Matemática Universitária, Nº 5, Junho de 1987, 25-32.

Solução de Equações por Radicais em Característica $p \geq 0$.

Otto Endler

Quando se fala da Teoria de Galois, não se pensa apenas no "teorema fundamental", o qual relaciona os corpos intermediários de uma extensão galoisiana (isto é, separável e normal) finita $N|K$ com os subgrupos do seu grupo de Galois $Aut(N|K)$, mas também na sua mais importante aplicação, a saber, o problema de resolver equações algébricas por meio de radicais. Realmente, foi este problema que motivou Galois a desenvolver a teoria que tem seu nome.

Recordemos que este problema teve um papel muito importante na história da Álgebra. Após a solução das equações do terceiro e quarto grau, conseguida no século XVI por Scipione del Ferro, Tartaglia, Cardano e Ferrari, muitos matemáticos esforçaram-se para resolver a equação do quinto grau, até que, no primeiro terço do século XIX, Abel mostrou a impossibilidade de resolver a equação geral do quinto grau e Galois caracterizou as equações solúveis através da solubilidade do grupo de Galois, definido na época como um certo grupo de permutações das raízes da equação. Mais detalhes podem ser encontrados no livro [5] de Van der Waerden e na "Note historique" de Bourbaki [2].

É óbvio que, nos séculos passados, consideravam-se apenas equações com coeficientes em corpos de característica zero. O problema, entretanto, formula-se da mesma maneira para equações sobre corpos de característica $p \neq 0$, de modo que é natural tentar estender os resultados neste sentido. Esta generalização é devida a Artin [1], que mostra que, no caso da característica $p \neq 0$, além dos radicais usuais $\sqrt[n]{a}$, representando uma raiz de $X^n - a$, se precisa admitir "radicais modificados" $\wedge\underline{a}$ que representam uma raiz do polinômio $X^p - X - a$.

É surpreendente que, em vários livros-textos recentes de Álgebra, esta teoria generalizada ou não se encontra ou é exposta de uma maneira incom-

pleta, apesar de se enquadrar facilmente num curso de Álgebra. De fato, além dos resultados usuais da teoria de Galois e da sua aplicação a extensões ciclotômicas e cíclicas, o único resultado mais "moderno" que se precisa é o teorema de Artin-Schreier sobre extensões cíclicas de grau p de corpos de característica $p \neq 0$, e este se destaca pela sua analogia ao teorema clássico de Kummer sobre extensões cíclicas cujo grau não é divisível pela característica.

Preliminares Sobre Extensões Cíclicas

Sejam K um corpo de característica p (zero ou um número primo) e Ω um fecho algébrico de K. Dado um polinômio separável (isto é, sem raízes múltiplas) $F \in K[X]$, denotamos por $\mathfrak{R}_F$ o conjunto das suas raízes em Ω. O corpo Ω possuirá uma raiz primitiva n-ésima da unidade, ζ_n, se e somente se n não for divisível por p. O corpo $K(\zeta_n) = K(\mathfrak{R}_{X^n-1})$ é chamado a *n-ésima extensão ciclotômica de K*; esta extensão é galoisiana e $Aut(K(\zeta_n)|K)$ é isomorfo a um subgrupo do grupo dos invertíveis do anel $\mathbf{Z}/(n)$; portanto, é abeliano, e sua ordem divide $\varphi(n)$, sendo φ a função de Euler.

Por uma extensão *cíclica* (respectivamente *abeliana*, respectivamente *solúvel*) entendemos uma extensão galoisiana finita $N|K$ tal que $Aut(N|K)$ seja um grupo cíclico (respectivamente abeliano, respectivamente solúvel). Em relação às extensões cíclicas, temos os seguintes teoremas.

Teorema de Kummer. *Suponhamos que K possua uma raiz primitiva n-ésima da unidade. Então, as extensões cíclicas de K de grau n são exatamente os corpos $K(\alpha)$, onde α é uma raiz de um "binômio" irredutível $X^n - a \in K[X]$.*

Note que a hipótese $\zeta_n \in K$ implica que n não é divisível por p.

Teorema de Artin-Schreier. *Suponhamos que $p \neq 0$. Então, as extensões cíclicas de K de grau p são exatamente os corpos $K(\alpha)$, onde α é uma raiz de um "trinômio" irredutível $X^p - X - a \in K[X]$.*

- A analogia entre estes dois teoremas não se restringe ao seu enunciado, mas revela-se também na sua demonstração. De fato, o teorema de Kummer baseia-se na forma multiplicativa e o teorema de Artin-Schreier baseia-se na forma aditiva do seguinte

Teorema 90 de Hilbert. *Seja $N|K$ uma extensão cíclica e seja σ um gerador de $Aut(N|K)$; então vale para todo $\beta \in N$:*

a) $\mathcal{N}\beta = 1$ *se e somente se* $\beta = \alpha \cdot (\sigma\alpha)^{-1}$ *para algum* $\alpha \in L$ (*"forma multiplicativa"*),

b) $\mathfrak{S}\beta = 0$ *se e somente se* $\beta = \alpha - \sigma\alpha$ *para algum* $\alpha \in L$ (*"forma aditiva"*),

onde $\mathcal{N}$ e $\mathfrak{S}$ representam a norma e o traço da extensão $N|K$ (veja por exemplo Lang [4], VIII, 6).

A seguir, queremos mostrar como é fácil desenvolver, a partir dos resultados acima indicados, a teoria de resolver equações por meio de radicais (usuais e modificados), em qualquer característica $p \geq 0$. Demonstrações completas podem ser encontradas em Endler [3].

O resultado final desta teoria pode ser resumido assim:

F é solúvel por radicais sobre $K \Leftrightarrow K(\mathfrak{R}_F)|K$ é solúvel.

O próximo parágrafo é dedicado à prova da implicação " $\Rightarrow$ ".

Extensões Radicais.

É conveniente e usual reduzir o problema de resolver equações por radicais ao estudo de extensões radicais, definidas da seguinte maneira. Uma extensão $L|K$ será chamada *radical* se existirem elementos $\alpha_1, \ldots, \alpha_s \in L$ e inteiros $n_1, \ldots, n_s \geq 1$, não divisíveis por ou iguais a p, tais que $L = K(\alpha_1, \ldots, \alpha_s)$ e, para todo $j \in \{1, \ldots, s\}$:

$$K(\alpha_1, \ldots, \alpha_{j-1}) \ni \begin{cases} \alpha_j^{n_j} & \text{quando } n_j \text{ não é divisível por } p; \\ \alpha_j^p - \alpha_j & \text{quando } n_j = p. \end{cases}$$

É fácil ver que a noção de extensão radical é transitiva e é preservada sob extensão do corpo base. Obviamente, toda extensão radical é separável, e prova-se por indução que está contida numa extensão radical galoisiana. Estes fatos são usados para provar o seguinte:

Teorema 1. *Se a extensão galoisiana N de K estiver contida numa extensão radical L de K, então $N|K$ será solúvel.*

Demonstração. Podemos supor que $L|K$ seja radical galoisiana. Sejam $\alpha_1, \ldots, \alpha_s, n_1, \ldots, n_s$ como na definição acima e seja $m \geq 1$ divisível por todos os n_j distintos de p. Então $L(\zeta_m)|K(\zeta_m)$ é uma extensão radical e galoisiana, e pelos teoremas de Kummer e Artin-Schreier existe uma cadeia de corpos $K(\zeta_m)^L = L_0 \subseteq \cdots \subseteq L_s = L(\zeta_m)$ tais que $L_j|L_{j-1}$ seja cíclica $(j = 1, \ldots, s)$; além disto, $K(\zeta_m)|K$ é abeliana. Como $L(\zeta_m)|K$ é galoisiana, resulta do teorema fundamental da teoria de Galois que $Aut(L(\zeta_m)|K)$ é um grupo solúvel; portanto, $Aut(N|K)$ também o é. □

Diremos que um polinômio mônico e separável $F \in K[X]$ é *solúvel por radicais sobre* K quando todas as suas raízes pertencerem a uma extensão radical L de K, ou seja, se $K(\mathfrak{R}_F) \subseteq L$. Nota-se que, no caso em que F é irredutível, basta exigir que alguma das suas raízes pertença a L. Do Teorema 1 resulta:

Corolário. *Se F for solúvel por radicais sobre K, então a extensão $K(\mathfrak{R}_F)|K$ será solúvel.*

Este corolário já é suficiente para dar exemplos de polinômios *não* solúveis por radicais:

a) O polinômio geral $F_U = X^n - U_1X^{n-1} + \cdots + (-1)^nU_n \in K_U[X]$ do grau n sobre K (onde $K_U = K(U_1, \ldots, U_n)$ e $U_1, \ldots, U_n$ são indeterminadas sobre K) não é solúvel por radicais no caso $n \geq 5$, pois $Aut(K_U(\mathfrak{R}_{F_U})|K_U)$ é isomorfo ao grupo simético $\mathcal{S}_n$.

b) $F = X^5 - 2X^4 + 2 \in \mathbf{Q}[X]$ não é solúvel por radicais, pois

$$Aut(\mathbf{Q}(\mathfrak{R}_F)|\mathbf{Q})$$

é isomorfo a $\mathcal{S}_5$.

Extensões Fortemente Radicais (radicais irredutíveis)

As definições "extensão radical" e "polinômio solúvel por radicais" são muito fracas, o que é conveniente quando elas são usadas como condições suficientes. Neste parágrafo, porém, no qual pretendemos provar a implicação

" $\Leftarrow$ " da equivalência indicada acima, elas ocorrem como condições necessárias. Por isto convém substituí-las por definições mais fortes que refletem a idéia de "radical" de uma maneira mais precisa.

É óbvio que a expressão $\sqrt[n]{a}$, representando uma das raízes do polinômio $X^n - a$, é ambígüa. Na verdade, é tão ambígüa que em geral não determina nem uma classe de elementos conjugados. Da mesma maneira, a condição "$L = K(\alpha)$ com $\alpha^n \in K$" não determina o corpo L nem a menos de um K-isomorfismo. Por exemplo, no caso $\alpha^n = 1$, $L = K(\alpha)$ pode ser a d-ésima extensão ciclotômica de K para qualquer divisor d de n. Além disto, toda extensão ciclotômica $K(\zeta_n)$ é trivialmente uma extensão radical simples (isto é, com $s = 1$), pois $\zeta_n^n = 1 \in K$; em particular, toda extensão finita de $\mathbf{F}_p$ tem esta propriedade. Em vista do Teorema de Artin-Schreier, o fato que $\mathbf{F}_{p^p} = \mathbf{F}_p(\zeta)$ para uma raiz $(p^p - 1)$-ésima da unidade ζ, certamente é de pouco valor e não corresponde à idéia de resolver a equação $X^p - X - 1$ por radicais.

Para fazer com que todos os elementos representados por $\sqrt[n]{a}$ sejam K-conjugados dois a dois, é necessário e suficiente exigir que o polinômio $X^n - a$ seja irredutível em $K[X]$, isto é, que $\sqrt[n]{a}$ seja um "radical irredutível". Além disto, embora sem necessidade, podemos exigir que n seja um número primo. Esta considerações dão origem à seguinte definição: Uma extensão $L|K$ será chamda *fortemente radical* se existirem elementos $\alpha_1, \ldots, \alpha_s \in L$ e números primos $p_1, \ldots, p_s$ tais que $L = K(\alpha_1, \ldots, \alpha_s)$ e, para todo $j \in \{1, \ldots, s\}$, α_j seja raiz de um polinômio irredutível da forma

$$X^{p_j} - \delta_{p,p_j} \cdot X - a_j \in K(\alpha_1, \ldots, \alpha_{j-1})[X]$$

(sendo δ o símbolo de Kronecker).

É óbvio que a noção de extensão fortemente radical é transitiva. Ela é estritamente mais forte que a noção de extensão radical. De fato, é fácil ver que nem toda extensão ciclotômica de um corpo primo é fortemente radical; por exemplo, $\mathbf{Q}(\zeta_{23})|\mathbf{Q}$ e $\mathbf{F}_{5^{11}}|\mathbf{F}_5$ não o são.

Provaremos o recíproco do Teorema 1, com "fortemente radical" em lugar de "radical", primeiramente sob uma hipótese relativa à existência de raízes da unidade em K.

Proposição. *Seja $N|K$ uma extensão solúvel, e suponhamos que $\zeta_m \in K$, sendo $m \geq 1$ divisível por todos os números primos, distintos de p, que dividem $[N : K]$. Então, $N|K$ é uma extensão fortemente radical.*

Demonstração. Pelo teorema fundamental existe uma cadeia de corpos $K = K_0 \subset K_1 \subset \cdots \subset K_s = N$ tais que $K_j|K_{j-1}$ seja cíclica de ordem prima p_j $(j = 1, \ldots, s)$. Aplicando à esta extensão o teorema de Kummer no caso $p_j \neq p$ e o teorema de Artin-Schreier no caso $p_j = p$, concluímos que $N|K$ é fortemente radical. □

Aplicando esta proposição a extensões ciclotômicas, obtemos:

Corolário. *Toda extensão ciclotômica L de K está contida numa extensão ciclotômica fortemente radical de K.*

Demonstração. Seja L a n-ésima extensão ciclotômica de K e seja m o produto dos números primos, distintos de p, que dividem $[L : K]$. Então m divide $\varphi(n)$ e, portanto, $m < n$. Podemos supor, por indução, que a m-ésima extensão ciclotômica de K esteja contida numa extensão ciclotômica fortemente radical K' de K. Então $K' \cdot L$ é uma extensão ciclotômica de K' com $\zeta_m \in K'$, logo, pela Proposição, $K' \cdot L$ é uma extensão fortemente radical de K' e, portanto, também de K. □

Utilizamos este corolário para provar o recíproco do Teorema 1 na seguinte versão forte e sem nenhuma hipótese adicional.

Teorema 2. *Seja $N|K$ uma extensão solúvel. Então existe uma raiz da unidade $\zeta \in \Omega$ tal que $N(\zeta)$ seja uma extensão solúvel e fortemente radical de K.*

Demonstração. Pelo Corolário acima existe uma raiz da unidade $\zeta \in \Omega$ tal que $K(\zeta)|K$ seja fortemente radical e $N(\zeta)|K(\zeta)$ satisfaça as hipóteses da Proposição. Então, $N(\zeta)$ é uma extensão fortemente radical de $K(\zeta)$ e, portanto, também de K. Além disto, $N(\zeta)|K$ é galoisiana, e $Aut(N(\zeta)|K)$ é solúvel, uma vez que $Aut(N(\zeta)|K(\zeta))$ é solúvel e o grupo quociente

$$Aut(N(\zeta)|K)/Aut(N(\zeta)|K(\zeta))$$

é isomorfo ao grupo abeliano $Aut(K(\zeta)|K)$. □

Diremos que um polinômio mônico e separável $F \in K[X]$ é *solúvel por radicais irredutíveis sobre K* se todas as suas raízes pertencerem a uma extensão fortemente radical L de K, ou seja, se $K(\mathfrak{R}_F) \subseteq L$. Do Teorema 2

resulta:

Corolário 1. *Se $K(\Re_F)|K$ for uma extensão solúvel, então F será solúvel por radicais irredutíveis sobre K.*

Concluímos do Corolário 1 que, em particular, os seguintes tipos de polinômios são solúveis por radicais irredutíveis:

a) Todo polinômio (mônico e separável) de grau $n \leq 4$;

b) Todo polinômio ciclotômico sobre qualquer corpo K;

c) Todo polinômio (mônico e separável) sobre qualquer corpo finito.

Em particular, para todo $a \neq 0$, o polinômio irredutível $F = X^p - X - a \in \mathbf{F}_p[X]$ tem esta propriedade, e $\mathbf{F}_{p^p} = \mathbf{F}_p(\Re_F) = \mathbf{F}_p(\alpha)$ para toda raiz α de F, a qual pode ser considerado como radical modificado $\wedge\underline{a}$. Note-se, entretanto, que radicais modificados são indispensáveis também no caso de polinômios $F \in \mathbf{F}_p[X]$ tais que o grau da extensão (necessariamente cíclica) $\mathbf{F}_p(\Re_F)|\mathbf{F}_p$ não seja divisível por p. Por exemplo, se $F \in \mathbf{F}_5[X]$ for um polinômio irredutível de grau 11, então $\mathbf{F}_{5^{11}} = \mathbf{F}_5(\Re_F)$ está contido na extensão fortemente radical $\mathbf{F}_{5^{55}} = \mathbf{F}_5(\alpha, \beta)$ de $\mathbf{F}_5$, sendo α uma raiz do trinômio irredutível $X^5 - X - 1$ e β uma raiz de um binômio irredutível $X^{11} - c \in \mathbf{F}_{5^5} = \mathbf{F}_5(\alpha)$.

Concluímos dos corolários dos Teoremas 1 e 2 que as noções "solúvel por radicais" e "solúvel por radicais irredutíveis" são equivalentes, isto é:

Corolário 2. *O polinômio mônico e separável $F \in K[X]$ será solúvel por radicais irredutíveis se e somente se for solúvel por radicais.*

Por outro lado, em relação às noções correspondentes de "extensão radical" e "extensão fortemente radical", podemos concluir dos Teoremas 1 e 2 apenas o seguinte:

Corolário 3. *Toda extensão radical L de K está contida numa extensão fortemente radical e solúvel N de K.*

Observemos ainda que se o polinômio $F \in K[X]$ for solúvel por radicais, então a extensão $K(\Re_F)|K$ nem sempre é uma extensão radical. Este fato já foi observado por Cardano no famoso "casus irreducibilis" de um polinômio $F = X^3 + aX^2 + bX + c \in \mathbf{Q}[X]$, irredutível de grau 3, com três raízes

reais: Na fórmula de Cardano, que representa estas raízes, aparece o número imaginário $\sqrt{-3D}$, sendo

$$D = a^2 \cdot b^2 - 4b^3 - 4a^3 \cdot c - 27c^2 + 18a \cdot b \cdot c > 0$$

o discriminante deste polinômio. De fato, pode-se demonstrar que, apesar de $\mathbf{Q}(\Re_F) \subseteq \mathbf{R}$, nenhuma extensão radical de $\mathbf{Q}(\Re_F)$ está contida em $\mathbf{R}$.

Referências

[1] ARTIN, E.: *Modern Higher Algebra. Galois Theory.* (Lecture Notes by A. Blank). New York University 1956.

[2] BOURBAKI, N.: *Algèbre,* Chapitres IV-5. Hermann, Paris, 1950.

[3] ENDLER, O.: *Teoria dos corpos.* A ser publicado na série "Monografias de Matemática", IMPA, Rio de Janeiro.

[4] LANG. S.: *Algebra.* Addison-Wesley 1965.

[5] VAN DER WAERDEN, B. L.: *A History of Algebra.* Springer-Verlag 1985.

Instituto de Matemática Pura e Aplicada — CNPq
Estrada Dona Castorina 110 — Jardim Botânico
22.460 Rio de Janeiro, RJ