Prime-degree cyclic extensions and applications

Antonio Aparecido de Andrade

Department of Mathematics, Ibilce - Unesp, São José do Rio Preto - SP

antonio.andrade@unesp.br

This work was supported by Fapesp 2013/25977-7 and 2022/02303-0.

Abstract

In this work, we calculate the expression of $Tr_{\mathbb{K}}(\alpha^2)$ in the case where p is ramified and is unramified, but the elements of the ring of integers are written over an integral basis obtained from Leopoldt's Theorem, since the Hilbert-Speiser's Theorem cannot be applied here. Using this trace form, we calculate the center density of algebraic lattices obtained from the ring of integers of $\mathbb{K}$ via the Minkowski embedding.

Introduction

Problems about packing objects such as circles and spheres have received the attention of mathematicians for many centuries, with some of them remaining open until recently, when very complex solutions were found. A classic problem of this nature, perhaps the most famous, is that of finding an arrangement (as dense as possible) of spheres of the same radius in 3-dimensional Euclidean space. A solution to this problem was conjectured by Kepler in 1611, but only in 2017 did Hales and his collaborators publish a proof of this conjecture. Corresponding problems in other dimensions were solved only for the case of dimension 2 (Fejes Tóth, 1942), and quite recently, for dimensions 8 and 24. Maryna Viazovska, one of the winners of the Fields Medal 2022, solved for dimension 8 (in 2017), and contributed to Proving for Dimension 24.

Basic results

Let $\mathbb{K}$ be a cyclic number field of prime degree $p > 2$ with conductor n. Thus, $\mathbb{K}/\mathbb{Q}$ is a Galoisian extension such that the Galois group $Gal(\mathbb{K}/\mathbb{Q}) =< \theta >$ is cyclic. Since the monomorphisms from $\mathbb{K}$ to $\mathbb{C}$ coincide with the elements of $Gal(\mathbb{K}/\mathbb{Q})$ and $\mathbb{K}$ is a totally real number field, the canonical embedding of $\mathbb{K}$, $\sigma : \mathbb{K} \to \mathbb{R}^p$ is given by

$$\sigma(x) = (x, \theta(x), \theta^2(x), \ldots, \theta^{p-1}(x)).$$

Trace form

The extension $\mathbb{K}/\mathbb{Q}$ is an Abelian extension of degree p. By Kronecker-Weber Theorem there exists $n > 0$ such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. We consider $n > 0$ to be the conductor of $\mathbb{K}$, that is, the smallest integer with this property. It is well known that n must be $p_1p_2 \ldots p_r$ or $p^2p_1p_2 \ldots p_r$, for distinct prime numbers $p_i \equiv 1(mod\, p)$, with $1 \leq i \leq r$. The first case occurs when p is unramified in $\mathbb{K}$ and the second case occurs when p is ramified.

Let $\mathcal{O}_{\mathbb{K}}$ be the ring of algebraic integers of $\mathbb{K}$. Let $\mathbb{L} = \mathbb{Q}(\zeta_n)$. Let θ be a generator of $Gal(\mathbb{K}/\mathbb{Q})$ and $t = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_n)$.

1. If p is unramified in $\mathbb{K}/\mathbb{Q}$, then $\mathbb{K} = \mathbb{Q}(t)$ and $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis for $\mathbb{K}$. If $\alpha = a_0t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{O}_{\mathbb{K}}$, where $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$, then

$$Tr_{\mathbb{K}}(\alpha^2) = n\left(\sum_{i=0}^{p-1} a_i^2\right) + \frac{1-n}{p}\left(\sum_{i=0}^{p-1} a_i\right)^2.$$

.

2. If p is ramified in $\mathbb{K}/\mathbb{Q}$, then $\mathbb{K} = \mathbb{Q}(t)$ and $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis for $\mathbb{K}$. If $\alpha = a_0 + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{O}_{\mathbb{K}}$, where $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$, then

$$Tr_{\mathbb{K}}(\alpha^2) = pa_0^2 + pp_1 \ldots p_r\left(\sum_{i=1}^{p-1} a_i^2 + \sum_{i<j}(a_i - a_j)^2\right),$$

where $i = 1, 2, \ldots, p-1$.

Algebraic lattices

Let $B = \{v_1, v_2, \ldots, v_m\}$ be a linearly independent set of vectors in R^p, with $1 \leq m \leq p$. The set

$$\Lambda = \{\sum_{i=1}^{m} a_iv_i : a_i \in \mathbb{Z},\ i = 1, 2, \ldots, m\}$$

is called a lattice in $\mathbb{R}^p$ of rank m and the set B is said to be a basis of Λ.

If $\mathcal{M}$ is a $\mathbb{Z}$-module contained in $\mathbb{K}$ of rank p, then the set $\Lambda = \sigma(\mathcal{M})$ is a complete lattice in $\mathbb{R}^p$ and that the center density of λ is given by

$$\delta(\Lambda) = \frac{\eta^{p/2}}{2^p[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]\sqrt{|D(\mathbb{K})}},$$

where $D(\mathbb{K})$ denotes the discriminant of $\mathbb{K}$, $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ denotes the index of $\mathcal{M}$, $\eta = \min\{Tr_{\mathbb{K}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\}$.

Examples

1. Let $\mathbb{K}$ be a cyclic field of degree $p = 3$ and conductor $n = 3^2$. In this case, the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\theta\rangle$ is cyclic of order 3, $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_{3^2})/\mathbb{K}}(\zeta_{3^2})$, and $D_{\mathbb{K}} = 3^4$. Let $\mathcal{M}$ be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 3 and index 6 given by

$$\mathcal{M} = \{a_0 + a_1\theta(t) + a_2\theta^2(t) \in \mathcal{O}_{\mathbb{K}}\}$$

such that $a_0 \equiv 0 \pmod 2, a_0 + a_1 + a_2 \equiv 0(mod\, 3)$. The trace form of $\mathbb{K}$ restricted to $\mathcal{M}$ is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 18(2x_0^2 + 2x_0x_1 + 4x_0x_2 + x_1^2 + 3x_1x_2 + 3x_2^2),$$

where x_0, x_1, x_2 are any integers. It follows that $\min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 18$ is attained at $a_1 = 1$ and $a_0 = a_2 = 0$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $\sqrt{|D_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 3^2 \cdot 6 = 54$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{18}/2)^3}{54} = \frac{1}{4\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_3.

2. Let $\mathbb{K}$ be a number field of degree $p = 5$ and conductor $n = 5^2$. In this case, the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$ is cyclic of order 5, $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_{5^2})/\mathbb{K}}(\zeta_{5^2})$, and $D_{\mathbb{K}} = 5^8$. Let $\mathcal{M}$ be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 5 and index 10 given by

$$\mathcal{M} = \{a_0 + a_1\sigma(t) + a_2\sigma^2(t) + a_3\sigma^3(t) + a_4\sigma^4(t) \in \mathcal{O}_{\mathbb{K}}\},$$

where $a_0 \equiv 0(mod\, 2)$ and $2a_0 + a_1 + a_2 + a_3 + a_4 \equiv 0(mod\, 5)$. The trace form of $\mathbb{K}$ restricted to $\mathcal{M}$ is given by $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 50 \cdot (2x_0^2 + 6x_0x_1 + 6x_0x_2 + 6x_0x_3 + 8x_0x_4 + 6x_1^2 + 11x_1x_2 + 11x_1x_3 + 15x_1x_4 + 6x_2^2 + 11x_2x_3 + 15x_2x_4 + 6x_3^2 + 15x_3x_4 + 10x_4^2)$, where $x_0, \ldots, x_4$ are any integers. It follows that $\min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}\} = 50$ is attained at $a_0 = a_1 = a_2 = 0$ and $a_3 = -a_4 = 1$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $\sqrt{|D_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 5^4 \cdot 10 = 5^5 \cdot 2$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{50}/2)^5}{5^2 \cdot 2} = \frac{1}{8\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_5.

References

[1] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito, Constructions of algebraic lattices, *Comput. Appl. Math.*, **29** (2010) 1–13.

[2] E. Luiz de Oliveira, J. C. Interlando, T. P. da Nóbrega Neto, and J. O. D. Lopes, The integral trace form of cyclic extensions of odd prime degree, *Rocky Mountain J. Math.*, **47** (2017), 1075–1088.