Sección Quinta

SOBRE

LAS FORMAS Y LAS ECUACIONES INDETERMINADAS DE SEGUNDO GRADO.

Propósito de la investigación: definición y notación de las formas.

153.

En esta sección, trataremos principalmente las funciones de dos indeterminadas x e y de esta forma:

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

donde a, b y c son enteros dados. Llamaremos a estas funciones *formas de segundo grado* o simplemente *formas.* En esta investigación se basa la resolución del famoso problema de encontrar todas las soluciones de cualquier ecuación indeterminada del segundo grado involucrando dos incógnitas, donde estas incógnitas pueden asumir tanto valores enteros como racionales. Este problema ciertamente ya fue resuelto por el ilustre Lagrange con toda generalidad. Además, muchos aspectos de la naturaleza *de las formas,* como la construcción de demostraciones, fueron encontrados tanto por este gran geómetra como por el ilustre Euler y antes por Fermat. Sin embargo, mediante una cuidadosa investigación de las formas, se nos presentaron tantos detalles nuevos que juzgamos valioso el trabajo de retomar completamente todo el argumento; primero, porque hemos conocido los descubrimientos difundidos en varios lugares por aquellos hombres, segundo, porque el método para tratar esto es, en su mayor parte, propio a nosotros, y, finalmente, porque nuestros nuevos hallazgos ciertamente no podrán comprenderse sin una exposición de los otros. Nos parece que no hay duda alguna de que muchos excelentes resultados de este género todavía están ocultos a

quienes se interesan en esta materia. Además, siempre presentaremos la historia de las proposiciones importantes en el lugar apropiado.

Cuando no nos conciernen las indeterminadas x e y, denotaremos por (a, b, c) a la forma $ax^2 + 2bxy + cy^2$. Por lo tanto, esta expresión denotará de manera indefinida una suma de tres partes: el producto del número dado a por un cuadrado indeterminado cualquiera, el producto del duplicado del número b por esta indeterminada y otra indeterminada, y el producto del número c por el cuadrado de esta segunda indeterminada. E.g., $(1, 0, 2)$ expresa la suma de un cuadrado y el duplicado de un cuadrado. Además, aunque las formas (a, b, c) y (c, b, a) denotan lo mismo, si sólo se consideran *sus términos,* difieren, sin embargo, si también prestamos atención al *orden.* Por esto las distinguiremos con cuidado en lo que sigue; más adelante se pondrá en claro lo que ganamos con esto.

Representación de los números; el determinante.

154.

Diremos que un número dado *se representa* por una forma dada si se puede dar valores enteros a las indeterminadas de la forma de modo que sea igual al número dado. Tendremos el siguiente:

TEOREMA. *Si el número M puede representarse por la forma (a, b, c) de manera que los valores de las indeterminadas, por los que esto se produce, son primos entre sí, entonces $b^2 - ac$ será un residuo cuadrático del número M.*

Demostración. Sean m y n los valores de las indeterminadas; i.e.,

$$am^2 + 2bmn + cn^2 = M$$

y tómense los números μ y ν de modo que sea $\mu m + \nu n = 1$ (art. 40). Entonces por multiplicación puede demostrarse fácilmente:

$$(am^2 + 2bmn + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2) \\ = (\mu(mb + nc) - \nu(ma + nb))^2 - (b^2 - ac)(m\mu + n\nu)^2$$

o sea

$$M(a\nu^2 - 2b\mu\nu + c\mu^2) = (\mu(mb + nc) - \nu(ma + nb))^2 - (b^2 - ac).$$

Por lo tanto será

$$b^2 - ac \equiv (\mu(mb + nc) - \nu(ma + nb))^2 \pmod{M}$$

i.e., $b^2 - ac$ será un residuo cuadrático de M.

Llamaremos al número $b^2 - ac$, de cuya índole dependen las propiedades de la forma (a, b, c), tal como lo enseñaremos en lo siguiente, el *determinante* de esta forma.

Los valores de la expresión $\sqrt{b^2 - ac} \pmod{M}$
a los cuales pertenece la representación del número M *por la forma* (a, b, c).

155.

Así

$$\mu(mb + nc) - \nu(ma + nb)$$

será un valor de la expresión

$$\sqrt{b^2 - ac} \pmod{M}$$

Pero es claro que los números μ y ν pueden determinarse de infinitas maneras de modo que $\mu m + \nu n = 1$, y así producirán unos y otros valores de esta expresión. Veremos qué relación tienen entre sí. Sea no sólo $\mu m + \nu n = 1$ sino también $\mu' m + \nu' n = 1$ y póngase

$$\mu(mb + nc) - \nu(ma + nb) = v, \quad \mu'(mb + nc) - \nu'(ma + nb) = v'.$$

Multiplicando la ecuación $\mu m + \nu n = 1$ por μ', la otra $\mu' m + \nu' n = 1$ por μ, y restando será $\mu' - \mu = n(\mu'\nu - \mu\nu')$, y al mismo tiempo multiplicando aquélla por ν' y ésta por ν, restando será $\nu' - \nu = m(\mu\nu' - \mu'\nu)$. De esto inmediatamente resulta

$$v' - v = (\mu'\nu - \mu\nu')(am^2 + 2bmn + cn^2) = (\mu'\nu - \mu\nu')M$$

o sea, $v' \equiv v \pmod{M}$. Por lo tanto, de cualquier modo que se determinen μ y ν, la fórmula $\mu(mb + nc) - \nu(ma + nb)$ no puede presentar valores *diferentes* (i.e., no congruentes) de la expresión $\sqrt{b^2 - ac} \pmod{M}$. Así pues, si v es un valor cualquiera de esta fórmula, diremos que la representación del número M por la forma

$ax^2 + 2bxy + cy^2$ donde $x = m$ e $y = n$, *pertenece al valor* v *de la expresión* $\sqrt{b^2 - ac}$ (mod. M). Además puede mostrarse fácilmente que, si algún valor de esta fórmula fuera v y $v' \equiv v \pmod{M}$, se puede tomar en lugar de los números μ y ν que dan v los otros μ' y ν' que dan v'. En efecto, si se hace

$$\mu' = \mu + \frac{n(v' - v)}{M}, \qquad \nu' = \nu - \frac{m(v' - v)}{M}$$

será

$$\mu' m + \nu' n = \mu m + \nu n = 1$$

y el valor de la fórmula producido por μ' y ν' excederá el valor producido por μ y ν en la cantidad $(\mu'\nu - \mu\nu')M$, que es $= (\mu m + \nu n)(v' - v) = v' - v$ o sea aquel valor será $= v'$.

156.

Si se tienen dos representaciones de un mismo número M por una misma forma (a, b, c) en las cuales las indeterminadas tienen valores primos entre sí, ellas pueden pertenecer o al mismo valor de la expresión $\sqrt{b^2 - ac} \pmod{M}$ o a valores diferentes. Sea

$$M = am^2 + 2bmn + cn^2 = am'^2 + 2bm'n' + cn'^2$$

y

$$\mu m + \nu n = 1, \quad \mu' m' + \nu' n' = 1$$

Es claro que si

$$\mu(mb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M}$$

entonces la congruencia siempre permanecerá válida, cualesquiera que sean los valores apropiados para μ y ν, μ' y ν'. En tal caso decimos que ambas representaciones pertenecen a un *mismo* valor de la expresión $\sqrt{b^2 - ac} \pmod{M}$; pero si la congruencia no vale para algunos valores de μ y ν, μ' y ν', no valdrá para ninguno, y diremos que las representaciones pertenecerán a valores *diferentes.* Pero si

$$\mu(mb + nc) - \nu(ma + nb) \equiv -(\mu'(m'b + n'c) - \nu'(m'a + n'b))$$

se dice que las representaciones pertenecen a valores *opuestos* de la expresión $\sqrt{b^2 - ac}$. También se usarán todas estas denominaciones cuando se tratan de varias representaciones de un mismo número por formas *diferentes,* pero que tienen el mismo determinante.

Ejemplo. Sea propuesta la forma $(3, 7, -8)$ cuyo determinante es $= 73$. Por esta forma se tendrán estas representaciones del número 57:

$$3 \cdot 13^2 + 14 \cdot 13 \cdot 25 - 8 \cdot 25^2; \quad 3 \cdot 5^2 + 14 \cdot 5 \cdot 9 - 8 \cdot 9^2$$

Para la primera, puede ponerse $\mu = 2$, $\nu = -1$ de donde resulta el valor de la expresión $\sqrt{73}$ (mod. 57) a la cual pertenece la representación

$$= 2(13 \cdot 7 - 25 \cdot 8) + (13 \cdot 3 + 25 \cdot 7) = -4$$

De modo semejante se descubrirá que la segunda representación, al hacer $\mu = 2$, $\nu = -1$, pertenece al valor $+4$. Por lo cual las dos representaciones pertenecen a valores opuestos.

Antes de proseguir, observamos que las formas de determinante $= 0$ están excluidas totalmente de las investigaciones siguientes. De hecho, ellas perturban únicamente la elegancia de los teoremas ya que exigen un tratamiento particular.

Una forma que implica otra o contenida en ella; la transformación propia e impropia.

157.

Si la forma F, cuyas indeterminadas son x e y, puede transmutarse en otra, F', cuyas indeterminadas son x' e y' por las sustituciones

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

de modo que α, β, γ, δ sean enteros; diremos que la primera *implica* la segunda o que la segunda *está contenida en la primera.* Sea F la forma

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

F' la forma

$$a'x'^2 + 2b'x'y' + cy'^2$$

y se tendrán las tres ecuaciones siguientes

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \end{aligned}$$

Multiplicando la segunda ecuación por sí misma, la primera por la tercera, restando y removiendo las partes canceladas, resultará

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2$$

De donde se deduce que el determinante de la forma F' es divisible por el determinante de la forma F y el cociente de ellos es un cuadrado. Por lo tanto es claro que estos determinantes tendrán el *mismo signo.* Además, si la forma F' puede transmutarse por una sustitución similar en la forma F, i.e., si tanto F' está contenida en F como F está contenida en F', los determinantes de las formas serán iguales*) y $(\alpha\delta - \beta\gamma)^2 = 1$. En este caso diremos que las formas son *equivalentes.* Por esto, para la equivalencia de formas, la igualdad de los determinantes es una condición necesaria, aunque aquélla no se deduzca sólo de ésta.— Llamaremos a la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ una *transformación propia,* si $\alpha\delta - \beta\gamma$ es un número positivo, *impropia* si $\alpha\delta - \beta\gamma$ es negativo. Diremos que la forma F' está contenida en la forma F *propiamente* o *impropiamente* si F puede transmutarse en la forma F' por una transformación propia o impropia. Así si las formas F y F' son equivalentes, será $(\alpha\delta - \beta\gamma)^2 = 1$, así que si la transformación es propia, $\alpha\delta - \beta\gamma = 1$, si es impropia, $\alpha\delta - \beta\gamma = -1$. Si varias transformaciones son al mismo tiempo propias, o al mismo tiempo impropias, las llamaremos *semejantes;* sin embargo, una propia y una impropia se llaman *desemejantes.*

La equivalencia propia e impropia.

158.

Si los determinantes de las formas F y F' son iguales y si F' está contenida en F, entonces F estará contenida en F', propia o impropiamente, según que F' esté contenida en F propia o impropiamente.

Consideremos que F se transforma en F' poniendo

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

y F' se transformará en F poniendo

$$x' = \delta x - \beta y, \qquad y' = -\gamma x + \alpha y.$$

*) Es claro por el análisis anterior que esta proposición también es válida para formas cuyo determinante es $= 0$. Pero no se debe extender la ecuación $(\alpha\delta - \beta\gamma)^2 = 1$ a este caso.

En efecto, por esta sustitución resulta lo mismo de F' que de F al poner

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \qquad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

o sea

$$x = (\alpha\delta - \beta\gamma)x, \qquad y = (\alpha\delta - \beta\gamma)y$$

De esto queda manifiesto que F se hace $(\alpha\delta - \beta\gamma)^2 F$, i.e., de nuevo, F (artículo anterior). También está claro que la segunda transformación será propia o impropia, según que la primera sea propia o impropia.

Si tanto F' está contenida *propiamente* en F como F lo está en F', las llamaremos formas *propiamente equivalentes;* si alternativamente están contenidas impropiamente, las llamaremos *impropiamente equivalentes.*— En lo restante, se verá pronto el uso de estas distinciones.

Ejemplo. La forma $2x^2 - 8xy + 3y^2$ se cambia, por la sustitución $x = 2x' + y'$, $y = 3x' + 2y'$, en la forma $-13x'^2 - 12x'y' - 2y'^2$, y ésta se transforma en la primera mediante la sustitución $x' = 2x - y$, $y' = -3x + 2y$. Por lo que las formas $(2, -4, 3)$ y $(-13, -6, -2)$ son *propiamente equivalentes.*

Los problemas que ahora trataremos son éstos :

I. Propuestas dos formas cualesquiera que tienen el mismo determinante, se debe investigar si son equivalentes o no, si lo son propia o impropiamente o ambas (puesto que esto también puede suceder). Cuando tienen determinantes diferentes, se debe investigar por lo menos si la una implica la otra, propia o impropiamente o ambas. Finalmente, se debe hallar todas las transformaciones de la una en la otra, tanto las propias como las impropias.

II. Dada una forma cualquiera, se debe determinar si un número dado puede representarse por ella y determinar todas las representaciones. Pero, ya que las formas de determinante negativo requieren otros métodos diferentes que las formas de determinante positivo, primero trataremos lo común a los dos, y luego consideraremos cada género por separado.

Formas opuestas.

159.

Si la forma F implica la forma F', y ésta implica la forma F'', también la forma F implicará la forma F''.

Sean las indeterminadas de las formas F, F', F'', respectivamente x e y, x' e y', x'' e y'', y transfórmese F en F' al poner

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

y F' en F'' al poner

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

Es claro que F será transmutada en F'' al poner

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y''), \qquad y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

o

$$x = (\alpha\alpha' + \beta\gamma')x'' + (\alpha\beta' + \beta\delta')y'', \qquad y = (\gamma\alpha' + \delta\gamma')x'' + (\gamma\beta' + \delta\delta')y''$$

Así F implicará F''.

Porque

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

será positivo si tanto $\alpha\delta - \beta\gamma$ como $\alpha'\delta' - \beta'\gamma'$ son positivos o ambos son negativos, y será negativo si uno de estos números es positivo y el otro negativo, la forma F implicará la forma F'' *propiamente* si F implica F' y F' a F'' del mismo modo, e *impropiamente* si es de modos diferentes.

De esto resulta que si se tienen las formas cualesquiera F, F', F'', F''', etc., cada una de las cuales implica la siguiente, la primera implicará la última *propiamente* si el número de formas que implican impropiamente a su sucesor es par, e *impropiamente* si este número es impar.

Si la forma F es equivalente a la forma F' y la forma F' es equivalente a la forma F'', entonces la forma F será equivalente a la forma F'' propiamente si la forma F equivale a la forma F' del mismo modo como la forma F' equivale a la forma F'', e impropiamente si son equivalencias de modos diferentes.

De hecho, ya que las formas F y F' son respectivamente equivalentes a las formas F' y F'', entonces aquéllas implicarán éstas, y así F implica a F'', tanto como las últimas implican a las primeras. Por lo tanto, F y F'' serán equivalentes. Pero se

sigue de lo anterior que F implicará F'' propiamente o impropiamente, según que la equivalencia de F y F', y F' y F'' sea del mismo modo o de modo diferente. De la misma manera F'' implicará F. Por lo tanto, F y F'' serán propiamente equivalentes en el primer caso, e impropiamente equivalentes en el segundo.

Las formas $(a, -b, c)$, (c, b, a), $(c, -b, a)$ *son equivalentes a la forma* (a, b, c), *con las dos primeras impropiamente, con la última propiamente.*

Ya que $ax^2 + 2bxy + cy^2$ se transforma en $ax'^2 - 2bx'y' + cy'^2$, al colocar $x = x' + 0 \cdot y'$, $y = 0 \cdot x' - y'$, esta transformación es impropia pues $(1)(-1) - (0)(0) = -1$; pero se transforma en $cx'^2 + 2bx'y' + ay'^2$ por la transformación impropia $x = 0 \cdot x' + y'$, $y = x' + 0 \cdot y'$; y en la forma $cx'^2 - 2bx'y' + ay'^2$ por la transformación propia $x = 0 \cdot x' - y'$, $y = x' + 0 \cdot y'$.

De esto queda claro que cualquier forma equivalente a la forma (a, b, c) equivaldrá *propiamente* o a ella misma o a la forma $(a, -b, c)$. Al mismo tiempo, si tal forma implica la forma (a, b, c) o está contenida en ella misma, ella implicará la forma (a, b, c) o la forma $(a, -b, c)$ *propiamente* o estará contenida *propiamente* en una de las dos. Llamaremos a (a, b, c) y $(a, -b, c)$ formas *opuestas.*

Formas contiguas.

160.

Si las formas (a, b, c) y (a', b', c') tienen el mismo determinante, y si además $c = a'$ y $b \equiv -b' \pmod{c}$, o sea $b + b' \equiv 0 \pmod{c}$, llamaremos a estas formas *contiguas.* Cuando es necesaria una determinación más exacta, diremos que la primera es contigua *a la parte primera* de la segunda, la segunda *a la parte última* de la primera.

Así, por ejemplo, la forma $(7, 3, 2)$ es contigua a la parte última de la forma $(3, 4, 7)$; la forma $(3, 1, 3)$ a ambas partes de su opuesta $(3, -1, 3)$.

Formas contiguas siempre son propiamente equivalentes. En efecto la forma $ax^2 + 2bxy + cy^2$ se transforma en su contigua por la sustitución $x = -y'$, $y = x' + \frac{b+b'}{c}y'$ (la cual es propia porque $0 \cdot (\frac{b+b'}{c}) - (1 \cdot -1) = 1$), como se demuestra fácilmente con la ayuda de la ecuación $b^2 - ac = b'^2 - cc'$, donde por hipótesis $\frac{b+b'}{c}$ es un entero. Por otra parte, estas definiciones y conclusiones no valen si $c = a' = 0$. Pero este caso no puede ocurrir aquí más que en formas cuyo determinante es un cuadrado.

Las formas (a, b, c) y (a', b', c') son propiamente equivalentes si $a = a'$, $b \equiv b' \pmod{a}$. En efecto, la forma (a, b, c) equivale propiamente a la forma $(c, -b, a)$

(artículo anterior), pero esta última será contigua a la parte primera de la forma (a', b', c').

Divisores comunes de los coeficientes de las formas.

161.

Si la forma (a, b, c) implica la forma (a', b', c'), cualquier divisor común de los números a, b y c también dividirá a los números a', b' y c' y cada divisor común de los números a, $2b$ y c dividirá a a', $2b'$ y c'.

De hecho, si la forma $ax^2 + 2bxy + cy^2$ mediante la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ se transforma en la forma $a'x'^2 + 2b'x'y' + c'y'^2$, se tendrán estas ecuaciones:

$$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$a\beta^2 + 2b\beta\delta + c\delta^2 = c'$$

de donde se sigue la proposición (para la segunda parte de la proposición, en lugar de la segunda ecuación se usa $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$.)

De esto se deduce que el máximo común divisor de los números a, $b\,(2b)$, c divide al máximo común divisor de los números a', $b'\,(2b')$, c'. Si además la forma (a', b', c') implica la forma (a, b, c), i.e., si las formas son equivalentes, el máximo común divisor de los números a, $b\,(2b)$, c será igual al máximo común divisor de los números a', $b'\,(2b')$, c', puesto que tanto aquél debe dividir a éste, como éste a aquél. Por eso, si en este caso a, $b\,(2b)$, c no tienen un divisor común, i.e., si el máximo común divisor $= 1$, tampoco tendrá a', $b'\,(2b')$, c' un divisor común.

El nexo de todas las transformaciones semejantes de una forma dada en otra forma.

162.

Problema. *Si la forma*

$$AX^2 + 2BXY + CY^2 \ldots F$$

implica la forma

$$ax^2 + 2bxy + cy^2 \ldots f$$

y si se da alguna transformación de la primera en la segunda: de ésta se deducen todas las transformaciones restantes semejantes a esta misma.

Solución. Sea la transformación dada $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$. Supongamos primero que la otra semejante a ésta es $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$, de donde investigaremos lo siguiente. Dados los determinantes de las formas F y f $= D$ y d y $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$, tendremos (art. 157) $d = De^2 = De'^2$, y puesto que por hipótesis e y e' tienen los mismos signos, $e = e'$. Se tendrán así las siguientes seis ecuaciones:

$$A\alpha^2 + 2B\alpha\gamma + C\gamma^2 = a \tag{1}$$
$$A\alpha'^2 + 2B\alpha'\gamma' + C\gamma'^2 = a \tag{2}$$
$$A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = b \tag{3}$$
$$A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' = b \tag{4}$$
$$A\beta^2 + 2B\beta\delta + C\delta^2 = c \tag{5}$$
$$A\beta'^2 + 2B\beta'\delta' + C\delta'^2 = c \tag{6}$$

Si por brevedad denotamos los números

$$A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'$$
$$A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')$$
$$A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta'$$

por a', $2b'$, c', de las ecuaciones precedentes deduciremos otras nuevas*)

$$a'^2 - D(\alpha\gamma' - \gamma\alpha')^2 = a^2 \tag{7}$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab \tag{8}$$
$$4b'^2 - D((\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee') = 2b^2 + 2ac$$

de donde resulta, sumando $2Dee' = 2d = 2b^2 - 2ac$

$$4b'^2 - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4b^2 \tag{9}$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = b^2$$

*) Estas ecuaciones se originan así: la (7) viene de (1)·(2) (i.e., si la ecuación (1) se multiplica por la ecuación (2), o mejor, si la parte primera de la primera se multiplica por la parte primera de la segunda, y la parte última de la primera por la parte última de la segunda, y luego se ponen iguales los productos). La (8) viene de $(1)\cdot(4) + (2)\cdot(3)$; la siguiente, la cual no está numerada de $(1)\cdot(6) + (2)\cdot(5) + (3)\cdot(4) + (3)\cdot(4)$; la siguiente, sin número, de $(3)\cdot(4)$; la (11) de $(3)\cdot(6) + (4)\cdot(5)$; la (12) de $(5)\cdot(6)$. Siempre usaremos una notación semejante en lo siguiente. Pero debemos dejar los cálculos a los lectores.

de donde, restando $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = b^2 - ac$ se tiene

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac \tag{10}$$

$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc \tag{11}$$

$$c'^2 - D(\beta\delta' - \delta\beta')^2 = c^2 \tag{12}$$

Ahora supongamos que el máximo común divisor de los números a, $2b$, c es m, y los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ determinados de tal manera que

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

(art. 40). Multiplíquense las ecuaciones (7), (8), (9), (10), (11), (12) respectivamente por $\mathfrak{A}^2$, $2\mathfrak{A}\mathfrak{B}$, $\mathfrak{B}^2$, $2\mathfrak{A}\mathfrak{C}$, $2\mathfrak{B}\mathfrak{C}$, $\mathfrak{C}^2$ y súmense los productos. Ahora si por brevedad ponemos

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T \tag{13}$$

$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') + \mathfrak{C}(\beta\delta' - \delta\beta') = U \tag{14}$$

donde claramente T y U serán enteros, resultará

$$T^2 - DU^2 = m^2$$

Así llegamos a esta conclusión elegante: *de dos transformaciones semejantes cualesquiera de la forma F en f se deduce la resolución de la ecuación indeterminada $t^2 - Du^2 = m^2$ en enteros,* es decir $t = T$, $u = U$. Además como en nuestros razonamientos no hemos supuesto que las transformaciones son *diferentes, una* transformación tal considerada dos veces debe producir una solución. Entonces, por razón de que $\alpha' = \alpha$, $\beta' = \beta$, etc., será $a' = a$, $b' = b$, $c' = c$, por tanto $T = m$, $U = 0$, que es una solución obvia por sí misma.

Ahora, primero consideremos conocidas una transformación y una solución de la ecuación indeterminada, y luego investiguemos cómo puede deducirse la otra transformación y cómo α', β', γ', δ' dependen de α, β, γ, δ, T, U. Para este fin, multiplicamos primero la ecuación (1) por $\delta\alpha' - \beta\gamma'$, la (2) por $\alpha\delta' - \gamma\beta'$, la (3) por $\alpha\gamma' - \gamma\alpha'$, la (4) por $\gamma\alpha' - \alpha\gamma'$ y sumamos los productos, de donde resultará

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a \tag{15}$$

De modo semejante, de

$$(\delta\beta' - \beta\delta')((1) - (2)) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')((3) + (4)) + (\alpha\gamma' - \gamma\alpha')((5) - (6))$$

se tiene

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b \tag{16}$$

Finalmente, de $(\delta\beta' - \beta\delta')((3) - (4)) + (\alpha\delta' - \gamma\beta')(5) + (\delta\alpha' - \beta\gamma')(6)$ resultará

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c \tag{17}$$

Sustituyendo estos valores ((15), (16), (17)) en la (13) se obtiene

$$(e + e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)$$

o

$$2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m \tag{18}$$

de donde T puede deducirse con más facilidad que de la (13). — Combinando esta ecuación con (15), (16), (17) se obtiene $ma' = Ta$, $2mb' = 2Tb$, $mc' = Tc$. Sustituyendo estos valores de a', $2b'$, c' en las ecuaciones (7)–(12) y escribiendo $m^2 + DU^2$ en lugar de T^2 después de las alteraciones necesarias se transforman en éstas:

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')^2 m^2 &= a^2 U^2 \\
(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m^2 &= 2abU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 m^2 &= 4b^2 U^2 \\
(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')m^2 &= acU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')m^2 &= 2bcU^2 \\
(\beta\delta' - \delta\beta')^2 m^2 &= c^2 U^2
\end{aligned}$$

De esto con la ayuda de la ecuación (14) y de $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, se deduce fácilmente (multiplicando la primera, la segunda y la cuarta; la segunda, la tercera y la quinta; la cuarta, la quinta y la sexta respectivamente por $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ y sumando los productos):

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')Um^2 &= maU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')Um^2 &= 2mbU^2 \\
(\beta\delta' - \delta\beta')Um^2 &= mcU^2
\end{aligned}$$

y de esto, dividiendo por mU*)

$$aU = (\alpha\gamma' - \gamma\alpha')m \tag{19}$$
$$2bU = (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m \tag{20}$$
$$cU = (\beta\delta' - \delta\beta')m \tag{21}$$

de tales ecuaciones puede deducirse algún U con más facilidad que de la (14). — De modo semejante se concluye que no importa cómo se determinen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ (porque puede ser de infinitas maneras diferentes), tanto T como U tomarán el mismo valor.

Ahora si la ecuación (18) se multiplica por α, la (19) por 2β, la (20) por $-\alpha$, la suma da

$$2aeT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m.$$

De modo semejante de $\beta(18) + \beta(20) - 2\alpha(21)$

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m$$

Además de $\gamma(18) + 2\delta(19) - \gamma(20)$ es

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m$$

Finalmente, de $\delta(18) + \delta(20) - 2\gamma(21)$ resulta

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m$$

Si en estas fórmulas se sustituyen para a, b, c sus valores de (1), (3), (5) se obtiene

$$\alpha' m = \alpha T - (\alpha B + \gamma C)U$$
$$\beta' m = \beta T - (\beta B + \delta C)U$$
$$\gamma' m = \gamma T + (\alpha A + \gamma B)U$$
$$\delta' m = \delta T + (\beta A + \delta B)U\dagger)$$

*) Esto no se permitiría si $U = 0$: pero entonces la verdad de las ecuaciones (19), (20), (21) se obtendría inmediatamente de la primera, la tercera, y la sexta de las anteriores.

Del análisis anterior se deduce que no existe ninguna transformación semejante de la forma F en la f que no esté contenida en la fórmula

$$X = \frac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \frac{1}{m}(\beta t - (\beta B + \delta C)u)y$$
$$Y = \frac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \frac{1}{m}(\delta t + (\beta A + \delta B)u)y \qquad (I)$$

donde t y u denotan números enteros indeterminados que satisfacen la ecuación $t^2 - Du^2 = m^2$. De esto no hemos podido concluir que todos los valores de t y u que satisfacen aquella ecuación proporcionarán transformaciones adecuadas al sustituirlos en la fórmula (I). Sin embargo,

1. Por medio de las ecuaciones (1), (3), (5) y $t^2 - Du^2 = m^2$, puede confirmarse fácilmente que la forma F siempre puede transformarse en la forma f por una sustitución proveniente de valores cualesquiera de t y u. Por brevedad, suprimimos un cálculo más prolijo que difícil.

2. Cada trasformación deducida de la fórmula será semejante a la propuesta porque

$$\frac{1}{m}(\alpha t-(\alpha B+\gamma C)u)\cdot\frac{1}{m}(\delta t+(\beta A+\delta B)u)-\frac{1}{m}(\beta t-(\beta B+\delta C)u)\cdot\frac{1}{m}(\gamma t+(\alpha A+\gamma B)u)$$
$$= \frac{1}{m^2}(\alpha\delta - \beta\gamma)(t^2 - Du^2) = \alpha\delta - \beta\gamma$$

3. Si las formas F y f tienen determinantes diferentes, puede ocurrir que la fórmula (I) para algunos valores de t y u produzca sustituciones que impliquen *fracciones:* éstas deben rechazarse. Todas las restantes serán transformaciones adecuadas y no existirán otras.

4. Si las formas F y f tienen el mismo determinante, y por tanto son *equivalentes,* la fórmula (I) no presentará ninguna transformación que implique

†) De esto se deduce fácilmente

$$AeU = (\delta\gamma' - \gamma\delta')m$$
$$2BeU = (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m$$
$$CeU = (\beta\alpha' - \alpha\beta')m$$

fracciones, de donde en este caso dará la solución completa del problema. Esto lo demostramos como sigue:

Del teorema del artículo anterior, resulta en este caso que m será un común divisor de los números $A, 2B$ y C. Ya que $t^2 - Du^2 = m^2$, es $t^2 - B^2u^2 = m^2 - ACu^2$, por lo que $t^2 - B^2u^2$ será divisible por m^2: de esto también $4t^2 - 4B^2u^2$, y por lo tanto (porque $2B$ es divisible por m) también $4t^2$ por m^2, y por eso $2t$ por m. De esto $\frac{2}{m}(t + Bu)$ y $\frac{2}{m}(t - Bu)$ serán enteros, y ambos son pares o ambos impares (ya que la diferencia entre ellos, $\frac{4}{m}Bu$, es par). Si ambos fueran impares, también su producto sería impar, pero ya que el cuádruplo del número $\frac{1}{m^2}(t^2 - B^2u^2)$, el cual hemos mostrado como entero, es necesariamente par; entonces este caso es imposible, y por tanto $\frac{2}{m}(t+Bu)$ y $\frac{2}{m}(t-Bu)$ son siempre pares, de donde $\frac{1}{m}(t+Bu)$ y $\frac{1}{m}(t-Bu)$ serán enteros. De esto se deduce sin dificultad que los cuatro coeficientes en la (I) son siempre enteros. *Q. E. D.*

De lo anterior se concluye que, si se tienen todas las soluciones de la ecuación $t^2 - D^2u^2 = m^2$, se derivarán todas las transformaciones de la forma (A, B, C) en (a, b, c) semejantes a la transformación dada. Desde luego, enseñaremos a encontrar estas soluciones en lo siguiente. Observamos que el número de soluciones es siempre finito cuando D es negativo o un cuadrado positivo; pero es infinito cuando D es positivo y no un cuadrado. Cuando se presenta este caso, y cuando D no es $= d$ (ver arriba 3), se debe investigar cuidadosamente la manera en que se puedan conocer *a priori* los valores de t y u que producen sustituciones libres de fracciones. Pero para este caso, expondremos más adelante otro método libre de este problema.

Ejemplo. La forma $x^2 + 2y^2$ se transforma por la sustitución propia $x = 2x' + 7y', y = x' + 5y'$ en la forma (6, 24, 99): se desean *todas* las transformaciones propias de la primera en la segunda. Aquí $D = -2, m = 3$, y por lo tanto la ecuación por resolverse es: $t^2 + 2u^2 = 9$. Ella se satisface de seis maneras diferentes poniendo $t = 3, -3, 1, -1, 1, -1; u = 0, 0, 2, 2, -2, -2$ respectivamente. La tercera y sexta resolución dan sustituciones en fracciones, por lo que deben rechazarse. De los restantes resultan cuatro sustituciones:

$$x = \begin{vmatrix} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{vmatrix} \qquad y = \begin{vmatrix} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y' \end{vmatrix}$$

de las cuales la primera es la propuesta.

Formas ambiguas.

163.

Ya hemos dicho que puede ser que alguna forma F implique otra tanto propia como impropiamente. Es claro que esto ocurre si entre las formas F y F' pudiera interponerse otra, G, de modo que F implique G, G implique F', y la forma G sea impropiamente equivalente consigo misma. Si, en efecto, se supone que F implica G propia o impropiamente: como G implica a G impropiamente, F implicará a G impropia o propiamente respectivamente y, por tanto, en los dos casos tanto propia como impropiamente (art. 159). Del mismo modo, no importa la forma en que se suponga que G implica F', F siempre debe implicar F' tanto propia como impropiamente. En el caso obvio donde el término medio de la forma es $= 0$, se ve que tales formas son impropiamente equivalentes a sí mismas. De hecho, tal forma será opuesta a sí misma (art. 159) y por lo tanto impropiamente equivalente. En general cada forma (a, b, c) en la cual $2b$ es divisible por a está provista de esta propiedad. En efecto, la forma (c, b, a) será contigua (art. 160) a la primera parte de ésta y propiamente equivalente a ella. Sin embargo, (c, b, a) por art. 159 es impropiamente equivalente a la forma (a, b, c); por lo que (a, b, c) equivaldrá a sí misma impropiamente. Llamaremos *ambiguas* a tales formas (a, b, c) en las cuales $2b$ es divisible por a.

Así tendremos este teorema:

La forma F implicará la forma F' tanto propia como impropiamente, si puede encontrarse una forma ambigua contenida en F que implica a F'. Es evidente que esta proposición también puede invertirse:

Teorema sobre el caso en que una forma está contenida en otra al mismo tiempo propia e impropiamente.

164.

Teorema. *Si la forma*

$$Ax^2 + 2Bxy + Cy^2 \qquad (F)$$

implica la forma

$$A'x'^2 + 2B'x'y' + C'y'^2 \qquad (F')$$

tanto propia como impropiamente, entonces puede encontrarse una forma ambigua contenida en F y que implica a F'.

Supongamos que la forma F se transforma en la forma F' tanto por la sustitución

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

como por ésta diferente a ella

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

Entonces, denotados los números $\alpha\delta - \beta\gamma$ y $\alpha'\delta' - \beta'\gamma'$ por e y e' se tendrá $B'^2 - A'C' = e^2(B^2 - AC) = e'^2(B^2 - AC)$; de esto $e^2 = e'^2$, y, ya que por la hipótesis e y e' tienen signos opuestos, $e = -e'$ o $e + e' = 0$. Es claro que si en F' para x' se sustituye $\delta' x'' - \beta' y''$, y para y', $-\gamma' x'' + \alpha' y''$ se producirá la misma forma como cuando en la F se escribe

o bien	1)	para x	$\alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'')$	
		i.e.	$(\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y''$	
		y para y	$\gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'')$	
		i.e.	$(\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y''$	
o bien	2)	para x	$\alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'')$	i.e., $e' x''$
		y para y	$\gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'')$	i.e., $e' y''$

Así pues, denotados los números $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$, $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$ por a, b, c, d, la forma F se transformará en la misma forma por las dos sustituciones

$$x = ax'' + by'', \quad y = cx'' + dy''; \qquad x = e'x'', \quad y = e'y'',$$

de donde obtendremos las siguientes tres ecuaciones:

$$Aa^2 + 2Bac + Cc^2 = Ae'^2 \tag{1}$$

$$Aab + B(ad + bc) + Ccd = Be'^2 \tag{2}$$

$$Ab^2 + 2Bbd + Cd^2 = Ce'^2 \tag{3}$$

Pero de los mismos valores de a, b, c, d se encuentra:

$$ad - bc = ee' = -e^2 = -e'^2 \tag{4}$$

De aquí y de $d(1) - c(2)$

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'^2$$

y por tanto

$$A(a+d)=0$$

Además, de $(a+d)(2)-b(1)-c(3)$ se tiene

$$(Ab+B(a+d)+Cc)(ad-bc)=(-Ab+B(a+d)-Cc)e'^2$$

y por lo tanto

$$B(a+d)=0$$

Finalmente de $a(3)-b(2)$ obtenemos

$$(Bb+Cd)(ad-bc)=(-Bb+Ca)e'^2$$

y por lo tanto

$$C(a+d)=0$$

Por esto, como no todos A, B, C pueden ser $=0$, será necesario que $a+d=0$, o $a=-d$.

De $a(2)-b(1)$ tenemos

$$(Ba+Cc)(ad-bc)=(Ba-Ab)e'^2$$

de donde

$$Ab-2Ba-Cc=0. \tag{5}$$

De las ecuaciones $e+e'=0$, $a+d=0$, o

$$\alpha\delta-\beta\gamma+\alpha'\delta'-\beta'\gamma'=0, \qquad \alpha\delta'-\beta\gamma'-\gamma\beta'+\delta\alpha'=0$$

resulta $(\alpha+\alpha')(\delta+\delta')=(\beta+\beta')(\gamma+\gamma')$ o

$$(\alpha+\alpha'):(\gamma+\gamma')=(\beta+\beta'):(\delta+\delta').$$

Sea la razón*) $m:n$ igual a esta razón con números mínimos, de modo que m y n sean primos entre sí, y se toman μ,ν de manera que $\mu m+\nu n=1$. Además sea r el

*) Si todos $\alpha+\alpha',\gamma+\gamma',\beta+\beta',\delta+\delta'$ fueran $=0$, la razón sería indeterminada, y por ende el método no aplicable. Pero con cuidado se puede mostrar que esto no puede darse con nuestras suposiciones; pues sería $\alpha\delta-\beta\gamma=\alpha'\delta'-\beta'\gamma'$ i.e. $e=e'$, porque $e=-e', e=e'=0$. También $B'^2-A'C'$, i.e. el determinante de la forma F' sería $=0$. Tales formas las hemos excluido por completo.

máximo común divisor de los números a, b, c, cuyo cuadrado divida $a^2 + bc$, o $bc - ad$, o e^2; por lo que r también dividirá a e. Determinado esto así, si se supone que la forma F se transforma por la sustitución

$$x = mt + \frac{\nu e}{r}u, \qquad y = nt - \frac{\mu e}{r}u$$

en la forma $Mt^2 + 2Ntu + Pu^2 \quad (G)$, ésta será ambigua e implicará la forma F'.

Demostración. I. Para que sea evidente que la forma G es ambigua, mostraremos

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr$$

de donde, ya que r divide a a, b, c, entonces $\frac{1}{r}(b\mu^2 - 2a\mu\nu - c\nu^2)$ será un entero, y por lo tanto $2N$ un múltiplo de M. De hecho tenemos:

$$M = Am^2 + 2Bmn + Cn^2, \qquad Nr = (Am\nu - B(m\mu - n\nu) - Cn\mu)e \tag{6}$$

Además se confirma mediante cálculos fáciles que

$$\begin{aligned} 2e + 2a = e - e' + a - d &= (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma') \\ 2b &= (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta') \end{aligned}$$

De esto, puesto que $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$ será

$$\begin{aligned} m(2e + 2a) &= -2nb \qquad \text{o} \\ me + ma + nb &= 0 \end{aligned} \tag{7}$$

Del mismo modo encontramos que

$$\begin{aligned} 2e - 2a = e - e' - a + d &= (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma') \\ 2c &= (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta') \end{aligned}$$

y de esto $n(2e - 2a) = -2mc$ o

$$ne - na + mc = 0 \tag{8}$$

Ahora si se suma $m^2(b\mu^2 - 2a\mu\nu - c\nu^2)$ a

$$(1 - m\mu - n\nu)(m\nu(e - a) + (m\mu + 1)b) + (me + ma + nb)(m\mu\nu + \nu) + (ne - na + mc)m\nu^2$$

que evidentemente $= 0$ pues

$$1 - \mu m - \nu n = 0, \qquad me + ma + nb = 0, \qquad ne - na + mc = 0$$

al desarrollar los productos y remover las partes canceladas, resulta $2m\nu e + b$. Por lo cual será

$$m^2(b\mu^2 - 2a\mu\nu - c\nu^2) = 2m\nu e + b \tag{9}$$

Del mismo modo sumando a $mn(b\mu^2 - 2a\mu\nu - c\nu^2)$ lo siguiente:

$$(1-m\mu-n\nu)((n\nu-m\mu)e-(1+m\mu+n\nu)a)-(me+ma+nb)m\mu^2+(ne-na+mc)n\nu^2$$

se encuentra

$$mn(b\mu^2 - 2a\mu\nu - c\nu^2) = (n\nu - m\mu)e - a \tag{10}$$

Finalmente sumando a $n^2(b\mu^2 - 2a\mu\nu - c\nu^2)$ lo siguiente:

$$(m\mu+n\nu-1)(n\mu(e+a)+(n\nu+1)c)-(me+ma+nb)n\mu^2-(ne-na+mc)(n\mu\nu+\mu)$$

obtenemos

$$n^2(b\mu^2 - 2a\mu\nu - c\nu^2) = -2n\mu e - c \tag{11}$$

Ahora se deduce de la (9), la (10) y la (11) que

$$\begin{aligned}(Am^2 + 2Bmn + Cn^2)&(b\mu^2 - 2a\mu\nu - c\nu^2)\\ &= 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc\end{aligned}$$

o por la (6),

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr. \qquad Q.\ E.\ D.$$

II. Para demostrar que la forma G implica la forma F', demostraremos *primero*, que G se transforma en F' al poner

$$t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y', \qquad u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y' \qquad (S)$$

segundo, que $\frac{r}{e}(n\alpha - m\gamma)$ y $\frac{r}{e}(n\beta - m\delta)$ son enteros.

1. Puesto que F se transforma en G al ponerse

$$x = mt + \frac{\nu e}{r}u, \quad y = nt - \frac{\mu e}{r}u$$

la forma G se transformará por la sustitución (S) en la misma forma en que se transforma F al ponerse

$$x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') + \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

i.e., $$= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y' \quad \text{o} \quad = \alpha x' + \beta y'$$

y $$y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

i.e., $$= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y' \quad \text{o} \quad = \gamma x' + \delta y'$$

Mediante esta sustitución F se transforma en F'; por lo tanto G se transformará en F' por la sustitución (S).

2. De los valores de e, b y d se encuentra $\alpha' e + \gamma b - \alpha d = 0$, o, ya que $d = -a$, $n\alpha' e + n\alpha a + n\gamma b = 0$; de esto, usando la (7), $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$ o

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e \tag{12}$$

Además, $\alpha n b = -\alpha m(e + a)$, $\gamma m b = -m(\alpha' e + \alpha a)$ y por lo tanto

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me \tag{13}$$

Finalmente, $\gamma' e - \gamma a + \alpha c = 0$; de esto multiplicando por n y sustituyendo para na su valor de (8) obtenemos

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne \tag{14}$$

De modo semejante se saca $\beta' e + \delta b - \beta d = 0$ ó sea $n\beta' e + n\delta b + n\beta a = 0$, y, por lo tanto, por la (7), $n\beta' e + n\beta a = m\delta e + m\delta a$ o

$$(n\beta - m\delta)a = (m\delta - n\beta')e \tag{15}$$

Además $\beta n b = -\beta m(e + a)$, $\delta m b = -m(\beta' e + \beta a)$ y por tanto

$$(n\beta - m\delta)b = (\beta' - \beta)me \tag{16}$$

Finalmente $\delta' e - \delta a + \beta c = 0$; de esto multiplicando por n y sustituyendo na por suvalor de la (8):

$$(n\beta - m\delta)c = (\delta - \delta')ne \tag{17}$$

Ahora, como el máximo común divisor de los números a, b, c es r, pueden encontrarse enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ de modo que

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

Hecho esto, de la (12), la (13), la (14); la (15), la (16) y la (17) se obtiene

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \frac{r}{e}(n\alpha - m\gamma)$$
$$\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n = \frac{r}{e}(n\beta - m\delta)$$

y por lo tanto $\frac{r}{e}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ son enteros. *Q. E. D.*

165.

Ejemplo. La forma $3x^2+14xy-4y^2$ se transforma en $-12x'^2-18x'y'+39y'^2$, tanto propiamente, con poner

$$x = 4x' + 11y', \qquad y = -x' - 2y',$$

como impropiamente, con poner

$$x = -74x' + 89y', \qquad y = 15x' - 18y'$$

Aquí, por lo tanto, $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ son -70, 100, 14, -20; y $-70 : 14 = 100 : -20 = 5 : -1$. Así, pongamos $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Los números a, b, c son -237, -1170, 48, de los cuales el máximo común divisor $= 3 = r$; finalmente $e = 3$. De esto la transformación (S) será $x = 5t - u$, $y = -t$. Por ella la forma $(3, 7, -4)$ se transforma en la forma ambigua $t^2 - 16tu + 3u^2$.

Si las formas F y F' son equivalentes, entonces la forma G contenida en la forma F también estará contenida en F'. Sin embargo, puesto que también implica la misma forma F', será equivalente a ella y por tanto también a la forma F. Por lo tanto, en este caso el teorema se enuncia así:

Si F y F' son equivalentes tanto propia como impropiamente, podrá encontrarse una forma ambigua equivalente a las dos. Además en este caso $e = \pm 1$, y por lo tanto r que divide a e, será $= 1$.

Lo anterior es suficiente acerca de la transformación de las formas en general; así que pasaremos a la consideración de *las representaciones.*

Generalidades sobre las representaciones de los números por las formas y su nexo con las transformaciones.

166.

Si la forma F implica la forma F', cualquier número que puede representarse por F' también podrá ser representado por F.

Sean x e y, x' e y' las indeterminadas de las formas F y F' respectivamente, y supongamos que se representa al número M por F'. Al hacer $x' = m$ e $y' = n$, la forma F se transforma en F' por la sustitución

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

Entonces, evidentemente, si se pone

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

F se transforma en M.

Si M puede representarse de varias maneras por la forma F', e.g. poniendo $x' = m'$ e $y' = n'$, seguirán varias representaciones de M por F. De hecho, si fuera tanto

$$\alpha m + \beta n = \alpha m' + \beta n' \quad \text{como} \quad \gamma m + \delta n = \gamma m' + \delta n'$$

sería o bien $\alpha\delta - \beta\gamma = 0$, y por lo tanto también el determinante de la forma $F = 0$ (contrariamente a la hipótesis), o bien $m = m'$, $n = n'$. De esto resulta que M puede representarse al menos de tantas maneras diferentes por F como por F'.

Por ende, si tanto F implica F' como F' implica F i.e., si F y F' son equivalentes, y el número M puede representarse por una de las dos, también puede representarse por la otra, de tantas maneras diferentes para la una como para la otra.

Finalmente, observamos que en este caso el máximo común divisor de los números m y n es igual al máximo común divisor de los números $\alpha m + \beta n$ y $\gamma m + \delta n$. Sea aquél $= \Delta$, y tomemos los números μ y ν de modo que resulte $\mu m + \nu n = \Delta$. Entonces, tendremos

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta$$

De esto, el máximo común divisor de los números $\alpha m + \beta n$ y $\gamma m + \delta n$ dividirá a Δ, y también Δ lo dividirá a él; pues, evidentemente dividirá a $\alpha m + \beta n$ y $\gamma m + \delta n$. Por lo que, necesariamente aquél será $= \Delta$. Por lo tanto, cuando m y n son primos entre sí, también $\alpha m + \beta n$ y $\gamma m + \delta n$ lo serán.