FACULTAD DE CIENCIAS

(SECCIÓN DE EXACTAS)

INVESTIGACIÓN

DE LAS

RAÍCES DE UNA SUSTITUCIÓN

TESIS DEL ÚLTIMO EJERCICIO DE DOCTORADO

POR

VICENTE MARTÍ ORTELLS

VALENCIA—1911

TIPOGRAFÍA MODERNA Á CARGO DE MIGUEL GIMENO

Avellanas, 11

Señores:

Después de haber vacilado bastante tiempo en la elección de la teoría que expondríamos en nuestra Tesis de Doctorado, hemos preferido la de Sustituciones, por creer que hay en ella algunos puntos que, aun tratados é indicados por los autores que de dicha teoría se ocupan, no insisten en ellos, sin duda porque, siendo muy elementales, no han creído prudente aumentar la materia de sus obras, con sobrada razón, ya que no tratan exclusivamente de la teoría indicada.

Hemos observado que el problema de la extracción de raíces de las sustituciones no se encuentra resuelto en ninguna de las obras por nosotros consultadas, ni se ocupan de él; si alguno lo nombra no es más que para dar la definición, y sólo el Sr. Echegaray, en sus «Lecciones», resuelve el caso particular de la extracción de la raíz cuadrada de una sustitución circular de tres letras, no con el objeto principal de encontrar dicha raíz, sino para demostrar la dificultad que hay para resolver ecuaciones en esta teoría, presentando el ejemplo, en apariencia sencillo, de la ecuación $X^2 = A$, la cual resuelve por medio de la representación analítica de las sustituciones.

A consecuencia de lo que acabamos de decir nos propusimos estudiar el problema de la extracción de raíces de las sustituciones, y el resultado de nuestra investigación es lo que vamos á exponer en esta Memoria con arreglo al orden siguiente:

En la primera parte definimos lo que se entiende por susti-

tución, exponemos la notación de éstas y justificamos más adelante el convenio de representar por la unidad y llamar sustitución unidad á la sustitución idéntica. Admitido este convenio, se define el producto de una permutación por una sustitución, como se define el producto de dos números; consecuencia del producto de una permutación por una sustitución es el producto de dos sustituciones, y seguimos después con el examen del cociente de dos sustituciones, la potencia y la raíz, si bien de esta última sólo hacemos un ligero estudio, por no tener aún elementos para resolver este problema.

La segunda parte la dedicamos al estudio de las sustituciones circulares por medio de su representación gráfica en la circunferencia, fijándonos especialmente en sus potencias y en las sustituciones regulares y potencias de las mismas.

En la tercera, después de estudiar la extracción de raíces de las sustituciones circulares, se investiga la condición necesaria y suficiente para que una sustitucion regular tenga raíz de cierto grado, de la cual se deduce el medio de extraer la raíz de dicho grado, la condición para que una sustitución cualquiera tenga raíz de grado K y su extracción.

Por último, en una nota final estudiamos el número de raíces iguales y diferentes de forma circular y grado *m* que tiene una sustitución regular de *m* ciclos.

Nos han servido de guía en nuestro trabajo las obras siguientes:

F. Echegaray.—Lecciones sobre resolución de ecuaciones y teoría de Galois.—Madrid 1897.

F. Petersen.—Théorie des equations algèbriques.--París 1897.

F. A. Serret.—Cours d' Algebre superieure. 3.ª edición.—París 1866.

INVESTIGACIÓN

DE LAS

RAICES DE UNA SUSTITUCIÓN

I

DE LAS SUSTITUCIONES EN GENERAL

1. *Definiciones y representación.*—Se llama sustitución á un conjunto de operaciones, mediante las cuales cambiamos algunas ó todas las letras de cierta expresión por otras de las mismas; de modo que si en la expresión $a\,b\,c + b\,c + d\,a + c\,b$ reemplazamos la letra a por la c, la b por la d, la c por b y la d por a, habremos efectuado una sustitución que transforma á la expresión dada en $c\,d\,b + d\,b + a\,c + b\,d$.

Generalmente se representan las sustituciones escribiendo unas á continuación de otras las letras que se cambian, y bajo de cada una de éstas aquella por la cual se reemplaza, encerrándolo todo por medio de unas líneas verticales ó por un paréntesis. La sustitución que antes hemos considerado se representará por $\begin{vmatrix} a\,b\,c\,d \\ c\,d\,b\,a \end{vmatrix}$ ó por $\begin{pmatrix} a\,b\,c\,d \\ c\,d\,b\,a \end{pmatrix}$; de este modo queda representada la sustitución por dos permutaciones: la superior, que es la de partida, y algunos llaman numerador, y la inferior, ó denominador.

También puede colocarse la permutación de partida como denominador y la segunda en el numerador, de modo que se co-

rrespondan las letras que se sustituyen; refiriéndonos á la sustitución anterior, y empleando esta nueva forma para representarla, obtendremos $\begin{vmatrix} c\,d\,b\,a \\ a\,b\,c\,d \end{vmatrix}$; mientras no se advierta lo contrario adoptaremos siempre la primera de estas notaciones.

Tanto en este caso como en otros podemos elegir para representar las permutaciones letras distintas, como hemos hecho hasta aquí, ó iguales con subíndices para distinguirlas y aun representar una de las permutaciones por una letra mayúscula y la otra por la misma letra con un subíndice.

Gráficamente se representan por dos segmentos rectilíneos horizontales divididos en partes iguales, colocando en cada uno de los puntos de división una letra, de modo que verticalmente se correspondan letras iguales, y uniendo por medio de transversales las letras de ambos segmentos que se correspondan en la sustitución. Así una sustitución tal como $\begin{vmatrix} x_1\,x_2\,x_3\,x_4\,x_5 \\ x_4\,x_2\,x_1\,x_5\,x_3 \end{vmatrix}$ se representará gráficamente por la figura primera.

Cuando no es necesario que aparezcan las letras que componen una sustitución para demostrar alguna propiedad de ésta, podemos representarla por una sola letra mayúscula, S, T, V, etc.; si varias sustituciones tienen una ó algunas propiedades comunes, se pueden representar por la misma letra afectada de subíndices.

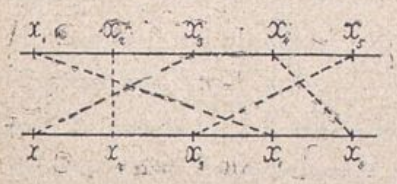

Figura 1.ª

Además de estas formas de representación, hay otras que expondremos á medida que nos hagan falta para el estudio que vamos á emprender.

2. *Propiedades elementales.*—El conjunto de cada dos letras correspondientes de una sustitución se llama *elemento*, así la sustitución $\begin{vmatrix} a\,b\,c \\ b\,a\,c \end{vmatrix}$ tiene tres elementos: el $\begin{vmatrix} a \\ b \end{vmatrix}$, el $\begin{vmatrix} b \\ a \end{vmatrix}$ y el $\begin{vmatrix} c \\ c \end{vmatrix}$.

Al aplicar una sustitución á una permutación, se observa que un elemento cualquiera actúa sobre la letra de la permutación que es igual á su letra superior, cambiándola por la inferior, de

modo que si las dos letras de un elemento fueran iguales, dicho elemento deja invariable la letra de la permutación sobre que actúa; por tanto, en la sustitución dada podremos suprimir este elemento, y la sustitución que así obtengamos será equivalente á la propuesta, ya que produce el mismo efecto sobre la permutación. Las mismas consideraciones haremos para los demás elementos de la sustitución cuyas letras sean iguales; luego *en una sustitución pueden suprimirse todos los elementos que dejen invariable su letra superior, sin que la sustitución deje de ser la misma.*

Inversamente, cuando se quiera que una sustitución tenga mayor número de letras del que tiene, podemos representarla por otra del número deseado, sin más que añadir tantos elementos de letras iguales como hagan falta, cuidando de que en dichos elementos no entren letras iguales á las que ya están en la sustitución dada.

Los elementos de una sustitución gozan de la propiedad de poder trasladarse de lugar sin que cambie la sustitución, porque lo esencial es que á cada letra de ésta corresponda siempre la misma, y esto se consigue dejando constantes los elementos de dicha sustitución, aunque estén colocados en distinto orden.

El número de sustituciones distintas que se pueden formar con n letras es igual á 1. 2. 3.... n = n!. En efecto: si escribimos las *n* letras en un orden cualquiera *a b c.... m* y colocamos bajo de esta permutación cada una de las *n!* permutaciones que pueden formarse con *n* letras, obtendremos *n!* sustituciones distintas; otra sustitución diferente de las *n!* que acabamos de obtener, sería diferente por tener numerador distinto del de las anteriores (distinto denominador no puede tenerlo, pues solo hay *n!*); pero fundándonos en la propiedad anterior, podemos ordenar los elementos de modo que el numerador de esta última sustitución sea el que tenían común todas las anteriores *a b c.... m;* en este caso, el denominador, por ser una permutación de *n* letras, estará ya como denominador de alguna de las *n!* sustituciones formadas al principio, y por tanto, la sustitución dada se reduce á una de las *n!* ya encontradas.

3. *Sustitución idéntica; justificación de un convenio.* — Se

llama sustitución idéntica á la sustitución en la cual cada letra se sustituye por ella misma. Esta sustitución tiene la propiedad de que, aplicada á cualquier expresión, la deja invariable.

Cuando en Algebra aparecen nuevos elementos de cálculo como resultado de algunas operaciones, se procura extender á ellos las reglas del cálculo algébrico, adaptándolas á la naturaleza de dichos elementos; pero tratándose de sustituciones, se comprende que es imposible operar con ellas como con cantidades algébricas, puesto que para nada entra en ellas el concepto de cantidad. A pesar de esto intentaremos justificar el motivo por que se designan con nombres de operaciones algébricas ciertas transformaciones efectuadas con sustituciones.

Si tomamos varias letras para formar una sustitución, la más sencilla de las que podemos obtener es la sustitución idéntica, puesto que aplicada á una expresión la deja invariable. En Álgebra, la expresión que sumada con otra deja invariable á ésta, equivale á cero, y una expresión que multiplicada por otra da por producto á la última, equivale á la unidad.

Para que haya alguna analogía entre el cálculo algébrico y el de sustituciones, debemos considerar á la sustitución idéntica como cero ó como la unidad; *cero* si llamamos suma á la operación de aplicar una sustitución á una permutación; *unidad* si le llamamos producto.

Aplicando una sustitución á una permutación resulta otra permutación de las mismas letras; y como la forma de representar los datos y el resultado de esta operación tiene cierta analogía con la del producto de un número entero por una fracción se le llamó *producto de una permutación por una sustitución.* Sea la permutación $p = a\,b\,c\,d$ y $S = \begin{vmatrix} a\,b\,c\,d \\ d\,c\,a\,b \end{vmatrix}$ la sustitución; aplicando S á p se convierte esta última en $d\,c\,a\,b$. Si la sustitución S la representamos bajo la forma $\begin{vmatrix} d\,c\,a\,b \\ a\,b\,c\,d \end{vmatrix}$ (tomando invertida la colocación de las permutaciones), podemos expresar la operación de este modo: $\begin{vmatrix} d\,c\,a\,b \\ a\,b\,c\,d \end{vmatrix}\ a\,b\,c\,d = d\,c\,a\,b$, forma que nos recuer-

da el producto de un número entero por otro fraccionario, pues ha desaparecido el denominador de la sustitución. Por este motivo se ha llamado producto de una permutación por una sustitución, el resultado de aplicar ésta á aquélla.

El nombre de producto que se le da á la operación dicha lo admitimos porque nos sirve para seguir en el estudio del cálculo de sustituciones una marcha análoga á la que se sigue en Análisis Matemático, aunque no está debidamente fundamentado, porque no basta sólo la forma para decidir un punto tan importante. Sin embargo, como estamos estableciendo los principios de una teoría nueva, tenemos libertad para aceptar cuantos convenios creamos necesarios, siempre que sean lógicos y no conduzcan á resultados absurdos.

Multiplicando una permutación por la sustitución idéntica, observaremos que ésta actúa del mismo modo que la unidad en Análisis Matemático; luego por comparación podemos decir que, en la teoría de que nos ocupamos, la unidad es la sustitución idéntica, por lo que se le llama también *sustitución unidad*, y se la representa por $S = 1$. En esta representación hay que tener en cuenta que se prescinde del valor numérico de la unidad para convertirla en un símbolo que representa la sustitución idéntica.

Tomando como producto de una permutación por una sustitución el resultado de aplicar ésta á aquélla, deducimos el concepto de unidad. Inversamente, admitiendo que la sustitución idéntica es la unidad en esta teoría, puede definirse directamente el producto de una permutación por una sustitución, sin necesidad de recurrir al artificio de compararlo con la forma del producto de un número entero por otro fraccionario; es decir, que si hubiéramos convenido desde un principio en que la sustitución idéntica fuese la unidad de las sustituciones, podríamos dar lógicamente el nombre de producto á la operación de aplicar una sustitución á una permutación, como veremos en el punto que sigue.

4. *Producto de una permutación por una sustitución.*—El producto de dos expresiones cualesquiera se define diciendo que es otra expresión que está formada con una de ellas, de igual manera que la otra lo está con la unidad. Si queremos definir di-

rectamente el producto de una permutación por una sustitución del modo que acabamos de hacerlo, se necesitará fijar la unidad de las sustituciones: *convengamos* en que ésta sea la sustitución idéntica, prescindiendo de lo dicho en el párrafo 3.° que precede.

Adaptando la definición anterior al caso que estudiamos, podremos decir que, multiplicar una permutación por una sustitución, es hallar otra permutación que esté formada de la primera, como la sustitución está formada con la unidad de las sustituciones, ó sea la sustitución idéntica. Vamos á aclararlo con un ejemplo: sea $p = a\,b\,c\,d\,e$ una permutación y vamos á multiplicarla por la sustitución $S = \left|\begin{matrix} a\,b\,c\,d\,e \\ c\,b\,d\,e\,a \end{matrix}\right|$; la sustitución unidad es $\left|\begin{matrix} a\,b\,c\,d\,e \\ a\,b\,c\,d\,e \end{matrix}\right|$, y según la definición anterior, para obtener dicho producto, debemos operar sobre la permutación p del mismo modo que hayamos operado con la sustitución idéntica para obtener á S. Tomando el primer elemento de la sustitución unidad $\left|\begin{matrix} a \\ a \end{matrix}\right|$, resulta que para pasar de éste al primero de S $\left|\begin{matrix} a \\ c \end{matrix}\right|$, hay que cambiar en c la a del denominador del elemento de la sustitución unidad, luego la letra a que aparece como primera de la permutación p, y que es igual á la del numerador del primer elemento de S, debe sufrir igual modificación para transformarse en la letra correspondiente de la permutación producto, y por tanto se convierte en la letra c. El segundo elemento de la sustitución unidad es $\left|\begin{matrix} b \\ b \end{matrix}\right|$ y el segundo de la sustitución multiplicador es también $\left|\begin{matrix} b \\ b \end{matrix}\right|$; por tanto, como estos elementos son iguales, ó sea que no se ha operado sobre el segundo elemento de la sustitución unidad para obtener la sustitución S, luego debemos dejar invariable también la letra correspondiente de la permutación que es b; hemos encontrado, pues, dos letras de la permutación producto $c\,b$. La tercera será d, porque el elemento $\left|\begin{matrix} c \\ c \end{matrix}\right|$ de

la sustitución unidad hay que transformarlo en $\left|\begin{matrix} c \\ d \end{matrix}\right|$ para obtener el correspondiente de S, luego la tercera letra c de la permutación dada se transformará en la letra d, y así iremos razonando hasta llegar á la última letra, por lo que el producto será

$$\left|\begin{matrix} a\,b\,c\,d\,e \\ c\,b\,d\,e\,a \end{matrix}\right| \times a\,b\,c\,d\,e = c\,b\,d\,e\,a.$$

El resultado obtenido multiplicando la permutación $a\,b\,c\,d\,e$ por la sustitución S es el mismo que obtendríamos aplicando á la permutación dicha la sustitución S; luego era lógico darle el nombre de producto á la operación aquella, conforme le llamamos, fundados solamente en la forma que afectaba.

Si el orden de las letras del numerador de la sustitución no coincide con el de las letras de la permutación, podremos alterar el orden de los elementos de aquélla y el de los de la sustitución unidad para que se verifique dicha coincidencia; pero ni aun esto es necesario, pues para la demostración basta tomar un elemento cualquiera de la sustitución y operar con él y con la letra de la permutación que sea igual á la del numerador del elemento elegido del modo que se ha operado antes, y colocar la letra que obtengamos en el mismo lugar del producto que ocupaba en la permutación dada la letra que la ha originado.

En la práctica se sustituye directamente la primera letra de la permutación por el denominador del elemento, cuyo numerador es igual á dicha letra; se hace la misma operación con la segunda letra y se continúa así hasta la última.

5. *Producto de sustituciones.*—Producto de una permutación por varias sustituciones es el resultado de multiplicar la permutución por la primera de las sustituciones que se dan, la permutación producto por la segunda sustitución, la permutación que resulta por la tercera, y así sucesivamente hasta agotarlas todas. De modo que si p es la permutación y S_1, S_2 .... S_m las sustituciones, llamando p' al resultado, tendremos $p' = S_m (S_{m-1} \cdots S_3 (S_2 (S_1 p).).\ldots)$, ó quitando los paréntesis, si tenemos en cuenta cómo hay que hallar esta expresión, aparece bajo la forma $p' = S_m \ldots S_3\, S_2\, S_1\, p$.

El producto que buscamos será siempre una permutación, pues al efectuar el producto de p por S_1, se obtiene una permutación que, multiplicada á su vez por S_2, dará otra, y así sucesivamente.

Aplicando la definición anterior á la permutación $p = a\,c\,e\,d\,b$ y á las sustituciones $S_1 = \begin{vmatrix} a\,b\,c\,d\,e \\ c\,a\,d\,e\,b \end{vmatrix}$, $S_2 = \begin{vmatrix} a\,b\,c\,d\,e \\ e\,c\,b\,a\,d \end{vmatrix}$ y $S_3 = \begin{vmatrix} a\,b\,c\,d\,e \\ c\,e\,a\,d\,b \end{vmatrix}$ resulta $S_1 p = c\,d\,b\,e\,a = p_1$; al multiplicar p_1 por S_2 se obtiene $S_2 p_1 = b\,a\,c\,d\,e = p_2$, y, por último, $S_3 p_2 = b\,a\,c\,d\,e = p_3$, que es el producto de la permutación p por las tres sustituciones dadas, y puede representarse por $p_3 = S_3 S_2 S_1 p$.

Fijándonos por ahora sólo en las sustituciones S_1 y S_2, observaremos que el efecto producido multiplicando sucesivamente por ellas á la permutación p es convertida en la p_2; si por cualquier medio encontrásemos otra sustitución P_1, tal que multiplicando por ella la permutación p obtuviéramos la permutación $p_2 = S_2 S_1 p = P_1 p_1$, podremos dar á P_1 el nombre de *producto de las sustituciones* S_1 y S_2, ya que p multiplicada por P_1 da el mismo producto que multiplicada por S_1 y S_2, y esto nos permitirá reemplazar dos de los factores del producto $p_3 = S_3 S_2 S_1 p$ por su producto efectuado P_1.

Dadas dos sustituciones S_1 y S_2, *siempre es posible encontrar una tercera* P_1 *que pueda reemplazar á las* S_1 y S_2 *en el producto* $p_2 = S_2 S_1 p$. Efectivamente, el primer elemento de S_1 $\begin{vmatrix} a \\ c \end{vmatrix}$, hace que, al buscar el producto $S_1 p = p_1$, la letra a de p se convierta en la letra c de p_1, y esta letra, al multiplicar p_1 por S_2, por efecto del elemento $\begin{vmatrix} c \\ b \end{vmatrix}$ de S_2, se convierta en b; luego la primera letra de p que era a por la multiplicación sucesiva por S_1 y S_2 se ha convertido en b. Ahora bien: una sustitución tal que uno de sus elementos fuese $\begin{vmatrix} a \\ b \end{vmatrix}$ cumpliría la condición de que, multiplicando por ella la permutación p, transformaría la primera letra de ésta que es a en b, letra igual á la que tiene p_2 en el mismo lugar. Haciendo iguales consideraciones para c, segunda

letra de p, veremos que al multiplicar p por S_1 se convierte en d, segunda letra de p_1, y al multiplicar este último producto p_1 por S_2 se convierte en a, letra que aparece en el segundo lugar de p_2. Luego una sustitución que tenga el elemento $\left|\begin{matrix} c \\ a \end{matrix}\right|$, al multiplicar por ella la permutación p convertirá la segunda letra de esta c en la letra a, que es la segunda de las de p_2. Siguiendo la misma marcha encontraríamos todos los elementos que transformaran la permutación p en la p_2, y con ellos formaremos la sustitución $P_1 = \left|\begin{matrix} a\,c\,e\,d\,b \\ b\,a\,c\,d\,e \end{matrix}\right|$ que satisface la condición impuesta, ya que $P_1 p = \left|\begin{matrix} a\,c\,e\,d\,b \\ b\,a\,c\,d\,e \end{matrix}\right| a\,c\,e\,d\,b = b\,a\,c\,d\,e = p_2$.

Queda, pues, demostrado que, dadas dos sustituciones, existe otra tal que, si multiplicamos por ella una permutación, da el mismo resultado que el producto de esta permutación por las dos sustituciones dadas. A la sustitución que tiene esta propiepiedad se le llama *producto de dos sustituciones*.

Para efectuar el producto de dos sustituciones no hay necesidad de hacer los razonamientos anteriores, sino se efectúa directamente sin considerar ninguna permutación.

Vamos á efectuar el producto $\left|\begin{matrix} a\,b\,c\,d \\ b\,c\,a\,d \end{matrix}\right| \left|\begin{matrix} a\,b\,c\,d \\ d\,c\,b\,a \end{matrix}\right|$: para encontrar el primer elemento del producto consideraremos que la sustitución de la derecha cambia la letra a en d y la otra sustituye á ésta por ella misma; luego el primer elemento del producto será $\left|\begin{matrix} a \\ d \end{matrix}\right|$ y siguiendo de este modo obtendremos por producto la sustitución $\left|\begin{matrix} a\,b\,c\,d \\ d\,a\,c\,b \end{matrix}\right|$.

Para facilitar esta operación se dan algunas reglas prácticas, como multiplicar entre sí, de la misma manera que si fuesen quebrados, los elementos de ambas sustituciones que tengan una letra común intermedia, y el producto es un elemento del producto de dichas sustituciones. En las dos sustituciones dadas se encuentra uno de los elementos del producto

efectuando la multiplicación de $\frac{a}{d} \times \frac{d}{d} = \frac{a}{d}$ y tomando $\left|\begin{matrix} a \\ d \end{matrix}\right|$ como elemento del mismo; sin embargo, no hay necesidad de recurrir á estas transformaciones, pues por la práctica se escribe directamente el producto de dos sustituciones.

El producto $p_3 = S_3\, S_2\, S_1\, p$ será el mismo, ya lo obtengamos por la multiplicación sucesiva de p por S_1, S_2 y S_3, ó multiplicando p por P_1 (que equivale á multiplicar primero por S_1 y luego por S_2) y el resultado por S_3; esto nos permite escribir $p_3 = S_3\, S_2\, S_1\, p = S_3\, P_1\, p$. Como el último es el producto de una permutación por dos sustituciones, podemos encontrarlo multiplicando la permutación p por la sustitución producto de P_1 y S_3; representando por P_2 dicho producto, tendremos: $p_3 = P_2\, p$. Comparando esta última expresión con $p_3 = S_3\, S_2\, S_1\, p$, se observa que P_2 equivale al producto de las tres sustituciones S_1, S_2 y S_3, ya que por multiplicación transforma á p en p_3.

Todas las consideraciones que hemos hecho para tres sustituciones pueden generalizarse para mayor número, lo que demuestra que el producto de varias sustituciones es otra sustitución.

De las igualdades $p_3 = S_3\, S_2\, S_1\, p$ y $p_3 = S_3\, P_1\, p$, se deduce que el producto de varias sustituciones goza de la propiedad asociativa.

En general, el producto de dos sustituciones, y por tanto el de varias, carece de la propiedad conmutativa, cualidad que es preciso tener muy en cuenta y que da origen á la dificultad y aun imposibilidad en muchos casos de resolver algunos problemas.

Es muy fácil comprobar que en un producto de sustituciones no es indiferente el orden en que se toman los factores, pues basta elegir dos sustituciones y multiplicarlas en cierto orden; repitiendo la operación en orden inverso, el resultado es distinto en general. Sea, por ejemplo, el producto $\left|\begin{matrix} a\,b\,c\,d \\ b\,c\,a\,d \end{matrix}\right| \quad \left|\begin{matrix} a\,b\,c\,d \\ d\,c\,b\,a \end{matrix}\right|$; empezando á multiplicar por la derecha se obtiene como producto

$\begin{vmatrix} a\,b\,c\,d \\ d\,a\,c\,b \end{vmatrix}$ y si invertimos el orden de los factores, el producto que resulta es: $\begin{vmatrix} a\,b\,c\,d \\ d\,c\,b\,a \end{vmatrix} \begin{vmatrix} a\,b\,c\,d \\ b\,c\,a\,d \end{vmatrix} = \begin{vmatrix} a\,b\,c\,d \\ c\,b\,d\,a \end{vmatrix}$; como vemos, este producto no es igual al anterior.

Hay algunos casos en que es posible alterar el orden de dos sustituciones que forman un producto sin que éste varíe, pero esto se verifica en un número relativamente pequeño de sustituciones que se llaman *sustituciones cambiables* con una dada. Dos sustituciones cuyas letras sean distintas serán cambiables, pues las letras que se hayan de sustituir por efecto de una de dichas sustituciones no vendrán transformadas por la otra. También es cambiable con cualquier sustitución la sustitución unidad.

Cuando hay que efectuar un producto de varias sustituciones, no basta sólo conocer éstas para obtenerlo, sino que debe conocerse además el orden en que se han de multiplicar, porque el producto de varias sustituciones carece de la propiedad conmutativa.

Establecido el orden en que se han de multiplicar varias sustituciones, podemos escribirlas en este orden de derecha á izquierda y empezar á multiplicar por el primer factor de la derecha (siguiendo el orden que hemos llevado hasta ahora), ó bien invertir esta colocación y empezar á multiplicar de izquierda á derecha. Así, dadas las sustituciones S_1 y S_2, efectuar su producto empezando por S_1: llamando P_1 al producto podemos representar la operación por $S_2\,S_1 = P_1$ ó $S_1\,S_2 = P_1$, empezando á multiplicar por el factor de la derecha en el primer caso y por la izquierda en el segundo; de los dos modos se obtiene la sustitución P_1.

Para la demostración de teoremas é investigación de propiedades de las sustituciones, es indiferente que en el curso de su estudio indiquemos la multiplicación de derecha á izquierda ó de izquierda á derecha, siempre que empezamos por la misma sustitución y que, una vez fijado el orden que se debe seguir, no se abandone durante toda la demostración; esto es algo parecido á lo que ocurre con la representación de las cantidades positivas y negativas sobre una recta, pues ya sabemos que es indiferente

contar las positivas hacia la derecha ó hacia la izquierda, siempre que las negativas se cuenten en sentido contrario.

Con el objeto de no tener que advertir en cada caso el orden en que se efectúan los productos, seguiremos siempre el orden preferido por los autores clásicos, que consiste en colocar los factores ordenados de derecha á izquierda, y por tanto empeza la multiplicación por la derecha.

De lo expuesto acerca del producto de dos sustituciones, se deduce la siguiente propiedad, que más adelante tendrá aplicación:

Si dos sustituciones P y P_1 son iguales y A es una sustitución cualquiera, se verificará $A\ P = A\ P_1$. En efecto; si multiplicamos una permutación cualquiera p por la sustitución P, dará por producto otra permutación p_1 y si á ésta la multiplicamos por A se convierte á su vez en p_2; multiplicando p por P_1, la permutación que resulta ha de ser igual á p_1, puesto que, por ser iguales P y P_1, el cambio que P produce en p lo ha de producir también P_1, y si á la permutación p_1 se le aplica la sustitución A, ya hemos dicho que resulta p_2. Luego si partiendo de la misma permutación y multiplicándola por A P hemos obtenido igual resultado que multiplicándola por $A\ P_1$, las sustituciones producto de A P y $A\ P_1$, serán iguales y por tanto $A\ P = A\ P_1$.

Del mismo modo se demostraría que $P\ A = P_1\ A$.

Como el producto de varias sustituciones es otra sustitución, la sustitución P puede representar un producto de sustituciones, y la P_1 otro producto igual á P formado por sustituciones distintas á las que forman á éste; por tanto, *una igualdad entre sustituciones no se altera si sus dos miembros se multiplican á la derecha ó á la izquierda por una misma sustitución.*

6. *Cociente de dos sustituciones.*—Estudiada la multiplicación puede definirse la división de sustituciones como la operación inversa de aquélla, si bien por no ser conmutativa la multiplicación debemos introducir esta propiedad en el cociente, para lo cual modificaremos la definición general en esta forma: cociente de dos sustituciones es una tercera sustitución que, multiplicada *á la derecha (ó á la izquierda)* por una de ellas, reproduce la otra.

Esta distinción es necesaria, porque si A, B y C son las sustituciones dividendo, divisor y cociente, el producto de B por C debe ser el dividendo A; pero como en general C . B no será igual B . C, para que el producto del divisor por el cociente sea igual á A, es preciso que C no sea el mismo en los dos casos, y el problema se reduce á hallar una de las dos sustituciones cociente, la que está multiplicada á la derecha por B ó la que lo está á la izquierda.

Vamos á exponer, por medio de un ejemplo, la marcha que se debe seguir para encontrar el cociente de dos sustituciones: sean éstas $A = \left|\begin{matrix} a\,b\,c\,d\,e \\ b\,a\,d\,e\,c \end{matrix}\right|$ y $B = \left|\begin{matrix} a\,b\,c\,d \\ b\,d\,a\,c \end{matrix}\right|$; nos proponemos encontrar otra C para la cual se verifique $A = B \,.\, C$. Como B sólo tiene cuatro letras y á A tiene cinco, completaremos la B con el elemento $\left|\begin{matrix} e \\ e \end{matrix}\right|$, puesto que carece de la letra *e*, luego $B = \left|\begin{matrix} a\,b\,c\,d\,e \\ b\,d\,a\,c\,e \end{matrix}\right|$, y á C podemos representarla por $C = \left|\begin{matrix} a\,b\,c\,d\,e \\ \alpha\,\beta\,\gamma\,\delta\,\varepsilon \end{matrix}\right|$, siendo $\alpha, \beta, \gamma, \delta$ y ε las mismas letras *a*, *b*, *c*, *d* y *e*, pero formando una permutación desconocida que, junto con la del numerador, constituye el cociente buscado.

Al efectuar el producto B . C, para encontrar el dividendo A empezaremos á multiplicar, según hemos convenido, por la sustitución C; un elemento de C, el primero, por ejemplo $\left|\begin{matrix} a \\ \alpha \end{matrix}\right|$, sustituye la letra *a* por α, y el elemento de B, cuyo numerador sea α, debe tener por denominador la letra *b*, para que al multiplicar C por B se obtenga el elemento $\left|\begin{matrix} a \\ b \end{matrix}\right|$ de A, cuyo numerador es el mismo que el del elemento de C por que hemos empezado la multiplicación; más claro: se ha de verificar $\left|\begin{matrix} \alpha \\ b \end{matrix}\right| \left|\begin{matrix} a \\ \alpha \end{matrix}\right| = \left|\begin{matrix} a \\ b \end{matrix}\right|$. El elemento de B, que tiene por denominador *b*, es elemento $\left|\begin{matrix} a \\ b \end{matrix}\right|$; por tanto, $\left|\begin{matrix} \alpha \\ b \end{matrix}\right| = \left|\begin{matrix} a \\ b \end{matrix}\right|$ y $\alpha = a$, luego el elemento $\left|\begin{matrix} a \\ \alpha \end{matrix}\right|$ del

cociente que buscamos es $\left|\begin{matrix} a \\ a \end{matrix}\right|$. El segundo elemento se obtiene de modo análogo, pues para que al efectuar el producto B . C resulte $\left|\begin{matrix} \beta \\ a \end{matrix}\right| \left|\begin{matrix} b \\ \beta \end{matrix}\right| = \left|\begin{matrix} b \\ a \end{matrix}\right|$, segundo elemento de A, se necesita que el elemento $\left|\begin{matrix} \beta \\ a \end{matrix}\right|$ sea el $\left|\begin{matrix} c \\ a \end{matrix}\right|$ del divisor *B*; de donde se deduce $\beta = c$, y el segundo elemento del cociente será $\left|\begin{matrix} b \\ c \end{matrix}\right|$. De $\left|\begin{matrix} \gamma \\ d \end{matrix}\right| \left|\begin{matrix} c \\ \gamma \end{matrix}\right| = \left|\begin{matrix} c \\ d \end{matrix}\right|$ y del elemento $\left|\begin{matrix} b \\ d \end{matrix}\right|$ de *B*, cuyo denominador es *d*, se deduce $\left|\begin{matrix} \gamma \\ d \end{matrix}\right| = \left|\begin{matrix} b \\ d \end{matrix}\right|$ y $\gamma = b$; luego el tercer elemento de C es $\left|\begin{matrix} c \\ \gamma \end{matrix}\right| = \left|\begin{matrix} c \\ b \end{matrix}\right|$; de $\left|\begin{matrix} \delta \\ e \end{matrix}\right| \left|\begin{matrix} d \\ \delta \end{matrix}\right| = \left|\begin{matrix} d \\ e \end{matrix}\right|$ y $\left|\begin{matrix} \delta \\ c \end{matrix}\right| = \left|\begin{matrix} e \\ e \end{matrix}\right|$ se deduce $\delta = e$ y de aquí $\left|\begin{matrix} d \\ \delta \end{matrix}\right| = \left|\begin{matrix} d \\ e \end{matrix}\right|$, cuarto elemento de C; finalmente, de $\left|\begin{matrix} \varepsilon \\ c \end{matrix}\right| \left|\begin{matrix} e \\ \varepsilon \end{matrix}\right| = \left|\begin{matrix} e \\ c \end{matrix}\right|$ y de $\left|\begin{matrix} \varepsilon \\ c \end{matrix}\right| = \left|\begin{matrix} d \\ e \end{matrix}\right|$ obtenemos $\varepsilon = d$, y por tanto el último elemento del cociente es $\left|\begin{matrix} e \\ d \end{matrix}\right|$. Resumiendo todos los elementos encontrados, podremos formar la sustitución cociente, que es $C = \left|\begin{matrix} a\,b\,c\,d\,e \\ a\,c\,b\,e\,d \end{matrix}\right|$, resultado que puede comprobarse efectuando el producto B C.

Si el cociente que buscamos estuviese á la izquierda de B en el producto $A = C_1 B$ empezaríamos las operaciones por los elementos de la sustitución B. Así diremos: el primer elemento de B $\left|\begin{matrix} a \\ b \end{matrix}\right|$ sustituye la letra *a* por la *b*, y el segundo elemento de C_1 sustituye á su vez esta última letra por β, es decir $\left|\begin{matrix} b \\ \beta \end{matrix}\right| \left|\begin{matrix} a \\ b \end{matrix}\right| = \left|\begin{matrix} a \\ \beta \end{matrix}\right|$; pero como, según la definición de cociente, el conjunto de estas modificaciones ha de ser un elemento de A y co-

nocemos su numerador a, no cabe duda que sólo puede ser el primero de ellos, ó sea el $\left|\begin{matrix} a \\ b \end{matrix}\right|$ y por lo tanto $\left|\begin{matrix} a \\ \beta \end{matrix}\right| = \left|\begin{matrix} a \\ b \end{matrix}\right|$, de donde $\beta = b$ y $\left|\begin{matrix} b \\ b \end{matrix}\right|$ es el elemento buscado del cociente C_1; el elemento $\left|\begin{matrix} b \\ d \end{matrix}\right|$, al multiplicar al $\left|\begin{matrix} d \\ \delta \end{matrix}\right|$ de C_1, debe dar el $\left|\begin{matrix} b \\ a \end{matrix}\right|$ de A, y por lo tanto $\delta = a$ y $\left|\begin{matrix} d \\ \delta \end{matrix}\right| = \left|\begin{matrix} d \\ a \end{matrix}\right|$ otro elemento del cociente buscado. Siguiendo así, encontraremos los tres elementos restantes: $\left|\begin{matrix} a \\ d \end{matrix}\right|$, $\left|\begin{matrix} c \\ e \end{matrix}\right|$ y $\left|\begin{matrix} e \\ c \end{matrix}\right|$, que, junto con los otros dos encontrados, forman el cociente $C_1 = \left|\begin{matrix} b\,d\,a\,c\,e \\ b\,a\,d\,e\,c \end{matrix}\right| = \left|\begin{matrix} a\,b\,c\,d\,e \\ d\,b\,e\,a\,c \end{matrix}\right|$, que no es igual á C.

Observando la igualdad $A = B \cdot C$, vemos que si se pudiera encontrar una sustitución X tal que multiplicando á la izquierda por ella á la sustitución B se obtuviese la sustitución unidad $X\,B = 1$, tendríamos resuelto el problema de la división con más facilidad, pues multiplicando á la izquierda por X los dos miembros de la primera igualdad, resulta $X\,A = X\,B\,C$, que por la condición establecida $X\,B = 1$ se convierte en $X\,A = C$, y la división de A por B queda reducida á encontrar C mediante un producto.

Para encontrar X, nos basta considerar á esta sustitución como el cociente de dividir por B la sustitución unidad $\left|\begin{matrix} a\,b\,c\,d\,e \\ a\,b\,c\,d\,e \end{matrix}\right|$; pero no nos conviene hacerlo así, porque volvemos al procedimiento que procuramos evitar. Podemos hallar X sin necesidad de hacer ninguna operación, teniendo presente que el producto $X\,B = 1$ aplicado á una permutación no la modifica; por tanto, la variación que introduzca B en dicha permutación debe deshacerla X; luego si la sustitución B cambia la letra a en b, la sustitución X debe cambiar la b en a, y lo mismo ocurre para las demás letras, de donde se deduce que los elementos en X los forman las mismas letras que los de B, pero

tomando el numerador por denominador y viceversa. A la sustitución X se le llama *sustitución inversa* de B.

En comprobación de lo expuesto hallaremos el cociente C obtenido antes, sirviéndonos de la sustitución X, que es en este caso $X = \begin{vmatrix} b\,d\,a\,c\,e \\ a\,b\,c\,d\,e \end{vmatrix}$; luego $C = \begin{vmatrix} b\,d\,a\,c\,e \\ a\,b\,c\,d\,e \end{vmatrix} \begin{vmatrix} a\,b\,c\,d\,e \\ b\,a\,d\,e\,c \end{vmatrix} = \begin{vmatrix} a\,b\,c\,d\,e \\ a\,c\,b\,e\,d \end{vmatrix}$.

Si se hubiera querido encontrar el cociente C_1, que está multiplicado á la derecha por B, hubiéramos seguido el mismo procedimiento multiplicando á la derecha por X', con la condición $B\,X' = 1$ y C_1 sería igual á $A\,X'$; pero esta sustitución X' es la misma X anterior, porque el efecto producido por ella en una permutación tiene que deshacerlo B, luego ha de ser su inversa; por tanto, $C_1 = A\,X$.

Por ser $X\,B = 1$ y $B\,X = 1$, resulta $X\,B = B\,X$, lo que prueba que una sustitución y su inversa son cambiables.

7. *Potencias de una sustitución.*—Potencia de una sustitución es el producto de varios factores iguales á ella. Al decir producto en esta definición debe entenderse que nos referimos al producto tal como lo hemos establecido para las sustituciones; de este modo queda adaptada á la teoría que estudiamos la definición general de potencia.

Las potencias de las sustituciones se representan lo mismo que las de los números, escribiendo á la parte superior de la derecha de la sustitución de que se trata un número igual á las veces que dicha sustitución se toma por factor. Así, la cuarta potencia de la sustitución S la representaremos por $S \cdot S \cdot S \cdot S = S^4$, y la emésima por $S \cdot S \cdot S \ldots S = S^m$.

El producto de dos potencias de la misma sustitución es otra potencia de ésta, cuyo exponente es la suma de los exponentes de los factores. En efecto: sean S^m y S^n dos potencias de la sustitución S: su producto será $S \cdot^m S^n = S \cdot S \ldots S \times S \cdot S \ldots S$, y como éste es un producto que se compone de $m + n$ factores iguales á S, según la definición es la potencia $(m + n)^a$ de S. Por tanto, $S \cdot^m S^n = S \cdot^{m+n}$.

También se puede introducir en esta teoría el concepto de

potencia de exponente negativo partiendo de las sustituciones inversas. Recordando que hemos llamado sustitución inversa de la A á otra sustitución A_1, tal que verifique la igualdad $A\,A_1 = 1$, si en esta igualdad consideramos á A_1 como el cociente de dividir la sustitución idéntica (representada por la unidad) por A, obtendremos $A_1 = \frac{1}{A}$; pero la fracción $\frac{1}{A}$ podremos representarla por A^{-1}, como se hace con los números recíprocos, luego $A_1 = A^{-1}$, y como A_1 es la sustitución inversa de A, A^{-1} también lo es; luego $A \,.\, A^{-1} = 1$. Queda demostrado, pues, que una sustitución elevada á — 1 representa la inversa de la base. A una sustitución inversa de otra se le llama también *recíproca*.

Las distintas potencias de S^{-1}, sustitución recíproca de S, se representan colocando á la parte superior de la derecha de la sustitución S un exponente negativo de tantas unidades como factores tiene la potencia. De esto se deduce que las potencias S^m y S^{-m} de la sustitución S son sustituciones recíprocas, ya que $S^m S^{-m} = S \,.\, S \ldots S \,.\, S \times S \,.\, {}^{-1}S^{-1} \ldots S \,.\, {}^{-1}S^{-1} = S \,.\, S \ldots S\,(S \,.\, S^{-1}) \,.\, S^{-1} \ldots S \,.\, {}^{-1}S^{-1} = \ldots = S \,.\, S^{-1} = 1$.

Las potencias de exponente negativo cuando entran en productos de potencias de la misma sustitución, pueden reducirse y simplificarse siguiendo la ley de los exponentes que se aplica en Algebra; porque si S^m y S^{-n} son dos potencias, una positiva y otra negativa, al efectuar el producto en la forma dicha antes, resulta: $S^m S^{-n} = S \,.\, S \ldots S \,.\, S \,.\, S^{-1} \ldots S^{-1} \,.\, S^{-1} = S \,.\, S \ldots S\,(S \,.\, S^{-1})\, S^{-1} \ldots S^{-1} \,.\, S^{-1} = S \,.\, S \ldots S$, y como operando de este modo el último miembro de esta igualdad se compone de $m-n$ sustituciones iguales á S, tendremos $S^m S^{-n} = S^{m-n}$.

Aplicando esta regla á dos potencias de exponentes iguales y de signo contrario, resulta: $S^m \,.\, S^{-m} = S^0$; pero, según hemos demostrado anteriormente, por ser S^m y S^{-m} sustituciones recíprocas, su producto es $S^m \,.\, S^{-m} = 1$, por lo cual podemos convenir en que la potencia cero de una sustitución representa la sustitución unidad y expresarlo por la igualdad $S^0 = 1$.

De estas consideraciones se deduce que podemos pasar de una potencia negativa S^{-n} á otra positiva, multiplicando á S^{-n} por S tantas veces como sea necesario, y del mismo modo pa-

saremos de una potencia positiva á otra negativa, multiplicando por S^{-1}. En ambos casos pasaremos por la sustitución unidad $S^o = 1$, que sirve de término intermedio entre las potencias negativas y positivas; por tanto, las distintas potencias de una sustitución puede decirse que forman una á modo de progresión por cociente, cuya razón es S ó S^{-1}, según que, partiendo de S^o se quiera obtener la parte de las potencias positivas ó las negativas. La progresión completa, á partir de las negativas, es:

$$\frac{\cdot\cdot}{\cdot\cdot} \ldots S^{-n} : S^{-(n-1)} : \ldots : S^{-2} : S^{-1} : S^o : S^1 : S^2 : \ldots : S^{n-1} : S^n : \ldots \frac{\cdot\cdot}{\cdot\cdot}$$

8. *Orden de una sustitución.*—Para obtener las potencias de una sustitución, multiplicamos repetidas veces á ésta por sí misma, y como podemos efectuar tantos productos como queramos, parece que las potencias de una sustitución serán infinitas en número; pero esto no es así, pues por muchos productos que se obtengan siempre resultan sustituciones del mismo número de letras que tiene la sustitución dada. Hemos demostrado ya que el número de sustituciones distintas que pueden formarse con n letras es $n!$, y como este número, aunque tal vez muy grande, siempre será limitado, resulta que la sustitución dada no puede tener infinitas potencias diferentes, por lo cual, al multiplicar por S alguna de sus potencias, el producto será igual á otra de las potencias obtenidas antes.

Si formamos la serie de las potencias sucesivas de una sustitución S, á partir de S^0, la primera potencia que se repite es la misma S^0.

En efecto: por ser S distinta de S^0, al multiplicarla por sí misma dará S^2, que no será igual á S; si S^2 fuera igual á S^0, el teorema está demostrado para este caso; pero si no lo es, multiplicando á S^2 por S se obtiene S^3; si $S^3 = S^0$, queda demostrada la proposición para la sustitución S; pero si S^3 no es igual á S^0, tampoco puede serlo á ninguno de los términos anteriores S^2 y S, porque para ser $S^3 = S^2 . S = S^2$ ó $S^3 = S^2 . S = S$, se necesita que $S = S^0$ ó que $S^2 = S^0$, lo cual es contrario á lo afirmado antes. Este razonamiento es general, pues suponiendo que no hay en la serie $S^0, S^1, S^2, \ldots S^{n-1} S^n$ ninguna potencia igual á S^0 y que hubiese una S^n, que fuese igual á otra S^{n-p} anterior á ella y comprendida entre S^0 y S^n, tendríamos $S^n = S^{n-p}$; pero

según la multiplicación de potencias se verificará $S^{n-p} S^p = S^n$, y sustituyendo en esta igualdad S^n por S^{n-p}, tendremos $S^{n-p} S^p = S^{n-p}$, igualdad que sólo es cierta si $S^p = S^n$. Ahora bien: como p es menor que n, resulta que antes de repetirse la potencia $S^{n-p} = S^n$ se ha repetido $S^0 = S^p$.

Esta propiedad puede demostrarse de otra manera considerando las series de las potencias positivas y negativas de una sustitución S, obtenidas multiplicando repetidas veces por S y S^{-1} hasta llegar á una potencia S^n para la que se verifique $S^n = S^0$. Operando así, obtendremos las dos series cuyos términos se corresponden (siendo la unidad el producto de cada dos términos que ocupan el mismo lugar), series que podemos disponer como sigue:

$$S^0 \begin{cases} S, \quad S^2, \quad S^3 \quad .... \; S^p \; .... \; S^q \quad .... \; S^n \quad = S^0 \\ S^{-1} S^{-2} S^{-3} .... S^{-p} .... S^{-q} .... S^{-n} = S^0 \end{cases}$$

Decimos que en la serie de las potencias positivas ó negativas de S no puede haber entre S y S^n dos potencias iguales. En efecto: supongamos que las haya y sea $S^p = S^q$; de esta igualdad se origina (sustituyendo S^p en $S^p . S^{-p} = S^0$) $S^q . S^{-p} = S^0$ ó $S^{p-q} = S^0$, igualdad que, por ser p y q menores que n, sólo puede verificarse si $q = p$, lo que demuestra que S^p y S^q no son potencias de distinto exponente, y que por tanto la primera potencia que se repite es igual á S^0.

Si $q - p = n$ ó $q - p = m . n$ también se verifica la igualdad $S^{q-p} = S^0$, porque si $q - p = n$, $S^{q-p} = S^n$, que por hipótesis es S^0, y si $q - p = m . n$ $S^{q-p} = S^{m . n} = S^n . S^n .... S^n = S^0$; y como para que $q - p = n$ ó $q - p = m . n$ se necesita $q = n + p$ ó $q = m . n + p$, deducimos que la potencia de grado q igual á otra de grado p comprendida en la serie entre S^0 y $S^n = S^0$ está colocada después de S^n.

Se llama *orden* de una sustitución al exponente de la primera potencia de la misma que es igual á la sustitución unidad.

Si la suma de los exponentes de dos potencias de una sustitución es n ó un múltiplo de n, siendo n el orden, las sustituciones dadas son inversas, porque $S^p . S^q = S^{p+q} = S^{m . n} = S^0$.

Multiplicando á la derecha por S^{-p} los dos miembros de la

igualdad $S^{n-p} . S^p = S^0$, resulta $S^{n-p} = S^{-p}$, igualdad que demuestra que la serie de las potencias negativas es la misma que la de las positivas, pero en orden inverso.

9. *Raíz de una sustitución.*—Raíz de grado m de una sustitución es otra sustitución que, elevada á m, reproduce la primera. Según esta definición, la extracción de raíces es la operación inversa de la elevación.

La extracción de raíces de las sustituciones se representa lo mismo que en Álgebra, escribiendo bajo el signo radical la sustitución cuya raíz se considera y poniendo un índice igual al grado de dicha raíz. Si X es la raíz m^a de S, se representará por $\sqrt[m]{S} = X$.

La raíz m^a del producto de dos sustituciones cuyas letras son distintas, es igual al producto de las raíces m^{as} de dichas sustituciones. Sean A y B dos sustituciones que no tienen letras iguales y X é Y sus raíces m^{as}. Según estas hipótesis podemos escribir $\sqrt[m]{A} = X \sqrt[m]{B} = Y$ y $\sqrt[m]{A}\sqrt[m]{B} = XY$. Elevando esta última igualdad á la potencia m^a, resulta $\left(\sqrt[m]{A} . \sqrt[m]{B}\right)^m = (XY)^m$; $(XY)^m = XY . XY .... XY$; pero X é Y sólo tienen letras distintas, porque por hipótesis las letras de A y B son diferentes, y estas dos sustituciones sólo pueden estar formadas por las letras que existan en X é Y, respectivamente; por tanto, en el producto $XY . XY .... XY$ podemos alterar el orden de los factores escribiéndolo en esta forma: $XY . XY .... XY = XXX.... X . YY .... Y = X.^m Y^m$. de donde se deduce $\left(\sqrt[m]{A} . \sqrt[m]{B}\right) m = X^m . Y^m$. Extrayendo la raíz m^a de esta expresión se obtiene $\sqrt[m]{A}\sqrt[m]{B} = \sqrt[m]{X^m . Y^m}$ ó bien sustituyendo y tomando como primer miembro el segundo $\sqrt[m]{AB} = \sqrt[m]{A}\sqrt[m]{B}$ que demuestra la proposición enunciada.

Una raíz cuyo grado sea un producto de dos factores puede extraerse por partes, extrayendo la raíz de grado igual á uno de

los factores, y del resultado se extrae la raíz de grado igual al otro factor. Sea X la raíz de grado $r \cdot t$ de la sustitución A; por la definición de raíz se verifica $A = X^{rt}$ ó $A = (X^r)^t$; extrayendo la raíz de grado t de los dos miembros de esta igualdad, tendremos: $\sqrt[t]{A} = X^r$, y operando lo mismo con esta última respecto al grado r $\sqrt[r]{\sqrt[t]{A}} = X$.

Estas propiedades de las raíces nos permitirán deducir la condición necesaria y suficiente para que una sustitución tenga raíz exacta de cierto grado, y la investigación de dicha raíz cuando la sustitución dada sea potencia perfecta del grado mencionado.

II

SUSTITUCIONES CIRCULARES

10. *Definición y representación.*—Vamos á ocuparnos ahora de las sustituciones circulares, que son sustituciones en las cuales cada letra de la permutación numerador se sustituye por la que le precede ó sigue.

Como podemos observar, la definición de esta especie de sustituciones está incluída en la definición general de sustituciones, de las que son un caso particular, y por tanto también son aplicables á ellas las demás definiciones que se dieron respecto á las sustituciones en general, lo mismo que las propiedades demostradas y modo de operar. A pesar de esto, las estudiamos en capítulo aparte para deducir sus propiedades directamente por medio de una representación especial.

La sustitución $\begin{vmatrix} a\,b\,c\,d\,e \\ b\,c\,d\,e\,a \end{vmatrix}$ es una sustitución circular. De la definición se deduce que no hay necesidad de representar estas sustituciones por sus dos permutaciones; basta escribir sólo la

permutación numerador, pues sabemos que cada letra se sustituye por la que le sigue inmediatamente. Representaremos, pues, estas sustituciones por la permutación numerador encerrada dentro de un paréntesis, de modo que la sustitución anterior se indicará por $(a\ b\ c\ d\ e)$.

A estas sustituciones que estamos estudiando se les llamó circulares porque también pueden representarse dividiendo una circunferencia en tantas partes iguales como letras tiene la sustitución de que se trata y colocando en cada una de los puntos de división una de las letras de la sustitución, siguiendo el orden que tiene en ésta. La sustitución circular $C = (a\ b\ c\ d\ e\ f)$ se representa como está en la figura 2.ª, conviniendo en que cada letra se sustituye por la que le sigue, en sentido contrario al indicado por la flecha. Si queremos que aparezcan los elementos de esta sustitución, supondremos que, dejando las letras exteriores donde están, gira la circunferencia una división en el sentido indicado por la flecha, y por este giro aparece junto á cada letra (en el interior de la circunferencia) la que le corresponde como denominador de su elemento.

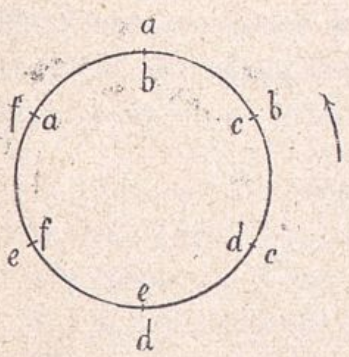

Fig. 2.ª

Observando la figura se deduce que se puede empezar la sustitución por cualquier letra, siempre que sigamos el orden convenido.

La sustitución unidad podremos representarla suponiendo que ha girado la circunferencia tantas divisiones como letras tiene la sustitución, por lo cual las letras interiores serán iguales á las exteriores, y los elementos que se obtienen son $\left|\begin{matrix} a \\ a \end{matrix}\right|$ $\left|\begin{matrix} b \\ b \end{matrix}\right|$ etc.

11. *Descomposición en ciclos.*—Pueden encontrarse en el cálculo algunas sustituciones que, siendo circulares, no lo parezcan por no tener colocados sus elementos en el orden conve-

niente. Así, la sustitución $C = \left|\begin{matrix} d\,b\,e\,c\,f\,a \\ e\,c\,f\,d\,a\,b \end{matrix}\right|$, tal como está escrita, no parece circular, y sin embargo lo es. En efecto: tomemos un elemento cualquiera, el $\left|\begin{matrix} a \\ b \end{matrix}\right|$; coloquemos á su lado el $\left|\begin{matrix} b \\ c \end{matrix}\right|$, que tiene por numerador la misma letra que el elemento anterior tiene por denominador; siguiendo la misma ley coloquemos á $\left|\begin{matrix} c \\ d \end{matrix}\right|$ junto á $\left|\begin{matrix} b \\ c \end{matrix}\right|$, y siguiendo de este modo pasaremos por todos los elementos, lo que nos permite escribir la sustitución C en la forma $C = \left|\begin{matrix} a\,b\,c\,d\,e\,f \\ b\,c\,d\,e\,f\,a \end{matrix}\right| = (a\,b\,c\,d\,e\,f)$.

Apliquemos esta manera de ordenar los elementos á la sustitución $S = \left|\begin{matrix} a_1\,c_2\,a_2\,b_1\,d_2\,c_1\,b_2 \\ b_1\,d_2\,b_2\,c_1\,a_2\,a_1\,c_2 \end{matrix}\right|$. Partiendo del elemento $\left|\begin{matrix} a_1 \\ b_1 \end{matrix}\right|$ obtendremos la sustitución circular $\left|\begin{matrix} a_1\,b_1\,c_1 \\ b_1\,c_1\,a_1 \end{matrix}\right|$, y no podemos continuar ordenando porque al llegar á $\left|\begin{matrix} c_1 \\ a_1 \end{matrix}\right|$ se repiten los elementos en el mismo orden; como faltan aún cuatro elementos de S, tomaremos otro cualquiera, el $\left|\begin{matrix} a_2 \\ b_2 \end{matrix}\right|$, y operando del mismo modo se obtiene $\left|\begin{matrix} a_2\,b_2\,c_2\,d_2 \\ b_2\,c_2\,d_2\,a_2 \end{matrix}\right|$, sustitución circular que, junto con con la anterior, constituye la sustitución propuesta, representada ahora por $S = \left|\begin{matrix} a_1\,b_1\,c_1 \\ b_1\,c_1\,a_1 \end{matrix}\right| \left|\begin{matrix} a_2\,b_2\,c_2\,d_2 \\ b_2\,c_2\,d_2\,a_2 \end{matrix}\right| = (a_1\,b_1\,c_1)\ (a_2\,b_2\,c_2\,d_2)$.

Por el modo como hemos operado se comprende que toda sustitución puede transformarse en un producto de sustituciones circulares.

A las sustituciones circulares cuyo producto forma una sustitución, se les llama *ciclos*, y la operación mediante la cual se obtienen éstos, se llama *descomposición de una sustitución en sus ciclos*. En realidad, más que una descomposición es sólo una manera de ordenar los elementos formando ciclos con ellos.

Se ha llamado *descomposicion* por la analogía que tiene con la descomposición de un número en sus factores primos, pues así como ésta de cualquier modo que se efectúe resultan siempre los mismos factores, en la descomposición en ciclos se obtienen los mismos aunque se empiece por distinto elemento, es decir, que *la descomposición de una sustitución en sus ciclos es única.* En efecto: si en la sustitución anterior S empezamos por el elemento $\begin{vmatrix} c_2 \\ d_2 \end{vmatrix}$ obtendremos $\begin{vmatrix} c_2 & d_2 & a_2 & b_2 \\ d_2 & a_2 & b_2 & c_2 \end{vmatrix}$, que es el mismo ciclo $\begin{vmatrix} a_2 & b_2 & c_2 & d_2 \\ b_2 & c_2 & d_2 & a_2 \end{vmatrix}$ ordenado de otro modo. Siguiendo con $\begin{vmatrix} b_1 \\ c_1 \end{vmatrix}$, uno de los tres elementos que quedan, obtenemos $\begin{vmatrix} b_1 & c_1 & a_1 \\ c_1 & a_1 & b_1 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ b_1 & c_1 & a_1 \end{vmatrix}$ por tanto la sustitución propuesta tendrá la forma: $S = (a_2\, b_2\, c_2\, d_2)\ (a_1\, b_1\, c_1\, d_1)$; pero como las letras del segundo ciclo son distintas de las del primero, puede cambiarse el orden de los factores circulares sin que cambie su producto, luego $S = (a_1 b_1 c_1)\ (a_2 b_2 c_2 d_2)$ nos demuestra que en ambos casos la descomposición es la misma.

Se llaman *sustituciones semejantes* á dos sustituciones que, teniendo igual número de ciclos, un ciclo cualquiera de una de ellas tiene el mismo número de letras que otro ciclo de la otra. La sustitución $T = (a\, b\, c\, d)\ (f\, g\, h)$ es semejante á la S.

La sustitución cuyos ciclos tienen todos igual número de letras se llama *sustitución regular:* así la sustitución $V = (a\, b\, c)\ (d\, e\, f)$ es una sustitución regular.

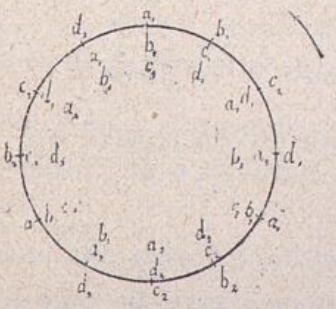

Fig. 3.ª

12. *Potencias de las sustituciones circulares.*—Sea la sustitución de doce letras $S = (a_1\, b_1\, c_1\ d_1\, a_2\, b_2\, c_2\, d_2\, a_3\, b_3\ c_3\, d_3)$, que representaremos, según hemos dicho, por una circunferencia dividida en doce partes iguales, señalando cada uno de los puntos de división por medio de las letras que forman la sustitución y por el orden como están colocadas en ésta. Haciendo girar una división á la circunferencia coincidirán cada dos letras que

forman un elemento de la sustitución S. Para que se comprenda claramente escribimos junto á cada letra, en el interior del círculo, la que le corresponde.

La segunda potencia de S puede obtenerse por el método general, multiplicando $S \cdot S = S^2$, pero no hay necesidad de efectuar este producto por la regla general, porque tomando un elemento cualquiera de S, el $\left|\begin{matrix} a_1 \\ b_1 \end{matrix}\right|$, observamos que á a_1 sustituye b_1 y para formar la segunda potencia, en el otro factor á b_1 sustituye c_1; luego el elemento correspondiente de la segunda potencia es $\left|\begin{matrix} a_1 \\ c_1 \end{matrix}\right|$. Lo mismo ocurre con otro elemento cualquiera; por tanto deducimos que, en la segunda potencia, á cada letra del numerador corresponde la letra que en la circunferencia dista dos divisiones de la primera.

Representada una sustitución circular por medio de una circunferencia, podemos obtener su segunda potencia haciendo que gire dos divisiones en el sentido de la flecha la circunferencia que representa á dicha sustitución, y escribiendo junto á cada punto de división la letra que le corresponda en virtud del giro, letra que, unida á la que ya había, forman los elementos de la segunda potencia pedida. De estas consideraciones se deduce que la segunda potencia de S es $S^2 = \left|\begin{matrix} a_1 b_1 c_1 d_1 a_2 b_2 c_2 d_2 a_3 b_3 c_3 d_3 \\ c_1 d_1 a_2 b_2 c_2 d_2 a_3 b_3 c_3 d_3 a_1 b_1 \end{matrix}\right|$.

Como hemos encontrado la segunda potencia de la sustitución dada encontraríamos la tercera, cuarta, etc., pues sólo tendríamos que repetir los razonamientos anteriores y hacer girar á la circunferencia tres, cuatro ó más divisiones.

En la práctica no hay necesidad de recurrir á la representación gráfica para hallar inmediatamente la potencia m^a de una sustitución circular; basta tener presente que en la potencia á cualquier letra de la permutación superior le corresponde en la inferior la que dista de la primera m lugares. Claro es que, si escribimos la permutación superior en el orden que guardan sus letras en la sustitución dada, la letra que corresponde á la primera de dicha permutación será la que le sigue en m lugares, colocando esta letra bajo de la primera, y á continuación, y par-

tiendo de ella, todas las restantes que hay en la permutación numerador por su orden tendremos formada la potencia pedida.

Como aplicación vamos á formar la potencia quinta de S. El numerador será el de la sustitución S, y la letra que sigue á a_1 en cinco lugares es b_2; á partir de ésta formamos el denominador $b_2\ c_2\ d_2\ a_3\ b_3\ c_3\ d_3\ a_1\ b_1\ c_1\ d_1\ a_2$, y la potencia será $S^5 = \left|\begin{matrix} a_1 b_1 c_1 d_1 a_2 b_2 c_2 d_2 a_3 b_3 c_3 d_3 \\ b_2 c_2 d_2 a_3 b_3 c_3 d_3 a_1 b_1 c_1 d_1 a_2 \end{matrix}\right|$.

También puede obtenerse la potencia m^a de una sustitución circular uniendo de m en m, á partir de un punto dado, los puntos de división de la circunferencia, con lo que se obtiene un polígono convexo estrellado ó una serie de polígonos, según los casos que estudiaremos más adelante.

13. *Orden de las sustituciones.*—Una sustitución circular de n letras sólo tiene n potencias distintas, es decir, *su orden es igual al número de sus letras.* En efecto: por medio de la representación gráfica y el modo como hemos obtenido las distintas potencias de las sustituciones circulares, se deduce que una letra no puede ocupar el lugar que ocupaba en la posición inicial, hasta que por medio de n giros de una división venga á colocarse donde antes estaba; y como en cada giro parcial á cada letra corresponde otra distinta, resulta que hay n potencias diferentes.

La primera potencia que se repite es la S^n, pues ésta es la posición inicial, que se puede considerar como S^0, ya que escribiendo las letras que le corresponden en el interior se ve que los elementos están formados por letras iguales. A partir de S^n se repiten otra vez todas las potencias de S, por lo cual sólo debemos estudiar las potencias de grado inferior á n.

El orden de una sustitución cualquiera es el mínimo común múltiplo de los órdenes de sus ciclos. Sean A, B, ... D los ciclos de una sustitución S, cuyo orden es m; elevando á m á la sustitución S obtendremos: $S^m = (A\,B\,....D)^m = A^m\,.\,B^m\,....\,D^m = 1$; pero como A, B, ... D tienen diferentes sus letras, para que se verifique esta igualdad es preciso que $A^m = 1, B^m = 1\,....\,D^m = 1$, lo que exige que m sea múltiplo del orden de cada uno de los

ciclos, y como el menor múltiplo es el mínimo común múltiplo de ellos, resulta que m debe ser dicho múltiplo.

Inversamente: cualquier número que no sea el mínimo común múltiplo de los órdenes de los ciclos de una sustitución, no puede ser el orden de la misma. Sea r un número que no es divisible por el orden de algunos de los ciclos de S; al elevar esta sustitución á r obtendremos $S^r = A^r \,.\, B^r \,.... \, D^r$ y como la potencia de grado r de los ciclos cuyos órdenes no dividen á r serán distintas de la sustitución unidad, S^r será distinta también de S^0, luego el mínimo común múltiplo de los órdenes de los ciclos es el número menor para el que se verifica $S^m = S^0$, y por tanto éste es el orden de la sustitución S.

14. *Formas de las potencias de una sustitución circular.*— Las potencias de una sustitución circular pueden representarse por medio de polígonos inscritos en la circunferencia que representa la sustitución circular, y cuyos lados subtienden m divisiones, siendo m el grado de la potencia. Esta representación nos servirá para demostrar el siguiente teorema:

Si el grado de la potencia de una sustitución circular es primo con el número de letras de ésta, dicha potencia es otra sustitución circular, y si el grado y el número de letras tienen un factor común, la potencia es una sustitución regular, cuyo número de ciclos es el factor común.

1.° Sea S una sustitución circular, cuyo número de letras, n, es primo con m. Representada la sustitución circular por medio de una circunferencia, si queremos encontrar la potencia m^a de la sustitución dada, hay que unir de m en m los puntos de división hasta llegar al primero por que se empezó; esto último sucede al tener recorridas $m \,.\, n$ divisiones. El polígono tiene n vértices, en cada uno de los cuales hay una letra de las que forman la sustitución circular, y si lo recorremos siguiendo el perímetro en el sentido en que se escribieron las letras, leeremos la potencia pedida, que es una sustitución circular por que podemos recorrer de la primera á la última de sus n letras.

Propongámonos encontrar la segunda potencia de la sustitución circular $S = (a\,b\,c\,d\,f\,g\,h\,i\,j)$. Uniendo de dos en dos las divisiones de la circunferencia (fig. 4.ª), resulta el polígono es-

trellado $a\,c\,f\,h\,j\,b\,d\,g\,i\,a$, cuyos vértices, señalados por las letras de la sustitución S, forman la segunda potencia de ésta, ó sea $S^2 = (a\,c\,f\,h\,j\,b\,d\,g\,i)$.

Consecuencia.—Si el número de letras de una sustitución circular es primo absoluto, todas sus potencias son sustituciones circulares.

2.° Sea $n = r\,.\,p$ el número de letras de la sustitución circular S, $m = s\,.\,p$ el grado de la potencia que se pide, y p el máximo común divisor de n y m. Siguiendo el mismo procedimiento que antes, uniremos, partiendo del primer punto de división, los puntos que distan entre sí m divisiones, continuando de este modo hasta llegar al de partida, lo que se obtiene cuando se han recorrido $r\,.\,s\,.\,p$ divisiones, puesto que $r\,.\,s\,.\,p$ es el mínimo común múltiplo de n y m; pero como se han unido de m en m divisiones, sólo habrá en el polígono $\frac{r\,.\,s\,.\,p}{m} = \frac{r\,.\,s\,.\,p}{s\,.\,p} = r$ vértices, y por tanto obtendremos una sustitución circular en la que entran r de las n letras de S. Para obtener los ciclos que faltan repetiremos la operación empezando por uno de los puntos no recorridos aún, y seguiremos hasta pasar por todos.

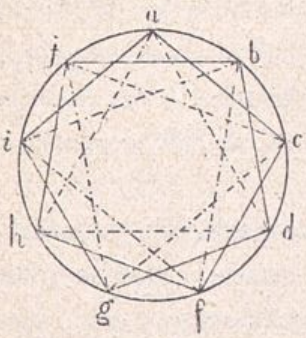

Fig. 4.ª

Como en cada una de estas operaciones encontramos una sustitución circular de r letras, resulta que habrá $\frac{n}{r} = p$ de estas sustituciones circulares, y todas juntas formarán la potencia pedida.

Aplicando lo que acabamos de decir á la sustitución $S = (a\,b\,c\,d\,f\,g\,h\,i\,j)$, resulta para sexta potencia de la misma una sustitución regular compuesta de tres ciclos, $S^6 = (ahd)\,(bif)\,(cjg)$, representada en la figura 4.ª por tres triángulos equiláteros.

Observaciones.—Cuando m sea un divisor de n, el número de ciclos es m.

Si la potencia á que se eleva la sustitución dada fuese igual al número de letras (ó un múltiplo de este número), se obtendría

la sustitución unidad, para la cual es cierto el teorema, si consideramos sus elementos $\left|\begin{matrix} a \\ a \end{matrix}\right|, \left|\begin{matrix} b \\ b \end{matrix}\right|$ .... como ciclos de una sola letra; admitiendo este convenio puede representarse la sustitución unidad por $U = (a)\,(b)\,\ldots\,(e)$.

Teorema.—Toda sustitución regular de m ciclos puede considerarse como la potencia de grado m de cierta sustitución circular. —En efecto; si tenemos una sustitución regular de m ciclos y cada ciclo tiene p letras, el número de letras que hay en la sustitución es $n = m \,.\, p$. Dividiendo la circunferencia en $m \,.\, p$ partes iguales, podremos colocar en una de las divisiones la primera letra del primer ciclo de los m que tiene la sustitución propuesta; á m divisiones de ésta colocaremos la segunda letra de dicho primer ciclo, y seguiremos así hasta colocar la última letra del primer ciclo, y como la letra que sigue en la circunferencia á m lugares de la última es la primeramente colocada, tenemos representado el primer ciclo. El segundo ciclo se representa del mismo modo, partiendo de su primera letra, que se coloca en la división contigua á la en que se ha colocado la primera letra del primer ciclo, la segunda á m divisiones de ésta, y así sucesivamente hasta tener representado el segundo ciclo.

Continuando de este modo la representación de los demás ciclos, obtendremos sobre la circunferencia una sustitución circular de $m \,.\, p$ letras iguales á las $m \,.\, p$ de la sustitución regular, y leyéndolas tal como aparecen ordenadas sobre dicha circunferencia, obtendremos una sustitución circular que, elevada á la potencia de grado m, dará la sustitución regular propuesta.

15. *Potencias de las sustituciones regulares.*—Las potencias de las sustituciones regulares, así como las de una sustitución cualquiera, son muy fáciles de deducir como consecuencia de las potencias de las circulares, porque descompuestas en sus ciclos, cada uno de éstos se puede considerar como una sustitución circular y reducir este caso al anterior por medio de esta proposición:

La potencia de grado q de una sustitución cualquiera se obtiene elevando á la potencia q cada uno de sus ciclos. Sea la sustitución $S = (a_1\, b_1\, c_1\, d_1)\ (a_2\, b_2\, c_2)\ (a_3\, b_3\, c_3)$, que elevada á la

potencia q se transforma en $S^q = [(a_1\, b_1\, c_1\, d_1)\,(a_2\, b_2\, c_2)\,(a_3\, b_3\, c_3)]^q$ $= (a_1\, b_1\, c_1\, d_1)\,(a_2\, b_2\, c_2)\,(a_3\, b_3\, c_3) \ldots\ldots (a_1\, b_1\, c_1\, d_1)\,(a_2\, b_2\, c_2)\,(a_3\, b_3\, c_3)$; pero como cada dos de los ciclos que componen la potencia son iguales ó no tienen letras comunes, serán cambiables, y por tanto $S^q = (a_1\, b_1\, c_1\, d_1) \ldots\ldots (a_1\, b_1\, c_1\, d_1)\,(a_2\, b_2\, c_2) \ldots\ldots (a_2\, b_2\, c_2)\,(a_3\, b_3\, c_3)$ $\ldots, (a_3\, b_3\, c_3) = (a_1\, b_1\, c_1\, d_1)^q\ (a_2\, b_2\, c_2)^q\ (a_3\, b_3\, c_3)^q$, según queríamos demostrar.

Aplicando á las sustituciones regulares la propiedad que acabamos de demostrar, se deduce:

1.° Si el grado de la potencia á que se eleva una sustitución regular es un número primo con el número de letras de cada ciclo, la sustitución potencia es otra sustitución semejante á la dada.

2.° Cuando el grado q y el número p de letras de los ciclos de una sustitución regular en la que hay m ciclos, tienen á q_1 por máximo común divisor, la potencia es otra sustitución regular de q_1 m ciclos. Esto se comprende fácilmente, pues al elevar cada ciclo de la sustitución primitiva á la potencia q, resulta una sustitución regular de de q_1 ciclos.

Si $q_1 = q$, el número de ciclos es $q \,.\, m$.

Respecto á las potencias de una sustitución cualquiera S compuesta de m_1 ciclos de p_1 letras, m_2 de p_2 .... m_r de p_r, se deduce fácilmente que si el grado de la potencia á que se eleva es primo con $p_1, p_2 \ldots\ldots p_r$, la potencia es una sustitución semejante á la dada, y si el grado no es primo con todos ó algunos de los números $p_1\, p_2 \ldots\ldots p_r$, llamando $d_1\ d_2 \ldots\ldots d_r$ al máximo común divisor del grado k y dichos números, la potencia k^a tiene $m_1\, d_1 + m_2\ d_2 + \ldots\ldots + m_r\ d_r$ ciclos, y será una sustitución regular si $\dfrac{p_1}{d_1} = \dfrac{p_2}{d_2} = \ldots\ldots = \dfrac{p_r}{d_r}$.

De estas consideraciones se deduce que una potencia de una sustitución cualquiera no puede ser una sustitución circular.

En el caso particular de una sustitución formada por dos ciclos, uno que tenga el número de sus letras primo con el grado de la potencia á que se eleva, y el otro ciclo con tantas letras como unidades tiene el grado, parece que se obtiene para potencia de este grado una sustitución circular, pues al elevar el primer ciclo se obtiene una sustitución circular, y al elevar el

segundo la sustitución unidad; pero como esta última tiene tantos ciclos como letras, aunque podemos prescindir de ellos, conviene tenerlos en cuenta para que entren á formar la potencia todas las letras que formaron la base. Por tanto la potencia pedida estará formada por una sustitución circular y los ciclos de la sustitución unidad.

Si en una serie de operaciones han de extraerse algunas raíces, no se puede prescindir de los ciclos de la sustitución unidad. Sea, por ejemplo, $S = (a\,b\,c)\ (d\,f\,g\,h)$ una sustitución y su tercera potencia $S^3 = (a\,b\,c)^3\ (d\,f\,g\,h)^3 = (a)\,(b)\,(c)\,(d\,h\,g\,f)$. Si prescindimos de los ciclos $(a)\,(b)\,(c)$, resulta $S^3 = (d\,h\,g\,f)$, que es la misma tercera potencia de S para todas las operaciones menos para la extracción de raíces, pues si extraemos la raíz cúbica de los dos miembros de esta expresión, resulta según la definición de raíz $\sqrt[3]{S^3} = S$ y $\sqrt[3]{(d\,h\,g\,f)} = \sqrt[3]{(d\,f\,g\,h)^3} = (dfgh)$. Ahora bien; S debía ser igual á $(d\,f\,g\,h)$, resultado contradictorio, (ya que $S = (a\,b\,c)\ (d\,f\,g\,h)$, que proviene de no tener en cuenta los ciclos mencionados.

III

RAÍCES DE LAS SUSTITUCIONES

16. *Raíces de una sustitución circular.*—Hemos demostrado que las potencias de una sustitución circular son sustituciones circulares ó regulares; ahora vamos á intentar resolver el problema inverso, ó sea encontrar la raíz de cierto grado de una sustitución circular.

Las raíces de una sustitución circular son sustituciones circulares, porque si una de estas raíces suponemos que no es una sustitución regular, descompuesta en sus ciclos y elevada á la potencia de grado igual al de la raíz de que se trata, no podrá reproducir la sustitución circular dada, pues nunca la potencia

de una sustitución es otra sustitución circular si ella misma no lo es, y además el grado de la potencia á que se eleva no es primo con el número de sus letras; luego la raíz de una sustitución circular será otra sustitución circular, y para que sea posible extraer dicha raíz es preciso que el grado de ésta sea un número primo con el número de letras de la sustitución.

Si la raíz que se pide cumple las condiciones dichas, puede extraerse inmediatamente con sólo colocar sobre una circunferencia dividida en n partes las n letras de la sustitución dada, de manera que cada letra, por el orden en que aparecen en la sustitución circular dada, ocupe uno de los vértices del polígono que se forma uniendo los puntos de división de la circunferencia que distan entre sí tantas divisiones como unidades tiene el grado de la raíz.

La raíz pedida es la sustitución circular que tenemos representada sobre la circunferencia, porque para elevarla á la potencia del mismo grado que el de la raíz propuesta, tendríamos que unir por medio de rectas los puntos de división que distan entre sí un número de divisiones igual al grado, y esto equivale á formar el polígono tal como lo acabamos de decir.

Sea la sustitución circular de nueve letras $S = (agbhcidjf)$, cuya raíz quinta nos proponemos encontrar siguiendo el procedimiento expuesto. Dividiendo la circunferencia en nueve partes iguales, uno de los puntos de división lo señalaremos por a, primera letra de S (fig. 5.ª); en la raíz que buscamos la letra g, que sigue á la a, debe estar á cinco lugares de ésta; la b, que sigue á la g, también la colocaremos á cinco divisiones de la anterior, y así sucesivamente. Es posible operar de este modo hasta llegar á la última, sin que ninguna de ellas recaiga en alguno de los puntos ya ocupados, porque el grado de la raíz, que es 5, cumple la condición de ser primo con nueve, número de letras de la sustitución. Por tanto, la raíz quinta de S es $\sqrt[5]{(agbhcidjf)} =$

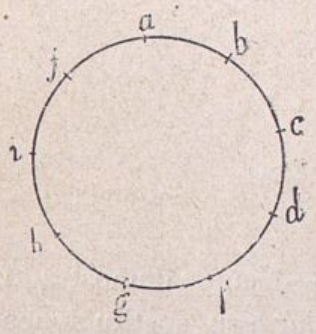

Fig. 5.

$(a\,b\,c\,d\,f\,g\,h\,i\,j)$; resultado cuya exactitud puede comprobarse elevándolo á la quinta potencia.

En la extracción de raíces de las sustituciones circulares sólo debe considerarse el caso en que el grado de la raíz pedida sea menor que el número de letras de la sustitución, porque si fuese mayor se reduce á aquél. En efecto: si el índice k es mayor que el número n de letras de la sustitución, podrá ponerse bajo la forma $k = n \cdot q + r$, llamando R á la raíz k^a de la sustitución circular S, tendremos: $\sqrt[k]{S} = \sqrt[nq+r]{S} = R$, y elevando á la potencia k, $S = R^k = R^{n \cdot q + r} = R^{n \cdot q} \cdot R^r$; pero como ya hemos dicho que R es una sustitución circular de n letras $R^{n \cdot q} = 1$, y por tanto $S = R^r$, luego $\sqrt[r]{S} = R$ é igualando $\sqrt[k]{S} = \sqrt[r]{S} = R$, según queríamos demostrar.

Como las sustituciones circulares sólo tienen raíz cuando el grado de ésta es primo con el número de sus letras, y además toda raíz de índice superior á este número se reduce á la extracción de otra de grado menor que dicho número, resulta que una sustitución circular tiene raíz de $\varphi(n)$ grados distintos, siendo $\varphi(n)$ el número de números primos con n y no mayores que él.

17. *Raíces de las sustituciones regulares.*—Hemos demostrado ya que si elevamos una sustitución circular á una potencia cuyo grado no sea un número primo con el número de sus letras, resulta una sustitución regular, y su forma está determinada por las relaciones que existen entre el número de letras de la sustitución y el grado de la potencia.

La raíz que deseamos hallar elevada á la potencia del mismo grado que la raíz pedida, debe reproducir la sustitución regular, para lo cual es preciso que entre el grado de dicha raíz (que luego se ha de convertir en exponente) y la forma de la sustitución que se haya de encontrar como raíz, no existan condiciones de incompatibilidad, porque si no será imposible que al elevar á dicha potencia la sustitución que suponemos raíz, obtengamos la sustitución regular propuesta.

Por último, toda sustitución descompuesta en ciclos puede

considerarse como un producto de sustituciones de letras diferentes, y generalizando la proposición demostrada en el número 9, tendremos que si $S = A \,.\, B \,.... \, T$ es una sustitución representada por sus ciclos, su raíz m^a será $\sqrt[m]{S} = \sqrt[m]{A}\,\sqrt[m]{B}\,....\,\sqrt[m]{T}$.

18. *Casos particulares.*—Vamos á estudiar ahora dos casos particulares de la extracción de raíces de una sustitución regular de m ciclos que nos servirán para resolver el problema en general.

Caso 1.°—Cuando el grado de la raíz de una sustitución regular de m ciclos, cada uno de los cuales tiene p letras, es igual al número de ciclos, la raíz de ese grado de la sustitución dada puede ser siempre una sustitución circular de m . p letras, porque una sustitución circular de $m \,.\, p$ letras elevada á la potencia de grado m produce una sustitución regular de m ciclos que tienen p letras cada uno.

El modo de encontrar la sustitución raíz es muy sencillo: basta recurrir á la división de la circunferencia en $m \,.\, p$ partes iguales, colocar la primera letra del primer ciclo en uno de los puntos de división, la segunda del mismo ciclo á m divisiones de la primera, y así hasta las p letras que contiene el ciclo. La primera letra del segundo ciclo se coloca en la segunda división, á partir de la primera letra que se escribió, la segunda á m lugares de la primera del segundo ciclo, y se sigue así hasta tener escritas las demás, continuando con los ciclos restantes hasta operar con todos. De este modo se obtiene la representación sobre la circunferencia de una sustitución circular de $m \,.\, p$ letras, y que tendrá por potencia m^a la sustitución regular dada.

Como ejercicio propongámonos extraer la raíz cúbica de la sustitución regular $T = (a_1\, d_1\, c_2\, b_3)\ (b_1\, a_2\, d_2\, c_3)\ (c_1\, b_2\, a_3\, d_3)$, que tiene tres ciclos, y cada ciclo cuatro letras.

Dividamos la circunferencia en doce partes iguales (fig. 3.ª): en el primer punto de división pongamos la letra a_1, en el que dista de él tres divisiones la d_1, el punto separado de éste por otras tres divisiones lo señalaremos con c_2, y á las tres divisio-

nes de ésta escribamos el b_3. Representado el ciclo primero representaremos el segundo del mismo modo, partiendo de la segunda división, y procederemos de la misma manera con el ciclo tercero, partiendo del tercer punto. Como se ve en la figura aparecerá la sustitución circular $S = (a_1 b_1 c_1 d_1 a_2 b_2 c_2 d_2 a_3 b_3 c_3 d_3)$, que es la raíz cúbica de la sustitución T, puesto que elevada S á la tercera potencia reproduce á aquélla.

Observando la figura 3.ª deducimos que los m primeros puntos de división están señalados por la primera letra de cada uno de los m ciclos de la sustitución propuesta, los m siguientes por las letras que ocupan el segundo lugar en cada uno de dichos ciclos, y lo mismo observaremos para cada agrupación de m letras, luego están juntas las letras que ocupan el mismo lugar en los ciclos de la sustitución T; por tanto, en la práctica no hay necesidad de recurrir al trazado de la circunferencia, basta escribir directamente unas á continuación de otras las letras que ocupan el primer lugar de cada ciclo, á continuación de éstas las del segundo lugar y así todas las demás. Estas letras, escritas en la forma dicha y encerradas dentro de un paréntesis, representan la sustitución circular, raíz de la sustitución regular dada.

Como una sustitución descompuesta en sus ciclos no se altera aunque se cambie el orden de colocación de éstos, ni los ciclos dejan de ser los mismos por empezar por distinta letra, siempre que las demás sigan el orden establecido en el ciclo de que se trata, se deduce que podremos representar la sustitución dada bajo muchas formas cambiando el orden de los ciclos, el orden de colocación de las letras dentro de éstas ó haciendo los dos cambios á la vez; pero las raíces de grado m obtenidas con cada una de estas formas de la sustitución no serán iguales todas.

El número de formas que puede tomar una sustitución regular de m ciclos y cuáles de estas formas dan raíces de grado m iguales ó diferentes, lo estudiaremos en la última parte de nuestro trabajo, con el objeto de no interrumpir la investigación de la extracción de las raíces de una sustitución.

Caso 2.º—La raíz de grado k de una sustitución regular de m ciclos y m . p letras puede tomar siempre la forma de una sus-

titución regular de $\frac{m}{k}$ *ciclos, cada uno de los cuales tenga* $p \,.\, k$ *letras si* k *es divisor de* m*—.*

Si se verifica la condición $m = k \,.\, m_1$, los m ciclos de la sustitución dada, pueden agruparse en m_1 secciones de k ciclos, cada una de las cuales formará una sustitución regular, y como estas sustituciones tienen diferentes sus letras, la raíz de grado k de su producto será el producto de las raíces de dicho grado de las m_1 sustituciones; pero cada sustitución regular parcial tiene por raíz de grado k una sustitución circular de $k \,.\, p$ letras, luego el producto de todas las raíces parciales, que es la raíz pedida, estará formado por $m_1 = \frac{m}{k}$ sustituciones circulares de $k \,.\, p$ letras, ó sea una sustitución regular de m_1 ciclos, cada uno de los cuales contiene $k \,.\, p$ letras.

Aplicando lo que acabamos de decir á la sustitución $S = (a_1\, a_2\, a_3)\,(b_1\, b_2\, b_3)\,(c_1\, c_2\, c_3)\,(d_1\, d_2\, d_3)$, para extraer su raíz cuadrada tendremos $\sqrt{S} = \sqrt{(a_1\, a_2\, a_3)\,(b_1\, b_2\, b_3)}\,\sqrt{(c_1 c_2 c_3)\,(d_1 d_2 d_3)}$; las dos raíces cuadradas sabemos extraerlas por el caso anterior; luego $\sqrt{(a_1\, a_2\, a_3)\,(b_1\, b_2\, b_3)} = (a_1 b_1 a_2 b_2 a_3 b_3)$ y $\sqrt{(c_1 c_2 c_3)(d_1 d_2 d_3)} = (c_1\, d_1\, c_2\, d_2\, c_3\, d_3)$; el producto de estas dos sustituciones será la raíz cuadrada pedida, de modo que $\sqrt{S} = (a_1\, b_1\, a_2\, b_2\, a_3\, b_3)\,(c_1\, d_1\, c_2\, d_2\, c_3\, d_3)$.

19. *Teorema.—La condición necesaria y suficiente para que una sustitución regular de m ciclos y orden p tenga raíz de grado k es que m sea múltiplo del producto de los factores comunes á k y p elevados á las potencias que tienen en k.—*

Hemos demostrado que las potencias de una sustitución regular son sustituciones regulares, y que pueden ser también sustituciones regulares las potencias de las sustituciones circulares y las de sustituciones cualesquiera si cumplen las condiciones estudiadas en la segunda parte de nuestro trabajo. Por tanto, la raíz de grado k de una sustitución regular de m ciclos puede ser una sustitución de cualquiera de las tres especies dichas, y á fin de

que la demostración sea general, supondremos que dicha raíz es una sustitución cualquiera.

Sea S una sustitución regular de m ciclos de p letras cada uno y R su raíz de grado k, formada por x_1 ciclos de p_1 letras, x_2 de p_2, y así sucesivamente hasta x_r ciclos de p_r.

Por ser R raíz de grado k de la sustitución regular S, al elevarla á k debe reproducir la sustitución dada, y para efectuar esta operación hay que elevar cada uno de los ciclos de R á la potencia k^a. Ahora bien: si d_1 es el máximo común divisor k y p_1, cada ciclo de p_1 letras al elevarlo á k se convierte en una sustitución regular de d_1 ciclos que tiene $\frac{p_1}{d_1}$ letras; pero estos ciclos son ciclos de la sustitución dada S, por lo que el número de sus letras debe ser p; luego $\frac{p_1}{d_1} = p$. Además, como hay x_1 ciclos de p_1 letras, el conjunto de las potencias de grado k de todos ellos tendrá $x_1 d_1$ ciclos.

Si d_2 es el máximo común divisor de k y p_2, por los mismos razonamientos llegaremos á que en la potencia k^a de R hay $x_2 d_2$ de p letras que proceden de los x_2 de p_2 letras que hay en dicha sustitución, y en general los x_r ciclos de p_r letras se convertirán al elevarlos á k en $x_r d_r$ ciclos, si d_r es el máximo común divisor de k y p_r.

Resulta, pues, que la potencia de grado k de la sustitución R está formada por $x_1 d_1 + x_2 d_2 + \ldots + x_r d_r$ ciclos de p letras; pero como por hipótesis esta potencia es la sustitución regular S que tiene m ciclos, tendremos:

$$x_1 d_1 + x_2 d_2 + \ldots x_r d_r = m \quad \text{(I)}$$

Por ser d_1 el máximo común divisor de k y p_1, los cocientes $\frac{k}{d_1}$ y $\frac{p_1}{d_1} = p$ son primos entre sí, y para que esto se verifique es preciso que d_1 contenga el producto (que representamos por q) de todos los factores comunes á k y p con los exponentes que tienen en k, porque si suponemos que alguno ó algunos de estos factores tienen mayor exponente en k que en p, si no en-

tran en d_1 con el exponente que tienen en k el cociente $\frac{k}{d_1}$ contendrá alguno de dichos factores y no sería primo con p. Queda, pues, demostrado que d_1 es divisible por q.

El producto q será el máximo común divisor de k y p, cuando todas las potencias de los factores primos comunes á k y p tengan menor exponente en k que en p.

Por medio de las mismas consideraciones deducimos que d_2, máximo común divisor del índice k y p_2 es divisible por el producto q, y lo mismo se verifica para los demás máximos comunes divisores hasta d_r.

Resulta, pues, que si R es raíz de grado k de la sustitución regular S, el primer miembro de la igualdad (I) es divisible por q, y el segundo miembro de la misma está obligado á serlo, luego m es un múltiplo de q, según queríamos demostrar.

La condición es suficiente, porque si se cumple la sustitución tiene raíz del grado dicho. En efecto, sea q el producto de los factores de k comunes á p tomados con los exponentes que tienen en k. Si se cumple la condición dicha tendremos: $k = k_1 \cdot q$, $m = m_1 \cdot q$ y la sustitución regular para la cual se verifiquen estas igualdades, tendrá por lo menos una raíz, porque como k_1 es primo con p, puede extraerse la raíz de grado k_1 de cada ciclo de la sustitución dada, el producto de estas raíces será la raíz de grado k_1, y extrayendo raíz q^a del resultado, como en el caso particular segundo, obtendremos la raíz k^a de la sustitución propuesta.

Corolario I.—La raíz k^a de una sustitución regular de m ciclos y $m \cdot p$ letras es otra sustitución regular de las mismas letras y $\frac{m}{k}$ ciclos si el índice de la raíz está formado sólo por factores de p. En efecto: si k sólo contiene factores de p, tendremos, según la notación establecida, $k = q$; los números d_1, d_2 .... d_r tienen todos el factor q, pero no pueden contener otros factores distintos de éstos, porque en k no los hay; luego $d_1 = d_2 .... = d_r = q$, igualdades que reducen la ecuación (I) á

$$(x_1 + x_2 + ... + x_r)\, q = m \text{ ó } x_1 + x_2 + ... + x_r = \frac{m}{q},$$

lo que demuestra el corolario, porque $x_1 + x_2 + \ldots + x_r$ es el número de ciclos de la sustitución raíz y $\frac{m}{q} = \frac{m}{k}$ por ser $k=q$. La sustitución raíz es una sustitución regular, porque si $d_1 = d_2 = \ldots = d_r = q$, $\frac{p_1}{d_1} = p$, $\frac{p_2}{d_2} = p \ldots \frac{p_r}{d_r} = p$, se obtiene $p_1 = p_2 = \ldots = p_r$.

Corolario II.—Cuando el número de ciclos m de una sustitución regular de m . p letras es igual al producto q, se obtiene por raíz de grado k de la sustitución S una sustitución circular. En este caso la ecuación (I) se convierte en

$$x_1 d_1 + x_2 d_2 + \ldots + x_r d_r = q;$$

todos los términos del primer miembro de esta expresión son esencialmente positivos, y $d_1, d_2, \ldots d_r$ son múltiplos de q; luego para que sea posible deben anularse $r - 1$ términos y ser $x_r = 1$ y $d_r = q$.

20. *Extracción de la raíz k^a de una sustitución regular.*— Para que pueda extraerse la raíz de cierto grado de una sustitución regular, es preciso que se cumpla la condición que hemos estudiado en el número anterior, de modo que todas las consideraciones que siguen están fundadas en la hipótesis de que el número de ciclos de la sustitución dada es divisible por el producto de todos los factores que el índice k tiene comunes con p, elevados á las potencias que tienen en k.

Una sustitución regular que cumple la condición dicha siempre tiene por raíz k^a una sustitución regular ó circular que se extrae directamente por medio de la extracción de dos raíces: primero la de grado $\frac{k}{q}$ de cada ciclo y luego la de grado q, agrupando los ciclos de q en q y extrayendo la raíz q^a de cada grupo.

Dada una sustitución regular de m ciclos de p letras cada uno, la extracción de su raíz de grado k depende de la ecuación (I), la cual hay que formar y resolver en números enteros y positivos si queremos obtener para raíz una sustitución cuyos ciclos no tengan todos igual número de letras.

Para que se comprenda más fácilmente el método que vamos á exponer, recordaremos las condiciones á que están sujetas las variables y constantes que entran en la ecuación (I).

Los coeficientes de esta ecuación son $d_1, d_2 \ldots d_r$; según hemos demostrado, tienen todos el factor común q producto de todos los factores comunes á k y p elevados á las potencias con que entran en k. Además son todos distintos unos de otros, porque si hubiera dos iguales d_1 y d_2, por ejemplo, de las igualdades $\frac{p_1}{d_1} = p$ y $\frac{p_2}{d_2} = p$, se deduce que p_1 sería igual á p_2, lo que es contrario á la hipótesis hecha en el número 19. Podemos representar los coeficientes por $d_1 = \delta_1 \cdot q$, $d_2 = \delta_2 q \ldots d_r = \delta_r \cdot q$. En estas igualdades $\delta_1, \delta_2 \ldots \delta_r$ son divisores diferentes de $\frac{k}{q}$ porque $d_1, d_2 \ldots d_r$ son divisores de k, y como los primeros carecen de los factores de q, sólo pueden dividir á $\frac{k}{q}$.

Como incógnitas de la ecuación (I) tomaremos á $x_1, x_2 \ldots x_r$ que son números enteros y positivos, porque representan el número de ciclos de $p_1, p_2 \ldots p_r$ letras respectivamente que tiene la sustitución raíz.

El segundo miembro m es conocido, pues representa el número de ciclos que tiene la sustitución regular dada.

La extracción de la raíz que tratamos de encontrar la dividiremos en dos partes: 1.ª, investigación de la forma de la raíz; 2.ª, extracción de la misma.

La primera parte del problema se resuelve por medio de la ecuación (I), encontrando las soluciones enteras y positivas de la misma. Para simplificar esta ecuación dividiremos sus dos miembros por q, lo que la reduce á

$$\delta_1 x_1 + \delta_2 x_2 + \ldots = \frac{m}{q} = m_1 \text{ (II).}$$

Los coeficientes $\delta_1, \delta_2 \ldots \delta_r$ son divisores indeterminados de $\frac{k}{q}$, por lo cual del cuadro de divisores de este número elegiremos una serie de ellos, de tal manera que su suma no sea supe-

rior á m_1, para que no hagan imposible la ecuación (II); sustituyendo estos divisores en dicha ecuación la resolveremos, si es posible, obteniendo soluciones enteras y positivas. Los valores que resulten para $x_1, x_2 \ldots x_r$ indican el número de ciclos de $p_1, p_2 \ldots p_r$ letras, respectivamente, que tendrá la raíz pedida. El número p_1 se determina por la igualdad $p_1 = p \cdot d_1$, y como $d_1 = \delta_1 \cdot q$ resulta $p_1 = p \cdot \delta_1 \cdot q$, y como δ_1 lo hemos elegido, p_1 queda determinado; análogamente se obtiene el valor de p_2 y en general de p_r.

Por medio de las consideraciones que acabamos de exponer conocemos la forma de la raíz k^a de la sustitución regular S, puesto que hemos determinado el número de sus ciclos y el de letras que tiene cada uno de ellos.

La extracción de la raíz se obtiene aplicando sucesivamente á la sustitución dada los dos principios demostrados en los números 9 y 17. En efecto: cada uno de los ciclos de la raíz que tienen p_1 letras procederá de d_1 ciclos de la sustitución dada, pues éstos tienen p letras y $p \cdot d_1 = p_1$; luego para obtener los x_1 ciclos de la raíz que contienen p_1 letras cada uno necesitamos $x_1 \cdot d_1$ ciclos de la sustitución dada. Separados $x_1 \cdot d_1$ ciclos de ésta, los consideraremos como una sustitución regular, de la que extraeremos la raíz de grado k por partes, extrayendo primero la raíz de grado $\frac{k}{d_1}$ de cada ciclo, lo cual es posible porque $\frac{k}{d_1}$ es primo con p; esta raíz es una sustitución regular de $x_1 d_1$ ciclos y extrayendo de ella la raíz de grado d_1, según el caso particular segundo, se obtiene una sustitución regular de x_1 ciclos de $p \cdot d_1$ letras que es la raíz k^a de los $x_1 d_1$ ciclos de p letras considerados como una sustitución regular.

Siguiendo el mismo procedimiento formaremos otra sección con $x_2 d_2$ ciclos, y extraeremos la raíz $\frac{k}{d_1}$ de cada ciclo, porque por ser $\frac{k}{d_2}$ primo con p tienen todos raíz de ese grado, y del resultado se extrae la raíz de grado d_2, como se hizo en el segundo caso particular. Finalmente, continuaremos haciendo las

mismas operaciones con los ciclos restantes, hasta que llegaremos á encontrar los x_r ciclos de p_r letras.

El conjunto de todas estas raíces de grado k forman una sustitución que es la raíz k^a de la sustitución regular dada, como puede comprobarse elevándola á la potencia k.

Del estudio que hemos hecho de la extracción de raíces de una sustitución regular se deduce que, para obtener como raíz de una sustitución regular otra sustitución que no sea regular ni circular, es preciso que la ecuación (I) ó su equivalente la (II) tengan por lo menos dos términos y puedan resolverse en números enteros y positivos.

Hemos supuesto que era posible la resolución de la ecuación (II) en números enteros y positivos para los valores de δ_1, δ_2 .... δ_r elegidos del cuadro de divisores de $\frac{k}{q}$; pero si no ocurre así podemos tomar otra combinación cualquiera de dichos divisores y ensayarla hasta ver si hace posible dicha ecuación; pero como $\frac{k}{q}$ puede ser un número cualquiera, sus divisores pueden ser tales que no haya ninguna combinación de ellos tomados dos á dos, tres á tres, etc., que hagan posible la ecuación (II), y por tanto la sustitución dada sólo tendrá sustituciones regulares ó circulares por raíces de aquel grado.

Cuando la ecuación (II) admite varias soluciones, cada una de éstas origina una raíz distinta, porque difieren unas de otras en el número de ciclos, si bien éstos se componen de los mismos números de letras p_1, p_2 .... p_r para un mismo sistema de divisores.

A fin de que la teoría expuesta se comprenda con más facilidad, la aplicaremos al siguiente ejemplo:

Investigar la forma de la raíz de grado $k = 2 \cdot 3^2 \cdot 7$ *de una sustitución regular formada por 56 ciclos de dos letras.*

En este caso $m = 56$ $p = 2$ el producto de todos los factores que tiene k comunes con p es $q = 2$, y por tanto la sustitución propuesta cumple la condición de tener raíz del grado di-

cho, pues m es divisible por q; además $\frac{k}{q} = 3^2 . 7\, m_1 = \frac{m}{q} =$ 28 y los divisores de $\frac{k}{q}$ son $\begin{matrix} 1 & 3 & 9 \\ 7 & 21 & 63 \end{matrix}$.

Para formar la ecuación (II) tomaremos un número cualquiera de estos divisores, tres, por ejemplo, $\delta_1 = 7$, $\delta_2 = 1$, $d_3 = 9$, y la ecuación será:

$$7x_1 + x_2 + 9x_3 = 28 \quad \text{(III)}.$$

Las soluciones enteras y positivas de dicha ecuación se obtienen dejando en el primer miembro dos de las incógnitas, cuyos coeficientes sean primos entre sí (para más detalles puede consultarse cualquier tratado de Algebra superior, como por ejemplo el de Ch. Comberausse), y dando á la otra un valor entero y positivo $x_3 = 1$. Resulta así la ecuación $7x_1 + x_2 = 28 - 9 = 19$ que, por tener el coeficiente del segundo término igual á la unidad, se deduce inmediatamente la solución $x_1 = 2$, $x_2 = 5$ que, junto con $x_3 = 1$, forman un sistema de valores de x_1, x_2, x_3 que satisface á la ecuación (III).

Como x_1, x_2, x_3 representan el número de ciclos de cada orden que tiene la sustitución raíz, resulta que habrá dos ciclos de p_1 letras, cinco de p_2 y uno de p_3.

Los números p_1, p_2 y p_3 los obtendremos por medio de las fórmulas $p_1 = p . d_1$, $p_2 = p . d_2$ y $p_3 = p . d_3$; pero como $d_1 = \delta_1 . q$, $d_2 = \delta_2 . q$, $d_3 = \delta_3 . q$, $p = 2$ $\delta_1 = 7$, $\delta_2 = 1$ y $\delta_3 = 9$, sustituyendo estos valores resulta $p_1 = 2 . 7 . 2 = 28$ $p_2 = 2 . 2 = 4$ y $p_3 = 2 . 9 . 2 = 36$.

Tiene, pues, la sustitución raíz que buscamos dos ciclos de 28 letras, cinco de cuatro y uno de treinta y seis.

Si la sustitución dada tiene para la hipótesis hecha $\delta_1 = 7$, $\delta_2 = 1$, $\delta_3 = 9$ y $x_3 = 1$, más raíces de grado k podemos obtenerlas investigando las demás soluciones enteras y positivas de la ecuación (III).

La forma general de las soluciones enteras de dicha ecuación es $x_1 = 2 - t$ y $x_2 = 5 + 7\, t$, en las que t puede recibir cualquier valor entero; para x_1 y x_2 tengan valores positivos, basta expresar algébricamente esta condición por medio de las des-

igualdades $x_1 = 2 - t > 0$ y $x_2 = 5 + 7t > 0$ y deducir los límites de t que son $t < 2$ y $t > \frac{5}{7}$; pero como t ha de ser entero, sólo puede tomar los valores $t = 0$ y $t = 1$. Para $t = 0$ se obtiene la solución encontrada directamente, y para $t = 1$ resulta $x_1 = 1$, $x_2 = 12$ y $x_3 = 1$, lo que nos demuestra que hay otra raíz de grado k de la sustitución dada que tiene un ciclo de p_1 letras, doce de p_2 y uno de p_3.

21. *Extracción de raíces de una sustitución cualquiera.*—La extracción de la raíz de cierto grado de una sustitución cualquiera se reduce á la extracción de la raíz del mismo grado de varias sustituciones regulares.

Sea M una sustitución cualquiera formada por $m_1, m_2 \ldots m_r$ ciclos que tienen $p_1, p_2 \ldots p_r$ letras, respectivamente, y R la raíz de grado k de la sustitución M. Los ciclos de esta última sustitución podremos agruparlos de modo que estén juntos los que tengan el mismo número de letras, ya que por este cambio de factores no dejará de ser la misma la sustitución propuesta. Si llamamos $M_1\ M_2 \ldots M_r$ á las sustituciones regulares formadas con los ciclos de $p_1, p_2 \ldots p_r$ letras de la sustitución M, quedará representada por $M = M_1 . M_2 \ldots M_r$.

Si la sustitución R es la raíz de grado k de M, elevándola á k debe reproducir á M; por tanto, elevando cada ciclo de R á la potencia k^a, los ciclos que resultan sólo pueden tener $p_1, p_2 \ldots p_r$ letras; pero como las potencias de las sustituciones circulares sólo pueden ser sustituciones circulares ó regulares, cada ciclo de la raíz elevado á k sólo puede producir ciclos de igual orden, siendo éste uno cualquiera de los números $p_1, p_2 \ldots p_r$.

Representando por X el producto de todos los ciclos de R, cuya potencia de grado k sea de orden p_1, representando por Y el producto de los que la tienen de orden p_2, y así sucesivamente hasta Z, que representará el producto de los ciclos, cuya potencia k^a sólo tiene ciclos de p_r letras, tendremos representada la sustitución raíz por $R = X\ Y \ldots Z$, igualdad en la cual $X = \sqrt[k]{M_1}$, puesto que X sólo está formada por los únicos ciclos de R que, elevados á k, producen ciclos de p_1 letras, y por la

misma razón $Y = \sqrt[k]{M_2}$ y así hasta $Z = \sqrt[k]{M_r}$. Por tanto, la raíz que buscamos será $R = \sqrt[k]{M_1}\,\sqrt[k]{M_2} \ldots \sqrt[k]{M_r}$, expresión que demuestra que *la raíz de cierto grado de una sustitución cualquiera es el producto de las raíces de igual grado de las distintas sustituciones regulares de que se puede suponer formada la sustitución propuesta.*

Es claro que si alguna de las sustituciones regulares que componen la sustitución M no tiene raíz del grado k, la sustitución dada tampoco la tendrá.

Resulta de todo lo expuesto, que la condición que debe cumplir una sustitución cualquiera para tener raíz de cierto grado, es que, descompuesta en sus ciclos, las sustituciones regulares que con ellos pueden formarse tengan todas raíz de dicho grado.

ESTUDIO DE LAS RAÍCES CIRCULARES

DE UNA

SUSTITUCIÓN REGULAR DE «M» CICLOS

---

1. *Número de formas de una sustitución regular.*—En el caso particular primero, expuesto en el número 18, indicamos que la raíz de forma circular y de grado m que se obtiene de una sustitución regular de m ciclos no es la misma en general, si cambiamos el orden de los ciclos que la representan ó el orden de las letras dentro del ciclo, sin que varie éste, ó efectuamos ambos cambios á la vez. Vamos, pues, á investigar qué formas de S tienen iguales su raíz de forma circular y grado m, y cuáles la tienen diferente.

Sea $S = (a_1\ a_2 \ldots a_p)\ (b_1\ b_2 \ldots b_p) \ldots (t_1\ t_2 \ldots t_p)$ una sustitución regular de m ciclos de orden p.

Si á los ciclos de la sustitución S los hacemos cambiar de lugar de todos los modos posibles sin que dejen de empezar por la misma letra que en la forma dada, se obtienen con ellos $1 \cdot 2 \cdot 3 \ldots m = m!$ permutaciones: uno cualquiera de los m ciclos de S puede escribirse de p maneras distintas sin dejar de ser el mismo; luego si en las $m!$ permutaciones de ciclos obtenidas suponemos invariable la forma de todos los ciclos menos uno, y que éste se escribe de las p formas posibles en cada una de las permutaciones dichas, obtendremos $m! \times p = H_1$, formas de representación de S en que sólo varía el modo de representar uno de los ciclos. Haciendo que otro ciclo distinto del anterior tome sus p formas en cada una de las H_1 que acabamos

de obtener, habrá $H_1 \times p = m ! p^2 = H_2$ formas de S, en que sólo dos ciclos han variado de todos los modos posibles. Continuando así llegaremos á hacer variar el último de los m ciclos, que dará

$$1 . 2 . 3 .... m . p^m = H_m ,$$

que es el número de formas que puede tomar la sustitución dada sin dejar de ser la misma.

Con el objeto de facilitar el estudio de las raíces circulares de grado m, de la sustitución S, representaremos cada ciclo por la letra mayúscula igual á la minúscula que hay en él, poniendo como subíndice de la mayúscula el de la primera letra del ciclo. Haciendo uso de esta notación representaremos la sustitución S por $S = A_1 B_1 C_1 .... T_1$; esta forma de S es la forma bajo la cual la hemos escrito al principio, y por esto la consideraremos como *forma primitiva.*

Las demás formas se obtienen cambiando de lugar las letras A B .... T y poniéndoles subíndices que pueden variar de *1* hasta p.

2. *Obtención de las raíces iguales.—Las formas de una sustitución regular de m ciclos qne tienen sus raíces de grado m iguales á la de otra forma* S_φ *conservan en la colocación de sus ciclos el orden de sucesión que tienen éstos en* S_φ, *aunque en general no conservan el lugar, y los subíndices de los ciclos se diferencian de los que tienen sus iguales de* S_φ *en* $r + 1$ *si en la forma que se examina están colocados dichos ciclos detrás del último ciclo de* S_φ *y en r en caso contrario.*

Si consideramos la sustitución S representada por $A_\alpha \ B_\beta$ .... T_τ su raíz m^a será $\sqrt[a]{A_\alpha \ B_\beta \ C_\gamma .... \ T_\tau} = (a_\alpha \ b_\beta \ c_\gamma .... \ t_\tau \ a_{\alpha+1} b_{\beta+1} c_{\gamma+1} .... t_{\tau+1} .... a_{\alpha-1} \ b_{\beta-1} \ c_{\gamma-1} .... t_{\tau-1})$. El segundo miembro de esta igualdad es una sustitución circular que es la raíz m^a de S, obtenida de la forma dicha; otra sustitución circular igual á ésta la obtendremos trasladando su primera letra a_α al último lugar, y la sustitución circular así obtenida también es raíz m^a de S, pero procede de otra forma. En efecto: elevan-

do á m la segunda sustitución circular resulta la igualdad $[(b_\beta\ c_\gamma \ldots t_\tau\ a_{\alpha+1}\ b_{\beta+1}\ c_{\gamma+1} \ldots t_{\tau+1} \ldots a_{\alpha-1}\ b_{\beta-1}\ c_{\gamma-1} \ldots t_{\tau-1}\ a_\alpha)]^m = B_\beta\ C_\gamma \ldots T_\tau\ A_{\alpha+1}$; su segundo miembro es la sustitución S bajo forma distinta á la anterior, lo que nos prueba que las formas $A_\alpha\ B_\beta\ C_\gamma \ldots T_\tau$ y $B_\beta\ C_\gamma \ldots T_\tau\ A_{\alpha+1}$ que tienen iguales sus raíces de grado m, conservan el orden de sucesión de los ciclos que las componen, si bien el ciclo primero ha pasado á ser último, aumentándole una unidad al subíndice $_\alpha$ del mismo.

Trasladando la letra b_β de la raíz últimamente hallada al último lugar, resulta otra sustitución circular que también es raíz m^a de la sustitución S, pues elevándola á m se obtiene á S bajo la forma $C_\gamma \ldots T_\tau\ A_{\alpha+1}\ B_{\beta+1}$, en la que también se cumplen las condiciones del enunciado. Continuando así llegaremos á $T_\tau\ A_{\alpha+1}\ B_{\beta+1}\ C_{\gamma+1} \ldots$ y si para la raíz m^a de esta última, repetimos las operaciones hechas antes, obtendremos la sustitución dada bajo la forma $A_{\alpha+1}\ B_{\beta+1}\ C_{\gamma+1} \ldots T_{\tau+1}$. Todas estas formas obtenidas hasta aquí tienen iguales sus raíces m^a y siguen la ley dicha.

Lo mismo que hemos conseguido aumentar una unidad á cada subíndice de la forma primera que hemos tomado, podríamos aumentarla en dos, tres ó más hasta p, pues basta repetir los razonamientos partiendo de la última de todas las formas encontradas, y así llegaríamos hasta $A_{\alpha+p}\ B_{\beta+p}\ C_{\gamma+p} \ldots T_{\tau+p}$, que es la forma de que hemos partido, porque como los subíndices no pueden ser mayores que p, hay que tomar el resto respecto á este número.

Todas las formas de S por las que hemos pasado para llegar otra vez á $A_\alpha\ B_\beta\ C_\gamma \ldots T_\tau$ tienen por sustitución raíz la misma sustitución circular y cumplen las condiciones dichas en el enunciado. En efecto: el conjunto de todas las formas de S que acabamos de encontrar, podemos suponerlo formado por secciones de m formas, siendo primer término de cada sección la for-

ma que tenga colocados sus ciclos en el mismo lugar que lo tiene $A_{\alpha}\ B_{\beta}\ C_{\gamma} \ldots T_{\tau}$ y los $m-1$ términos restantes las formas que se deducen del primero por el cambio sucesivo de su primer ciclo; los subíndices de los ciclos de cada uno de los primeros términos dichos difieren de los subíndices de los ciclos correspondientes de la forma dada en una cantidad constante para todos los ciclos, que puede variar de 1 á $p-1$, según la sección.

Una forma cualquiera de las obtenidas S_{φ} estará incluída en alguna de las secciones y cumplirá la ley respecto á la primera forma de su sección, es decir, que sus ciclos seguirán el orden de sucesión establecido, y los ciclos que tenga á la derecha del T aumentan su subíndice en una unidad. Ahora bien: como los subíndices de la primera forma de la sección en que está S_{φ} difieren en una cantidad constante r de los de $A_{\alpha}\ B_{\beta}\ C_{\gamma} \ldots T_{\tau}$, los subíndices de los ciclos de S_{φ} que siguen á T difieren de los de aquella forma en $r+1$ y los demás en r.

Las formas obtenidas del modo dicho son las únicas que tienen por raíz m^{a} la misma sustitución circular, y toda forma que no esté entre ellas tendrá su raíz m^{a} distinta á ésta. Si una forma no está entre las obtenidas antes, será por no guardar sus ciclos el orden de sucesión que tienen los de la forma de que partimos, ó por no cumplir los subíndices de sus ciclos la condición ya dicha. Si ocurre lo primero, supongamos que el orden que sigan los ciclos de esta forma sea A C B .... T; al extraer su raíz m^{a} en la sustitución circular que se obtiene, la letra a se sustituye por la c, cualquiera que sea el subíndice que les corresponde, mientras que en la raíz anterior la letra a siempre se sustituye por la b, luego estas raíces no son iguales; si el orden de sucesión es el mismo, pero los subíndices no siguen la ley, es decir, que al ciclo B_{β} sigue el $C_{\gamma+\lambda}$, en la sustitución raíz á b_{β} sustituirá $c_{\gamma+\lambda}$, siendo así que antes b_{β} era sustituído por c_{γ}, luego tampoco son iguales las raíces.

Como resumen de todo lo expuesto podemos decir que las formas de una sustitución regular de m ciclos que cumplen res-

pecto á otra de sus formas la condición dicha al principio de este número, tienen su raíz m^a circular igual á la de ésta, y las que no la cumplen la tienen diferente.

El número de formas cuya raíz m^a es la misma sustitución circular es la de $m \cdot p$, lo cual se deduce fácilmente del modo de obtener dichas formas, pues según se ha dicho hay m en cada sección y el número de éstas es p.

3. *Problema.*—La resolución del ejercicio siguiente aclarará estas ideas.

Dada la sustitución regular $S = A_1 B_1 C_1 D_1$, *cuyos ciclos tienen cinco letras, hallar una forma de esta sustitución, cuyo primer ciclo sea* D_2 *y su raíz cuarta igual á la que procede de la forma* $S_\varphi = B_3 A_1 D_4 C_5$.

Como la forma que buscamos debe tener sus ciclos colocados en el orden que los tiene S_φ y el primero de ellos es D_2, podemos representar la forma que buscamos por $D_2 C_\gamma B_\beta A_\alpha$, en la que hay que determinar α, β y γ.

Según la regla dada en el número anterior, todos los subíndices de los ciclos de esta última forma que no sean posteriores á C_γ (C_γ es el ciclo C_5 de S_φ aunque empieza por otra letra) se diferencian en r unidades de los subíndices de los ciclos de S_φ iguales á ellos; como el subíndice del ciclo dado D_2 se diferencia del de su igual en S_φ, ó sea D_4 en -2 unidades, resulta $r = -2$, y los subíndices de los ciclos de la forma buscada que no sean posteriores á C_γ se obtienen disminuyendo en 2 unidades los subíndices de los ciclos que les son iguales en S_φ; luego el valor de γ es $\gamma = 5 - 2 = 3$.

Por estar B_β detrás de C_γ se obtiene β sumándole á 3, subíndice de B en S_φ, la constante $r + 1$, y por tanto en este caso $\beta = 3 + (-2) + 1 = 2$, y por la misma razón $\alpha = 1 + (-2) + 1$.

Para interpretar este valor de α basta tener en cuenta que si á 1, subíndice de A en S_φ se le suman cinco unidades, resulta A_6; pero como los ciclos sólo pueden tener cinco letras, A_6 representará A_1, y entonces $\alpha = 6 + (-2) + 1 = 5$.

De todas estas consideraciones se deduce que la forma buscada es $D_2 C_3 B_2 A_5$, lo que puede comprobarse extrayendo su raíz cuarta de forma circular que, comparada con la de $B_3 A_1 D_4 C_5$, observaríamos que son iguales.

4. *Raíces diferentes.—Las formas de una sustitución regular de m ciclos de p letras cada uno, que tienen raíz m^a circular diferente unas de otras, se obtienen dejando invariables y en su lugar la letra y subíndice que representan uno de los ciclos, y cambiando entre sí de todos los modos posibles las letras y subíndices que representan á los demás ciclos.*

Sea S una sustitución regular de m ciclos de p letras; su representación general será $S = A_\alpha B_\beta C_\gamma \ldots T_\tau$. Si prescindimos de su último ciclo T_τ, los restantes forman una sustitución regular de $m - 1$ ciclos y $(m-1)p$ letras, sustitución que podemos representar por V.

Según hemos demostrado, la sustitución V puede tomar $H_{m-1} = 1 \cdot 2 \cdot 3 \ldots (m-1) p^{m-1}$ formas distintas, estando entre dichas formas las que tienen sus raíces m^a circulares iguales y las que las tienen diferentes. Añadiendo á cada forma, como último ciclo, el ciclo T_τ obtendremos H_{m-1} formas de la sustitución S, con la particularidad de que todas estas formas tienen diferente su raíz m^a de forma circular, según demostraremos inmediatamente.

Dos cualesquiera de estas formas, S_1 y S_2, se compondrán de dos partes: una común á las dos, el ciclo T_τ; otra distinta para ambas, una de las formas que puede tomar la sustitución regular constituída por los demás ciclos de la sustitución S. Representando por V_1 y V_2 á estas dos formas, tendremos $S_1 = V_1 T_\tau$ y $S_2 = V_2 T_\tau$.

Las formas V_1 y V_2 pueden tener la misma raíz circular de grado $m - 1$ ó tenerla diferente.

Examinemos el primer caso. Si V_1 y V_2 tienen igual su raíz $(m-1)^a$ sus ciclos tendrán el mismo orden de sucesión, y si ambas terminan con el mismo ciclo, D por ejemplo, todos los subíndices de V_2 se diferencian en r de los de V_1, y al poner á

T_τ como último ciclo de V_1 y V_2 para obtener S_1 y S_2, se comprende que estas formas de S no tienen igual raíz m^a, porque aunque sus ciclos siguen el mismo orden de sucesión, el subíndice de T_τ no ha recibido en S_2 el incremento r que tienen los demás ciclos.

Si el último ciclo de V_1 no fuese igual al último ciclo de V_2, al colocar á T_τ como último ciclo, se interrumpe el orden de sucesión en S_1 y S_2, pues el ciclo que precede á T_τ no es el mismo en ambas formas, y por tanto éstas tampoco tienen igual su raíz m^a circular.

En el segundo caso, cuando V_1 y V_2 tienen distinta su raíz de grado $m - 1$, el orden de sucesión de sus ciclos será distinto en ambos ó los subíndices no cumplirán la condición estudiada en el número 2 de esta nota, y al colocar el ciclo T_τ á continuación de V_1 y V_2 para obtener S_1 y S_2, estas formas no pueden tener igual su raíz circular de grado m, porque continúan en las mismas condiciones que V_1 y V_2.

Hemos examinado ya todos los casos que pueden ocurrir en la formación de S_1 y S_2, y como en ninguno de ellos hay dos formas que tengan igual su raíz m^a circular, resulta que todas las formas que hemos obtenido del modo dicho tienen diferente su raíz m^a.

Además, no puede haber otras formas que tengan su raíz m^a circular distinta de las anteriores, porque éstas son en número de $(m-1)!\,p^{m-1}$, y como cada raíz puede obtenerse de $m \cdot p$ formas de S, resulta que en total tenemos $(m-1)!\,p^{m-1} \times m \cdot p = m!\,p^m$ formas, que es el número de éstas que puede tener S; por tanto no habrá más, y el teorema queda demostrado, porque fuera de las obtenidas no hay otras.

Para facilitar la demostración hemos supuesto que T_τ ocupaba el último lugar; pero se comprende que puede ocupar un lugar cualquiera, porque bastará hacer las transformaciones necesarias en cada una de las formas obtenidas, para encontrar otras que tengan la misma raíz y el ciclo T_τ ocupe en ellas el lugar deseado.

Como aplicación de la regla dada, vamos á encontrar las raíces cúbicas circulares diferentes de la sustitución regular $S = (a_1\, a_2)\,(b_1\, b_2)\,(c_1\, c_2)$, en la cual $m = 3$ y $p = 2$. El número de formas de esta sustitución es $H^m = 1 \,.\, 2 \,.\, 3 \times 2^3 = 48$ y el de raíces diferentes $H^{m-1}\, 1 \,.\, 2 \,.\, 2^2 = 8$.

Siguiendo la regla se obtienen las formas y raíces como expresa el cuadro siguiente, en el que el ciclo invariable es el $(a_1\, a_2)$:

$$\sqrt[3]{(a_1 a_2)\,(b_1 b_2)\,(c_1 c_2)} = (a_1\, b_1\, c_1\; a_2\, b_2\, c_2)$$

$$\sqrt[3]{(a_1 a_2)\,(b_1 b_2)\,(c_2 c_1)} = (a_1\, b_1\, c_2\; a_2\, b_2\, c_1)$$

$$\sqrt[3]{(a_1 a_2)\,(b_2 b_1)\,(c_1 c_2)} = (a_1\, b_2\, c_1\; a_2\, b_1\, c_2)$$

$$\sqrt[3]{(a_1 a_2)\,(b_2 b_1)\,(c_2 c_1)} = (a_1\, b_2\, c_2\; a_2\, b_1\, c_1)$$

$$\sqrt[3]{(a_1 a_2)\,(c_1 c_2)\,(b_1 b_2)} = (a_1\, c_1\, b_1\; a_2\, c_2\, b_2)$$

$$\sqrt[3]{(a_1 a_2)\,(c_1 c_2)\,(b_2 b_1)} = (a_1\, c_1\, b_2\; a_2\, c_2\, b_1)$$

$$\sqrt[3]{(a_1 a_2)\,(c_2 c_1)\,(b_1 b_2)} = (a_1\, c_2\, b_1\; a_2\, c_1\, b_2)$$

$$\sqrt[3]{(a_1 a_2)\,(c_2 c_2)\,(b_1 b_1)} = (a_1\, c_2\, b_2\; a_2\, c_1\, b_1)$$

Estas son las únicas raíces cúbicas de la sustitución propuesta, y cualquier forma distinta de las anteriores tendrá por raíz cúbica alguna de las raíces incluídas en el cuadro anterior.

VICENTE MARTÍ ORTELLS.

Madrid 6 de Septiembre de 1909.

El día 13 de Diciembre de 1909 se leyó este trabajo y fué aprobado por el tribunal, compuesto de los señores

Dr. D. José Andrés Irueste y García, Presidente.
» » Eduardo León y Ortiz, Vocal.
» » Luis Octavio de Toledo, ídem.
» » José Ruiz Castizo, ídem.
» » Martín Pastells y Papell, Secretario.