Uma nota sobre o p-ésimo corpo ciclotômico e aplicações

Eliani Magalhães Beloni & Antonio Aparecido de Andrade

Ibilce - Unesp, São José do Rio Preto/SP

elianimb2010@bol.com.br

Resumo

Os corpos ciclotômicos desempenham um papel fundamental na Teoria dos Números Algébricos, já que é possível caracterizar o seu anel de inteiros algébricos e também seu discriminante. Neste trabalho apresentamos e caracterizamos completamente o anel de inteiros dos corpos ciclotômicos da forma $\mathbb{Q}(\zeta_p)$, onde p é um número primo ímpar.

Introdução

O n-ésimo corpo ciclotômico é a menor extensão de $\mathbb{Q}$ que contém as raízes de $f(x) = x^n - 1, \quad n \in \mathbb{N}, \quad n \geq 1$. O número complexo $\zeta_n = e^{\frac{2\pi i}{n}}$ é uma raiz de $f(x)$ e assim, o n-ésimo polinômio ciclotômico é um fator do polinômio $f(x)$. Quando $n = p$, um número primo ímpar, segue que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ e o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, denotado por $\mathcal{O}_{\mathbb{K}}$, é o conjunto formado pelos elementos de $\mathbb{K}$ que são inteiros sobre $\mathbb{Z}$, ou seja, $\alpha \in \mathcal{O}_{\mathbb{K}}$ se, e só se, $\alpha \in \mathbb{K}$ é raiz de um polinômio mônico sobre $\mathbb{Z}$.

Resultados

Provaremos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Observe que $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_{\mathbb{K}}$. Para provar isso, basta mostrar que $\zeta_p \in \mathcal{O}_{\mathbb{K}}$, já que $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}}$ e de fato, como ζ_p é raiz de $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + ... + 1)$ e $\zeta_p \neq 1$, segue que ζ_p é raiz do polinômio $x^{p-1} + x^{p-2} + ... + 1$. Agora, para mostrarmos que $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$, precisaremos de alguns resultados e também utilizaremos a definição e propriedades de traço.

Lema 1. *Se r e s são inteiros tais que $mdc(p, rs) = 1$, então $(\zeta_p^r - 1)/(\zeta_p^s - 1)$ é um elemento inversível de $\mathbb{Z}[\zeta_p]$.*

Demonstração: Como $mdc(p, rs) = 1$, segue que existem $m, n \in \mathbb{Z}$ tais que $pm + rsn = 1$, logo $r = rpm + rrsn$, e assim, $r \equiv st \pmod p$, onde $t \equiv r^2 n \pmod p$ e $t \in \mathbb{Z}$. Assim $\dfrac{\zeta_p^r - 1}{\zeta_p^s - 1} = \dfrac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + ... + \zeta_p^{s(t-1)} \in \mathbb{Z}[\zeta_p]$, e de modo análogo, $\dfrac{\zeta_p^s - 1}{\zeta_p^r - 1} \in \mathbb{Z}[\zeta_p]$. Portanto, $\dfrac{\zeta_p^r - 1}{\zeta_p^s - 1}$ é invertível em $\mathbb{Z}[\zeta_p]$. □

Lema 2. $((1 - \zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1} = p\mathcal{O}_{\mathbb{K}}$.

Demonstração: Para $1 \leq i \leq p-1$, segue que $mdc(p, i \cdot 1) = 1$. Logo, pelo Lema 1, segue que $\dfrac{\zeta_p^i - 1}{\zeta_p - 1}$ é invertível em $\mathbb{Z}[\zeta_p]$, ou seja, invertível em $\mathcal{O}_{\mathbb{K}}$, e assim existe $a \in \mathcal{O}_{\mathbb{K}}$ tal que $\dfrac{\zeta_p^i - 1}{\zeta_p - 1} a = 1$. Logo, $(\zeta_p^i - 1)a = \zeta_p - 1$, e assim, $(\zeta_p - 1)\mathcal{O}_{\mathbb{K}} \subset (\zeta_p^i - 1)\mathcal{O}_{\mathbb{K}}$. De modo análogo, $\dfrac{\zeta_p - 1}{\zeta_p^i - 1}$ é invertível em $\mathcal{O}_{\mathbb{K}}$, donde concluímos que $(\zeta_p - 1)\mathcal{O}_{\mathbb{K}} = (\zeta_p^i - 1)\mathcal{O}_{\mathbb{K}}$ $(*)$. Agora, visto que $p(x) = \prod_{i=1}^{p-1}(x - \zeta_p^i)$ é o polinômio minimal de ζ_p sobre $\mathbb{Q}$ e que ζ_p é uma raiz de $x^{p-1} + ... + x + 1$, segue que $x^{p-1} + ... + x + 1 = \prod_{i=1}^{p-1}(x - \zeta_p^i)$.

Para $x = 1$, segue que $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$, donde concluímos que $((1 - \zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1} = p\mathcal{O}_{\mathbb{K}}$, já que vale $(*)$. □

Lema 3. $(1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

Demonstração: Pelo Lema 2, segue que $((1 - \zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1} = p\mathcal{O}_{\mathbb{K}}$. Assim, $p\mathcal{O}_{\mathbb{K}} \subset (1 - \zeta_p)\mathcal{O}_{\mathbb{K}}$. Logo, $p\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} \subset (1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$. Como $p\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, segue que $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$ ou $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Se $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$, então $1 - \zeta_p$ é um elemento invertível de $\mathcal{O}_{\mathbb{K}}$. Assim, p é invertível em $\mathcal{O}_{\mathbb{K}}$. Como p tem inverso em $\mathbb{Q}$, segue que p tem inverso em $\mathbb{Z} = \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q}$, o que é um absurdo. Logo, $(1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.□

Lema 4. $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$, *para todo* $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Demonstração: Cada conjugado $\alpha_i(1 - \zeta_p^i)$ de $\alpha(1 - \zeta_p)$ é um múltiplo de $(1-\zeta_p^i)$ em $\mathcal{O}_{\mathbb{K}}$, onde $i = 1, \cdots, p-1$. Como $1-\zeta_p^i = (1-\zeta_p)(\zeta_p^{i-1}+\zeta_p^{i-2}+\cdots+\zeta_p+1)$, segue que $1-\zeta_p^i$ é um múltiplo de $1 - \zeta_p$ em $\mathcal{O}_{\mathbb{K}}$. Como o traço é a soma dos conjugados, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) = \alpha_1(1-\zeta_p)+\alpha_2(1-\zeta_p^2)+\cdots+\alpha_p(1-\zeta_p^p) = = \beta(1 - \zeta_p)$, onde $\beta \in \mathcal{O}_{\mathbb{K}}$. Portanto, $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p)) \in \mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é integralmente fechado, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathbb{Z}$. Assim, $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p)) \in (1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}=p\mathbb{Z}$, o que prova o lema. □

Teorema 5. *O anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo ímpar, é dado por $\mathbb{Z}[\zeta_p]$.*

Demonstração: Vimos que $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_{\mathbb{K}}$. Provemos que $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$. De fato, se $\alpha \in \mathcal{O}_{\mathbb{K}} \subset \mathbb{Q}(\zeta_p)$, então $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, com $a_i \in \mathbb{Q}$, para $i \in \{0, 1, \cdots, p-2\}$. Multiplicando por $1 - \zeta_p$ em ambos os lados, segue que $\alpha(1 - \zeta_p) = a_0(1 - \zeta_p) + a_1(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1})$. Pelo Lema 4, temos: $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p)) = a_0 Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) + a_1 Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2} Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{p-2} - \zeta_p^{p-1}) \in p\mathbb{Z}$. Assim, como $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i \in \{1, 2, \cdots, p-2\}$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p)) = a_0 Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) = a_0 p \in p\mathbb{Z}$, onde $a_0 \in \mathbb{Z}$. Analogamente, como $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_{\mathbb{K}}$, segue que $(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3}$. Multiplicando ambos os lados por $1 - \zeta_p$, segue que $(\alpha - a_0)\zeta_p^{-1}(1 - \zeta_p) = a_1(1 - \zeta_p) + a_2\zeta_p(1 - \zeta_p) + \cdots + a_{p-2}\zeta_p^{p-3}(1 - \zeta_p)$, e assim, pelo Lema 4, $Tr_{\mathbb{K}/\mathbb{Q}}((\alpha - a_0)\zeta_p^{-1}(1 - \zeta_p)) = a_1 Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) + a_2 Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2} Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{p-3} - \zeta_p^{p-2}) \in p\mathbb{Z}$. Logo, $a_1 Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) = a_1 p \in p\mathbb{Z}$, onde $a_1 \in \mathbb{Z}$. Prosseguindo, desta forma, teremos que $a_i \in \mathbb{Z}$, para cada $i \in \{1, \cdots, n\}$. Assim, $\alpha \in \mathbb{Z}[\zeta_p]$. Portanto, $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{K}}$. □

Conclusão

Com isso concluímos que os únicos elementos de $\mathbb{Q}(\zeta_p)$ que são inteiros sobre $\mathbb{Z}$ são os elementos que estão em $\mathbb{Z}[\zeta_p]$.

Referências

[1] R. Araújo , *Anéis de inteiros de corpos de números e aplicações*, Dissertação de Mestrado, Ibilce - Unesp, São José do Rio Preto - SP, 2015.

[2] P. Samuel , *Algebraic theory of numbers* , Hermann, Paris, 1982.

[3] D. Marcus , *Number fields* , Springer-Verlag, New-York, 1945.

Agradecimentos

Agradeço ao meu orientador pelo apoio e incentivo e também ao SESu/MEC pelo auxílio financeiro.