235.

Si la forma $AX^2 + 2BXY + CY^2 \ldots F$ se transforma en el producto de dos formas

$$ax^2 + 2bxy + cy^2 \ldots f, \quad \text{y} \quad a'x'^2 + 2b'x'y' + c'y'^2 \ldots f'$$

mediante la sustitución

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

(para abreviar, en lo que sigue expresaremos esta situación de la siguiente manera: Si F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q'''*)), diremos simplemente que la forma F es *transformable* en ff'. Si además se construye esta transformación de tal manera que los seis números

$$pq' - qp',\ pq'' - qp'',\ pq''' - qp''',\ p'q'' - q'p'',\ p'q''' - q'p''',\ p''q''' - q''p'''$$

no tienen un divisor común, llamaremos a F una forma *compuesta* de las formas f y f'.

Iniciaremos esta discusión con la suposición más general de que la forma F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q''' y descubriremos qué es lo que deducimos de ésto. Claramente las nueve ecuaciones siguientes son completamente equivalentes a esta suposición (i.e. cuando estas ecuaciones se cumplen F será transformada, mediante las sustituciones dadas, en ff', y vice-versa):

$$Ap^2 + 2Bpq + Cq^2 = aa' \qquad [1]$$
$$Ap'^2 + 2Bp'q' + Cq'^2 = ac' \qquad [2]$$
$$Ap''^2 + 2Bp''q'' + Cq''^2 = ca' \qquad [3]$$
$$Ap'''^2 + 2Bp'''q''' + Cq'''^2 = cc' \qquad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \qquad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \qquad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \qquad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \qquad [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb' \qquad [9]$$

*) En esta expresión debemos poner mucho cuidado en el orden de los coeficientes p, p', etc. y de las formas f y f'. Es fácil ver que si el orden de las formas f y f' se cambia tal que la primera se convierte en la segunda, los coeficientes p' y q' deben intercambiarse con p'' y q'' y los otros deben permanecer iguales.

Sean D, d y d' los determinantes de las formas F, f y f' respectivamente; y sean M, m y m' los máximos comunes divisores de los números A, $2B$, C; a, $2b$, c; a', $2b'$, c', respectivamente (suponemos que todos estos números son positivos). Además sean los seis enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ determinados de modo que

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

Finalmente desígnense los números

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''', \quad p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

por P, Q, R, S, T, U respectivamente y sea k su máximo común divisor tomado positivamente. Ahora, haciendo

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \qquad [10]$$

de la ecuación [9] obtenemos

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \qquad [11]$$

A partir de esas once ecuaciones desarrollamos las siguientes*):

$$DP^2 = d'a^2 \qquad [12]$$
$$DP(R-S) = 2d'ab \qquad [13]$$
$$DPU = d'ac - (\Delta^2 - dd') \qquad [14]$$
$$D(R-S)^2 = 4d'b^2 + 2(\Delta^2 - dd') \qquad [15]$$
$$D(R-S)U = 2d'bc \qquad [16]$$
$$DU^2 = d'c^2 \qquad [17]$$
$$DQ^2 = da'^2 \qquad [18]$$
$$DQ(R+S) = 2da'b' \qquad [19]$$
$$DQT = da'c' - (\Delta^2 - dd') \qquad [20]$$
$$D(R+S)^2 = 4db'^2 + 2(\Delta^2 - dd') \qquad [21]$$
$$D(R+S)T = 2db'c' \qquad [22]$$
$$DT^2 = dc'^2 \qquad [23]$$

*) El origen de estas ecuaciones es como sigue: [12] de $[5]^2 - [1][2]$; [13] de $[5][9] - [1][7] - [2][6]$; [14] de $[10][11] - [6][7]$; [15] de $2[5][8] + [10]^2 + [11]^2 - [1][4] - [2][3] - 2[6][7]$; [16] de $[8][9] - [3][7] - [4][6]$; [17] de $[8]^2 - [3][4]$. Podemos deducir las seis ecuaciones restantes por medio de los mismos esquemas, si reemplazamos las ecuaciones [3], [6], [8] por las ecuaciones [2], [5], [7] respectivamente y dejamos [1], [4], [9], [10], [11] tal como aparecen. Por ejemplo, la ecuación [18] viene de $[6]^2 - [1][3]$, etc.

Y a partir de ellas deducimos las dos siguientes:

$$0 = 2d'a^2(\Delta^2 - dd')$$
$$0 = (\Delta^2 - dd')^2 - 2d'ac(\Delta^2 - dd')$$

la primera a partir de las ecuaciones $[12][15] - [13]^2$, la segunda a partir de las ecuaciones $[14]^2 - [12][17]$; y es fácil notar que $\Delta^2 - dd' = 0$ tanto si a es igual a cero como si no lo es*). Supongamos que se ha cancelado $\Delta^2 - dd'$ de las ecuaciones [14], [15], [20] y [21].

Ahora

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n$$

(donde n y n' pueden ser fracciones siempre que mn' y $m'n$ sean enteros). A partir de las ecuaciones [12]-[17] se deduce que

$$Dm^2n'^2 = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'm^2$$

y de las ecuaciones [18]-[23]

$$Dm'^2n^2 = d'(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'^2$$

Tenemos entonces $d = Dn^2$, $d' = Dn'^2$ y a partir de esto obtenemos una PRIMERA CONCLUSIÓN: *Los cocientes de los determinantes de las formas F, f y f' necesariamente son cuadrados*; y una SEGUNDA: *D siempre divide a los números dm'^2 y $d'm^2$.* Entonces es claro que D, d y d' tienen el mismo signo y que ninguna forma puede transformarse en el producto ff' si su determinante es mayor que el máximo común divisor de dm'^2 y $d'm^2$.

Multiplicamos las ecuaciones [12], [13], [14] por $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ respectivamente y similarmente a las ecuaciones [13], [15], [16] y [14], [16], [17] por los mismos números y sumamos los tres productos. Divida la suma por Dmn', escribiendo Dn'^2 en vez de d'. Entonces se obtiene

$$P = an', \quad R - S = 2bn', \quad U = cn'$$

*) Esta manera de derivar la ecuación $\Delta^2 = dd'$ es suficiente para nuestros propósitos actuales. Podríamos haber deducido directamente de las ecuaciones [1] a [11] que $0 = (\Delta^2 - dd')^2$. Este podría haber sido un análisis más elegante pero demasiado prolongado en este punto.

De manera semejante, multiplicando las ecuaciones [18], [19], [20] y [19], [21], [22] y [20], [22], [23] por $\mathfrak{A}'$, $\mathfrak{B}'$ y $\mathfrak{C}'$ resulta

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n$$

A partir de esto obtenemos una TERCERA CONCLUSIÓN: *Los números a, $2b$, y c son proporcionales a los números P, $R-S$ y U. Si la razón del primero al segundo se toma como 1 a n', n' será la raíz cuadrada de $\frac{d'}{D}$; de la misma manera los números a', $2b'$ y c' son proporcionales a los números Q, $R+S$ y T y si tomamos la razón como 1 a n, n será la raíz cuadrada de $\frac{d}{D}$.*

Ahora, las cantidades n y n' pueden ser o raíces positivas o raíces negativas de $\frac{d}{D}$ y $\frac{d'}{D'}$, así haremos una distinción que puede parecer estéril a primera vista, pero su uso quedará claro en lo que sigue. Diremos que en la transformación de la forma F en ff' la forma f se toma *directamente* cuando n es positivo e *inversamente* cuando n es negativo; de manera análoga f' se toma directamente o inversamente de acuerdo con que n' sea positivo o negativo. Dada la condición de que k sea igual a 1, se dice que la forma F está compuesta de las dos formas f y f' directamente *o* de las dos inversamente *o* de f directamente y de f' inversamente *o* de f inversamente y de f' directamente según que n y n' sean ambos positivos o ambos negativos o que el primero sea positivo y el segundo negativo o el primero negativo y el segundo positivo. Es fácil notar que estas relaciones no dependen del orden en que se hayan tomado las formas (véase la primera nota de este artículo).

Notamos además que k, el máximo común divisor de los números P, Q, R, S, T y U, divide a los números mn' y $m'n$ (como queda claro a partir de los valores que establecimos más arriba). Por tanto el cuadrado k^2 divide a $m^2n'^2$ y m'^2n^2, y Dk^2 divide a $d'm^2$ y $d'm'^2$. Pero recíprocamente, todo divisor común de mn' y $m'n$ divide a k. Sea e un divisor tal: evidentemente este dividirá a an', $2bn'$, cn', $a'n$, $2b'n$ y $c'n$; i.e., a los números P, $R-S$, U, Q, $R+S$ y T y también a $2R$ y $2S$. Ahora si $\frac{2R}{e}$ es un número impar, $\frac{2S}{e}$ también debe ser impar (pues la suma y la diferencia son pares) y el producto también deberá ser impar. Este producto es igual a $\frac{4}{e^2}(b'^2n^2 - b^2n'^2) = \frac{4}{e^2}(d'n^2 + a'c'n^2 - dn'^2 - acn'^2) = \frac{4}{e^2}(a'c'n^2 - acn'^2)$ y por tanto par, porque e divide a $a'n$, $c'n$, an' y cn'. Así $\frac{2R}{e}$ es necesariamente par y ambos R y S son divisibles por e. Ya que e divide a los seis P, Q, R, S, T y U, también dividirá a k, su máximo común divisor. *Q. E. D.* Concluimos que k es el máximo común divisor de los números mn' y $m'n$, y *Dk^2 será el máximo común divisor de los números dm'^2, $d'm^2$.* Esta es nuestra CUARTA CONCLUSIÓN. Ahora es claro

que siempre que F se componga de f y f', D será el máximo común divisor de los números dm'^2 y $d'm^2$ y vice versa. Estas propiedades pudieron también utilizarse como la definición de las formas compuestas. Por ende, la forma que está compuesta de las formas f y f', posee el máximo determinante posible de todas las formas que son transformables en el producto ff'.

Antes de que continuemos más adelante, definiremos primero el valor de Δ más exactamente. Mostramos que $\Delta = \sqrt{dd'} = \sqrt{D^2n^2n'^2}$, pero no se ha determinado aún su *signo*. Para tal propósito deducimos a partir de las ecuaciones fundamentales [1] a [11] que $DPQ = \Delta aa'$ (obtenemos esto a partir de [5][6] − [1][11]). Así $Daa'nn' = \Delta aa'$, y a menos que uno de los números a o a' sea igual a 0, tenemos $\Delta = Dnn'$. Exactamente de la misma forma, a partir de las ecuaciones fundamentales podemos deducir otras ocho en las cuales tenemos Dnn' a la izquierda y Δ en la derecha multiplicados por $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$ y cc'*). Ahora, dado que no todos a, $2b$ y c ni todos a', $2b'$ y c' pueden ser iguales a 0, en todos los casos $\Delta = Dnn'$ y Δ posee el mismo signo que D, d y d' o el opuesto, según que n y n' posean el mismo signo o signos diferentes.

Observamos que los números aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb' + 2\Delta$ y $2bb' - 2\Delta$ son todos divisibles por mm'. Esto es obvio para los primeros nueve números. Para los otros dos podemos mostrar, como hicimos al principio, que R y S son divisibles por e. Es claro que $4bb' + 4\Delta$ y $4bb' - 4\Delta$ son divisibles por mm' (dado que $4\Delta = \sqrt{16dd'}$ y $4d$ es divisible por m^2, $4d'$ por m'^2, y así $16dd'$ por $m^2m'^2$ y 4Δ por mm') y que la diferencia de los cocientes es par. Es fácil demostrar que el producto de los cocientes es par, y así que cada cociente es par y que $2bb' + 2\Delta$, $2bb' - 2\Delta$ son divisibles por mm'.

Ahora a partir de las once ecuaciones fundamentales derivamos las seis siguientes:

$$
\begin{aligned}
AP^2 &= aa'q'^2 - 2ab'qq' + ac'q^2 \\
AQ^2 &= aa'q''^2 - 2ba'qq'' + ca'q^2 \\
AR^2 &= aa'q'''^2 - 2(bb' + \Delta)qq''' + cc'q^2 \\
AS^2 &= ac'q''^2 - 2(bb' - \Delta)q'q'' + ca'q'^2 \\
AT^2 &= ac'q'''^2 - 2bc'q'q''' + cc'q'^2 \\
AU^2 &= ca'q'''^2 - 2cb'q''q''' + cc'q''^2
\end{aligned}
$$

*) El lector puede verificar este análisis fácilmente. Lo omitimos en aras de la brevedad.

Se sigue por lo tanto que todos AP^2, AQ^2, etc. son divisibles por mm' y dado que k^2 es el máximo común divisor de los números P^2, Q^2, R^2, etc., Ak^2 será también divisible por mm'. Si sustituimos por a, $2b$, c, a', $2b'$ y c' sus valores $\frac{P}{n'}$, etc. o $\frac{1}{n'}(pq' - qp')$, etc., ellos podrían cambiarse por otras seis ecuaciones en las cuales tendremos, en el lado derecho, productos de la cantidad $\frac{1}{nn'}(q'q'' - qq''')$ por P^2, Q^2, R^2, etc. Dejaremos estos sencillos cálculos al lector. Se sigue (puesto que no todo P^2, Q^2, etc. $= 0$) que $Ann' = q'q'' - qq'''$.

Similarmente, a partir de las ecuaciones fundamentales podemos obtener otras seis ecuaciones que difieren de las anteriores en que se reemplazan A y q, q', q'', q''' por C y p, p', p'', p''' respectivamente. Para abreviar omitimos los detalles. Finalmente, de modo semejante se sigue que Ck^2 es divisible por mm' y $Cnn' = p'p'' - pp'''$.

Nuevamente podemos deducir otras seis ecuaciones a partir de los mismos datos:

$$\begin{aligned}
BP^2 &= -aa'p'q' + ab'(pq' + qp') - ac'pq \\
BQ^2 &= -aa'p''q'' + ba'(pq'' + qp'') - ca'pq \\
BR^2 &= -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq \\
BS^2 &= -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q' \\
BT^2 &= -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q' \\
BU^2 &= -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q''
\end{aligned}$$

y a partir de esto, como en el caso anterior, concluimos que $2Bk^2$ es divisible por mm' y $2Bnn' = pq''' + qp''' - p'q'' - q'p''$.

Ahora, puesto que Ak^2, $2Bk^2$ y Ck^2 son divisibles por mm', es fácil ver que Mk^2 también debe ser divisible por mm'. De las ecuaciones fundamentales sabemos que M es divisor de aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$ y cc' y por lo tanto también de am', $2bm'$ y cm' (los cuales son los máximos comunes divisores de los primeros, segundos y últimos tres respectivamente); y finalmente que también es divisor de mm', el cual es el máximo común divisor de todos éstos. Por lo tanto, en este caso, donde la forma F está compuesta por las formas f, f', eso es $k = 1$, M necesariamente $= mm'$. Esta es nuestra Quinta Conclusión.

Si designamos el máximo común divisor de los números A, B y C por $\mathfrak{M}$, será $= M$ (cuando la forma F es propiamente primitiva o se obtiene a partir de una forma propiamente primitiva) ó $= \frac{1}{2}M$ (cuando F es impropiamente primitiva o se obtiene a partir de una forma impropiamente primitiva); similarmente, si designamos los máximos comunes divisores de los números a, b y c; a', b' y c' por $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente, $\mathfrak{m}$ será $= m$ ó $= \frac{1}{2}m$ y $\mathfrak{m}'$ será $= m'$ ó $= \frac{1}{2}m'$. Ahora, es claro

que $\mathfrak{m}^2$ es divisor de d, $\mathfrak{m}'^2$ es divisor de d'. Por lo tanto $\mathfrak{m}^2\mathfrak{m}'^2$ es divisor de dd' o de Δ^2, y $\mathfrak{m}\mathfrak{m}'$ es divisor de Δ. De las últimas seis ecuaciones para BP^2 etc. se sigue que $\mathfrak{m}\mathfrak{m}'$ es divisor de Bk^2 y (puesto que también es divisor de Ak^2 y de Ck^2) de $\mathfrak{M}k^2$. Por lo tanto, cada vez que F esté compuesta por f y f', $\mathfrak{m}\mathfrak{m}'$ será divisor de $\mathfrak{M}$. Y cuando ambos f y f' son propiamente primitivas u obtenidas a partir de formas propiamente primitivas, o $\mathfrak{m}\mathfrak{m}' = mm' = M$, entonces $\mathfrak{M} = M$ ó F es una forma similar. Pero, si bajo las mismas condiciones una o ambas formas f y f' son impropiamente primitivas u obtenidas a partir de formas impropiamente primitivas, entonces (si la forma f por ejemplo lo es) a partir de las ecuaciones fundamentales se sigue que aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc' son divisibles por $\mathfrak{M}$ y así también am', bm', cm' y $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$; en este caso $\mathfrak{M} = \frac{1}{2}M$ y la forma F es impropiamente primitiva u obtenida a partir de una forma impropiamente primitiva. Esta es nuestra SEXTA CONCLUSIÓN.

Finalmente observamos que, si *se supone* que las siguientes nueve ecuaciones son verdaderas,

$$\begin{gathered} an' = P, \quad 2bn' = R - S, \quad cn' = U \\ a'n = Q, \quad 2b'n = R + S, \quad c'n = T \\ Ann' = q'q'' - qq''', \quad 2Bnn' = pq''' + qp''' - p'q'' - q'p'', \quad Cnn' = p'p'' - pp''' \end{gathered}$$

(en lo que sigue, designaremos estas condiciones por Ω, ya que las retomaremos frecuentemente) entonces, tomando n y n' como incógnitas pero ninguna $= 0$, encontramos mediante una sustitución sencilla que las ecuaciones fundamentales [1] a [9] son necesariamente verdaderas, o sea, que la forma (A, B, C) será transformada en el producto de las formas $(a, b, c)(a', b', c')$ mediante la sustitución p, p', p'', p'''; q, q', q'', q'''. También tendremos

$$b^2 - ac = n^2(B^2 - AC), \qquad b'^2 - a'c' = n'^2(B^2 - AC)$$

El cálculo, que sería demasiado largo para exponerlo aquí, lo dejamos al lector.

236.

PROBLEMA. *Dadas dos formas cuyos determinantes son iguales o por lo menos difieren por factores cuadrados: encontrar una forma compuesta por estas dos.*

Solución. Sean $(a,b,c)\dots f$ y $(a',b',c')\dots f'$ las formas iniciales; d y d' sus determinantes; m y m' los máximos comunes divisores de los números a, $2b$, c; a', $2b'$, c' respectivamente; D el máximo común divisor de los números dm'^2 y $d'm^2$ tomados con el mismo signo que d y d'. Entonces $\frac{dm'^2}{D}$ y $\frac{d'm^2}{D}$ serán números positivos primos relativos y su producto será un cuadrado; por lo tanto cada uno de ellos será un cuadrado (art. 21). Así pues, $\sqrt{\frac{d}{D}}$ y $\sqrt{\frac{d'}{D}}$ serán cantidades racionales que dejaremos ser $= n$, n' y escogeremos para n un valor positivo o negativo dependiendo de si la forma f debe entrar directa o inversamente en la composición. De manera similar determinaremos el signo de n' según la manera en la cual la forma f' debe entrar en la composición. Entonces mn' y $m'n$ serán enteros primos entre sí; n y n' pueden ser fracciones. Ahora observamos que an', cn', $a'n$, $c'n$, $bn'+b'n$ y $bn'-b'n$ son enteros. Esto es obvio para los primeros cuatro (puesto que $an' = \frac{a}{m}mn'$ etc.); para los últimos dos lo probamos tal como se hizo en el último artículo para probar que R y S son divisibles por e.

Tomemos ahora cuatro enteros $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$ y $\mathfrak{Q}'''$ arbitrarios con sólo una condición, que las cuatro cantidades a la izquierda de las siguientes ecuaciones (I) no sean todas $= 0$. Ahora, considérense las ecuaciones:

$$\begin{aligned}
\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn'+b'n) &= \mu q \\
-\mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}''(bn'-b'n) &= \mu q' \\
\mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn'-b'n) &= \mu q'' \\
-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn'+b'n) &= \mu q'''
\end{aligned} \qquad (I)$$

tales que q, q', q'' y q''' son enteros sin un divisor común. Esto se puede lograr tomando para μ el máximo común divisor de los cuatro números que están a la izquierda de las ecuaciones. Ahora, según el artículo 40 podemos encontrar cuatro enteros $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ tales que

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

Una vez logrado ésto, determínense los números p, p', p'' y p''' mediante las siguientes ecuaciones:

$$\begin{aligned}
\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn'+b'n) &= p \\
-\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn'-b'n) &= p' \\
\mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn'-b'n) &= p'' \\
-\mathfrak{P}''cn' - \mathfrak{P}'c'n' - \mathfrak{P}(bn'+b'n) &= p'''
\end{aligned} \qquad (II)$$

Ahora se hacen las siguientes sustituciones:

$$q'q'' - qq''' = Ann', \quad pq''' + qp''' - p'q'' - q'p'' = 2Bnn', \quad p'p'' - pp''' = Cnn'$$

Entonces A, B y C serán enteros y la forma $(A, B, C) \ldots F$ será compuesta por las formas f y f'.

Demostración. I. A partir de (I) obtenemos las siguientes cuatro ecuaciones:

$$\begin{aligned} 0 &= q'cn' - q''c'n - q'''(bn' - b'n) \\ 0 &= qcn' + q'''a'n - q''(bn' + b'n) \\ 0 &= q'''an' + qc'n - q'(bn' + b'n) \\ 0 &= q''an' - q'a'n - q(bn' - b'n) \end{aligned} \qquad (III)$$

II. Ahora supongamos que los enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{N}$, $\mathfrak{N}'$ se determinan de modo que

$$\begin{aligned} \mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m \\ \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m' \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1 \end{aligned}$$

Entonces tendremos

$$\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1$$

A partir de esto y las ecuaciones (III), si dejamos que

$$\begin{aligned} -q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q} \\ q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}' \\ -q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'' \\ q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}''' \end{aligned}$$

obtendremos

$$\begin{aligned} \mathfrak{q}'an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) &= q \\ -\mathfrak{q}an' + \mathfrak{q}'''c'n - \mathfrak{q}''(bn' - b'n) &= q' \\ \mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) &= q'' \\ -\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) &= q''' \end{aligned} \qquad (IV)$$

Cuando $\mu = 1$ estas ecuaciones son innecesarias y se pueden utilizar las ecuaciones (I), que son enteramente análogas, en su lugar. Ahora, a partir de las ecuaciones (II) y (IV) determinamos los valores de Ann', $2Bnn'$ y Cnn' (i.e. de los números $q'q'' - qq'''$ etc.) y suprimimos los valores que se anulan entre sí, y encontramos que los términos diferentes son productos de enteros por nn', dn'^2 o $d'n^2$. Además, todos los términos de $2Bnn'$ contienen el factor 2. Concluimos que A, B y C son enteros (porque $dn'^2 = d'n^2$ y por lo tanto $\frac{dn'^2}{nn'} = d'\frac{n^2}{nn'} = \sqrt{dd'}$ son enteros). *Q. E. P.*

III. Si tomamos los valores de p, p', p'' y p''' de (II), utilizamos las ecuaciones (III) y la siguiente:

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

encontramos que

$$\begin{array}{llll} pq' - qp' = an', & pq''' - qp''' - p'q'' + q'p'' = 2bn', & p''q''' - q''p''' = cn' \\ pq'' - qp'' = a'n, & pq''' - qp''' + p'q'' - q'p'' = 2b'n, & p'q''' - q'p''' = c'n \end{array}$$

Estas ecuaciones son idénticas a las primeras seis (Ω) del artículo anterior. Las tres restantes son parte de la hipótesis. Por lo tanto (final del mismo artículo) la forma F se transformará en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q'''; su determinante será $= D$, o sea, será igual al máximo común divisor de los números dm'^2 y $d'm^2$. Según la cuarta conclusión del artículo anterior esto significa que F está compuesta por f y f', *Q. E. S.* Y finalmente se sabe que F se compone de f y f' según la forma prescrita puesto que los signos de n y n' se determinaron correctamente al comienzo.

237.

TEOREMA. *Si la forma F es transformable en el producto de dos formas f y f', y la forma f' implica la forma f'', entonces F también será transformable en el producto de las formas f y f''.*

Demostración. Para las formas F, f y f' todas las notaciones del artículo 235 se mantienen; sea $f'' = (a'', b'', c'')$ y sea f' transformado en f'' mediante la sustitución α, β, γ, δ. Entonces F se transformará en ff'' mediante la sustitución

$$\begin{array}{llll} \alpha p + \gamma p', & \beta p + \delta p', & \alpha p'' + \gamma p''', & \beta p'' + \delta p''' \\ \alpha q + \gamma q', & \beta q + \delta q', & \alpha q'' + \gamma q''', & \beta q'' + \delta q''' \end{array} \quad Q.\ E.\ D.$$

Para abreviar designaremos estos coeficientes como sigue:

$$\alpha p + \gamma p', \quad \beta p + \delta p' \text{ etc.} = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \ \mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$$

y sea el número $\alpha\delta - \beta\gamma = e$. A partir de las ecuaciones Ω, artículo 235, es fácil ver que

$$\begin{aligned}
\mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' &= an'e \\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' &= 2bn'e \\
\mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' &= cn'e \\
\mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' = \alpha^2 a'n + 2\alpha\gamma b'n + \gamma^2 c'n &= a''n \\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2b''n \\
\mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' &= c''n \\
\mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' &= Ann'e \\
\mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2Bnn'e \\
\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e
\end{aligned}$$

Ahora, si designamos el determinante de la forma f'' por d'', e será una raíz cuadrada de $\frac{d''}{d'}$, positiva o negativa según la forma f' implica la forma f'' propia o impropiamente. Así pues $n'e$ será una raíz cuadrada de $\frac{d''}{D}$; y las nueve ecuaciones anteriores serán completamente análogas a las ecuaciones Ω del artículo 235. La forma f se tomará en la transformación de la forma F en ff'' de manera idéntica a como se tomó en la transformación de la forma F en ff'. La forma f'' en la primera debe tomarse como se tomó f' en la segunda si f' implica f'' propiamente. Si f' implica f'' impropiamente, debe tomarse de manera opuesta.

238.

Teorema. *Si la forma F está contenida en la forma F' y es transformable en el producto de las formas f y f'; entonces la forma F' será transformable en el mismo producto.*

Demostración. Si para las formas F, f y f' se retiene la misma notación que en el caso anterior y si se supone además que la forma F' se transforma en F mediante la sustitución α, β, γ, δ, es fácil ver que, mediante la sustitución

$$\begin{matrix}
\alpha p + \beta q, & \alpha p' + \beta q', & \alpha p'' + \beta q'', & \alpha p''' + \beta q''' \\
\gamma p + \delta q, & \gamma p' + \delta q', & \gamma p'' + \delta q'', & \gamma p''' + \delta q'''
\end{matrix}$$

F' se convierte en lo mismo que F mediante la sustitución p, p', p'', p'''; q, q', q'', q''' y por lo tanto a través de esta transformación F' se transforma en ff'. *Q. E. D.*

Mediante un cálculo similar al del artículo anterior también es posible comprobar que F' es transformable en ff' de la misma manera que F, cuando F' implica F propiamente. Pero cuando F está contenida impropiamente en F' las transformaciones de las formas F y F' en ff' serán opuestas respecto a cada una de las formas f y f'; eso es, si una forma aparece en una de las transformaciones directamente, aparecerá en la otra de manera inversa.

Si combinamos este teorema con el del artículo anterior obtendremos la siguiente generalización. *Si la forma F es transformable en el producto ff', si las formas f y f' implican las formas g y g' respectivamente, y si la forma F está contenida en la forma G: entonces G será transformable en el producto gg'.* En efecto, según el teorema de éste artículo G es transformable en ff' y así según el teorema anterior en fg' y así también en gg'. También es claro que, si todas las tres formas f, f' y G implican las formas g, g' y F propiamente, G será transformable en gg' con respecto a las formas g y g' de igual manera que F en ff' con respecto a las formas f y f'. Lo mismo es cierto si las tres implicaciones son impropias. Si una de las implicaciones es diferente de las otras dos, es igualmente fácil determinar *cómo* G es transformable en gg'.

Si las formas F, f y f' son equivalentes a las formas G, g y g' respectivamente, los segundos tendrán los mismos determinantes que los primeros. Y m y m' serán para g y g' los mismos que para f y f' (art. 161). Así pues, según la cuarta conclusión del artículo 235 se deduce que G está *compuesta* por g y g' si F está compuesta por f y f'; y de hecho la forma g entrará en la primera composición de igual manera que f lo hace en la segunda, siempre y cuando F sea equivalente a G de la misma manera que f lo es a g y vice versa. Similarmente g' debe tomarse en la primera composición de manera igual u opuesta a como se tomó f' en la segunda, según la equivalencia de las formas f' y g' sea similar o no a la equivalencia de las formas F y G.

239.

Teorema. *Si la forma F está compuesta por las formas f y f', cualquier otra forma que sea transformable en el producto ff' de la misma manera que F, implicará a F propiamente.*

Demostración. Si mantenemos la notación del artículo 235 para las formas F, f y f', las ecuaciones Ω también tendrán lugar aquí. Supongamos que la forma

$F' = (A', B', C')$ cuyo determinante $= D'$ se transforma en el producto ff' mediante la sustitución $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$; $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$, $\mathfrak{q}'''$. Designemos los números

$$\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', \quad \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', \quad \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''', \quad \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', \quad \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', \quad \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$$

respectivamente por

$$P', \quad Q', \quad R', \quad S', \quad T', \quad U'$$

Entonces se tendrán nueve ecuaciones que son completamente similares a las de Ω, a saber

$$\begin{gathered} P' = a\mathfrak{n}', \quad R' - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}' \\ Q' = a'\mathfrak{n}, \quad R' + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n} \\ q'q'' - qq''' = A'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}' \end{gathered}$$

Designaremos estas ecuaciones por Ω'. Las cantidades $\mathfrak{n}$ y $\mathfrak{n}'$ son, en este caso, las raíces cuadradas de $\frac{d}{D'}$ y $\frac{d'}{D'}$, y tienen el mismo signo que n y n' respectivamente; entonces, si tomamos la raíz cuadrada positiva de $\frac{D}{D'}$ (será un entero) y lo hacemos $= k$, tendremos $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. Entonces, a partir de las primeras seis ecuaciones de Ω y Ω' obtenemos

$$\begin{gathered} P' = kP, \quad Q' = kQ, \quad R' = kR \\ S' = kS, \quad T' = kT, \quad U' = kU \end{gathered}$$

Según el lema del artículo 234 podrán encontrarse cuatro enteros α, β, γ, δ tales que

$$\begin{gathered} \alpha p + \beta q = \mathfrak{p}, \quad \gamma p + \delta q = \mathfrak{q} \\ \alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}' \text{ etc.} \end{gathered}$$

y

$$\alpha\delta - \beta\gamma = k$$

Sustituyendo estos valores de $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{q}'$, etc. en las últimas tres ecuaciones de Ω' y utilizando las ecuaciones $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ y las últimas tres ecuaciones de Ω encontramos que

$$\begin{gathered} A'\alpha^2 + 2B'\alpha\gamma + C'\gamma^2 = A \\ A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B \\ A'\beta^2 + 2B'\beta\delta + C'\delta^2 = C \end{gathered}$$

Por lo tanto, mediante la sustitución α, β, γ, δ (que será propia puesto que $\alpha\delta - \beta\gamma = k$ es positivo) F' se transformará en F i.e. implicará la forma F propiamente. *Q. E. D.*

Por lo tanto si F' está compuesta por las formas f y f' (de la misma manera que F), las formas F y F' tendrán el mismo determinante y serán propiamente equivalentes. De manera más general, si la forma G está compuesta por las formas g y g' de la misma manera que F está compuesta por las formas f y f' respectivamente y las formas g y g' son propiamente equivalentes a f y f': entonces las formas F y G son propiamente equivalentes.

Puesto que este caso, donde ambas formas a componer entran directamente en la composición, es el más sencillo y los otros se pueden reducir fácilmente a él, sólo consideraremos éste en lo que sigue. Entonces si alguna forma se dice estar compuesta por otras dos, se debe interpretar siempre como si estuviera propiamente compuesta de cada una de ellas*). La misma restricción quedará implícita cuando se dice que una forma es transformable en un producto de otras dos.

240.

Teorema. *Si la forma F está compuesta de las formas f y f'; la forma $\mathfrak{F}$ de F y f''; la forma F' de f y f''; la forma $\mathfrak{F}'$ de F' y f': entonces las formas $\mathfrak{F}$ y $\mathfrak{F}'$ serán propiamente equivalentes.*

Demostración. I. Sea

$$\begin{aligned}
f &= ax^2 + 2bxy + cy^2 \\
f' &= a'x'^2 + 2b'x'y' + c'y'^2 \\
f'' &= a''x''^2 + 2b''x''y'' + c''y''^2 \\
F &= AX^2 + 2BXY + CY^2 \\
F' &= A'X'^2 + 2B'X'Y' + C'Y'^2 \\
\mathfrak{F} &= \mathfrak{A}\mathfrak{X}^2 + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}^2 \\
\mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'^2 + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'^2
\end{aligned}$$

y sean d, d', d'', D, D', $\mathfrak{D}$ y $\mathfrak{D}'$ los determinantes de las siete formas respectivamente. Todos tendrán los mismos signos y diferirán por factores cuadrados. Además, sea m el

*) Tal como en una composición de razones (la cual es muy similar a la composición de formas) normalmente entendemos que las razones son tomadas directamente a menos que se indique lo contrario.

máximo común divisor de los números a, $2b$, c y sean m', m'' y M con el mismo sentido respecto a las formas f', f'' y F. Entonces a partir de la cuarta conclusión del artículo 235, D será el máximo común divisor de los números dm'^2, $d'm^2$; Dm''^2 el máximo común divisor de los números $dm'^2m''^2$, $dm^2m''^2$; $M = mm'$; $\mathfrak{D}$ el máximo común divisor de los números Dm''^2, $d''M^2$ o de los números Dm''^2, $d''m^2m'^2$. Concluimos que $\mathfrak{D}$ es el máximo común divisor de los tres números $dm'^2m''^2$, $d'm^2m''^2$, $d''m^2m'^2$. Por razones similares $\mathfrak{D}'$ será el máximo común divisor de los mismos tres números. Entonces, puesto que $\mathfrak{D}$ y $\mathfrak{D}'$ tienen el mismo signo, $\mathfrak{D} = \mathfrak{D}'$ y las formas $\mathfrak{F}$ y $\mathfrak{F}'$ tendrán el mismo determinante.

II. Ahora, sea F que se transforma en ff' mediante la sustitución

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

y $\mathfrak{F}$ en Ff' mediante la sustitución

$$\mathfrak{X} = \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy''$$
$$\mathfrak{Y} = \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy''$$

y designemos las raíces positivas de $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\mathfrak{D}}$, $\frac{d''}{\mathfrak{D}}$ por n, n', $\mathfrak{N}$, $\mathfrak{n}''$. Entonces, según el artículo 235 habrá 18 ecuaciones, la mitad de las cuales pertenecen a la transformación de la forma F en ff' y la otra mitad a la transformación de la forma $\mathfrak{F}$ en Ff''. La primera de ellas será $pq' - qp' = an'$. Las demás se podrán generar de la misma manera, pero para abreviar, las omitiremos aquí. Note que las cantidades n, n', $\mathfrak{N}$, $\mathfrak{n}''$ serán racionales pero no necesariamente enteros.

III. Si los valores de X e Y se sustituyen en los valores de $\mathfrak{X}$ e $\mathfrak{Y}$ obtenemos un resultado de la forma:

$$\begin{aligned}\mathfrak{X} = \quad & (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' \\ & + (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y'' \\ \mathfrak{Y} = \quad & (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' \\ & + (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y''\end{aligned}$$

Obviamente, mediante esta sustitución $\mathfrak{F}$ se transformará en el producto $ff'f''$. El coeficiente (1) será $= p\mathfrak{p}+q\mathfrak{p}''$ y el lector podrá desarrollar los quince valores restantes. Designaremos el número $(1)(10) - (2)(9)$ por $(1,2)$, el número $(1)(11) - (3)(9)$ por $(1,3)$ y en general $(g)(8+h) - (h)(8+g)$ por (g,h) donde g y h son enteros diferentes

entre 1 y 16 con h el mayor de ellos*); de esta manera tenemos 28 símbolos en total. Ahora si designamos las raíces cuadradas positivas de $\frac{d}{\mathfrak{D}}$ y $\frac{d'}{\mathfrak{D}}$ por $\mathfrak{n}$ y $\mathfrak{n}'$ (serán $= n\mathfrak{N}$ y $n'\mathfrak{N}$) tendremos las siguientes 28 ecuaciones:

$$
\begin{aligned}
(1,2) &= aa'\mathfrak{n}'' & (3,5) &= a''b'\mathfrak{n} - a''b\mathfrak{n}' \\
(1,3) &= aa''\mathfrak{n}' & (3,6) &= bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(1,4) &= ab'\mathfrak{n}'' + ab''\mathfrak{n}' & (3,7) &= a''c'\mathfrak{n} \\
(1,5) &= a'a''\mathfrak{n} & (3,8) &= bc'\mathfrak{n}'' + b''c'\mathfrak{n} \\
(1,6) &= a'b\mathfrak{n}'' + a'b''\mathfrak{n} & (4,5) &= b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(1,7) &= a''b\mathfrak{n}' + a''b'\mathfrak{n} & (4,6) &= b'c''\mathfrak{n} - bc''\mathfrak{n}' \\
(1,8) &= bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' & (4,7) &= b''c'\mathfrak{n} - bc'\mathfrak{n}'' \\
(2,3) &= ab''\mathfrak{n}' - ab'\mathfrak{n}'' & (4,8) &= c'c''\mathfrak{n} \\
(2,4) &= ac''\mathfrak{n}' & (5,6) &= ca'\mathfrak{n}'' \\
(2,5) &= a'b''\mathfrak{n} - a'b\mathfrak{n}'' & (5,7) &= ca''\mathfrak{n}' \\
(2,6) &= a'c''\mathfrak{n} & (5,8) &= b'c\mathfrak{n}'' + b''c\mathfrak{n}' \\
(2,7) &= bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' & (6,7) &= b''c\mathfrak{n}' - b'c\mathfrak{n}'' \\
(2,8) &= bc''\mathfrak{n}' + b'c''\mathfrak{n} & (6,8) &= cc''\mathfrak{n}' \\
(3,4) &= ac'\mathfrak{n}'' & (7,8) &= cc'\mathfrak{n}''
\end{aligned}
$$

Designaremos estas ecuaciones por Φ, y tendremos otras nueve:

$$
\begin{aligned}
(10)(11) - (9)(12) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(12) - (2)(11) - (3)(10) + (4)(9) &= 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(2)(3) - (1)(4) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
-(9)(16) + (10)(15) + (11)(14) - (12)(13) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
\left.\begin{aligned}(1)(16) - (2)(15) - (3)(14) + (4)(13) \\ + (5)(12) - (6)(11) - (7)(10) + (8)(9)\end{aligned}\right\} &= 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
-(1)(8) + (2)(7) + (3)(6) - (4)(5) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
(14)(15) - (13)(16) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(5)(16) - (6)(15) - (7)(14) + (8)(13) &= 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(6)(7) - (5)(8) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}
\end{aligned}
$$

*) El significado actual de estos símbolos no debe confundirse con su significado en el artículo 234 pues los números que se expresan mediante estos signos *aquí* corresponden más bien a los del artículo 234 que son multiplicados por números denotados por símbolos similares.

a las que designaremos por Ψ*).

IV. Tomaría demasiado tiempo deducir todas las 37 ecuaciones, nos conformaremos con establecer algunas de ellas como un modelo para las demás.

1) Tenemos

$$\begin{aligned}(1,2) &= (1)(10) - (2)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')p^2 + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' + \mathfrak{q}'\mathfrak{p}'')pq + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')q^2\\ &= \mathfrak{n}''(Ap^2 + 2Bpq + Cq^2) = \mathfrak{n}''aa'\end{aligned}$$

que es la primera ecuación.

2) Tenemos

$$(1,3) = (1)(11) - (3)(9) = (\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'')(pq' - qp') = a''\mathfrak{N}an' = aa''\mathfrak{n}'$$

la segunda ecuación

3) Y tenemos

$$\begin{aligned}(1,8) &= (1)(16) - (8)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp''' + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''')pq''' - (\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'')qp''' + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq'''\\ &= \mathfrak{n}''(App''' + B(pq''' + qp''') + Cqq''') + b''\mathfrak{N}(pq''' - qp''')\\ &= \mathfrak{n}''(bb' + \sqrt{dd'}) + b''\mathfrak{N}(b'n + bn') \quad \dagger)\\ &= \mathfrak{n}''bb' + \mathfrak{n}'bb'' + \mathfrak{n}b'b'' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'',\end{aligned}$$

la octava ecuación en Φ. Dejamos al lector la comprobación de las restantes ecuaciones.

V. Mediante las ecuaciones Φ, mostraremos que los 28 números $(1,2)$, $(1,3)$ etc. no tienen ningún divisor común. Primero observamos que se puede hacer 27 productos de tres factores tales que el primero es $\mathfrak{n}$, el segundo es uno de los números a', $2b'$, c' y el tercero es uno de los números a'', $2b''$, c''; o que el primero es $\mathfrak{n}'$, el segundo es uno de los números a, $2b$, c y el tercero uno de los números a'', $2b''$, c''; o finalmente que el primero es $\mathfrak{n}''$, el segundo uno de los números a, $2b$,

*) Observe que podríamos deducir otras 18 ecuaciones similares a Ψ reemplazando los factores a, $2b$, c por a', $2b'$, c'; a'', $2b''$, c''; pero puesto que no son necesarias para nuestros propósitos, las omitiremos.

†) Esto sigue de la ecuación 10 del artículo 235 ff. La cantidad $\sqrt{dd'}$ se hace $= Dnn' = \mathfrak{D}nn'\mathfrak{N}^2 = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

c y el tercero uno de los números a', $2b'$, c'. Cada uno de estos 27 productos, debido a las ecuaciones Φ, será igual a uno de los 28 números $(1,2)$, $(1,3)$ etc. o la suma o diferencia de algunos de ellos (ej. $\mathfrak{n}a'a'' = (1,5)$, $2\mathfrak{n}a'b'' = (1,6)+(2,5)$, $4\mathfrak{n}b'b'' = (1,8)+(2,7)+(3,6)+(4,5)$ etc.). Por lo tanto si estos números tuvieran un divisor común, necesariamente dividiría todos estos productos. Entonces mediante el artículo 40 y el método utilizado tantas veces anteriormente, el mismo divisor también debe dividir los números $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$ y el cuadrado de este divisor debe también dividir a los cuadrados de estos números, es decir, $\frac{dm'^2m''^2}{\mathfrak{D}}$, $\frac{d'm^2m''^2}{\mathfrak{D}}$, $\frac{d'''m^2m'^2}{\mathfrak{D}}$, *Q. E. A.* , pues según I el máximo común divisor de los tres numeradores es $\mathfrak{D}$ y así estos tres cuadrados no pueden tener un divisor común.

VI. Todo esto se refiere a la transformación de la forma $\mathfrak{F}$ en $ff'f''$; y se puede deducir de la transformación de la forma F en ff' y de la forma $\mathfrak{F}$ en Ff''. De manera completamente similar se deriva la transformación de la forma $\mathfrak{F}'$ en $ff'f''$ a partir de transformaciones de la forma F' en ff'' y de la forma $\mathfrak{F}'$ en $F'f'$:

$$\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \text{ etc.}$$
$$\mathfrak{Y}' = (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \text{ etc.}$$

(aquí los coeficientes son designados de la misma manera que en la transformación de la forma $\mathfrak{F}$ en $ff'f''$, pero se les ha puesto primos para distinguirlos). A partir de estas transformaciones deducimos, igual que antes, 28 ecuaciones análogas a las ecuaciones Φ que llamaremos Φ' y otras nueve análogas a las ecuaciones Ψ que llamaremos Ψ'. Así pues si denotamos

$$(1)'(10)' - (2)'(9)' \quad \text{por} \quad (1,2)', \qquad (1)'(11)' - (3)'(9)' \quad \text{por} \quad (1,3)', \text{ etc.}$$

las ecuaciones Φ' serán

$$(1,2)' = aa'\mathfrak{n}'', \qquad (1,3)' = aa''\mathfrak{n}', \text{ etc.}$$

y las ecuaciones Ψ' serán

$$(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}' \text{ etc.}$$

(Para abreviar dejamos un estudio más detallado de esto al lector; el experto no necesitará realizar nuevos cálculos puesto que hay una analogía entre éste y el primer análisis). Ahora, a partir de Φ y Φ' se sigue inmediatamente que

$$(1,2) = (1,2)', \quad (1,3) = (1,3)', \quad (1,4) = (1,4)', \quad (2,3) = (2,3)', \text{ etc.}$$

Y puesto que todos los $(1,2)$, $(1,3)$, $(2,3)$, etc. no poseen un divisor común (según V), con la ayuda del lema del artículo 234 podemos determinar cuatro enteros α, β, γ, δ tales que

$$\begin{array}{lll} \alpha(1)' + \beta(9)' = (1), & \alpha(2)' + \beta(10)' = (2), & \alpha(3)' + \beta(11)' = (3) \text{ etc.} \\ \gamma(1)' + \delta(9)' = (9), & \gamma(2)' + \delta(10)' = (10), & \gamma(3)' + \delta(11)' = (11) \text{ etc.} \end{array}$$

y $\alpha\delta - \beta\gamma = 1$.

VII. Ahora, si sustituimos de las tres primeras ecuaciones de Ψ, valores para $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$, y de las tres primeras ecuaciones de Ψ' los valores de $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$ se confirma fácilmente que:

$$\begin{aligned} a(\mathfrak{A}\alpha^2 + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma^2) &= a\mathfrak{A}' \\ a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}' \\ a(\mathfrak{A}\beta^2 + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta^2) &= a\mathfrak{C}' \end{aligned}$$

y a menos que $a = 0$ se sigue que la forma $\mathfrak{F}$ se transforma en la forma $\mathfrak{F}'$ mediante la sustitución propia α, β, γ, δ. Si en lugar de las primeras tres ecuaciones de Ψ y Ψ' utilizamos las tres siguientes, obtendremos tres ecuaciones como las anteriores excepto que ahora los factores a serían reemplazados con b; y la misma conclusión es válida siempre y cuando no sea $b = 0$. Finalmente si utilizamos las últimas tres ecuaciones en Ψ y Ψ' las conclusiones son las mismas a menos que $c = 0$. Y puesto que ciertamente no todos los factores a, b, c pueden ser $= 0$ simultáneamente, la forma $\mathfrak{F}$ necesariamente se transformará en la forma $\mathfrak{F}'$ mediante la sustitución α, β, γ, δ y las formas serán propiamente equivalentes. *Q. E. D.*

241.

Si tenemos una forma como $\mathfrak{F}$ o $\mathfrak{F}'$ que resulta de la composición de una de tres formas dadas con otra la cual es la composición de las dos formas restantes, diremos que está *compuesta por estas tres formas*. Queda claro del artículo anterior que no importa el orden en el cual se componen las tres formas. Similarmente, si tenemos cualquier número de formas f, f', f'', f''', etc. (y los cocientes de sus determinantes son cuadrados) y se compone la forma f con f', la forma resultante con f'' y la resultante con f''', etc.: diremos que la última forma que se obtiene de esta operación está compuesta por *todas las formas* f, f', f'', f''', etc. Y es fácil mostrar aquí

también que el orden de composición es arbitrario; i.e. no importa en qué orden se componen estas formas, las formas resultantes serán propiamente equivalentes. Es claro también que si las formas g, g', g'', etc. son propiamente equivalentes a las formas f, f', f'', etc. respectivamente, la forma compuesta de las primeras será propiamente equivalente a la forma compuesta de las últimas.

242.

Las proposiciones anteriores se refieren a la composición de formas en toda su universalidad. Ahora pasaremos a aplicaciones más particulares que no estudiamos anteriormente para no interrumpir el orden del desarrollo. Primero retomaremos el problema del artículo 236 limitándolo según las siguientes condiciones: *primero* las formas a componer deben tener el mismo determinante, i.e. $d = d'$; *segundo*, m y m' deben ser primos relativos; *tercero*, la forma que buscamos debe ser compuesta directamente por f y f'. Entonces m^2 y m'^2 también serán primos relativos; y así el máximo común divisor de los números dm'^2 y $d'm^2$ i.e. D será $= d = d'$ y $n = n' = 1$. Puesto que podemos escogerlos libremente, haremos que las cuatro cantidades $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}''' = -1$, 0, 0, 0 respectivamente. Esto está permitido excepto cuando a, a', $b + b'$ son todos $= 0$ simultáneamente, así que omitiremos este caso. Claramente esto no puede ocurrir excepto en formas con un determinante cuadrado positivo. Ahora, si μ es el máximo común divisor de los números a, a', $b + b'$, los números $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ pueden escogerse tales que

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$$

En cuanto a $\mathfrak{P}$, éste puede escogerse arbitrariamente. Como resultado, si sustituimos p, q, p', q' etc. por sus valores, tenemos:

$$A = \frac{aa'}{\mu^2}, \qquad B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

y C puede determinarse de la ecuación $AC = B^2 - D$ siempre y cuando a y a' no sean simultáneamente $= 0$.

Ahora, en esta solución el valor de A es independiente de los valores de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (los cuales se pueden determinar de una infinidad de maneras); pero B tendrá valores diferentes al asignar valores variados a estos números. Entonces vale

la pena investigar cómo están interconectados todos estos valores de B. Para esto observamos

I. No importa cómo se determinan $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, todos los valores de B son congruentes según el módulo A. Supongamos que si

$$\mathfrak{P} = \mathfrak{p}, \quad \mathfrak{P}' = \mathfrak{p}', \quad \mathfrak{P}'' = \mathfrak{p}'', \quad \mathfrak{P}''' = \mathfrak{p}''' \quad \text{tenemos} \quad B = \mathfrak{B}$$

pero haciendo

$$\mathfrak{P} = \mathfrak{p} + \mathfrak{d}, \quad \mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}', \quad \mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}'', \quad \mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}''' \quad \text{tenemos} \quad B = \mathfrak{B} + \mathfrak{D}$$

Entonces tendremos

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0, \qquad aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \mu\mathfrak{D}$$

Multiplicando el primer miembro de la segunda ecuación por $a\mathfrak{p}' + a'\mathfrak{p}'' + (b+b')\mathfrak{p}'''$, el segundo miembro por μ, y restando del primer producto la cantidad

$$(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (bb' + D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''')$$

lo cual según la primera ecuación anterior es claramente $= 0$, se encontrará, después de cancelar los términos nulos que

$$aa'\{\mu\mathfrak{d} + ((b'-b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' - ((b-b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' - (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}'''\} = \mu^2\mathfrak{D}$$

De donde es claro que $\mu^2\mathfrak{D}$ será divisible por aa' y $\mathfrak{D}$ por $\frac{aa'}{\mu^2}$ i.e. por A y

$$\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D} \pmod{A}$$

II. Si los valores $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$ de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ hacen $B = \mathfrak{B}$, entonces se pueden encontrar otros valores de estos números que harán que B sea igual a cualquier número dado que sea congruente a $\mathfrak{B}$ según el módulo A, a saber $\mathfrak{B} + kA$. Primero observamos que los cuatro números μ, c, c', $b-b'$ no pueden tener un divisor común; pues si lo hubiera, sería un divisor de los seis números a, a', $b+b'$, c, c', $b-b'$ y luego de a, $2b$, c y a', $2b'$, c' y por lo tanto también de m y m' que son por hipótesis primos relativos. Así pues, se pueden encontrar cuatro enteros h, h', h'' y h''' tales que

$$h\mu + h'c + h''c' + h'''(b-b') = 1$$

Y si ponemos

$$\begin{aligned} kh &= \mathfrak{d}, & k(h''(b+b') - h'''a') &= \mu\mathfrak{d}' \\ k(h'(b+b') + h'''a) &= \mu\mathfrak{d}'', & -k(h'a' + h''a) &= \mu\mathfrak{d}''' \end{aligned}$$

es claro que $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$ y $\mathfrak{d}'''$ son enteros y

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0$$
$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb'+D)\mathfrak{d}''' = \frac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b-b')h''') = \mu kA$$

A partir de la primera ecuación es claro que $\mathfrak{p}+\mathfrak{d}$, $\mathfrak{p}'+\mathfrak{d}'$, $\mathfrak{p}''+\mathfrak{d}''$ y $\mathfrak{p}'''+\mathfrak{d}'''$ son también valores de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$; y de la última, que estos valores nos dan $B = \mathfrak{B} + kA$, *Q. E. D.* En este caso queda claro que B siempre puede escogerse tal que quede entre 0 y $A-1$ inclusive, para A positivo; o entre 0 y $-A-1$ para A negativo.

243.

De las ecuaciones

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b+b') = \mu, \qquad B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb'+D))$$

deducimos

$$B = b + \frac{a}{\mu}(\mathfrak{P}a' + \mathfrak{P}'(b'-b) - \mathfrak{P}'''c) = b' + \frac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b-b') - \mathfrak{P}'''c')$$

y por lo tanto

$$B \equiv b \pmod{\frac{a}{\mu}} \quad \text{y} \quad B \equiv b' \pmod{\frac{a'}{\mu}}$$

Ahora, cuando $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ son primos relativos, existirá entre 0 y $A-1$ (o entre 0 y $-A-1$ cuando A es negativo) sólo un número que será $\equiv b \pmod{\frac{a}{\mu}}$ y $\equiv b' \pmod{\frac{a'}{\mu}}$. Si dejamos que sea $= B$ y $\frac{B^2-D}{A} = C$ es claro que (A, B, C) estará compuesta de las formas (a, b, c) y (a', b', c'). Entonces en este caso no es necesario considerar los

números $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ para encontrar la forma compuesta*). Así pues, si se busca la forma compuesta por las formas $(10, 3, 11)$ y $(15, 2, 7)$ tendremos a, a', $b + b' = 10$, 15, 5 respectivamente; $\mu = 5$; tal que $A = 6; B \equiv 3 \pmod 2$ y $\equiv 2 \pmod 3$. Por lo tanto $B = 5$ y $(6, 5, 21)$ es la forma buscada. Pero la condición de que $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ sean primos relativos es equivalente a pedir que los dos números a y a' no tengan divisor común mayor que los tres números a, a', $b + b'$ o lo que es lo mismo, que el máximo común divisor de a y a' también sea divisor del número $b + b'$. Se notan los siguientes casos particulares.

1) Suponga que tenemos dos formas (a, b, c) y (a', b', c') con el mismo determinante D y relacionadas tales que el máximo común divisor de los números a, $2b$, c es primo relativo al máximo común divisor de a', $2b'$, c' y que a y a' son primos relativos: entonces la forma (A, B, C), que es la composición de estas dos, se encuentra haciendo $A = aa'$, $B \equiv b \pmod a$ y $\equiv b' \pmod{a'}$, $C = \frac{B^2 - D}{A}$. Este caso siempre ocurrirá cuando una de las dos formas a ser compuestas es la forma principal; esto es $a = 1$, $b = 0$, $c = -D$. Luego $A = a'$, B se puede tomar $= b'$ y tendremos $C = c'$; así pues *cualquier forma está compuesta de sí misma y de la forma principal del mismo determinante.*

2) Si queremos componer dos formas *opuestas* propiamente primitivas, esto es (a, b, c) y $(a, -b, c)$, tendremos $\mu = a$. Es fácil ver que la forma principal $(1, 0, -D)$ está compuesta por estas dos.

3) Suponga que tenemos un número arbitrario de formas propiamente primitivas (a, b, c), (a', b', c'), (a'', b'', c''), etc. con el mismo determinante y con los primeros términos a, a', a'', etc. primos relativos entre sí. Entonces se puede encontrar la forma (A, B, C) compuesta por todas ellas fijando A igual al producto de todos los a, a', a'', etc.; tomando B congruente a b, b', b'', etc. respecto a los módulos a, a', a'', etc. respectivamente; y haciendo $C = \frac{B^2 - D}{A}$. Obviamente la forma $(aa', B, \frac{B^2 - D}{aa'})$ estará compuesta por las dos formas (a, b, c) y (a', b', c'); la forma $(aa'a'', B, \frac{B^2 - D}{aa'a''})$ estará compuesta por las formas $(aa', B, \frac{B^2 - D}{aa'})$ y (a'', b'', c'') etc. En cambio

4) Suponga que tenemos una forma (A, B, C) propiamente primitiva de determinante D. Si se resuelve el término A en un número cualquiera de factores

*) Podemos lograrlo siempre utilizando las congruencias

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b + b')B}{\mu} \equiv \frac{(bb' + D)}{\mu} \pmod A.$$

primos relativos a, a', a'', etc.; si se toman los números b, b', b'', etc. todos iguales a B o por lo menos congruentes a B según los módulos a, a', a'', etc. respectivamente; y si c, c', c'', etc. son tales que $ac = b^2 - D$, $a'c' = b'^2 - D$, $a''c'' = b''^2 - D$, etc.: entonces la forma (A, B, C) estará compuesta por las formas (a, b, c), (a', b', c'), (a'', b'', c''), etc., o diremos que *se puede descomponer en estas formas*. Es fácil demostrar que esta proposición es también válida cuando la forma (A, B, C) es impropiamente primitiva u obtenida a partir de una forma de tal tipo. Así, de esta manera, cualquier forma puede resolverse en otras con el mismo determinante, en las cuales los primeros términos son números primos o potencias de números primos. Tal descomposición en muchos casos puede ser muy útil si queremos componer una forma a partir de varias formas dadas. Así pues, por ejemplo, si queremos una forma compuesta de las formas $(3, 1, 134)$, $(10, 3, 41)$ y $(15, 2, 27)$, descomponemos la segunda en $(2, 1, 201)$ y $(5, -2, 81)$, la tercera en $(3, -1, 134)$ y $(5, 2, 81)$. Es claro que la forma compuesta por las cinco formas $(3, 1, 134)$, $(2, 1, 201)$, $(5, -2, 81)$, $(3, -1, 134)$ y $(5, 2, 81)$ independientemente del orden en el cual se toman, también será una composición de las tres formas originales. Ahora, la composición de la primera con la cuarta da la forma principal $(1, 0, 401)$; y lo mismo resulta de la composición de la tercera con la quinta; así de la composición de las cinco obtenemos la forma $(2, 1, 201)$.

5) Debido a su utilidad es conveniente describir más detalladamente este método. De la observación anterior es claro que siempre y cuando las formas dadas son propiamente primitivas con el mismo determinante, el problema se puede reducir a la composición de formas cuyos términos iniciales son potencias de números primos (puesto que un número primo se puede considerar como su propia primera potencia). Por esta razón es apropiado considerar el caso especial en el cual se componen dos formas propiamente primitivas (a, b, c) y (a', b', c') siendo a y a' potencias del *mismo* número primo. Por lo tanto, sean $a = h^\chi$, $a' = h^\lambda$, donde h es un número primo y vamos a suponer que χ no es menor que λ (lo cual es legítimo). Ahora h^λ será el máximo común divisor de los números a, a'. Si además es divisor de $b + b'$ tendremos el caso que consideramos al inicio del artículo y la forma (A, B, C) será la forma compuesta si $A = h^{\chi-\lambda}$, $B \equiv b \pmod{h^{\chi-\lambda}}$ y $\equiv b' \pmod{1}$. Esta última condición obviamente puede omitirse. Finalmente $C = \frac{B^2 - D}{A}$. Si h^λ no divide a $b + b'$, el máximo común divisor de estos números será necesariamente una potencia de h, digamos h^ν con $\nu < \lambda$ (donde $\nu = 0$ si h^λ y $b + b'$ son primos entre sí). Si $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ se determinan de modo que

$$\mathfrak{P}' h^\chi + \mathfrak{P}'' h^\lambda + \mathfrak{P}'''(b + b') = h^\nu$$

con $\mathfrak{P}$ arbitrario, la forma (A, B, C) será compuesta de las formas dadas si se escoge

$$A = h^{\chi+\lambda-2\nu}, \qquad B = b + h^{\chi-\nu}(\mathfrak{P}h^{\lambda} - \mathfrak{P}'(b-b') - \mathfrak{P}'''c), \qquad C = \frac{B^2 - D}{A}$$

Pero es fácil ver que en este caso también $\mathfrak{P}'$ puede escogerse arbitrariamente; entonces poniendo $\mathfrak{P} = \mathfrak{P}' = 0$ resulta

$$B = b - \mathfrak{P}'''ch^{\chi-\nu}$$

o más generalmente

$$B = kA + b - \mathfrak{P}'''ch^{\chi-\nu}$$

donde k es un número arbitrario (artículo anterior). Sólo $\mathfrak{P}'''$ entra en esta fórmula muy sencilla, y es el valor de la expresión $\frac{h^{\nu}}{b+b'} \pmod{h^{\lambda}}$*). Si, por ejemplo, se busca la forma compuesta de $(16, 3, 19)$ y $(8, 1, 37)$, resulta $h = 2$, $\chi = 4$, $\lambda = 3$, $\nu = 2$. Por esto $A = 8$ y $\mathfrak{P}'''$ es un valor de la expresión $\frac{4}{4} \pmod 8$, digamos 1, de donde $B = 8k - 73$, y poniendo $k = 9$, $B = -1$ y $C = 37$, la forma buscada es $(8, -1, 37)$.

Entonces, si se proponen varias formas cuyos términos iniciales son todos potencias de números primos, hay que examinar si algunos de estos términos son potencias del *mismo* número primo y, en este caso, las formas se componen de acuerdo con las reglas que acabamos de dar. Así se obtienen formas cuyos primeros términos son potencias de números primos diferentes. La forma compuesta de éstas puede encontrarse por la tercera observación. Por ejemplo, cuando se proponen las formas $(3, 1, 47)$, $(4, 0, 35)$, $(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$ y $(16, 6, 11)$, de la primera y la quinta resulta $(27, 7, 7)$; de la segunda y la cuarta $(16, -6, 11)$; y de ésta y la sexta $(1, 0, 140)$, que puede omitirse. Se quedan $(5, 0, 28)$ y $(27, 7, 7)$ que producen $(135, -20, 4)$, que se reemplaza con la forma propiamente equivalente $(4, 0, 35)$. Esta es la forma que resulta de la composición de las seis formas propuestas.

Similarmente pueden desarrollarse más artificios útiles en la práctica, pero nos obligamos a suprimir esta dirección para pasar a asuntos más difíciles.

244.

Si el número a puede ser representado por alguna forma f, el número a' por la forma f', y si la forma F es transformable en ff': no es difícil ver que el producto

*) o sea, de la expresión $\frac{1}{\frac{b+b'}{h^{\nu}}} \pmod{h^{\lambda-\nu}}$, de donde $B \equiv b - \frac{ch^{\chi-\lambda}}{\frac{b+b'}{h^{\nu}}} \equiv \frac{(D+bb')/h^{\nu}}{(b+b')/h^{\nu}} \pmod A$.

aa' será representable por la forma F. Se sigue inmediatamente que cuando los determinantes de estas formas sean negativos, la forma F será positiva si ambas f y f' son positivas o ambas negativas; al contrario F será negativa si una de las formas f y f' es positiva y la otra es negativa. Detengámonos particularmente en el caso que hemos considerado en el artículo previo, donde F está compuesta por f y f' y f, f' y F tienen el mismo determinante D. Además, supongamos que las representaciones de los números a y a' por las formas f y f' se hacen por medio de valores relativamente primos de los incógnitas. Supondremos también que la primera pertenece al valor b de la expresión $\sqrt{D} \pmod{a}$, la última al valor b' de la expresión $\sqrt{D} \pmod{a'}$ y que $b^2 - D = ac$, $b'^2 - D = a'c'$. Luego, por el artículo 168, las formas (a, b, c) y (a', b', c') serán propiamente equivalentes a las formas f y f', de modo que F estará compuesta por esas dos formas. Pero la forma (A, B, C) estará compuesta por las mismas formas si el máximo común divisor de los números a, a', $b + b'$ es μ, y si se fijan $A = \frac{aa'}{\mu^2}$, $B \equiv b, \equiv b'$ según los módulos $\frac{a}{\mu}$, $\frac{a'}{\mu}$ respectivamente, $AC = B^2 - D$; y esta forma será propiamente equivalente a la forma F. Ahora bien, el número aa' está representado por la forma $Ax^2 + 2Bxy + Cy^2$, haciendo $x = \mu$, $y = 0$ cuyo máximo común divisor es μ; de modo que aa' puede ser también representado por la forma F de manera que los valores de las incógnitas tengan a μ como su máximo común divisor (art. 166). Siempre y cuando μ sea 1, aa' puede ser representado por la forma F asignando valores primos entre sí a las incógnitas, y esta representación pertenecerá al valor B de la expresión $\sqrt{D} \pmod{aa'}$, la cual es congruente con b y b' según los módulos a y a' respectivamente. La condición $\mu = 1$ siempre tiene lugar cuando a y a' son primos entre sí; o más generalmente cuando el máximo común divisor de a y a' es primo a $b + b'$.

Composición de órdenes.

245.

TEOREMA. *Si la forma f pertenece al mismo orden que g, y f' es del mismo orden que g', entonces la forma F compuesta por f y f' tendrá el mismo determinante y será del mismo orden que la forma G compuesta por g y g'.*

Demostración. Sean las formas f, f' y F que son $= (a, b, c)$, (a', b', c') y (A, B, C), respectivamente, y sean sus determinantes $= d$, d' y D. Seguidamente sea m el máximo común divisor de los números a, $2b$ y c y sea $\mathfrak{m}$ el máximo común divisor de los números a, b y c; y que m', $\mathfrak{m}'$ con respecto a la forma f' y M, $\mathfrak{M}$ con respecto a la forma F tengan similares significados. Entonces el orden de la forma

f será determinado por los números d, m y $\mathfrak{m}$, de donde estos números también serán válidos para la forma g; por la misma razón los números d', m' y $\mathfrak{m}'$ jugarán el mismo rol para la forma g' como para la forma f'. Ahora bien, por el artículo 235, los números D, M y $\mathfrak{M}$ están determinados por d, d', m, m', $\mathfrak{m}$ y $\mathfrak{m}'$; esto es, D será el máximo común divisor de $dm'^2, d'm^2$; $M = mm'$; $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (si $m = \mathfrak{m}$ y $m' = \mathfrak{m}'$) ó $= 2\mathfrak{m}\mathfrak{m}'$ (si $m = 2\mathfrak{m}$ ó $m' = 2\mathfrak{m}'$). Dado que estas propiedades de D, M y $\mathfrak{M}$ se siguen del hecho de que F está compuesta por f y f', es fácil ver que D, M y $\mathfrak{M}$ juegan la misma función para la forma G, así que G es del mismo orden que F. *Q. E. D.*

Por esta razón diremos que el orden de la forma F está compuesto de los órdenes de las formas f y f'. De este modo, p.ej., si tenemos dos órdenes propiamente primitivos, su composición será propiamente primitiva; si uno es propiamente primitivo y el otro impropiamente primitivo, la composición será impropiamente primitiva. Se debe entender de una manera similar si se dice que un orden está compuesto de varios otros órdenes.

Composición de géneros.

246.

PROBLEMA. *Propuestas dos formas primitivas cualesquiera f y f' y la forma F compuesta de estas dos: determinar el género al cual pertenece F a partir de los géneros a los cuales pertenecen f y f'.*

Solución. I. Consideremos primero el caso donde al menos una de las formas f o f' (p.ej. la primera) es propiamente primitiva, y designemos los determinantes de las formas f, f' y F por d, d' y D. D será el máximo común divisor de los números dm'^2 y d', donde m' es 1 ó 2 según la forma f' sea propia o impropiamente primitiva. En el primer caso F pertenecerá a un orden propiamente primitivo, en el segundo a un orden impropiamente primitivo. Ahora bien, el género de la forma F estará definido por sus caracteres particulares, esto es con respecto a los divisores impares primos individuales de D y también para algunos casos con respecto a los números 4 y 8. Será conveniente considerar estos casos separadamente.

1. Si p es un divisor impar primo de D, necesariamente dividirá a d y a d', y así también entre los caracteres de las formas f y f' se encuentran las relaciones de F con p. Ahora bien, si el número a puede ser representado por f, y el número a' por f', el producto aa' puede ser representado por F. Así que si los residuos cuadráticos de p (no divisibles por p) pueden ser representados tanto por f como por f', ellos

pueden ser también representados por F; i.e. si ambos f y f' tienen el carácter Rp, la forma F tendrá el mismo carácter. Por una razón similar F tendrá el carácter Rp si ambos f y f' tienen el carácter Np; contrariamente F tendrá al carácter Np si una de las formas f o f' tiene el carácter Rp y la otra tiene el carácter Np.

2. Si una relación con el número 4 entra dentro del carácter total de la forma F, tal relación también debe entrar dentro de los caracteres de las formas f y f'. En efecto, esto sólo puede pasar cuando D es $\equiv 0$ ó $\equiv 3 \pmod 4$. Cuando D es divisible por 4, dm'^2 y d' son también divisibles por 4, y es inmediatamente claro que f' no puede ser impropiamante primitiva y así $m' = 1$. Luego tanto d como d' son divisibles por 4 y una relación con 4 entrará dentro del carácter de cada cual. Cuando $D \equiv 3 \pmod 4$, D dividirá a d y a d', los cocientes serán cuadrados y así d y d' serán necesariamente $\equiv 0$ ó $\equiv 3 \pmod 4$ y una relación con el número 4 estará incluida entre los caracteres de f y f'. De este modo, así como en (1), se seguirá que el carácter de la forma F será 1, 4 si ambos f y f' tienen el carácter 1, 4 ó 3, 4; contrariamente el carácter de la forma F será 3, 4 si una de las formas f o f' tiene el carácter 1, 4 y la otra 3, 4.

3. Cuando D es divisible por 8, d' lo será también; de donde f' seguramente será propiamente primitivo, $m' = 1$ y d también será divisible por 8. Y así uno de los caracteres 1, 8; 3, 8; 5, 8; 7, 8 aparecerá entre los caracteres de la forma F sólo si tal relación con 8 aparece también en el carácter de ambas formas f y f'. De la misma manera como antes, es fácil ver que 1, 8 será un carácter de la forma F si f y f' tienen el mismo carácter con respecto a 8; que 3, 8 será un carácter de la forma F si una de las formas f o f' tiene el carácter 1, 8, la otra 3, 8; ó una de ellas tiene el carácter 5, 8 y la otra 7, 8; F tendrá el carácter 5, 8 si f y f' tienen 1, 8 y 5, 8 ó 3, 8 y 7, 8; y F tendrá el carácter 7, 8 si f y f' tienen ya sea 1, 8 y 7, 8 ó 3, 8 y 5, 8 como caracteres.

4. Cuando $D \equiv 2 \pmod 8$, d' será $\equiv 0$ ó $\equiv 2 \pmod 8$, así que $m' = 1$ y d será también $\equiv 0$ ó $\equiv 2 \pmod 8$; pero dado que D es el *máximo* común divisor de d y d', ellos no pueden ser ambos divisibles por 8. Entonces en este caso el carácter de la forma F sólo puede ser 1 *y* 7, 8 ó 3 *y* 5, 8 cuando ambas formas f y f' tienen uno de estos caracteres y el otro tiene uno de los siguientes: 1, 8; 3, 8; 5, 8; 7, 8. La siguiente tabla determinará el carácter de la forma F. El carácter en el margen pertenece a una de las formas f o f', y el carácter en la cabeza de las columnas pertenece a la otra.

	1 *y* 7, 8 o 1,8 o 7, 8	3 *y* 5, 8 o 3, 8 o 5, 8
1 *y* 7, 8	1 *y* 7, 8	3 *y* 5, 8
3 *y* 5, 8	3 *y* 5, 8	1 *y* 7, 8

5. De la misma manera, puede ser probado que F no puede tener el carácter 1 *y* 3, 8 ó 5 *y* 7, 8 a no ser que al menos una de las formas f o f' tenga a uno de estos caracteres. La otra puede tener uno de ellos también o uno de éstos: 1, 8; 3, 8; 5, 8; 7, 8. El carácter de la forma F está determinado por la siguiente tabla. Los caracteres de las formas f y f' de nuevo aparecen en el margen y en la cabeza de las columnas.

	1 *y* 3, 8 o 1,8 o 3, 8	5 *y* 7, 8 o 5, 8 o 7, 8
1 *y* 3, 8	1 *y* 3, 8	5 *y* 7, 8
5 *y* 7, 8	5 *y* 7, 8	1 *y* 3, 8

II. Si cada una de las formas f y f' es impropiamente primitiva, D será el máximo común divisor de los números $4d$, $4d'$ o sea $\frac{1}{4}D$ el máximo común divisor de los números d, d'. Se sigue que d, d' y $\frac{1}{4}D$ serán todos $\equiv 1 \pmod 4$. Poniendo $F = (A, B, C)$, el máximo común divisor de los números A, B, C será $= 2$, y el máximo común divisor de los números A, $2B$, C será 4. Luego F será una forma derivada de la forma impropiamente primitiva $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, cuyo determinante será $\frac{1}{4}D$, y su género determinará el género de la forma F. Pero, dado que es impropiamente primitiva, su carácter no implicará relaciones con 4 u 8, sino sólo con los divisores impares primos individuales de $\frac{1}{4}D$. Ahora todos estos divisores manifiestamente dividen también a d y a d', y si los dos factores de un producto son representables uno por f, el otro por f', entonces la mitad del producto es representable por la forma $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$. Se sigue que el carácter de esta forma con respecto a cualquier número impar primo p que divida a $\frac{1}{4}D$ será Rp cuando $2Rp$ y las formas f, f' tengan el mismo carácter con respecto a p y cuando $2Np$ y los caracteres de f y f' con respecto a p son opuestos. Contrariamente el carácter de la forma será Np cuando f y f' tengan iguales caracteres con respecto a p y $2Np$, y cuando f y f' tengan caracteres opuestos y se tiene $2Rp$.