a, 2b, 2c)$; et la forme $(2m, l, n)$ à la forme $(a, b, c)$. Le déterminant D étant $\equiv 1 \pmod 8$ et $\frac{4D}{d}$ un carré, $\frac{d}{4}$ sera $\equiv 1 \pmod 8$, et dans l'équation $\frac{d}{4} = bb - ac = l^2 - 2mn$ le nombre $n$ pair, donc la forme $(2m, l, n)$ est improprement primitive; mais, d'après l'article 161 des *Disquisitiones Arithmeticæ*, une telle forme ne peut équivaloir à une forme proprement primitive $(a, b, c)$. Il résulte de là que le déterminant D ne peut être $\equiv 1 \pmod 8$.

4°. Si $e$ est $=1$, $E=2$, le nombre des classes improprement primitives de déterminant $\frac{d}{4}$ doit être égal au nombre des classes proprement primitives de même déterminant.

La forme (2A, B, 2C) est (d'après l'article 243 des *Disquisitiones Arithmeticæ*) la composée de la forme proprement primitive (A, B, 4C) et de $\left(2, 1, \frac{1-D}{2}\right)$, parce que celle-ci équivaut à (2, B, 2AC). Soit $\mathfrak{L}$ la classe de la forme (A, B, 4C), et $\mathfrak{H}$ la classe de l'une des formes proprement primitives $\left(4, 1, \frac{1-D}{4}\right)\left(4, -1, \frac{1-D}{4}\right)$, celle de l'autre est $2\mathfrak{H}$, et la composition de $\left(2, 1, \frac{1-D}{2}\right)$ avec toute forme des classes $\mathfrak{L}$, $\mathfrak{L}+\mathfrak{H}$, $\mathfrak{L}+2\mathfrak{H}$, a pour résultante (2A, B, 2C) (article 256, 7°, des

*Disquisitiones Arithmeticæ*). Désignons par $p$ un nombre premier non diviseur de 2D et représenté par une forme de la classe $\mathfrak{L}+\mathfrak{H}$, il y aura dans celle-ci une forme $(p, r\delta, s\delta\delta)$, où $\delta$ est $=\frac{4D}{d}$, et $r$ une racine impaire de la congruence

$$rr\delta\delta \equiv D \equiv \frac{d}{4}\delta\delta \pmod{p}.$$

La forme $(2A, B, 2C)$, qui est la composée de $\left(2, 1, \frac{1-D}{2}\right)$ et de toute forme de la classe $\mathfrak{L}+\mathfrak{H}$ représentera le produit $2p$.

Si le nombre $2p$ peut être représenté par $(2a, 2b, 2c)$, la forme $(a, b, c)$ de déterminant $\frac{d}{4}$ représentera $p$, et sera par conséquent équivalente à l'une des deux $(p, r, s)$ $(p, -r, s)$, ce qui résulte de l'article 168, comme nous avons vu auparavant. La forme $(p, \pm r, s)$ se change en $(p, r\delta, s\delta\delta)$ par la substitution $\begin{pmatrix} 1, & 0 \\ 0, & \pm\delta \end{pmatrix}$; donc la classe $\lambda$ de la forme $(a, b, c)$ contient proprement ou improprement la classe $\mathfrak{L}+\mathfrak{H}$ de la forme $(p, r\delta, s\delta\delta)$. De la même manière on prouve que $\lambda$ contient $\mathfrak{L}$ et $\mathfrak{L}+2\mathfrak{H}$. Chacune des formes $\left(4, +1, \frac{1-D}{4}\right)\left(4, -1, \frac{1-D}{4}\right)$, équivaut proprement ou improprement à chacune des $\left(4, \delta, \frac{4-d}{16}\delta\delta\right)$ $\left(4, -\delta, \frac{4-d}{16}\delta\delta\right)$, ces dernières formes sont contenues sous $\left(4, 1, \frac{4-d}{16}\right)$ $\left(4, -1, \frac{4-d}{16}\right)$; donc les classes $\eta$ et $2\eta$ de celles-ci contiendront les classes $\mathfrak{H}$ et $2\mathfrak{H}$. Comme les classes $\lambda$ et $\eta$ contiennent respectivement $\mathfrak{L}$ et $\mathfrak{H}$, la composée $\lambda+\eta$ des deux premières contiendra (d'après l'article 238 des *Disquisitiones Arithmeticæ*) la composée $\mathfrak{L}+\mathfrak{H}$ des deux dernières, et comme $\lambda$ et $2\eta$ contiennent $\mathfrak{L}+2\mathfrak{H}$ et $2\mathfrak{H}$, la composée $\lambda+2\eta$ contiendra $\mathfrak{L}+2\mathfrak{H}+2\mathfrak{H}$, c'est-à-dire $\mathfrak{L}+\mathfrak{H}$, parce que la classe $3\mathfrak{H}$ est la principale. Les trois classes $\lambda$, $\lambda+\eta$, $\lambda+2\eta$ contenant ainsi toutes celle $\mathfrak{L}+\mathfrak{H}$, chaque forme de ces classes représentera le nombre premier $p$, que nous avons supposé représentable par une forme de la classe $\mathfrak{L}+\mathfrak{H}$. Il résulte de là que les deux formes $(p, r, s)$ $(p, -r, s)$, appartiennent aux trois classes $\lambda$, $\lambda+\eta$, $\lambda+2\eta$;

donc, au moins, deux de ces classes sont identiques. On voit facilement que cela ne peut avoir lieu si $\eta$ n'est pas la classe principale, mais dans ce cas le nombre des classes improprement primitives est égal à celui des proprement primitives de déterminant $\frac{d}{4}$ (article 256, 7°).

5°. Si $e$ est $= 1$, $E = 2$, la forme $\left(2a, b, \frac{c}{2}\right)$ doit contenir proprement ou improprement $(2A, B, 2C)$.

Nous avons vu que $(2A, B, 2C)$ est la composée de $\left(2, 1, \frac{1-D}{2}\right)$ et de toute forme des classes $\mathfrak{L}$, $\mathfrak{L}+\mathfrak{H}$, $\mathfrak{L}+2\mathfrak{H}$. Comme $(p, r\delta, s\delta\delta)$ appartient à $\mathfrak{L}+\mathfrak{H}$, la composée $\left(2p, r\delta, \frac{s}{2}\delta\delta\right)$ de $(p, r\delta, s\delta\delta)$ et de $\left(2, 1, \frac{1-D}{2}\right)$ ou de $\left(2, r, \frac{rr-D}{2}\right)$ sera équivalente à $(2A, B, 2C)$. Dans la forme $(a, b, c)$ le coefficient $c$ est divisible par 4, puisque $a$ et $b$ sont impairs et $bb - ac$ est $= \frac{d}{4} \equiv D \equiv 1 \pmod 4$, la composée de cette forme et de $\left(2, 1, \frac{4-d}{8}\right)$ sera donc $\left(2a, b, \frac{c}{2}\right)$. Comme $(a, b, c)$ équivaut à l'une des deux $(p, r, s)$ $(p, -r, s)$, la forme $\left(2a, b, \frac{c}{2}\right)$ équivaut aussi à l'une des deux $\left(2p, \pm r, \frac{s}{2}\right)$, qui résulte de la composition de $(p, \pm r, s)$ et de $\left(2, 1, \frac{4-d}{8}\right)$. Mais $\left(2p, \pm r, \frac{s}{2}\right)$ se change en $\left(2p, \pm r\delta, \frac{s}{2}\delta\delta\right)$ par la substitution $\begin{pmatrix} 1, & 0 \\ 0, & \pm\delta \end{pmatrix}$; ainsi la forme $\left(2a, b, \frac{c}{2}\right)$ qui est équivalente à la première, contiendra proprement ou improprement $(2A, B, 2C)$, qui est équivalente à la seconde.

6°. La dernière partie du théorème, savoir, que ces trois conditions sont suffisantes pour que la forme $(2a, 2b, 2c)$ représente tous les nombres représentés par $(2A, B, 2C)$, peut être démontrée au moyen des principes de la représentation des nombres par des formes, et de ceux de la composition des formes; mais nous préférons donner ici une substitution en nombres rompus, par laquelle on obtient, pour tout système de valeurs X, Y en nombres entiers, qui satisfont à l'équation

$$m = 2AXX + 2BXY + 2CYY,$$

un système de nombres entiers $x$, $y$, qui servent à représenter le nombre $m$ par la forme $2axx + 4bxy + 2cyy$.

Les deux premières conditions (en 3° et 4°) peuvent être remplacées par celle-ci, que les plus petites valeurs positives T, U qui satisfont à l'équation

$$TT - \frac{d}{4}UU = 4,$$

soient des nombres impairs. En effet, si D est $\equiv 1 \pmod 8$, $\frac{d}{4}$ le sera aussi, et les nombres T, U pairs. Si $\frac{d}{4}$ est $= -3$, nous aurons $T = 1$, $U = 1$; mais pour le déterminant $-3$, il n'y a qu'une seule classe proprement primitive, et une seule improprement primitive. Pour les autres déterminants $\frac{d}{4}$ négatifs congrus à 5 (mod 8), T est $= 2$, $U = 0$, et le nombre des classes improprement primitives plus petit que celui des classes proprement primitives. Si $\frac{d}{4}$ est positif $\equiv 5 \pmod 8$, d'après un théorème de M. Dirichlet (*Recherches sur diverses applications de l'Analyse infinitésimale à la théorie des Nombres*, § 8, III. Journal de Crelle, t. XXI, p. 11) les entiers T et U seront impairs ou pairs, selon que le nombre des classes proprement primitives est égal au nombre des classes improprement primitives ou égal au triple de celui-ci.

Au moyen de cet énoncé des conditions, il est facile de démontrer qu'il y a toujours des nombres $u$, $t$, tels que la substitution

$$2x = \alpha x' + 6y',$$
$$2y = \gamma x' + \delta y',$$

dans laquelle les coefficients satisfont aux équations

$$\alpha = t - bu,$$
$$6 = -\frac{c}{2}u,$$
$$\gamma = au,$$
$$2\delta = t + bu,$$
$$tt - \frac{d}{4}uu = 4,$$

et par laquelle la forme

$$2axx + 4bxy + 2cyy$$

se change en

$$2ax'x' + 2bx'y' + \frac{c}{2}y'y',$$

donne des entiers $x, y$ pour chaque système de nombres entiers $x'$, $y'$. En effet, $\alpha$ et $\beta$ sont toujours pairs et $\delta$ entier, parce que $b$ est impair, $\frac{c}{2}$ pair, $t$ et $u$ ensemble pairs ou impairs; si $y'$ est pair, toute solution en nombres pairs $t$, $u$ de l'équation

$$tt - \frac{d}{4}uu = 4$$

remplira notre but, parce qu'elle fait $\gamma$ pair. Si $y'$ est impair, $x'$ pair, on prendra celle des deux solutions en nombres impairs $t = \mathrm{T}$, $u = \mathrm{U}$ et $t = \mathrm{T}$, $u = -\mathrm{U}$, pour laquelle $t + bu$ est divisible par 4, car alors $\delta$ sera pair. On voit facilement que l'un, et seulement l'un des deux nombres pairs $\mathrm{T} + b\mathrm{U}$ et $\mathrm{T} - b\mathrm{U}$, est divisible par 4, puisque leur somme $2\mathrm{T}$ ne l'est pas. Dans le cas de $y'$ et $x'$ impairs, nous prenons celle des deux solutions en nombres impairs $t = \mathrm{T}$, $u = \mathrm{U}$ et $t = \mathrm{T}$, $u = -\mathrm{U}$, pour laquelle $t + bu$ n'est pas divisible par 4, car celle-ci fait $\gamma$ et $\delta$ impairs, ainsi $\gamma x' + \delta y'$ est pair.

La forme $(2a, 2b, 2c)$ représente donc tous les nombres qui peuvent être représentés par $\left(2a, b, \frac{c}{2}\right)$, et comme celle-ci contient $(2\mathrm{A}, \mathrm{B}, 2\mathrm{C})$, et représente ainsi tous les nombres représentés par $(2\mathrm{A}, \mathrm{B}, 2\mathrm{C})$, la première $(2a, 2b, 2c)$ représentera tous les nombres qui peuvent être représentés par $(2\mathrm{A}, \mathrm{B}, 2\mathrm{C})$.

Troisième théorème. — *Pour que la forme* $(a, b, c)$ *de déterminant* $d$, *de l'ordre* $o$, *de la* $e^{\text{ième}}$ *espèce, et la forme* $(\mathrm{A}, \mathrm{B}, \mathrm{C})$ *de déterminant* D, *de l'ordre* O, *de la* $\mathrm{E}^{\text{ième}}$ *espèce, représentent toujours les mêmes nombres, il est nécessaire et suffisant qu'au moins l'une des deux formes contienne l'autre, que* $oe$ *soit* $= \mathrm{OE}$ *et* $eed = \mathrm{EED}$, *et outre cela, si* $e$ *et* E *sont inégaux, que* $\frac{d}{oo} = \frac{\mathrm{D}}{\mathrm{OO}}$ *ait la forme* $8k + 5$, *et que pour ce*

*nombre comme déterminant, il y ait autant de classes improprement primitives que de classes proprement primitives.*

Comme la forme $(a, b, c)$ représente tous les nombres représentés par $(A, B, C)$, et que celle-ci représente tous les nombres représentés par $(a, b, c)$, on a, d'après le premier théorème $eo = EO$, $eed = EED$. En multipliant les six coefficients des deux formes par 2, et les divisant par $eo = EO$, on obtient des formes $\left(2a', \frac{2}{e}b', 2c\right)\left(2A', \frac{2}{E}B', 2C'\right)$, qui sont des ordres $\frac{2}{e}$ et $\frac{2}{E}$, et de la $e^{ième}$ et $E^{ième}$ espèce. Il est aisé de voir que ces deux formes doivent représenter toujours les mêmes nombres, et qu'on peut leur appliquer directement le théorème précédent : on trouvera de cette manière le théorème proposé.