UMA DISCUSSÃO SOBRE EXTENSÕES ALGÉBRICAS DE SUBCORPOS DO CORPO DOS NÚMEROS COMPLEXOS

SORAYA COSTA SOARES[1], RODRIGO RAFAEL GOMES[2]

[1] Graduando em Licenciatura em Matemática, Bolsista PIBIFSP, IFSP, Câmpus Bragança Paulista, sorayacsoares@yahoo.com.br.
[2] Professor do curso de Licenciatura em Matemática, IFSP, Câmpus Bragança
Área de conhecimento (Tabela CNPq): 1.01.01.05-5 Álgebra Comutativa

Apresentado no
8° Congresso de Inovação, Ciência e Tecnologia do IFSP
06 a 09 de novembro de 2017 - Cubatão-SP, Brasil

RESUMO: A extensão algébrica de um corpo surge quando se quer ampliar um dado corpo, preservando as propriedades que lhe dão essa estrutura e ao mesmo tempo estendendo o número de soluções de uma dada equação polinomial com coeficientes nesse corpo. O propósito do trabalho foi investigar segundo o método hipotético-dedutivo as propriedades mais elementares que caracterizam o conceito de extensão algébrica simples, a partir de pesquisa bibliográfica sobre o tema. Verificou-se que algumas dessas propriedades podem ser estabelecidas a partir de propriedades dos conceitos de ideal e homomorfismo.

PALAVRAS-CHAVE: teoria de Galois; ideais; teorema fundamental do homomorfismo; polinômios; equações algébricas.

A DISCUSSION ABOUT FIELD ALGEBRAIC EXTENSIONS IN THE FIELD OF COMPLEX NUMBERS

ABSTRACT: An algebraic field extension appears when we want to enlarge a certain field maintaining its field properties while extending the number of solutions of a polynomial equation with coefficients on the field. The aim of this work was investigating by hypothetical-deductive reasoning and from a bibliographic research about the elementary properties that describe the concept of simple algebraic extension. It was found that some of such properties can be established from ideal e homomorphism properties.

KEYWORDS: Galois theory; ideals; fundamental homomorphism theorem; polynomials; algebraic equations.

INTRODUÇÃO

Embora a teoria de Galois original tivesse como objeto os polinômios com coeficientes em subcorpos do corpo dos números complexos, uma abordagem mais moderna deslocou o foco dessa teoria para as extensões desses subcorpos. A ideia por trás do conceito de extensão de corpos é, basicamente, a de conceber um corpo maior a partir de um dado corpo de modo que o primeiro tenha propriedades além das já possuídas pelo último. Pode ser desejável, em particular, que seja ampliada a quantidade de soluções, sobre esse corpo, de uma equação polinomial cujos coeficientes sejam elementos desse mesmo corpo. Tomemos como exemplo uma equação que tem duas soluções, de modo que apenas uma está contida no corpo $\boldsymbol{Q}$ dos números racionais e que possua todos os seus coeficientes nesse corpo. Se fosse possível acrescentar a $\boldsymbol{Q}$ a outra solução dessa equação de modo que o resultado dessa união ainda fosse um corpo, teríamos uma extensão de $\boldsymbol{Q}$ que, além de preservar as propriedades algébricas do corpo menor, teria todas as soluções da equação considerada. Isso nos leva ao estudo do conceito de extensão algébrica de um corpo, em particular ao de extensão simples – interessante pelas suas conexões com outros conceitos e importante por suas implicações no estudo da teoria de Galois elementar – cujas propriedades fundamentais discutimos aqui.

MATERIAL E MÉTODOS

O trabalho consistiu de pesquisa bibliográfica sobre o tema, seguindo, principalmente o texto de STEWART (2004), e a metodologia empregada na validação dos resultados foi a hipotético-dedutiva.

Nossa discussão diz respeito a polinômios cujos coeficientes são elementos de um subcorpo do corpo $\boldsymbol{C}$ dos números complexos.

A importância do estudo acerca do conceito de extensão algébrica de subcorpos dos números complexos se dá conforme compreendemos o tema como um assunto preliminar necessário ao estudo da teoria de Galois, cujo fim é o de demonstrar os critérios que permeiam a impossibilidade de solução de determinadas equações de grau igual ou maior do que cinco.

RESULTADOS E DISCUSSÃO

Se K é um subcorpo do corpo $\boldsymbol{C}$ dos números complexos, α é um elemento de $\boldsymbol{C}$ e $K[t]$ é o conjunto dos polinômios com coeficientes em K, então por $K[\alpha]$ denota-se o conjunto $\{f(\alpha): f \in K[t]\}$. Demonstremos que $K[\alpha]$ não apenas é um subanel de $\boldsymbol{C}$ como também é o menor subanel de $\boldsymbol{C}$ que contém K e o número α. Pela definição de $K[\alpha]$, seus elementos possuem o formato $p = a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ com $a_i \in K \subset \boldsymbol{C}$ e $i \in \boldsymbol{N}$. Percebe-se facilmente que tomando dois elementos de $K[\alpha]$, a subtração de um desses elementos pelo outro e o produto entre eles pertencem a $\boldsymbol{C}$. Logo, $K[\alpha]$ é subanel de $\boldsymbol{C}$. Para mostrarmos que $K[\alpha]$ é o menor subanel de $\boldsymbol{C}$ que contém K e α, é necessário, agora, que mostremos que, qualquer que seja o subanel Y de $\boldsymbol{C}$ que contém K e α, $K[\alpha] \subset Y$. Suponhamos um subanel de $\boldsymbol{C}$ que contém K e o número α; chamemo-lo de Y. Sendo assim, em outras palavras, $K \cup \{\alpha\} \subset Y$. Deste modo, se um elemento $p = a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ qualquer pertence a $K[\alpha]$, com $a_i \in K \subset Y$ e $\alpha \in Y$, então $p \in Y$ e, portanto, $K[\alpha] \subset Y$. Assim, pode-se dizer $K[\alpha]$ é uma extensão do anel K obtida pela adjunção de α a K. Contudo, se α for um elemento algébrico sobre K, garante-se mais: que $K[\alpha]$ é, ele próprio, um corpo. Obtém-se, desse modo, uma extensão algébrica simples do corpo K. A seguir, descrevemos como esse fato pode ser estabelecido.

Dizemos que $\alpha \in C$ é algébrico sobre o corpo K se há algum polinômio em $K[t]$, não nulo, tal que α seja uma raiz desse polinômio. O número $\sqrt{2}$ é um exemplo de elemento algébrico sobre o corpo $\boldsymbol{Q}$ dos números racionais, mas o número π, como demonstrado pela primeira vez por Lindemann, em 1882, não o é (MONTEIRO, 1969). Entre os polinômios em $K[t]$ que têm entre suas raízes o número α, há polinômios que são mônicos e entre os últimos escolhe-se o polinômio m de menor grau, denominado polinômio mínimo de α sobre o corpo K. Esse polinômio é irredutível sobre K, pois, se assim não fosse, encontrar-se-ia dois polinômios mônicos f e g de graus menores do que o de m tais que $m = fg$, donde $0 = m(\alpha) = f(\alpha)g(\alpha)$, de modo que, como K é anel de integridade, ter-se-ia que $f(\alpha) = 0$ ou $g(\alpha) = 0$, uma contradição.

O próximo passo na demonstração do fato acima é mostrar que, sendo α algébrico sobre K, o conjunto $J = \{f \in K[t]: f(\alpha) = 0\}$ é um ideal maximal em $K[t]$. Uma vez que a diferença de dois elementos de J é um elemento de J e o produto de um elemento de J por um elemento qualquer de $K[t]$ é também um elemento de J, tem-se que J é um ideal de $K[t]$. Agora, se m é o polinômio mínimo de α sobre o corpo K e $h \in J$, então existem $q, r \in K[t]$ tais que $h = mq + r$ e onde $r = \boldsymbol{0}$ ou o grau de r é menor do que o de m. Isso significa que $0 = h(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$ e, portanto, que $r = \boldsymbol{0}$, donde $J = \langle m \rangle$. Por outro lado, se I for um ideal de $K[t]$ que contém J, segue que $I = K[t] \cdot f$, para algum $f \in K[t]$, pois $K[t]$ é um anel principal. Sendo assim, existe $g \in K[t]$ tal que $m = fg$ e, como m é irredutível, um dos dois polinômios f e g é uma constante não nula. Se for g, então $g = a \in K^*$, donde $f = a^{-1}m$ e, por conseguinte, $I = K[t] \cdot f = K[t] \cdot (a^{-1}m) = (K[t] \cdot a^{-1}) \cdot m == K[t] \cdot m =$

$\langle m \rangle = J$. Se for f, então $f = b \in K^*$, donde $I = K[t] \cdot b = K[t]$. Os únicos ideais de $K[t]$ que contêm J são, portanto, o próprio J e $K[t]$, o que se desejava demonstrar.

Segue do resultado anterior, cuja última parte da prova se baseia em GONÇALVES (2012), que o anel quociente $K[t]/J$ é um corpo. Para verificar isso, basta mostrar que todo elemento $\bar{f} \in (K[t]/J)^*$ é invertível, uma vez que $K[t]/J$ é um anel comutativo com unidade. Se $\bar{f} \in (K[t]/J)^*$, então f não é elemento de J, mas pertence ao ideal $J + L = \{g + h: g \in J \text{ e } h \in L\}$, onde $L = \langle f \rangle$. Como J é ideal maximal de $K[t]$ e é subconjunto próprio de $J + L$, segue que $J + L = K[t]$. Sendo assim, $\mathbf{1} \in J + L$, isto é, existem $u \in J$ e $v \in L$ tais que $\mathbf{1} = u + v$. Por outro lado, pela maneira que L foi definido, há um $b \in K[t]$ tal que $v = bf$, ou seja, tal que $\mathbf{1} = u + bf$. Por conseguinte, $\bar{\mathbf{1}} = \overline{u + bf} = \bar{u} + \overline{bf} = = \bar{\mathbf{0}} + \bar{b}\bar{f} = \bar{b}\bar{f}$.

Como, pelo teorema do homomorfismo (IEZZI & DOMINGUES, 1982), $K[t]/J$ e $K[\alpha]$ são isomorfos (J e $K[\alpha]$ são, respectivamente, o núcleo e o contradomínio do epimorfismo $\sigma_\alpha: K[t] \to K[\alpha]$ que associa a cada elemento $a_r t^r + \ldots + a_1 \mathrm{t} + a_0$ de $K[t]$ o número $a_r \alpha^r + \ldots + a_1 \alpha + a_0$ de $K[\alpha]$), a conclusão é que $K[\alpha]$ é um corpo.

Como um exemplo do que foi exposto, temos que $\boldsymbol{Q}[\sqrt{2}]$ é uma extensão algébrica simples do corpo $\boldsymbol{Q}$. Isso significa que ele é o corpo que se obtém a partir de $\boldsymbol{Q}$ pela adjunção de $\sqrt{2}$. Logo, o polinômio $t^3 + t^2 - 2t - 2$, que tinha apenas uma raiz em $\boldsymbol{Q}$, passa a ter pelo menos duas raízes em $\boldsymbol{Q}[\sqrt{2}]$. É possível, então, estender o corpo $\boldsymbol{Q}[\sqrt{2}]$ pela adjunção de $-\sqrt{2}$, a terceira raiz do polinômio, a fim de que esse polinômio tenha todas as suas raízes nesse corpo. Nesse caso, em particular, a nova extensão coincide com o próprio $\boldsymbol{Q}[\sqrt{2}]$, que conterá todas as raízes do polinômio (ou todas as soluções da equação $t^3 + t^2 - 2t - 2 = 0$).

CONCLUSÕES

O propósito deste trabalho era estabelecer alguns fatos básicos a respeito das extensões algébricas de subcorpos do corpo dos números complexos. Percebemos a partir dos inúmeros casos particulares que temos estudado que essas extensões podiam ser obtidas simplesmente determinando-se o anel $K[\alpha]$, fato que foi possível confirmar a partir de propriedades dos conceitos de ideal e homomorfismo.

AGRADECIMENTOS

Agradecemos ao Programa Institucional de Bolsas de Iniciação Científica e Tecnológica (PIBIFSP), do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, pelo apoio.

REFERÊNCIAS

GONÇALVES, A. **Introdução à álgebra**. 5. ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2012.

IEZZI, G.; DOMINGUES, H. H. **Álgebra moderna**. 2. ed. São Paulo: Atual, 1982.

MONTEIRO, L. H. J. **Teoria de Galois**. Poços de Caldas, MG: 7º Colóquio Brasileiro de Matemática, 1969.

STEWART, I. N. **Galois theory**. 3rd. ed. [S.l.]: Chapman & Hall, 2004.