ASSOCIAÇÃO PORTUGUESA

PARA

O PROGRESSO DAS CIÊNCIAS

QUARTO CONGRESSO

CELEBRADO NA CIDADE DO PÔRTO
DE 18 A 24 DE JUNHO DE 1942
JUNTAMENTE COM
O XVII CONGRESSO DA ASSOCIAÇÃO ESPANHOLA
PARA O PROGRESSO DAS CIÊNCIAS

TÔMO II

1.ª SECÇÃO — CIÊNCIAS MATEMÁTICAS

PÔRTO
IMPRENSA PORTUGUESA
1943

A NOÇÃO DE GRUPO DE GALOIS E A CONDIÇÃO SUFICIENTE DE RESOLUBILIDADE POR MEIO DE RADICAIS

POR

J. SEBASTIÃO E SILVA

Na maioria dos tratados, a teoria de Galois (forma clássica) aparece exposta com tal desenvolvimento, tal acumulação de conceitos e complexidade de raciocínios, que o principiante, por muito vivo que seja o seu interêsse inicial, desanima ràpidamente e perde a esperança de vir a conhecer, como desejaria, êsse admirável capítulo da Álgebra moderna. Ora não é impossível fazer uma exposição correcta da teoria de Galois, pelo menos no que ela tem de essencial – pondo de parte um grande número de proposições, que de nenhum modo são necessárias para atingir os pontos culminantes da teoria. Isto, porém, não se consegue sem uma certa dificuldade: torna-se indispensável modificar o encadeamento dos raciocínios, fazer novas demonstrações e introduzir até novos conceitos e novas proposições auxiliares.

O objectivo desta nota consiste justamente em indicar um modo de tornar mais breve a exposição duma parte importante da teoria de Galois, tornando-a mais acessível, e contribuindo porventura para o esclarecimento de alguns dos seus aspectos. Como se verá, a condição suficiente de resolubilidade por meio de radicais pode ser apresentada com maior generalidade do que habitualmente se faz – antes ainda de introduzir o conceito de grupo de Galois. Por sua vez, êste conceito é aqui introduzido dum modo

novo, independente de quaisquer considerações relativas a resolventes de Galois ou corpo de Galois.

1—Diremos que uma função racional φ das raízes duma equação algébrica *pertence estrictamente* a um grupo G de substituïções sôbre as raízes da equação, quando as seguintes condições se verificam: 1—a função mantém-se *algèbricamente* invariante para tôdas as substituïções de G; 2—as funções conjugadas de φ são *numèricamente* distintas duas a duas.

Recordemos o conhecido teorema de Lagrange (1): «*Se* $F(z)=0$ *fôr uma equação algébrica de coeficientes situados num corpo* Δ *e* φ *uma função racional das raízes daquela equação, que pertence estrictamente a um grupo,* G, *qualquer função racional das raízes, que se mantenha invariante para as substituïções de* G, *terá o seu valor numérico situado em* Δ (φ).

Sabe-se que tôda a função racional simétrica das raízes duma equação de coeficientes situados num corpo Δ terá o seu valor numérico também situado em Δ. Mas pode isto não suceder ùnicamente com as funções racionais simétricas: podem existir funções racionais não simétricas das raízes, cujo valor pertença ainda a Δ. Introduzamos então a seguinte definição:

Dizemos que um grupo G de substituïções sôbre as raízes de $F(z)=0$ (de coeficientes em Δ) *possui a propriedade* α *em relação a* Δ, quando exista uma função racional φ das raízes, que pertença estrictamente a G e cujo valor numérico esteja situado em Δ. É claro que, se tal sucede com uma função φ que pertence estrictamente a G, o mesmo sucederá, em virtude do teorema de Lagrange, com qualquer outra função racional das raízes que pertença àquêle grupo. Portanto, para saber se um dado grupo G de substituïções sôbre as raízes de $F(z)=0$ possui ou não a propriedade α em relação a Δ, basta proceder do seguinte modo:

1.º—Construir uma função racional φ das raízes de $F(z)=0$ que pertença estrictamente a G.

2.º—Formar a equação $P(z)=(z-\varphi_1)(z-\varphi_2)\ldots(z-\varphi_m)=0$, em que $\varphi_1, \varphi_2, \ldots, \varphi_m$ são as funções conjugadas de φ.

---

(1) Aqui o teorema de Lagrange é apresentado sob uma forma diferente da usual.

3.º—Averiguar se a equação $P(z)=0$ admite pelo menos uma raiz pertencente a Δ: conforme isto se der ou não, assim o grupo G possuïrá ou não a propriedade α em relação a Δ (podemos sempre supor escolhida a notação das raízes, de modo que seja φ a raiz pertencente a Δ).

Podemos agora, a partir do teorema de Lagrange, estabelecer sem dificuldade a seguinte proposição:

É condição suficiente para que a equação $F(z)=0$, *seja resolúvel por meio de radicais em relação a* Δ, *que exista, para esta equação, um grupo* G, *resolúvel, que possua a propriedade* α *em relação a* Δ.

Êste teorema pode ser demonstrado, tendo em consideração os seguintes factos:

1.º—Seja G um grupo de substituïções sôbre as raízes de $F(z)=0$ que possua a propriedade α em relação a Δ, H um subgrupo de G e ψ uma função que pertença estrictamente a H: então se forem $\psi_1, \psi_2, \ldots, \psi_p$ as funções conjugadas de ψ em relação a G, podemos afirmar que o grupo G/H de substituïções sôbre os ψ_i possui a propriedade α em relação a Δ. Em particular, os coeficientes da equação $R(z)=(z-\psi_1)\ (z-\psi_2)\ \ldots\ (z-\psi_p)=O$ são elementos de Δ.

2.º—Se H fôr um subgrupo de índice primo de G, o grupo G/H será cíclico.

2—Foi enunciada no parágrafo anterior uma condição suficiente para que uma dada equação seja resolúvel por meio de radicais. Para estabelecer uma condição de resolubilidade por meio de radicais, que seja ao mesmo tempo necessária e suficiente, é indispensável introduzir o conceito do grupo de Galois. Isto pode fazer-se, recorrendo à seguinte generalização do teorema de Lagrange:

Dada uma equação algébrica $F(z)=0$, *de coeficientes situados num corpo* Δ, *se forem* φ *e* ψ *duas funções racionais das raízes dessa equação que pertençam estrictamente aos grupos* H *e* K, *respectivamente, qualquer função racional* χ *que se mantenha algèbricamente invariante para as substituïções do grupo* $H \cap K$ *terá o seu valor numérico situado em* $\Delta(\varphi, \psi)$.

Para demonstrar êste teorema pode seguir-se um método inteiramente análogo ao que utilizamos para a demonstração do teorema de Lagrange, no trabalho «Problemas relativos a funções

racionais das raízes duma equação algébrica» (Port. Math., fasc. 1, vol. 2). Basta considerar as igualdades
$\chi_i = P_o \varphi_i^{n_1-1} + P_1 \varphi_i^{n_1-2} + \ldots + P_{m-1}$ $(i = 1, 2, \ldots, m)$, que formam um sistema de Cramer, quando se tomam P_o, $P_1, \ldots P_{m-1}$ para incógnitas ($\varphi_1 = \varphi, \varphi_2, \ldots, \varphi_m$ são as funções conjugadas de φ em relação a K e $\chi_1, \chi_2, \ldots, \chi_m$ os valores correspondentes de χ). Então é fácil ver que P_o, P_1, ... P_{m-1} são funções racionais das raízes que não mudam algèbricamente para as substituïções do grupo K, o que permite exprimi-las em ψ, por meio de funções inteiras, de coeficientes em Δ.

Desta proposição deduz-se imediatamente o seguinte corolário:

Se os grupos H *e* K, *de substituïções sôbre as raízes de* $F(z) = 0$, *possuem a propriedade* α *em relação a* Δ, *o mesmo sucederá com o grupo* $C = H \cap K$.

Consideremos então o conjunto (A) de todos os grupos de substituïções sôbre as raízes de $F(z) = 0$, que possuem a propriedade α em relação a Δ; é claro que o grupo simétrico pertencerá a (A), mas é possível que outros grupos além dêste pertençam a (A). Seja então G a intersecção de todos os grupos $H_1, H_2, \ldots H_p$ que pertencem a (A): em virtude do corolário anterior, G pertencerá ainda a (A) e recebe o nome de grupo de Galois da equação $F(z) = 0$ em relação a Δ. Podemos assim dizer que o grupo de Galois $F(z) = 0$ em relação a Δ é o menor dos grupos que possuem a propriedade α em relação a Δ.

É fácil ver que esta definição é construtiva, isto é, sugere o caminho a seguir para determinar, efectivamente, o grupo de Galois, da equação proposta. Seria interessante ver agora como, a partir desta definição e de proposições auxiliares, se pode chegar ao critério de resolubilidade de Galois: mas tal excede o objectivo que fixamos a esta nota.

Observaremos, por último, que a generalização atrás enunciada do teorema de Lagrange permite estabelecer, còmodamente, a resolubilidade por meio de radicais das equações cíclicas.

Centro de Estudos Matemáticos de Lisboa.