Exposición de algunos teoremas clásicos de Teoría de Galois

por

Ricardo San Juan Llosá

SUMARIO.—En este artículo vamos a exponer algunos teoremas clásicos de Teoría de Galois con demostraciones originales, o simplificadas, más sencillas que las expuestas en los tratados, merced a una concadenación conveniente.

1. Cuatro propiedades de los grupos de sustituciones.

He aquí estas cuatro propiedades muy conocidas, en la forma que vamos a utilizarlas.

I. *Todo grupo cíclico de orden primo* p *puede engendrarse por las potencias de una cualquiera de sus sustituciones no idénticas.*

Pues siendo todo $h < p$ primo con p, los exponentes h, $2h$, $3h$, ... $(p-1)h$ forman un sistema completo de números incongruentes (mod. p).

II. Si dos grupos cíclicos de órdenes primos tienen una sustitución común (distinta de la identidad), coinciden.

Basta elegir ésta para engendrarlos.

III. Efectuada la transformación de una sustitución S por otra T aplicando T a las dos permutaciones de S, se ve inmediatamente que

El conjunto de todas las sustituciones permutables con un grupo g, *esto es, que lo transforman en si mismo, es otro grupo, que contiene al* g.

IV. *Si las sustituciones de un grupo de orden* p *son permutables con un grupo de orden* q, *el conjunto de todas las sustituciones del primero (segundo) por cada una del segundo (primero), es otro grupo, cuyo orden es* p q *si aquellos no tienen ninguna sustitución común, salvo, naturalmente, la identidad* (*).

(*) Este grupo se llama *producto directo* de ambos cuando además las sustituciones del segundo son permutables con las del primero o sea cuando cada sustitución de uno es permutable con cada una del otro (véase, por ejemplo, van der Waerden Moderne Algebra, B. I.) Pero esta noción no vamos a utilizarla en este artículo.

Pues si S y S′ son sustituciones del primero y T y T′ del segundo, se tiene:

$$(S\,T)\;(S'\,T') = (S\,S')\;(T_1'\,T')$$

llamando T_1' a la transformada de T por S'^{-1} (inversa de S′), la cual pertenece también al segundo, por ser éste permutable con S′.

Si formamos los productos T S de cada sustitución T del segundo por cada una S del primero, obtenemos el cuadro inverso de este en el grupo total formado con todos los productos S T, cuadro que coincide con el directo de Lagrange, por ser dicho grupo invariante; resultan, pues, los mismos productos S T de éste en orden distinto.

Finalmente, si ambos grupos sólo tienen común la identidad, de $S\,T = S'\,T'$, resulta $S\,S'^{-1} = T^{-1}\,T' = 1$, luego $S = S_1$ y $T = T'$.

2. Propiedades del grupo metacíclico

Se llama *grupo metacíclico* entre p elementos al máximo grupo que contiene como subgrupo invariante al grupo cíclico de orden p: $1, S, S^2, \ldots S^{p-1}$; o al conjunto de todas las sustituciones permutables con este grupo, las cuales forman efectivamente grupo en virtud de (I, III).

I. *La condición necesaria y suficiente para que una sustitución* T *pertenezca al grupo metacíclico entre* p *elementos, es decir, para que sea permutable con el grupo cíclico* $1, S, \ldots S^{p-1}$, *es que transforme la sustitución generatriz*

$$S = (x_0\,x_1\;\ldots\;x_{p-1})$$

en una potencia de ésta.

La condición es necesaria por definición; y recíprocamente, pues de $T^{-1}\,S\,T = S'$, resulta:

$$T^{-1}\,S^h\,T = T^{-1}\,\widehat{(T\,S'\,T^{-1})^h}\;T = T^{-1}\,(T\,S^{ih}\,T^{-1})\,T = S^{ih}$$

II. *El orden del grupo metacíclico entre un número primo* p *de elementos es* p (p — 1). Por esto lo designaremos siempre por $G_{p(p-1)}$.

Basta observar que siendo p primo, todas las potencias de S son un ciclo único; y se obtienen, por tanto, todas las sustituciones que transforman S en una $S^i \pm 1$, escribiendo como numerador la permutación que representa esta y como denominador la de S a partir de cada elemento $x_0, x_1, \ldots x_{p-1}$. Hay, pues, p sustituciones distintas que transforman S en $S^i \pm 1$; y como el número de potencias distintas $S^i \pm 1$ de S es $p - 1$, resultan en total $p\,(p-1)$.

Ejemplo. Si es $S = (91234)$, todas las sustituciones que transforman S en $S^2 = (02413)$, Son:

$$\begin{pmatrix}02413\\01234\end{pmatrix},\ \begin{pmatrix}02413\\12340\end{pmatrix},\ \begin{pmatrix}02413\\23401\end{pmatrix},\ \begin{pmatrix}02413\\34012\end{pmatrix},\ \begin{pmatrix}02413\\40123\end{pmatrix}$$

III. Vemos así que si es T_1 la sustitución que transforma S en S^i, escrita S a partir de x_0, las que la transforman escrita a partir de $x_1, x_2, \ldots x_{p-1}$ son, respectivamente. $S^{-1} T_i$, $S^{-2} T_i$, ... $S^{-(p-1)}$, que salvo el orden forman una fila del cuadro de Lagrange; y obtenemos este resultado:

Si formamos el cuadro de Lagrange del grupo metaciclico $G^{p(p-1)}$ *respecto al cíclico:*

$$\begin{array}{lllll}
1, & S, & S^2, & \ldots & S^{p-1} \\
T_1, & S\,T_1, & S^2 T_1, & \ldots & S^{p-1} T_1 \\
T_2, & S\,T_2, & S^2 T_2, & \ldots & S^{p-1} T_2 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
T_{p-2}, & S\,T_{p-2}, & S^2 T_{p-2}, & \ldots & S^{p-1} T_{p-2}
\end{array}$$

poniendo en la primera columna las sustituciones que dejan invariante x_0, *las sustituciones de cada fila, transforman* S *en una misma potencia* S^i

IV. Estas sustituciones $1, T_1, T_2, \ldots T_{p-2}$ forman grupo por conservar fijo x_0; y para ver que este grupo es cíclico, bastará comprobar que una sustitución es un ciclo de orden $p - 1$. En efecto, si escribimos los indices incrementados en un múltiplo conveniente de i, la sustitución T_i que conserva x_0 y transforma S en S_i es:

$$T_i = \begin{pmatrix} x_0 & x_i & x_{2i} & \ldots & x_{(p-2)i} \\ x_0 & x_1 & x_i & \ldots & x_{p-1} \end{pmatrix},$$

y para que al descomponerla en ciclos se obtenga un ciclo único de orden $p - 1$

$$T_i = (x_1\, x_i\, x_{2i} \ldots x_{(p-1)i}),$$

basta que sea $(p - 1)^i$ el primer múltiplo que da resto 1, lo cual acontece seguramente, porque, siendo p primo, y por consiguiente, primo con todo $i < p$, los indices $i, 2i, \ldots (p-1)i$ forman un sistema (completo) de números incongruentes.

Las sustituciones $1, T_1, T_2 \ldots T_{p-2}$ *del grupo metacíclico* $G_{p(p-1)}$ *que conservan fijo un elemento* x_0, *forman pues, un grupo cíclico de orden* $p - 1$.

V. Pero nótese que este subgrupo $1, T_1, T_2, \ldots T_{p-2}$ no es invariante en $G_{p(1-p)}$; pues al transformar cada sustitución de él por cualquier potencia de S, queda alternada x_0. No son, por tanto, permutables las sustituciones de ambos subgrupos y el grupo metacíclico no es producto directo de estos. Se puede, sin embargo, alterar el orden en *cada* producto del cuadro anterior, porque siendo invariante al grupo cíclico, coinciden el cuadro directo y el inverso. Por consiguiente:

El grupo metacíclico $G_{p(p-1)}$ *de orden* p (p — 1 *se obtiene multiplicando cada sustitución del grupo cíclico de orden* p, *engendrado por* $(x_0\,x_1\,x_2\;\ldots\;x_{p-1})$, *por cada sustitución del grupo cíclico de orden* p — 1, *engendrado por* $(x_1\,x_2\ldots\,x_{p-1})$ *y cada una de éste por una de aquél.*

3. Grupo de la resolvente

I. Recordemos la propiedad fundamental del grupo de Galois que puede verse en cualquier tratado (*).

La condición necesaria y suficiente para que un grupo de sustituciones que conserva todas las relaciones racionales entre las raíces, sea el grupo de Galois, es que toda función racional que admita dicho grupo, pertenezca al campo.

II. Como aplicación inmediata resulta:

El grupo de Galois Γ *de la resolvente de Lagrange obtenido con una función racional* $\varphi(x_d, x_1\ldots x_{n-1})$ *de* p *valores* $\varphi, \varphi_1\ldots\varphi_{-p}$ *se compone de las sustituciones que resultan entre las* $\varphi, \varphi_1\ldots\varphi_{p-1}$ *al aplicar a las* $x_0, x_1, \ldots x_{n-1}$ *las sustituciones del grupo* G *de la ecuación dada.*

Basta observar que toda ecuación racional $\Phi(\varphi, \varphi_1, \ldots\varphi_{p-1}) = o$ entre las $\varphi, \varphi_1, \ldots\varphi_{p-1}$ con coeficientes del campo se convierte por sustitución en una ecuación $F(x_0\,x_1, \ldots x_{n-1})$ que admite las sustituciones de G, luego aquella admite las de Γ; y recíprocamente, si una función $\Phi(\varphi, \varphi_1\ldots\varphi_{p-1})$ admite las sustituciones de Γ, la $F(x_0, x_1\ldots x_{n-1}) \equiv \Phi(\varphi, \varphi_1, \varphi_{p-1})$ admite las de G, luego pertenece al campo.

III. Con razonamiento análogo aún más sencillo, resulta:

El grupo de Galois de cada factor irreducible de una ecuación se compone de las sustituciones que subordinan entre sus raíces las sustituciones del grupo de la ecuación total.

4. Grupo de Galois de la ecuación binómica

Se demuestra muy fácilmente que el grupo de Galois en la ecuación binómica $x^p - a = o$ de grado primo p, en un campo $[\Omega, \varepsilon]$ que contenga una raíz p^a imaginaria, ε de 1, pero ningún valor del radical $\sqrt[p]{a}$, es el grupo cíclico de orden p sobre sus p raíces $x_0, x_1, \ldots x_{p-1}$.

Si el campo $[\Omega, x_0]$ no contiene ninguna raíz p^a imaginaria de 1, pero sí en cambio, un valor x_0 del radical $\sqrt[p]{a}$, las p — 1 raíces restantes.

$$x_1 = \varepsilon\,x_0,\; x_2 = \varepsilon^2\,x_0, \;\ldots\; x_{p-1} = \varepsilon^{p-1}\,x_0$$

(*) Véase, por ejemplo, las *Lecciones de Algebra* de Rey Pastor (3.ª ed.), o el apéndice de nuestra *Teoría de las magnitudes, etc.*, publicada en esta Revista.

son homométicas en dicho campo $[\pi, x_0]$ de las $p - 1$ raíces $\varepsilon, \varepsilon^2, \ldots \varepsilon^{p-1}$ de la ecuación ciclotómica $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$, y como el grupo de esta es el cíclico, resulta en virtud de la definición misma de grupo de Galois o del teorema (3, II), que aquella tiene también como grupo el cíclico sobre $x_1, x_2, \ldots x_{p-1}$.

Por consiguiente, si el campo Ω no contiene ninguna raíz p^a imaginaria de 1, ni ningún valor del radical $\sqrt[p]{a}$, el grupo de Galois en el debe contener como subgrupos el grupo cíclico $1, S, S^2, \ldots S^{p-1}$ engendrado por $S = (x_0\, x_1 \ldots x_{p-2})$ y el $1, T_1, T_2, \ldots T_{p-2}$ engendrado por $(x_1\, x_2 \ldots x_{p-1})$; contiene, pues (2, V) como subgrupo el metacíclico $G_{p(p-1)}$; y como su orden es exactamente $p(p-1)$, en virtud del teorema fundamental sobre adjunción de una ecuación (*), coincide con este. Obtenemos, en resumen, estas tres conclusiones:

I. *El grupo de Galois de la ecuación binómica de grado primo* p *en un campo* $[\Omega, \varepsilon]$ *que contenga una raíz* p^a *imaginaria de* 1, *pero ningún valor del radical* $\sqrt[p]{a}$ *es el grupo cíclico de orden* p.

II. *Si el campo* $[\Omega, x_0]$ *no contiene ninguna raíz* p^a *imaginaria de* 1, *pero sí, en cambio, son valor* x_0 *del radical* $\sqrt[p]{a}$, *el grupo de Galois es el grupo cíclico de orden* $p - 1$.

III. *Si el campo* Ω *no contiene ningún valor del radical* $\sqrt[p]{a}$, *ni ninguna raíz* p^a *imaginaria de* 1, *el grupo de Galois de la ecuación binómica* $x^p - a = 0$ *es el grupo metacíclico* $G_{p(p-1)}$.

5. Irresolubilidad parcial por radicales.

I. La demostración de la imposibilidad de la resolubilidad parcial por radicales expuesta en la obra de Rey Pastor o en el apéndice citado de nuestra Teoria de las magnitudes, que se refiere, naturalmente, o sistemas de intransitividad con un sólo elemento, se generaliza fácilmente a sistemas con varios elementos, y resulta así el siguiente teorema, que vamos a utilizar después.

Si un grupo transitivo G *admite un subgrupo normal intransitivo* G, *los sistemas de intransitividad de este tienen todos igual número de elementos y las sustituciones del grupo* G *transforman siempre los elementos de un mismo sistema en otras pertenecientes también a un mismo sistema, que puede ser o no el anterior.*

Sea, en efecto, $x_0 \ldots x_i \ldots$ un sistema de intransitividad de g; cada elemento x_i de este, resulta de x_0 por una sustitución, S_i, de g en virtud de la intransitividad de g. Sea $y_0 \ldots y_j \ldots$ otro sistema de intransitividad de g, y T la sustitución de G, existente en virtud de la transitividad de G, que transforma x_0 en y_0; la transformada de x_i por T pertenece también al mismo sistema, puesto que resulta de y_0 por $T^{-1} S_i T$, que, como S_i, pertenece a g, por ser g invariante en G.

(*) Véase Rey Pastor Loc. cit. n.° 251 o nuestro apéndice citado.

Los grupos que tienen esta propiedad, de que sus sustituciones transforman elementos de un sistema, en elementos de otro, se llaman *imprimitivos* y estos conjuntos de igual número de elementos, se llaman *sistemas de imprimitividad*. Con esta nomenclatura, el teorema anterior puede enumerarse así:

Todo grupo transitivo que admite un subgrupo normal intransitivo, es imprimitivo, y los sistemas de imprimitividad de este son los sistemas de intransitividad de aquel.

Corolario: *Si un grupo transitivo operá sobre un número primo de elementos no contiene niugún subgrupo invariante transitivo.*

II. Como consecuencia resulta la irresolubilidad parcial por radicales que expresa el siguiente teorema.

Si una ecuación irreducible tiene algunas raíces expresables por. radicales, son todas calculables por radicales.

Pues como al adjuntar sucesivamente las radicales, quedan adjuntadas las raíces expresadas por estos, el nuevo grupo, que es invariante por resultar mediante la adjunción de ecuaciones binómicas no podrá contener ninguna sustitución que altere cada una de aquellas, y forman, por tanto, cada una un sistema de intransitividad. Pero teniendo todos estos sistemas un mismo número de elementos, cada una de las raíces restantes constituirá por sí sola sistema de intransitividad, es decir, quedará invariante por toda sustitución del grupo, que será, por tanto, la identidad.

6. Propiedades de los grupos resolubles o metacíclicos

Veamos ahora que el grupo metacíclico $G_{p(p-1)}$ contiene como subgrupos a los grupos de Galois de las ecuaciones resolubles por radicales que suelen llamarse *grupos metacíclicos o resolubles*, empleando aquí preferentemente la segunda denominación para evitar confusiones con el $G_{p(p-1)}$.

Todo grupo resoluble G *sobre un número primo* p *de elementos, contiene como subgrupo invariante al grupo cíclico de orden* p, *y es, por tanto, subgrupo del metacíclico* $G_{p(p-1)}$ *de orden* p (p — 1).

Formada la cadena G, G_1, G_2 ... G_r, 1 de subgrupos, invariantes cada uno en el anterior y de índice primo en éste, son todos transitivos en virtud del contrarrecíproco del corolario de *I*, 5; y el último es cíclico, por ser de orden primo, siendo este orden exactamente p por la transitividad. Para ver que este grupo es invariante en todos los de la cadena se procede por inducción. Desde luego lo es en G_{r-1} por hipótesis; y si lo es en G_i $(i > r)$, al transformarlo por una sustitución cualquiera T del anterior G_{i-1}, resulta otro subgrupo $T^{-1} G_r T$ del mismo S_i, por ser este invariante en el G_{i-1}; y este subgrupo $T^{-1} G_r T$ ha de tener alguna sustitución común con el primitivo G_r, porque de lo contrario contendría G_i un subgrupo de orden p^2, lo cual no es posible por no ser p^2 divisor de $p!$ Pero teniendo ambos subgrupos una sustitución común, como los dos son cíclicos de orden primo p, coinciden (1, II); o sea que es G_r invariante en G_{i-1}; y en definitivo es G.

7. Ecuaciones sin afecto.

I. Uno de los métodos para la obtención de ecuaciones númericas *sin afecto*, esto es, cuyo grupo de Galois sea el simétrico (*), resulta de aplicar el teorema siguiente, que aquí exponemos con demostración simplificada.

Si un grupo transitivo contiene una transposición $(o, 1)$, *es imprimitivo o coincide con el grupo simétrico.*

Sean $(0, 1), (0, 2), (0, 3) \ldots (0, \mu - 1)$ todas las transposiciones del grupo en que entra 0. Este contiene, por tanto, toda transposición entre los índices $0, 1, 2, \ldots \mu - 1$, y no contiene, en cambio, ninguna (ij) entre uno i de éstos y otro nuevo j, porque entonces contendría también la $(0, j)$, transformada de aquella (ij) por la $(0, i)$. Es, pues, el grupo simétrico si sólo opera con los índices $0, 1, 2, \ldots \mu - 1$; y si hay otro índice μ, la sustitución S_1 que transforma 0 en μ, convierte $0, 1, 2, \ldots \mu - 1$ en nuevos índices distintos de éstos, pues si alguno de aquellos $i_1 < \mu$ se convirtiese en otro $j_1 < \mu$, la sustitución S_1 transformaría la transposición $(0, i_1)$ del grupo en otra (μ, j_1), que según hemos visto no pertenece a él. Sean, pues,

$$\mu, \mu + 1, \mu + 2, \ldots 2\mu - 1$$

los transformados de $0, 1, 2, \ldots \mu - 1$ por S_1; sucede también que no hay ninguna transposición $(i_2 j_2)$, entre uno i_2 de estos $\mu, \mu + 1, \mu + 2, \ldots 2\mu - 1$ y otro j_2 distinto de ellos; pues esta (i_2, j_2) se transformaría por la S_1^{-1} en otra (i_1, j_1) entre uno de los $0, 1, 2, \ldots \mu - 2$ y otro j_1 no perteneciente a ellos; resultando de aquí como antes, que si hay otro índice 2μ, los transformados de aquellos $\mu, \mu + 2, \ldots 2\mu - 1$ por la sustitución S_2, que convierte μ en 2μ, son todos distintos de ellos. Seán estos $2\mu + 2, 2\mu + 2, \ldots 3\mu - 1$.

Así continuando, quedan clasificados los índices en sistemas de μ elementos sin ninguno común,

$$\begin{array}{c}
0, 1, 2, \ldots \mu - 1 \\
\mu, \mu + 1, \mu + 2, \ldots 2\mu - 1 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\nu\mu, \nu\mu + 1, \nu\mu + 2, \ldots n - 1;
\end{array}$$

y como los índices manejados en el razonamiento anterior, y que hemos ido llamando $0, \mu, 2\mu \ldots \nu\mu$, son los de cualquier sistema, resulta que si una

(*) Véase cualquier tratado, por ejemplo, la obra de Bianchi. Gruppi di sustituzioni.

sustitución del grupo convierte un índice cualquiera de un sistema en un indice de otro sistema distinto, transforma todos los de aquél en todos los de éste. Es, pues, el grupo imprimitivo y estos sus sistemas de imprimitividad.

Corolario: *Si el número de elementos es primo, el único grupo transitivo que contiene una transposición es el simétrieo.*

II. Esto permite dar una condición necesaría para que una ecuación tenga afecto:

Si una ecuación irreducible tiene afecto, es decir, si su grupo de Galois no es el simétrico, dos cualquiera de sus raíces pueden expresarse como función racional de las demas.

Pues al adjuntar estas, no pudiendo reducirse el grupo de Galois a la única sustitución posible entre las raíces, debe obtenerse la identidad.

Corolario: *Si una ecuación de grado primo, irreducible en el campo de los números racionales, tiene dos raíces reales y las restantes imaginarias, su grupo de Galois es el simétrico.*

Ejemplo clásico de tales ecuaciones es:

$$x^5 + p x^2 - p x - p = 0$$

siendo p un número primo cualquiera. Desde luego es irreducible en virtud del teorema de *Einsestein,* porque, siendo todos los coeficientes múltiplos de p y el primero igual a 1, el último no es múltiplo de p^2. Además tiene a lo sumo una raíz positiva y otra negativa según la regla de *Descartes.*