New constructions of algebraic lattices

Antonio Aparecido de Andrade[1] **and Robson Ricardo de Araujo**[2]

[1]Department of Mathematics, São Paulo State Universtiy of São Paulo at São José do Rio Preto, Brasil
[2]Department of Mathematics, State University of Campinas, Brasil

Abstract

The Kronecker-Weber Theorem, states that every abelian number field is contained in a cyclotomic field. Thinking about this, we can ask ourselves what is the ring of integers of each abelian number field and if this ring of integers has a power basis, this is, if the ring of integers is generated by an element over $\mathbb{Z}$. In this line, to construct lattices in odd dimensions, we can not use cyclotomic fields, but we can use their subfields. Also, the maximal real cyclotomic subfields are not suficient to solve the problem of find algebraic lattices that has better center density. Trying to solve this problem mainly in odd dimensions, we are using abelian number fields. For this task we need the ring of integers of abelian number fields, which is presented by the Leopoldt's Theorem (1959) or its version given by Lettl (1990). In this work, we intend to present the Leopoldt's Theorem in the version of Lettl and elucidate why it can be useful to construct algebraic lattices with better center desnsity.

1 Introduction

The knowledge of the ring of integers of a number field is important in studies about lattices (discrete subgroups of $\mathbb{R}^n$) and coding theory. it is possible develop algebraic lattices from $\mathbb{Z}$-submodules of a number field using the Minkowski Homomorphism. In particular, taking the ring of integers or its ideals it is possible to obtain lattices. One of the goals in the studies of lattices is find the better structure of discrete points that can be center of tangent spheres covering $\mathbb{R}^n$ minimizing unfilled space. To be more specific if Λ is a lattice of rank n in $\mathbb{R}^n$, the goal is maximize the density center $\delta(\Lambda) = \rho^n/vol(\Lambda)$, where ρ is the packing radius of Λ and $vol(\Lambda)$ is its volume. In case of algebraic lattices, if a lattice is produced by an ideal $\mathcal{M}$ of the ring of integers of a galoisian number field $\mathbb{K}$, the density center has a more detailed expression that depends on the norm of $\mathcal{M}$, the discriminant of the field and the trace form. Thus, the knowledge of the ring of integers of an abelian number field is important to define its ideals and the parameters used to calculate the density center of algebraic lattices. Aware of this application, we dedicate efforts to study ring of integers of an abelian number field. In this work, we present an important result that gives an expression for ring of integers of all abelian number field by the called Leopoldt-Lettl Theorem. After this, we discuss about construction of algebraic lattices.

2 Number field

If $\mathbb{K}$ is a number field of degree n, then $\mathbb{K} = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of a monic irreducible polynomial $p(x) \in \mathbb{Z}[x]$. The n distinct roots of $p(x)$, namely, $\alpha_1, \alpha_2, \cdots, \alpha_n$, are the conjugates of α. If $\sigma : \mathbb{K} \to \mathbb{C}$ is a $\mathbb{Q}$-homomorphism, then $\sigma(\alpha) = \alpha_i$ for some $i = 1, 2, \cdots, n$. Furthermore, there are exactly n $\mathbb{Q}$-homomorphism σ_i, for $i = 1, 2, \cdots, n$, of $\mathbb{K}$ in $\mathbb{C}$. The trace of any element $\alpha \in \mathbb{K}$ is defined as the rational number $T_{\mathbb{K}:\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$. The Galois group of $\mathbb{K}/\mathbb{Q}$ is defined as the set of all automorphisms σ of $\mathbb{K}$ that fix every elements of $\mathbb{Q}$. An element $\alpha \in \mathbb{K}$ is called an algebraic integer if there is a monic polynomial $f(x)\mathbb{Z}[x]$ such that $f(\alpha) = 0$. The set $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \text{ is an algebraic integer}\}$ is a ring called *ring of algebraic integers* of $\mathbb{K}$. It can be shown that $\mathcal{O}_{\mathbb{K}}$, as a $\mathbb{Z}$-module, has a basis $\{\alpha_1, \cdots, \alpha_n\}$, called *integral basis*. The *discriminant* of $\mathbb{K}$ over $\mathbb{Q}$ is defined by $D(\mathbb{K}) = \det(T_{\mathbb{K}:\mathbb{Q}}(\alpha_i\alpha_j))_{i,j=1}^{n}$ and the *norm* of an ideal $\mathcal{A}$ of $\mathbb{K}$ is defined by $N_{\mathbb{K}:\mathbb{Q}}(\mathcal{A}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{A}|$,i.e., is the cardinality of the quotient ring $\mathcal{O}_{\mathbb{L}}/\mathcal{A}$. A cyclotomic field is a number field $\mathbb{K}$ such that $\mathbb{K} = \mathbb{Q}(\zeta_n)$, where $\zeta_n = exp(\frac{2\pi i}{n})$ for some integer $n \geq 3$, that is, ζ_n is a primitive n-th root of unity. It can be shown that $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$, where φ is the Euler function, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Z}[\zeta_n]$ and $\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{\varphi(n)-1}\}$ is an integral basis of $\mathbb{K}$.

3 Algebraic lattices

Let $\mathbb{K}$ be a number field of degree n. It is known that exist n distinct monomorphisms $\sigma_i : \mathbb{K} \to \mathbb{C}$. Of these, there is r_1 real monomorphisms ($\sigma_i((K)) \subseteq \mathbb{R}$) and $2r_2 = n - r_1$ non-real monomorphisms. Let $\{\sigma_1, \cdots, \sigma_{r_1}\}$ be the set of the real monomorphisms and $\{\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}\}$ be the set of the non-real monomorphisms that has not two conjugated monomorphisms (the others r_2 monomorphisms are conjugated of some monomorphism of the last set). For any $x \in \mathbb{K}$, the Minkowski Homomorphism is defined by

$$\sigma(x) = (\sigma_1(x), \cdots, \sigma_{r_1+r-2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}.$$

If $I(\cdot)$ and $R(\cdot)$ denote the imaginary part and the real part of a complex number, respectively, then

$$\sigma(x) = (\sigma_1(x), \cdots, \sigma_{r_1}(x), R(\sigma_{r_1+1}(x)), \cdots, I(\sigma_{r_1+r_2}(x))).$$

Se $r_2 = 0$, then $\mathbb{K}$ is called tottaly real number field. If $r_1 = 0$, then $\mathbb{K}$ is called tottaly imaginary number field. In case of $\mathbb{Q} \subseteq \mathbb{K}$ be a finite galoisian extension, $\mathbb{K}$ is tottaly real or $\mathbb{K}$ is tottaly imaginary.
If $\mathcal{M}$ is a free $\mathbb{Z}$-submodule of $\mathbb{K}$ of rank n and $\{\alpha_1, \cdots, \alpha_n\}$ is a $\mathbb{Z}$-basis to $\mathcal{M}$, then $\sigma(\mathcal{M})$ is a lattice in $\mathbb{R}^n$ and its volume is

$$vol(\sigma(M)) = 2^{-r_2} \left| \det_{1 \leq i,j \leq n} (\sigma_i(\alpha_j)) \right|.$$

The lattice $\sigma(\mathcal{M})$ is called **algebraic lattice**.The density center of the algebraic lattice $\sigma(\mathcal{M})I$ is given by

$$\delta = \frac{t_{\mathcal{M}}^{n/2}}{2^n \sqrt{|D(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} \tag{1}$$

where $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ is the index (if $\mathcal{M}$ for an ideal of $\mathcal{O}_{\mathbb{K}}$, then the index is the norm of the ideal $\mathcal{M}$ and $t_{\mathcal{M}} = min\{Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\overline{\alpha}) \ : \ \alpha \in I, \alpha \neq 0\}$. Thus, via algebraic number theory it is possible construct algebraic lattices in a dimension n using free $\mathbb{Z}$-submodule of $\mathbb{K}$. In the special case where $\mathbb{K}$ is galoisian over $\mathbb{Q}$ and $\mathcal{M}$ has a known index (for example, when $\mathcal{M}$ is a principal ideal or a tottaly ramified ideal), the dificulty to calculate the density center depends on the dificulty to calculate the parameter t, since there is results that present the value of $D(\mathbb{K})$. For this, is important to know the structure of the ring of integers of the number field.
If $\mathbb{K}$ is a abelian number field of conductor $m = \prod_{i=1}^{r} p_i^{e_i}$ (factorization of m in power of primes), then

$$| \ D(\mathbb{K}) \ | = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{r} p_i^{\beta_i}},$$

where $\beta_i = \sum_{k=1}^{e_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^k}) : \mathbb{Q}]$. This, we can focus on knowledge of ring of integers of abelian number fields.

4 Leopold-Lettl theorem

Let $\mathbb{Q}^{(n)} \triangleq \mathbb{Q}(\zeta_n)$ the n-th cyclotomic field and $G^{(n)} \triangleq Gal(\mathbb{Q}^{(n)} : \mathbb{Q})$ the Galois Group of $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$. A Dirichlet **character** modulus m is a mapping $\chi : \mathbb{Z} \longrightarrow \mathbb{C}^{\times}$ such that:
(a) $\chi(a) = 0$ if and only if $gcd(a, m) \neq 1$;
(b) if $a \equiv b \ (mod \ m)$ then $\chi(a) = \chi(b)$;
(c) $\chi(ab) = \chi(a)\chi(b)$.
Looking in the image of a character χ, is possible to define a minimal positive integer f_χ to be the modulo of χ. This value f_χ is called conductor of χ. Denoting by $X^{(n)}$ the group multiplicative of characters having conductor $f_\chi \mid n$, then $X^{(n)}$ is one-to-one in correspondence to $G^{(n)}$.
If $\mathbb{K}$ is an abelian number field, then from Theorem of Kronecker-Weber, there is a minimal n such that $\mathbb{K} \subseteq \mathbb{Q}^{(n)}$. If $G = Gal(\mathbb{K} : \mathbb{Q})$, then from Galois Correspondence and results about characters, it exists a subgroup $X \subseteq X^{(n)}$ such that X is in correspondence with G, which in turn is in correspondence with $\mathbb{K}$. In fact, there is an one-to-one correspondence between the subgroups of $X^{(n)}$ and the subgroups of $G^{(n)}$. Furthermore, $n = lcm\{f_\chi : \chi \in X\}$.
For any $n \in \mathbb{N}$, considering $P_n = \{p \ prime : p \mid n, p \neq 2\}$, we define

$$\mathcal{D}(n) = \left\{ d \in \mathbb{N} : \left(\prod_{p \in P_n} p \right) \mid d, d \mid n, d \not\equiv 2 \ (4) \right\},$$

$$q(n) = \prod_{p \ prime, \ v_p(n) \geq 2} p^{v_p(n)} \ \ (powerful \ part \ of \ n)$$

and

$$\phi_d = \{\chi \in X : q(f_\chi) = q(d)\}.$$

The set $\phi_d \subset X$ is called **branch class** of X. Then, $X = \dot{\bigcup}_{d \in \mathcal{D}(n)} \phi_d$ is a partition of X into disjoints subsets. Moreover, $\phi_n \neq \emptyset$ and $\langle \phi_n \rangle = X$. For $\chi \in X$, consider

$$\epsilon_\chi \triangleq \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\sigma \in G} \overline{\chi(\sigma)}\sigma \in \mathbb{C}[G].$$

It is possible show that $\sum_{\chi \in X} \epsilon_\chi = 1$, $\epsilon_\chi^2 = \epsilon_\chi$ and $\epsilon_\chi \epsilon_\psi = 0$ if $\psi \neq \chi$. Therefore, the set of ϵ_χ is a set of orthogonal idempotents of $\mathbb{C}[G]$.
For each $d \in \mathcal{D}(n)$ (n conductor of $\mathbb{K}$), denote

$$\mathbb{K}_d \triangleq \mathbb{K} \cap \mathbb{Q}^{(d)} \qquad and \qquad \eta_d \triangleq Tr_{\mathbb{Q}^{(d)}:\mathbb{K}_d} \zeta_d.$$

It is possible verify that $\eta_d = 0$ if and only if $\phi_d = \emptyset$, what occurs only when $d \equiv 4 (mod \ 8)$. Then, we define

$$T = \sum_{d \in \mathcal{D}(n)} \eta_d.$$

It is proven that $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]T]$ is finite.

Teorema 4.1. $\mathbb{K} = \mathbb{Q}[G]T$.

This theorem is important because it ensures all abelian number field $\mathbb{K}$ has a **normal basis**, this is, it exists an element T of $\mathbb{K}$ such that the images of T by the automorphisms in $G = Gal(\mathbb{K} : \mathbb{Q})$ forms a basis to $\mathbb{K}$ over $\mathbb{Q}$. For each $d \in \mathcal{D}(n)$ take

$$\epsilon_d \triangleq \sum_{\chi \in \phi_d} \epsilon_\chi \in \mathbb{Q}[G].$$

Then

$$A_{\mathbb{K}} = \mathbb{Z}[G][\epsilon_d : d \in \mathcal{D}(n)]$$

is an order of $\mathbb{Q}[G]$.
From $\epsilon_d(T) = \eta_d$, then $rank_{\mathbb{Z}}\mathbb{Z}[G]\eta_d = rank_{\mathbb{Z}}\mathbb{Z}[G]\epsilon_d = \#\phi_d$ and

$$\mathbb{K} = \mathbb{Q}[G]T = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Q}[G]\eta_d.$$

Teorema 4.2 (Leopoldt-Lettl Theorem)**.** $\mathcal{O}_{\mathbb{K}} = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d = A_{\mathbb{K}}T$.

In particular, we obtain with corollary that if n is a product of distinct odd prime numbers then $\mathcal{O}_{\mathbb{K}}$ has a **normal integral basis**.

Teorema 4.3 (Hilbert-Speiser Theorem)**.** *The ring $\mathcal{O}_{\mathbb{K}}$ admits an integral normal basis if and only if the conductor of $\mathbb{K}$ is a product of odd prime numbers square-free.*

5 Examples of algebraic lattices

Dimension 2: Consider $\mathbb{K} = \mathbb{Q}(\zeta_3)$ a cyclotomic field of degree 2 and discriminant $D(\mathbb{K}) = -3$. Let $\mathcal{M} = (1 - \zeta_3)\mathcal{O}_(\mathbb{K})$ be a prime ideal which ramifies totally in $\mathbb{K}$. It is possible see that $\alpha \in \mathcal{M}$ if and only if $\alpha = a + b\zeta_3$, with $a + b \equiv 0 \ (mod \ 3)$. Moreover, $N(\mathcal{M}) = 3$. For any $\alpha = a + b\zeta_3 \in \mathcal{M}$, let k be an integer such that $a + b = 3k$. Then, $Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\overline{\alpha}) = a^2 + b^2 + (b - a)^2 = 6(a^2 + 3k^2 - 3ka)$ so $t_{\mathcal{M}} = min\{Tr(\alpha\overline{\alpha}) \ : \ \alpha \in \mathcal{M}, \alpha \neq 0\} = 6$. Therefore, of Equation (1),

$$\delta = \frac{t_{\mathcal{M}}^{n/2}}{2^n \sqrt{|D(\mathbb{K})|N(\mathcal{M})}} = \frac{6^{2/2}}{2^2 \times 3 \times \sqrt{3}} = \frac{1}{2\sqrt{3}}$$

that is the optimal density center in dimension 2.
Dimension 4: Let $\mathbb{K} = \mathbb{Q}(\zeta_8)$ be a cyclotomic field of degree 4 and discriminant equal to 256. Consider the principal ideal $\mathcal{M} = (1 + \zeta_8 + \zeta_8^2 + \zeta_8^3)\mathcal{O}_(\mathbb{K})$ whose norm is $N(\mathcal{M}) = 8$. For each $\alpha = \alpha(i + j\zeta_8 + k\zeta_8^2 + l\zeta_8^3) \in \mathcal{M}$, with $i, j, k, l \in \mathbb{Z}$ and $\alpha = 1 + \zeta_8 + \zeta_8^2 + \zeta_8^3$, $Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\overline{\alpha}) = 16i^2 + 16ij + 16j^2 + 16jk + 16k^2 - 16il + 16kl + 16l^2$ so $t_I = 16$. Therefore,

$$\delta = \frac{t_{\mathcal{M}}^{n/2}}{2^n \sqrt{|D(\mathbb{K})|N(\mathcal{M})}} = \frac{16^{4/2}}{2^4 \times 8 \times \sqrt{256}} = \frac{1}{8}$$

this is the algebraic lattice produced by $\mathcal{M}$ has the optimal density center in dimension 4.
Dimension 6: Consider $\mathbb{K} = \mathbb{Q}(\zeta_9)$ the cyclotomic field of degree 6 and $|\mathcal{D}(\mathbb{K})| = 3^9$. Let $\mathcal{M} = (1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^4 + \zeta_9^5)\mathcal{O}_(\mathbb{K})$ be a principal ideal of norm $N(\mathcal{M}) = 9$. For any $\alpha \in \mathcal{M}$, $\alpha = (1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^4 + \zeta_9^5)(a_0 + a_1\zeta_9 + a_2\zeta_9^2 + a_3\zeta_9^3 + a_4\zeta_9^4 + a_5\zeta_9^5)$, whee $a_i \in \mathbb{Z}$. Then $Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\overline{\alpha}) = 18\left(S + \sum_{i=0}^{5} a_i^2\right)$ where $S \in \mathbb{Z}$. So $t_{\mathcal{M}} = 18$ and

$$\delta = \frac{18^3}{2^6 \times 9 \times \sqrt{3^9}} = \frac{1}{8\sqrt{3}}$$

that is the optimal density center in dimension 6.
Dimension 8: Let $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ be a cyclotimic field of degree 8 and $|D(\mathbb{K})| = 2^8 \times 5^6$. Consider the principal ideal $\mathcal{M} = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)\mathcal{O}_{\mathbb{K}}$ of norm $N(\mathcal{M}) = 80$. For any $\alpha \in \mathcal{M}$, $\alpha = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)\left(\sum_{i=0}^{7} a_i\zeta_{20}^i\right)$, $a_i \in \mathbb{Z}$. Then, $Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\overline{\alpha}) = 40\left(S + \sum_{i=0}^{7} a_i^2\right)$ where $S \in \mathbb{Z}$. So $t_{\mathcal{M}} = 40$ and

$$\delta = \frac{40^4}{2^8 \times 80 \times \sqrt{2^8.5^6}} = \frac{1}{16}$$

that is the optimal density center in dimension 8.

6 Acknowledgments

We are grateful to FAPESP, 2013/25977-7, by financial support.

7 References

[1] Leopoldt, H.-W., *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. 201 (1959), 119-149.

[2] Lettl, Günter. *The ring of integers of an abelian number field*, J. reine angew. Math. 404 (1990), 162-170.

[3] Shah, S.I.A., Nakahara, T. *Monogenesis of the rings of integers in certain imaginary abelian fields*, Nagoya Math. J. Vol. 168 (2002), 85-92.

[4] Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer Verlag, New York, 2001.

[5] Laurent, W., *Introduction to cyclotomic fields*, Springer Verlag, New York, 1982.