ALGUNAS APLICACIONES A LA TEORIA DE LAS FORMAS BINARIAS.

Encontrar una forma cuya duplicación produce una forma dada del género principal.

Puesto que los elementos básicos de la teoría de formas ternarias se han desarrollado de manera concisa, procederemos a algunas aplicaciones especiales. Entre ellas, el siguiente problema merece el primer lugar.

286.

PROBLEMA. *Dada una forma binaria $F = (A,\ B,\ C)$ de determinante D que pertenece al género principal: encontrar una forma binaria f cuya duplicación nos da F.*

Solución. I. Sea F' la opuesta de la forma F. Se busca una representación propia de $F' = AT^2 - 2BTU + CU^2$ por la forma ternaria $x^2 - 2yz$. Suponga que es

$$x = \alpha T + \beta U, \qquad y = \alpha' T + \beta' U, \qquad z = \alpha'' T + \beta'' U.$$

Es claro que esto se puede realizar a partir de la teoría anterior sobre formas ternarias, ya que, por hipótesis, F pertenece al género principal, así que hay un valor para la expresión $\sqrt{(A,B,C)}$ (mod. D), a partir del cual se puede encontrar una forma ternaria φ de determinante 1 en la cual $(A,-B,C)$ será una parte y todos sus coeficientes serán enteros. Es igualmente obvio que φ será una forma indefinida (pues por hipótesis F ciertamente no es una forma negativa); y por lo tanto será necesariamente equivalente a la forma $x^2 - 2yz$. Por consiguiente, se podrá encontrar una transformación de ésa a φ, la cual da una representación propia de la forma F' por la forma $x^2 - 2yz$. Como resultado

$$A = \alpha^2 - 2\alpha'\alpha'', \qquad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \qquad C = \beta^2 - 2\beta'\beta''$$

además, designando los números $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ por a, b, c respectivamente, éstos no tendrán un divisor común y $D = b^2 - 2ac$.

II. Con la ayuda de la última observación del artículo 235, es fácil concluír que F, mediante la sustitución $2\beta'$, β, β, β''; $2\alpha'$, α, α, α'', se transformará en el producto de la forma $(2a,-b,c)$ con ella misma, y por la sustitución β', β, β, $2\beta''$; α', α, α, $2\alpha''$, en el producto de la forma $(a,-b,2c)$ con ella misma. Ahora el máximo común divisor de los números $2a$, $2b$ y $2c$ es 2; por lo tanto si el número c es

impar, los números $2a$, $2b$ y c no tendrán un divisor común, así $(2a, -b, c)$ será una forma propiamente primitiva; similarmente si a es impar $(a, -b, 2c)$ será una forma propiamente primitiva. En el primer caso F será obtenida a partir de la duplicación de la forma $(2a, -b, c)$ y en segundo caso a partir de una duplicación de la forma $(a, -b, 2c)$ (ver conclusión 4, art. 235). Ciertamente uno de estos casos siempre se cumplirá. En efecto, si ambas a y c fueran pares, b sería necesariamente impar; ahora es fácil confirmar que $\beta''a + \beta b + \beta' c = 0$, $\alpha''a + \alpha b + \alpha' c = 0$ y se sigue que βb y αb serán pares y así también lo serán α y β. De esto seguiría que A y C son pares pero esto contradice a la hipótesis según la cual F es una forma del género principal y así de orden propiamente primitiva. Pero puede ocurrir que a y c sean impares. En este caso inmediatamente habrá dos formas que producirán F mediante su duplicación.

Ejemplo. Propóngase la forma $F = (5, 2, 31)$ con determinante -151. Un valor de la expresión $\sqrt{(5, 2, 31)}$ será $(55, 22)$; por los métodos del artículo 272 encontramos que la forma ternaria $\varphi = \left(\begin{smallmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{smallmatrix}\right)$ es equivalente a la forma $\left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ y ésta se transformará en φ mediante la sustitución $\left\{\begin{matrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{matrix}\right\}$; y con la ayuda de las transformaciones dadas en el artículo 277 encontramos que $\left(\begin{smallmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{smallmatrix}\right)$ es transformada en φ por la sustitución $\left\{\begin{matrix} 3, & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3 \end{matrix}\right\}$. Así pues $a = 11$, $b = -17$, $c = 20$; por lo tanto puesto que a es impar, F se obtendrá de la duplicación de la forma $(11, 17, 40)$ y se transformará en el producto de esta forma con ella misma por la sustitución -1, -7, -7, -18; 2, 3, 3, 2.

287.

Agregamos las siguientes observaciones sobre el problema que se resolvió en el artículo anterior.

I. Si la forma F es transformada en un producto de las dos formas (h, i, k) y (h', i', k') por la sustitución p, p', p'', p'''; q, q', q'', q''' (supongamos que cada una se toma propiamente) se tendrán las siguientes ecuaciones que son fácilmente deducidas

de la conclusión 3 del artículo 235:

$$\begin{aligned} p''hn' - p'h'n - p(in' - i'n) &= 0 \\ (p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) &= 0 \\ p'kn' - p''k'n - p'''(in' - i'n) &= 0 \end{aligned}$$

y tres más que se derivan de éstas intercambiando los números p, p', p'', p''' y q, q', q'', q'''; n y n' son las raíces cuadradas positivas que resultan de la división de los determinantes de las formas (h, i, k) y (h', i', k') por el determinante de la forma F. Así, si estas formas son idénticas, eso es, $n = n'$, $h = h'$, $i = i'$, $k = k'$, las ecuaciones serán

$$(p'' - p')hn = 0, \qquad (p'' - p')in = 0, \qquad (p'' - p')kn = 0$$

y *necesariamente* $p' = p''$ y similarmente $q' = q''$. Por lo tanto, asignando a las formas (h, i, k) y (h', i', k') las *mismas* incógnitas t y u y designando las incógnitas de F por T y U, entonces F será transformada por la sustitución

$$T = pt^2 + 2p'tu + p'''u^2, \qquad U = qt^2 + 2q'tu + q'''u^2 \quad \text{en} \quad (ht^2 + 2itu + ku^2)^2$$

II. Si la forma F se obtiene a partir de una duplicación de la forma f, será también obtenida a partir de una duplicación de cualquier otra forma contenida en la misma clase que f; eso es, la clase de la forma F se obtendrá a partir de una duplicación de la clase de la forma f (ver art. 238). Así en el ejemplo del artículo anterior, $(5, 2, 31)$ también se obtendrá de una duplicación de la forma $(11, -5, 16)$ la cual es propiamente equivalente a la forma $(11, 17, 40)$. A partir de una clase que por duplicación produce a la clase de la forma F, se encuentran *todas* (si hay más que una) aquellas clases con la ayuda del problema 260; en nuestro ejemplo no hay ninguna otra clase positiva porque existe sólo una clase ambigua positiva propiamente primitiva de determinante -151 (la clase principal); y puesto que, a partir de la composición de la única clase ambigua negativa $(-1, 0, -151)$ con la clase $(11, -5, 16)$ resulta la clase $(-11, -5, -16)$, ésta será la única clase negativa y de su duplicación resulta la clase $(5, 2, 31)$.

III. Puesto que por la solución del problema del artículo anterior queda claro que cualquier clase propiamente primitiva (positiva) de formas binarias perteneciendo al género principal se puede obtener de la duplicación de alguna clase propiamente primitiva del mismo determinante, podemos ampliar el teorema del artículo 261. Este teorema afirmaba que podríamos estar seguros de que *al menos* la mitad de todos los

caracteres asignables para un determinante no cuadrado D no pueden corresponder a géneros propiamente primitivos (positivos). Ahora podemos decir que *exactamente* la mitad de todos estos caracteres corresponden a tales géneros y ninguno de los de la otra mitad puede corresponder a ellos (ver demostración del teorema). En el artículo 264 distribuimos todos esos caracteres entre dos grupos iguales P y Q. Se probó que ninguno de los de Q puede corresponder a formas propiamente primitivas (positivas). Aún se dudaba de si había géneros que correspondían a cada uno de los caracteres de P. Ahora la duda se ha aclarado y estamos seguros de que entre el conjunto completo de caracteres de P no hay ninguno que no corresponda a un género. Se mostró en el artículo 264, I que para un determinante negativo es imposible para P y *sólo* posible para Q el tener miembros en un orden *negativo* propiamente primitivo. Mostraremos en efecto que *todos* los miembros de Q son posibles. Si K es cualquier carácter en Q, f una forma arbitraria en el orden de formas negativas propiamente primitivas de determinante D, y K' su carácter, entonces K' estará en Q; a partir de esto es fácil ver que el carácter compuesto por K y K' (según la norma del art. 246) pertenece a P y entonces hay formas propiamente primitivas positivas de determinante D que le corresponden. La composición de esta forma con f da raíz a una forma propiamente primitiva negativa de determinante D cuyo carácter será K. De manera similar se prueba que aquellos caracteres en un orden impropiamente primitivo, que según los métodos de los artículos 264 II, III resultan ser los *únicos* posibles, son realmente del *todo* posibles, independientemente de si pertenecen a P o a Q. Creemos que estos teoremas están entre los más bellos de la teoría de las formas binarias, especialmente porque, a pesar de ser sumamente simples, son tan profundos que sus demostraciones rigurosas requieren de muchas otras investigaciones.

La teoría de la descomposición de números y formas binarias en tres cuadrados.

Veamos ahora otra aplicación de la divagación anterior, la descomposición de números y formas binarias en tres cuadrados. Empezamos con lo siguiente.

288.

PROBLEMA. *Dado un número positivo M, encontrar los requisitos que formas binarias primitivas negativas de determinante $-M$ deben satisfacer para que sean residuos cuadráticos de M, eso es, para que tengan* 1 *como un número característico.*

Solución. Designemos por Ω el conjunto de todos los caracteres particulares que dan las relaciones del número 1 tanto a los divisores primos (impares) de M como a los números 8 ó 4 cuando divide a M. Estos caracteres serán Rp, Rp', Rp'', etc., donde p, p', p'', etc. son los divisores primos, y 1, 4 cuando 4 divide a M; 1, 8 cuando 8 divide a M. Además utilizaremos las letras P y Q con el mismo significado que en el artículo anterior y en el artículo 264. Ahora distinguimos los siguientes casos.

I. Cuando M es divisible por 4, Ω será un carácter completo, y es claro por el artículo 233 V que 1 puede ser un número característico solamente de aquellas formas cuyo carácter es Ω. Pero es claro que Ω es el carácter de la forma principal $(1, 0, M)$ y así pertenece a P y no puede resultar de una forma propiamente primitiva negativa; por lo tanto, puesto que no hay formas impropiamente primitivas para este determinante, en este caso no habrá formas primitivas negativas que sean residuos de M.

II. Cuando $M \equiv 3 \pmod 4$ el mismo razonamiento es válido con la excepción de que en este caso existe un orden *impropiamente* primitivo negativo en el cual los caracteres P serán posibles o no según $M \equiv 3$ ó $M \equiv 7 \pmod 8$ (ver art. 264 III). En el primer caso habrá un género para este orden cuyo carácter es Ω, así 1 será el número característico de todas las formas contenida en ella; en el segundo caso no puede haber ninguna forma negativa con esta propiedad.

III. Cuando $M \equiv 1 \pmod 4$, Ω aún no es un carácter completo, pero debemos agregarle una relación con el número 4; es claro sin embargo, que Ω debe pertenecer al carácter de una forma cuyo número característico es 1, y recíprocamente cualquier forma cuyo carácter es ó Ω; 1, 4, ó Ω; 3, 4, tiene 1 como número característico. Ahora Ω; 1, 4 es claramente el carácter del género principal que pertenece a P y por lo tanto es imposible dentro de un orden propiamente primitivo negativo; por la misma razón Ω; 3, 4 pertenecerá a Q (art. 263). Por esto habrá un género correspondiente al orden propiamente primitivo negativo de todas aquellas formas que tendrán 1 como número característico. En este caso, tal como en el siguiente no habrá ningún orden impropiamente primitivo.

IV. Cuando $M \equiv 2 \pmod 4$ debemos agregarle a Ω una relación con 8 para obtener un carácter completo. Estas relaciones serán 1 *y* 3, 8 ó 5 *y* 7, 8 cuando $M \equiv 2 \pmod 8$; y ó 1 *y* 7, 8 ó 3 *y* 5, 8 cuando $M \equiv 6 \pmod 8$. En el primer caso el carácter Ω; 1 *y* 3, 8 evidentemente pertenecerán a P y así Ω; 5 *y* 7, 8 a Q. Como consecuencia de esto, habrá un género propiamente primitivo negativo que le corresponde. Por una razón similar, en el segundo caso habrá un género en el orden

propiamente primitivo negativo, cuya forma tiene la propiedad prescrita; eso es, su carácter es Ω; 3 *y* 5, 8.

A partir de todo eso se sigue que no hay formas primitivas negativas de determinante $-M$ con número característico 1 excepto cuando M es congruente con uno de los números 1, 2, 3, 5 ó 6 según el módulo 8 y ellos pertenecerán a sólo un género, que es impropio cuando $M \equiv 3$; no hay tales formas cuando $M \equiv 0$, 4 ó 7 (mod. 8). Pero si $(-a, -b, -c)$ es una forma primitiva negativa con número característico $+1$, (a, b, c) será una forma primitiva positiva con número característico -1. De esto es claro que en los cinco casos anteriores (cuando $M \equiv 1$, 2, 3, 5, 6) hay un género primitivo positivo cuyas formas tienen número característico -1, y es *impropio* si $M \equiv 3$; sin embargo en el último de los tres casos (cuando $M \equiv 0$, 4, 7) no hay tales formas positivas.

289.

En cuanto a las representaciones propias de las formas binarias por la forma ternaria $x^2 + y^2 + z^2 = f$, podemos obtener lo siguiente a partir de la teoría general del artículo 282.

I. La forma binaria φ no se puede representar propiamente por f a menos que sea una forma positiva primitiva y -1 (i.e., el determinante de la forma f) sea su número característico. Así para un determinante positivo y además para un determinante negativo $-M$, cuando M es divisible por 4 o es de la forma $8n + 7$, no hay formas binarias propiamente representables por f.

II. Ahora si $\varphi = (p, q, r)$ es una forma positiva primitiva de determinante $-M$, y -1 es un número característico de la forma φ y también de la forma opuesta $(p, -q, r)$, habrá una representación propia de la forma φ por f que pertenece a cualquier valor de la expresión $\sqrt{-(p, -q, r)}$. Eso es, todos los coeficientes de la forma ternaria g de determinante -1 (art. 283) necesariamente serán enteros, la forma g será definida y así equivalente a f (art. 285.I).

III. Por el artículo 283.III el número de representaciones que pertenecen al mismo valor de la expresión $\sqrt{-(p, -q, r)}$ en todos los casos, excepto cuando $M = 1$ y $M = 2$, es igual en magnitud al número de transformaciones de la forma f en g, y así, por el artículo 285, $= 48$; así si se conoce una representación que pertenece a un valor dado, los 47 restantes se pueden obtener a partir de ella permutando los valores de x, y, z en todas las maneras posibles y cambiando sus signos; como resultado,

las 48 representaciones presentarán *una sola* descomposición de la forma φ en tres cuadrados, si consideramos los cuadrados en sí y no su orden o el signo de sus raíces.

IV. Sea μ el número de todos los enteros primos impares diferentes que dividen a M; no es difícil concluir del artículo 233 que el número de valores diferentes de la expresión $\sqrt{-(p,-q,r)}$ (mod. M) será $= 2^\mu$, donde, según el artículo 283, necesitamos considerar sólo la mitad de éstos (cuando $M > 2$). Por lo tanto el número de todas las representaciones propias de la forma φ por f será $= 48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$; pero el número de descomposiciones diferentes en tres cuadrados es $= 2^{\mu-1}$.

Ejemplo. Sea $\varphi = 19t^2 + 6tu + 41u^2$, de modo que $M = 770$; aquí se debe considerar (art. 283) los cuatro valores siguientes de la expresión $\sqrt{-(19,-3,41)}$ (mod. 770): $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$. Para encontrar las representaciones que pertenecen a los valores $(39, 237)$, debemos determinar la forma ternaria $\left(\begin{smallmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{smallmatrix}\right) = g$. Mediante los métodos de los artículos 272 y 275, encontramos que f se transformará en esta forma por la sustitución

$$\left\{\begin{matrix} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{matrix}\right\}$$

y la representación de la forma φ por f es:

$$x = t - 6u, \qquad y = -3t - 2u, \qquad z = -3t - u$$

Por razones de brevedad no escribiremos las 47 representaciones restantes que pertenecen a ese mismo valor, las cuales resultan de las permutaciones de estos valores y el cambio de signos. Todas las 48 representaciones producen la misma descomposición de la forma φ en tres cuadrados

$$t^2 - 12tu + 36u^2, \qquad 9t^2 + 12tu + 4u^2, \qquad 9t^2 + 6tu + u^2.$$

De manera similar el valor $(171, -27)$ dará una descomposición en cuadrados $(3t + 5u)^2$, $(3t - 4u)^2$, t^2; el valor $(269, -83)$ dará $(t + 6u)^2 + (3t + u)^2 + (3t - 2u)^2$; y finalmente el valor $(291, -127)$ dará $(t + 3u)^2 + (3t + 4u)^2 + (3t - 4u)^2$; cada una de estas descomposiciones es equivalente a 48 representaciones. Fuera de estas 192 representaciones o cuatro descomposiciones no hay otras, puesto que 770 no es divisible por ningún cuadrado y por lo tanto no puede haber ninguna representación impropia.