Root Systems and Root Lattices in Number Fields

Vladimir L. Popov

Steklov Mathematical Institute
Russian Academy of Sciences, Moscow

Online seminar
Quadratic Forms, Linear Algebraic Groups and Beyond
March 10, 2021
`https://qflag.org/`

This talk is based on the following papers joint with Yu. G. Zarhin:

[1] Vladimir L. Popov, Yuri G. Zarhin, *Root systems in number fields*, Indiana University Mathematics Journal **70** (2021), no. 1, 285–300.

[2] Vladimir L. Popov, Yuri G. Zarhin, *Root lattices in number fields*, Bulletin of Mathematical Sciences (2020), `https://doi.org/10.1142/S1664360720500216`.

[3] V. L. Popov, Yu. G. Zarhin, *Rings of integers in number fields, and root lattices*, Doklady Mathematics **101** (2020), no. 3, 221–223.

Starting point

Construction of a root system $\mathbf{G_2}$:

J-P. Serre, ***Lie Algèbres de Lie Semi-simples Complexes*****, Benjamin, New York, 1966, §16:**

"This system can be described as the set of algebraic integers of a cyclotomic field generated by a cubic root of unity, with the norm 1 or 3."

Part 1: Realization of root systems in number fields

Root systems: reminder

Let V be a finite-dimensional vector space over $\mathbb{Q}$ and let $v \in V$ be a nonzero vector.

A linear map $\varrho\colon V \to V$ is called a **reflection with respect to v** if

- $\varrho(v) = -v$,
- V^{ϱ} is a hyperplane in V.

In this case, for the linear operator $\varrho - \mathrm{id}$,

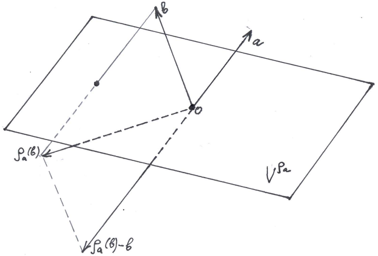
- the *image* of $\varrho - \mathrm{id}$ is the line $\mathbb{Q}v$,
- the *kernel* of $\varrho - \mathrm{id}$ is the hyperplane V^{ϱ}.

Root systems: reminder

Definition

Let V be the $\mathbb{Q}$-linear span of a finite set R and $0 \notin R$. If the following hold, then R is called a <u>**root system in V**</u>:

- for every $a \in R$, there is a reflection ϱ_a with respect to a such that $\varrho_a(R) = R$ (such a ϱ_a is automatically unique);
- $(\varrho_a - \mathrm{id})(b) \in \mathbb{Z}a$ for all $a, b \in R$.



Root systems: reminder

Properties and terminology:

Let R be a root system in V.

• The $\mathbb{Z}$-linear span of R in V is a free $\mathbb{Z}$-module of rank $\dim V$. Its rank is called the **rank of R**.

• The group $W(R)$ generated by all reflections ϱ_a, $a \in R$, is finite and called the **Weyl group** of the root system R.

The type of Dynkin diagram of R is called the **type of R.**

Let L be a free $\mathbb{Z}$-module of finite rank $n > 0$ considered as a subset of the $\mathbb{Q}$-vector space $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$.

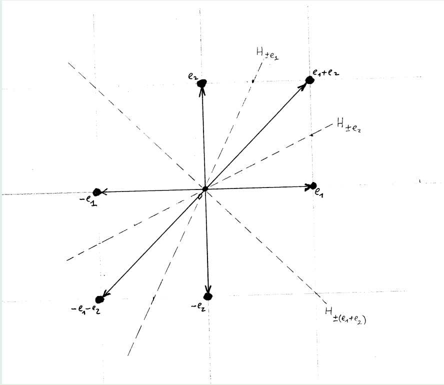
Every type R of root systems of rank n is realizable in L:

there is a root system R in V of type R such that $R \subset L$.

However, if the pair (V, L) is endowed with an additional structure, then the Weyl $W(R)$ may not be consistent with it. For instance, if V is endowed with an inner product, then $W(R)$ may contain nonorthogonal transformations.

Example

Let $n = 2$ and let $e_1, e_2 \in L$ be an orthonormal basis in V. Then $R = \{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}$ is the root system in V of type A_2. Not all transformations from the Weyl group $W(R)$ are orthogonal.



A natural source of pairs (V, L) is **algebraic number theory**, in which they arise in the form $(K, \mathscr{O})$, where **K is a number field** and **$\mathscr{O}$ is the ring of integers of K**.

Some additional structures/objects are naturally associated with every pair $(K, \mathscr{O})$. Among them are the following **three subgroups in $\mathrm{GL}_{\mathbb{Q}}(K)$**:

- the automorphism group $\mathrm{Aut}(K)$ of the field K;

- the group $\mathrm{mult}(K^*)$, where $\mathrm{mult}(a)$ is the operator of multiplication by $a \in K^*$:

$$\mathrm{mult}(a)\colon\ K \to K,\ x \mapsto ax.$$

- the group $\mathcal{L}(K)$ generated by $\mathrm{Aut}(K)$ and $\mathrm{mult}(K^*)$.

Realizations of a root system type in a number field

Definition

We say that a type R of (not necessarily reduced) root systems **admits a realization in a number field** K, if

- $[K:\mathbb{Q}] = \mathrm{rk}(\mathrm{R})$;

- there is a subset R of rank $\mathrm{rk}(\mathrm{R})$ in $\mathscr{O}$, which is a root system of type R such that $W(R)$ is a subgroup of the group $\mathcal{L}(K)$.

In this case, R is called a **realization of the type** R **in the field** K.

Remark

In this definition, replacing $\mathscr{O}$ by K does not yield a broader concept

Explanation:

In this case, there is a nonzero $m \in \mathbb{Z}$ such that

$$m \cdot R := \{m\alpha \mid \alpha \in R\} \subset \mathscr{O}.$$

The set $m \cdot R$ has rank $\mathrm{rk}(\mathrm{R})$, it is a root system in K of type R, and $W(m \cdot R) = W(R)$.

Integer elements of a fixed norm

Notation:

$\mathscr{O}(d)$ is the set of all elements of $\mathscr{O}$, whose norm is d.

Realizations of rank 1 root system types in number fields

Root systems of types A_1 and BC_1:

Take $K = \mathbb{Q}$. Then $\mathscr{O} = \mathbb{Z}$ and $\mathcal{L}(K) = \mathrm{mult}(\mathbb{Q}^*)$.

Let $\alpha \in \mathbb{Z}$, $\alpha \neq 0$. Then

$$R := \{\pm\alpha\} \text{ и } R := \{\pm\alpha, \pm 2\alpha\}$$

are the realizations of types A_1 and BC_1 in the field K.

Root systems of types $\mathbf{A_2}$ and $\mathbf{G_2}$:

Let K be the third cyclotomic field:

$$K = \mathbb{Q}(\sqrt{-3}).$$

Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = e^{2\pi i/6} = (1 + i\sqrt{3})/2$, and $\mathrm{Aut}(K) = \langle c \rangle$, where c is the complex conjugation $a \mapsto \overline{a}$.

Every element $a \in \mathcal{L}(K)$ of a finite order is the orthogonal transformation $a : K \to K$ with respect to the Euclidean structure on K:

$$K \times K \to \mathbb{Q},\ (a, b) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(a\overline{b}) = 2\mathrm{Re}(a\overline{b}),$$

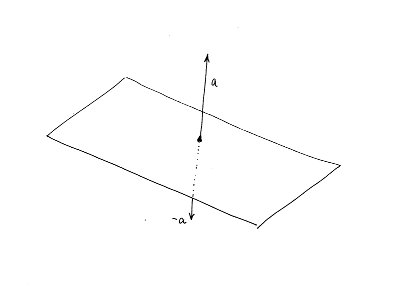
Realizations of rank 2 root system types in number fields

Example

For every nonzero element $a \in K$, the operator

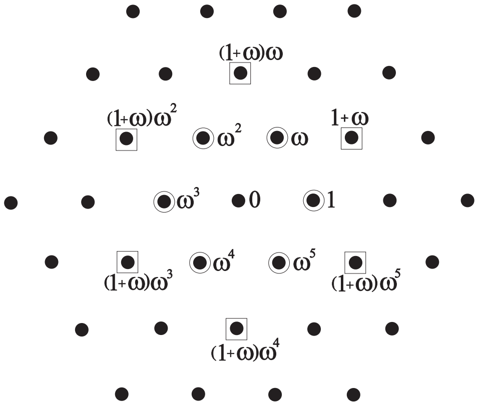
$$r_a := \mathrm{mult}(-a\overline{a}^{-1})c \in \mathcal{L}(K)$$

is a reflection with respect to a.



Realizations of rank 2 root system types in number fields

$\mathscr{O}(1) = \{\pm 1, \pm\omega, \pm\omega^2\}$ (all 6th roots of 1).
$\mathscr{O}(3) = (1+\omega)\mathscr{O}(1)$.



Realizations of rank 2 root system types in number fields

$$\mathscr{O}(1) = \{\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1+\alpha_2)\} \text{ where } \alpha_1 = 1,\ \alpha_2 = \omega^2.$$

Therefore,

- $\mathscr{O}(1)$ is the root system in K of type A_2 with the base α_1, α_2.
- $\mathscr{O}(3)$ is the root system in K of type A_2 with the base $\beta_1 = (1+\omega)\alpha_1$, $\beta_2 = (1+\omega)\alpha_2$.
- $\mathscr{O}(1) \bigcup \mathscr{O}(3)$

$$= \{\pm\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2), \pm(3\alpha_1+\beta_2), \pm(3\alpha_1+2\beta_2)\}$$

is the root system in K of type G_2 with the base α_1, β_2.

Realizations of rank 2 root system types in number fields

For every $a \in \mathscr{O}(1) \bigcup \mathscr{O}(3)$ and positive integer d,

$$r_a(\mathscr{O}(d)) = \mathscr{O}(d).$$

Therefore, $W(\mathscr{O}(1))$, $W(\mathscr{O}(3))$, and $W(\mathscr{O}(1) \bigcup \mathscr{O}(3))$ are the subgroups of $\mathcal{L}(K)$. Hence

- $\mathscr{O}(1)$ is the realization of type A_2 in the field K,
- $\mathscr{O}(3)$ is the realization of type A_2 in the field K,
- $\mathscr{O}(1) \bigcup \mathscr{O}(3)$ is the realization of type G_2 in the field K

Realizations of rank 2 root system types in number fields

Root systems of types $\mathbf{B}_2$, $\mathbf{2A}_1$, $\mathbf{BC}_2$, $\mathbf{2BC}_1$, and $\mathbf{A}_1 \dot{+} \mathbf{BC}_1$:

Let K be the fourth cyclotomic field:

$$K = \mathbb{Q}(\sqrt{-1}).$$

Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}i$ and $\mathrm{Aut}(K) = \langle c \rangle$, where c is the complex conjugation $a \mapsto \overline{a}$.

Every element $a \in \mathcal{L}(K)$ of a finite order is the orthogonal transformation $a : K \to K$ with respect to the same Euclidean structure on K as above:

$$K \times K \to \mathbb{Q},\ (a, b) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(a\overline{b}) = 2\mathrm{Re}(a\overline{b}),$$

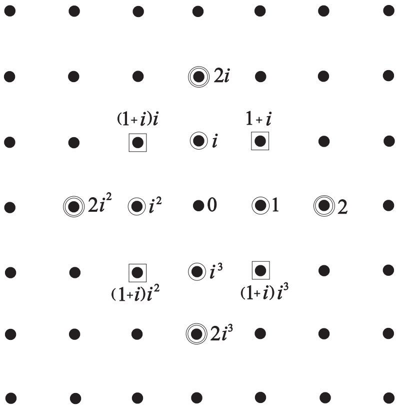
As above, for every nonzero element $a \in K$, the operator

$$r_a := \mathrm{mult}(-a\overline{a}^{-1})c \in \mathcal{L}(K)$$

is a reflectrion with respect to a.

Realizations of rank 2 root system types in number fields

$\mathscr{O}(1) = \{\pm 1, \pm i\}$ (all 4th of 1).
$\mathscr{O}(2) = (1+i)\mathscr{O}(1)$.
$\mathscr{O}(4) = 2\mathscr{O}(1)$.



Realizations of rank 2 root system types in number fields

$\mathscr{O}(1) = \{\pm\alpha_1, \pm\alpha_2\}$ where $\alpha_1 = 1$, $\alpha_2 = i$.

Therefore,

• $\mathscr{O}(1)$, $\mathscr{O}(2)$, $\mathscr{O}(4)$ are the root systems in K of type $\mathrm{A}_1 \dot{+} \mathrm{A}_1$ resp. with the base

$$\alpha_1, \alpha_2, \quad \beta_1 = (1+i)\alpha_1, \beta_2 = (1+i)\alpha_2, \quad \text{and} \quad 2\alpha_1,\ 2\alpha_2.$$

• $\mathscr{O}(1) \bigcup \mathscr{O}(2) = \{\pm\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2)\}$, is the root system in K of type B_2 with the base α_1, β_2.

Realizations of rank 2 root system types in number fields

- $\mathscr{O}(1)\bigcup\mathscr{O}(4)$ is the root system in K of type $2\mathsf{BC}_1$ with the base α_1, α_2.

- $\mathscr{O}(1)\bigcup\{\pm 2\}$ is the root system in K of type $\mathsf{A}_1 \dotplus \mathsf{BC}_1$ with the base α_1, α_2.

- $\mathscr{O}(1)\bigcup\mathscr{O}(2)\bigcup\mathscr{O}(4)$
$$= \{\pm\alpha_1, \pm 2\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm 2(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2)\},$$

is the root system in K of type BC_2 with the base α_1, β_2.

Realizations of rank 2 root system types in number fields

For every $a \in \mathscr{O}(1) \bigcup \mathscr{O}(2)$ and positive integer d,

$$r_a(\mathscr{O}(d)) = \mathscr{O}(d).$$

Therefore, $W(\mathscr{O}(1))$, $W(\mathscr{O}(1)) \bigcup W(\mathscr{O}(2))$, $W(\mathscr{O}(1) \bigcup \mathscr{O}(4))$, $W(\mathscr{O}(1) \bigcup \mathscr{O}(2) \bigcup \mathscr{O}(4))$, $W(\mathscr{O}(1) \bigcup \{\pm 2\})$ are the subgroups of $\mathcal{L}(K)$. Hence

- $\mathscr{O}(1)$ is the realization of type $\mathsf{A}_1 \dot{+} \mathsf{A}_1$ in the field K,
- $\mathscr{O}(1) \bigcup \mathscr{O}(2)$ is the realizations of type B_2 in the field K,
- $\mathscr{O}(1) \bigcup \mathscr{O}(4)$ is the realizations of type $\mathsf{BC}_1 \dot{+} \mathsf{BC}_1$ in the field K,
- $\mathscr{O}(1) \bigcup \mathscr{O}(2) \bigcup \mathscr{O}(4)$ is therealizations of type BC_2 in the field K,
- $\mathscr{O}(1) \bigcup \{\pm 2\}$ is the realizations of type $\mathsf{A}_1 \dot{+} \mathsf{BC}_1$ in the field K

Arbitrary rank case

Theorem

The following properties of the Weyl group of a reduced root system of type R *and rank* n *are equivalent:*

- *This Weyl group is isomorphic to a subgroup of the group* $\mathcal{L}(K)$*, where* K *is a number field of degree* n *over* $\mathbb{Q}$*.*
- R *is contained in the following list:*

$$\mathsf{A}_1,\quad \mathsf{A}_2,\quad \mathsf{B}_2,\quad \mathsf{G}_2,\quad \mathsf{A}_1 \dotplus \mathsf{A}_1,\quad \mathsf{A}_1 \dotplus \mathsf{A}_1 \dotplus \mathsf{A}_2,\quad \mathsf{A}_2 \dotplus \mathsf{B}_2.$$

Comparing this theorem with the next one shows the following:

The existence of an isomorphism between a subgroup G of the group $\mathcal{L}(K)$ and the Weyl group of a root system of rank $[K : \mathbb{Q}]$ and type R **is not equivalent** to the fact that $G = W(R)$, where R is a root system of type R in $\mathscr{O}$.

Classification of root systems types realizable in numeric fields

Theorem

For every type R *of root systems (not necessarily reduced), the following properties are* *equivalent:*

- *There is a number field, in which* R *admits a realization;*
- $\mathrm{rk}(\mathrm{R}) = 1$ *or* 2.

Part 2: Realizations of root lattices in number fields

Lattices

Definition

We call a **lattice** every pair (L, b), where L is a free $\mathbb{Z}$-module of a finite rank, and

$$b\colon L \times L \to \mathbb{Z}$$

is a *nondegerate symmetric* bilinear form.

In what follows, L is always considered as an additive subgroup in the vector space $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$ над $\mathbb{Q}$.

Definitions

Definition

A nonzero lattice (L, b) is called **primitive**, if the greatest common divisor of all integers $b(x, y)$, where $x, y \in L$, equals 1.

Definition

A lattice (L, b) is called **even** if $b(x, x) \in 2\mathbb{Z}$ for all $x \in L$.

Definitions

Definition

A lattice is called **indecomposable** if it is inexpressible as orthogonal direct sum of nonzero sublattices

Definition

A lattice (L_1, b_1) is called **similar** to a lattice (L_2, b_2) if there are integers $m_1, m_2 \in \mathbb{Z}$ such that $(L_1, m_1 b_1)$ and $(L_2, m_2 b_2)$ are isometric.

Notation

The orthogonal direct sum of s copies of a lattice (L, b) is denoted by $(L, b)^s$.

Root lattices

Definition

A nonzero lattice is called a **root lattice** if it is isometric to orthogonal direct sum of lattices belonging to the union of two infinite series $\mathbb{A}_\ell$ $(\ell \geqslant 1)$, $\mathbb{D}_\ell$ $(\ell \geqslant 4)$, and four sporadic lattices $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$, whose explicit description is given below.

Notation

• $\mathbb{R}^m$ is the m-dimensional coordinate real vector space of rows endowed with the standard Euclidean structure

$$\mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}, \quad ((x_1, \ldots, x_m), (y_1, \ldots, y_m)) := \textstyle\sum_{j=1}^m x_j y_j. \quad (*)$$

• $e_j := (0, \ldots, 0, 1, 0, \ldots, 0)$, where 1 is on the jth position.

• If L is the $\mathbb{Z}$-linear span of a set of linearly independent elements of $\mathbb{R}^m$ such that $b(L \times L) \subseteq \mathbb{Z}$, where b is the restriction of map $(*)$ to $L \times L$, then (L, b) is called a lattice in $\mathbb{R}^m$ and denoted just by L.

Then, using these notation and conventions,

- $\mathbb{Z}^n$ is the lattice $\{(x_1, \dots, x_n) \mid x_j \in \mathbb{Z} \text{ for all } j\}$ in $\mathbb{R}^n$.
- $\mathbb{A}_n$ is the lattice $\{(x_1, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid \sum_{j=1}^{n+1} x_j = 0\}$ in $\mathbb{R}^{n+1}$.
- $\mathbb{D}_n$ is the lattice $\{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid \sum_{j=1}^{n} x_j \text{ is even}\}$ in $\mathbb{R}^n$, $n \geqslant 4$.
- $\mathbb{E}_8$ is the lattice $\mathbb{D}_8 \bigcup \left(\mathbb{D}_8 + \frac{1}{2}(e_1 + \cdots + e_8)\right)$ in $\mathbb{R}^8$.
- $\mathbb{E}_7$ is the orthogonal in $\mathbb{E}_8$ of the sublattice $\mathbb{Z}(e_7 + e_8)$.
- $\mathbb{E}_6$ is the orthogonal in $\mathbb{E}_8$ of the sublattice $\mathbb{Z}(e_7 + e_8) + \mathbb{Z}(e_6 + e_8)$.

Properties of lattices $\mathbb{A}_\ell$, $\mathbb{D}_\ell$, $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$

- $\mathbb{A}_\ell$, $\mathbb{D}_\ell$, $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ are indecomposable.

- Decomposition of any root lattice as orthogonal direct sum of indecomposable lattices (called its **indecomposable components**) is unique.

- $\mathbb{A}_\ell$ при $\ell \neq 1$, $\mathbb{D}_\ell$, $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ are primitive.

- $\mathbb{A}_1$ is not primitive.

- $\mathbb{A}_\ell$, $\mathbb{D}_\ell$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ are even.

- $\mathbb{Z}^1$ is not even.

Root lattices and root systems

• If R is a root system in a vector space V over $\mathbb{Q}$, and $L = \mathbb{Z}R$, then there is bilinear form $b\colon L \times L \to \mathbb{Z}$ such that (L, b) is a root lattice.

• Every root lattice is obtained in this fashion (generally speaking, not in the only way).

• If R is irreducible, then in all cases except type $\mathbb{A}_1$, the bilinear form b is uniquely determined by R and the set of following four conditions:

(a) b is invariant with respect to the Weyl group $W(R)$,
(b) b takes values in $\mathbb{Z}$,
(c) b is positive-definite.
(d) (L, b) is primitive.

Root lattices and root systems

For an irreducible reduced root system R, the relationship between the type of R and the type of the root lattice (L, b) is given by the following table:

type of R	type of (L, b)
A_ℓ, $\ell \geqslant 1$	$\mathbb{A}_\ell$
B_ℓ, $\ell \geqslant 2$	$\mathbb{Z}^\ell$
C_ℓ, $\ell \geqslant 3$	$\mathbb{D}_\ell$
C_2	$\mathbb{Z}^2$
D_ℓ, $\ell \geqslant 3$	$\mathbb{D}_\ell$
E_ℓ, $\ell = 6, 7, 8$	$\mathbb{E}_\ell$
F_4	$\mathbb{D}_4$
G_2	$\mathbb{A}_2$

Theorem (E. Witt)

A lattice (L, b) is a root lattice if and only if the following two conditions hold:

(i) *the form b is positive-definite;*

(ii) *the $\mathbb{Z}$-module L is generated by the set*

$$\{x \in L \mid b(x,x) = 1 \text{ or } 2\}.$$

In view of Witt's theorem, all root lattices are split into the following **three disjoint types**:

Three types of root lattices

- **Root lattices of unmixed type** I

These are the lattices (L, b), for which the $\mathbb{Z}$-module L is generated by the set $\{x \in L \mid b(x, x) = 1\}$.

Equivalent description :

These are exactly all lattices isometric to $\mathbb{Z}^n$.

Three types of root lattices

- **Root lattices of unmixed type** II

These are the lattices (L, b), for which the $\mathbb{Z}$-module L is generated by the set $\{x \in L \mid b(x,x) = 2\}$.

Equivalent description:

These are exactly all even root lattices.

One more equivalent description:

These are exactly all root lattices, all of whose indecomposable components are not isometric to $\mathbb{Z}^1$.

Three types of root lattices

- **Root lattices of mixed type**

These are all other root lattices.

Constructions of lattices in number fields

Algebraic number theory is a natural source of lattices. Namely:

Let K be a number field, let $\mathscr{O}$ be the ring of integers of K, and

$$n := [K : \mathbb{Q}] < \infty.$$

Let $\sigma_1, \ldots, \sigma_n$ be the set of all field embeddings $K \hookrightarrow \mathbb{C}$.

A classical construction of geometric representation of algebraic numbers embeds K into the space $\mathbb{R}^n$ endowed with the standard Euclidean structure. This endows K (and hence $\mathscr{O}$) with the following $\mathbb{Q}$-bilinear form:

$$b_K\colon K \times K \to \mathbb{C}, \quad b_K(x,y) := \textstyle\sum_{j=1}^n \sigma_j(x)\overline{\sigma_j(y)}.$$

Constructions of lattices in number fields

Theorem

- *The $\mathbb{Q}$-linear span of the set $b_K(K \times K)$ is a proper subset of $\mathbb{R}$ containing $\mathbb{Q}$.*
- *The bilinear form b_K is symmetric and positive-definite.*
- *Properties (a), (b), (c) listed below are equivalent:*
  - (a) $b_K(K \times K) = \mathbb{Q}$.
  - (b) $b_K(\mathscr{O} \times \mathscr{O}) \subseteq \mathbb{Q}$.
  - (c) *There is $\tau \in \operatorname{Aut} K$ such that $\tau^2 = \operatorname{id}$ and*

$$b_K(x, y) = \operatorname{Trace}_{K/\mathbb{Q}}(x \cdot \tau(y)) \quad \text{for all } x, y \in K.$$

- *If (c) holds, then either K is totally real and $\tau = \operatorname{id}$ or K is a CM-field and τ is the complex conjugation.*

Constructions of lattices in number fields

Generalization of the classical construction

We fix an involutive automorphism

$$\theta \in \operatorname{Aut} K, \quad \theta^2 = \mathrm{id}.$$

Then

$$\mathrm{tr}_{K,\theta}\colon K \times K \to \mathbb{Q}, \quad \mathrm{tr}_{K,\theta}(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \theta(y))$$

is a nondegenerate symmetric bilinear form and for every nonzero ideal I in $\mathscr{O}$, the pair

$$(I, \mathrm{tr}_{K,\theta}) := (I, \mathrm{tr}_{K,\theta}|_{I \times I})$$

is a lattice of rank n.

Constructions of lattices in number fields

Further generalization

Let J be a nonzero (fractional) ideal of K, and let $a \in K$ be a nonzero element such that $\theta(a) = a$, $\mathrm{Trace}_{K/\mathbb{Q}}(ax \cdot \theta(y)) \in \mathbb{Z}$ for all $x, y \in J$. Let

$$\mathrm{tr}_{K,\theta,J,a}\colon J \times J \to \mathbb{Z}, \quad \mathrm{tr}_{K,\theta,J,a}(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(ax \cdot \theta(y)).$$

Then $(J, \mathrm{tr}_{K,\theta,J,a})$ is a lattice of rank n.

The origins of this construction essentially go back to Gauss:

for $n = 2$ and $a = 1/\mathrm{Norm}_{K/\mathbb{Q}}(J)$ it gives the classical correspondence between ideals and quadratic binary forms established by Gauss.

Remarkable lattices of the form $(J, \mathrm{tr}_{K,\theta,J,a})$

Some remarkable lattices are isometric to lattices of the form $(J, \mathrm{tr}_{K,\theta,J,a})$.

Examples, in which K is a dth cyclotomic field

- Root lattices $\mathbb{A}_{p-1}$ with odd prime p for $d = p$ (Ebeling).
- Root lattices $\mathbb{E}_6$ and $\mathbb{E}_8$, for $d = 9$ and resp. $d = 15, 20, 24$ (Bayer-Fluckiger).
- Coxeter–Todd lattice for $d = 21$ (Bayer-Fluckiger, Martinet).
- Leech lattice for $d = 35, 39, 52, 56, 84$ (Bayer-Fluckiger, Quebbemann).
- Classification of root lattices isometric to $(J, \mathrm{tr}_{K,\theta,J,a})$ type lattices is known (Bayer-Fluckiger, Martinet).

Problems

- *Given a lattice* (L, b), *find out whether it is isometric to a lattice of the form* $(J, \mathrm{tr}_{K,\theta,J,a})$ *for suitable* K, θ, J, a.
- *Given a lattice* (L, b), *a field* K, *and its nonzero ideal* J, *find out if there are* θ *and* a *such that* $(J, \mathrm{tr}_{K,\theta,J,a})$ *and* (L, b) *are isometric lattices.*

Among all nonzero ideals of K there is a naturally distinguished one, namely, $\mathscr{O}$. For it, there is a naturally distinguished a suitable for all automorphisms θ, namely, $a = 1$.

This leads to the **problem of finding remarkable lattices isometric (or, more generally, similar) to lattices of the form $(\mathscr{O}, \mathrm{tr}_{K,\theta})$**.

Below this problem is considered for root lattices.

Problems

Problems

(**R**) *Classify pairs K, θ, for which $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is a root lattice.*

(**S**) *Generalization: Classify pairs K, θ, for which $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to a root lattice.*

The following examples show that pairs K, θ with the indicated properties do exist.

Example

Let $n = 1$.
Тогда $K = \mathbb{Q}$, $\mathscr{O} = \mathbb{Z}$, $\theta = \mathrm{id}$, and $\mathrm{Trace}_{K/\mathbb{Q}}(x) = x$ for all $x \in K$.
Therefore, in this case, $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is the root lattice $\mathbb{Z}^1$ (which is similar but not isometric to the lattice $\mathbb{A}_1$).

Examples of root lattices of the form $(\mathscr{O}, \mathrm{tr}_{K,\theta})$

Example

Let $n = 2$ and let K be the 3rd cyclotomic field: $K = \mathbb{Q}(\sqrt{-3})$. Let θ be the complex conjugation. Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + \sqrt{-3})/2$, and

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = x + \theta(x) = 2\mathrm{Re}(x) \text{ for all } x \in K.$$

Therefore, $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is the root lattice isometric to $\mathbb{A}_2$.

Example

Let $n = 2$ and let K be the 4th cyclotomic field: $K = \mathbb{Q}(\sqrt{-1})$. Let θ be the complex conjugation. Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ and

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = x + \theta(x) = 2\mathrm{Re}(x) \text{ for all } x \in K.$$

Therefore, $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is the root lattice isometric to $\mathbb{A}_1^2$.

Solution to Problem (R):

Theorem

The following properties of a pair K, θ are equivalent:

- $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is a root lattice;*
- K, θ *is one of the following three pairs:*
  - $K = \mathbb{Q}$, $\theta = \mathrm{id}$;
  - $K = \mathbb{Q}(\sqrt{-3})$, θ *is the complex conjugation;*
  - $K = \mathbb{Q}(\sqrt{-1})$, θ *is the complex conjugation.*

Problem (S)

Let us now consider problem (S) on the classification of lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$, which are similar (but not necessarily isometric) to root lattices. It appears that there are many more of them, than the lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$, which are root ones.

Notation:

m is the unique positive integer such that

$$\mathrm{Trace}_{K/\mathbb{Q}}(\mathscr{O}) = m\mathbb{Z}$$

(such m exists because $\mathrm{Trace}_{K/\mathbb{Q}}\colon \mathscr{O} \to \mathbb{Z}$ is a nonzero additive group homomorphism).

Classification of lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of unmixed type I

Theorem

The following properties of a pair K, θ are equivalent:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to* $\mathbb{Z}^n$;

(b) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to* $\mathbb{A}_1^n$;

(c) $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is isometric to* $\mathbb{Z}^n$;

(d) $(\mathscr{O}, 2\,\mathrm{tr}_{K,\theta}/m)$ *is isometric to* $\mathbb{A}_1^n$;

(e) K *is a* 2^a*th cyclotomic field, where* $a \in \mathbb{Z}$, $a > 0$, *and* θ *is the complex conjugation if* $a > 1$, *and* $\theta = \mathrm{id}$ *if* $a = 1$.

If these properties hold, then $n = 2^{a-1}$ *and* $m = n$.

In (e), *let* $\zeta_{2^a} \in K$ *be a* 2^a*th primitive root of* 1, *and let* $x_j := \zeta_{2^a}^j$. *Then the set of all indecomposable components of the root lattice* $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *coincides with the set of all its sublattices* $\mathbb{Z}x_j$, $0 \leqslant j \leqslant 2^{a-1} - 1$. *For every* j, *the value of* $\mathrm{tr}_{K,\theta}/m$ *at* (x_j, x_j) *is* 1.

Classification of lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of unmixed type II

Theorem

The following properties of a pair K, θ are equivalent:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to an even primitive root lattice.*

(b) $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is an even primitive root lattice.*

(c) *n is even and $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is isometric to $\mathbb{A}_2^{n/2}$.*

(d) *K is a 2^a3^bth cyclotomic field, where $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, and θ is the complex conjugation.*

If these properties hold, then $n = 2^a3^{b-1}$ and $m = n/2$.

In (d), let ζ_{2^a} and $\zeta_{3^b} \in K$ be respectively a primitive 2^ath and $3^b$the roots of 1. Let $x_{i,j} := \zeta_{2^a}^i \zeta_{3^b}^j$. Then the set of all indecomposable components of the root lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ coincides with the set of all its sublattices $\mathbb{Z}x_{i,j} + \mathbb{Z}x_{i,j+3^{b-1}}$, $0 \leqslant i \leqslant 2^{a-1} - 1$, $0 \leqslant j \leqslant 3^{b-1} - 1$. For all i, j, the values of $\mathrm{tr}_{K,\theta}/m$ at $(x_{i,j}, x_{i,j})$, $(x_{i,j+3^{b-1}}, x_{i,j+3^{b-1}})$, and $(x_{i,j}, x_{i,j+3^{b-1}})$ are, respectively, 2, 2 and -1.

Application: $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ and the Leech lattice

Since $\mathbb{E}_8$ is the unique (up to isometry) positive-definite even unimodular lattice of rank 8, as a corollary of the previous theorem, we obtain

Theorem

Every lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is not similar to the Leech lattice.

Application: $(\mathscr{O}, \operatorname{tr}_{K,\theta})$ and positive-definite even unimodular lattices

In fact, we obtain a more general result:

Theorem

Every positive-definite even unimodular lattice of rank $\leqslant 48$
not similar to a lattice of the form $(\mathscr{O}, \operatorname{tr}_{K,\theta})$.

This theorem excludes many lattices from being similar to lattices of the form $(\mathscr{O}, \operatorname{tr}_{K,\theta})$. Indeed, if $\Phi(r)$ is the number of pairwise nonisometric positive-definite even unimodular lattices of rank r, then

$$\Phi(8) = 1,\ \Phi(16) = 2,\ \Phi(24) = 24,\ \Phi(32) \geqslant 10^7,\ \Phi(48) \geqslant 10^{51}.$$

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type

Notation:

μ_K is the (finite cyclic) multiplicative group of all roots of 1 in K.

$\bigoplus$ denotes the orthogonal direct sum of lattices.

Restrictions on lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$, similar to root lattices of mixed type

Theorem

If $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to a root lattice of mixed type, then

(a) $m = n > 1$;

(b) *all prime numbers dividing the number n are ramified in the field extension $K/\mathbb{Q}$ and if a prime $p \in \mathbb{Z}$ is ramified in $K/\mathbb{Q}$, then $p \leqslant n$;*

(c) *the discriminant of $K/\mathbb{Q}$ is divisible by n^n;*

(d) $|\mu_K| = 2^a$ *for a certain $a \in \mathbb{Z}$, $a > 0$; the number 2^{a-1} divides n, but is not equal to it;*

(e) $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is isometric to a root lattice $\mathbb{Z}^{2^{a-1}} \oplus L$, where L is a nonzero even root lattice whose rank is divisible by 2^{a-1}, and $\mu_K = \{x \in \mathscr{O} \mid (\mathrm{tr}_{K,\theta}/m)(x, x) = 1\}$;*

Quadratic fields K with lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to a root lattice of mixed type

Theorem

If K is a quadratic (i.e., $n = 2$) field, then the following two properties of a pair K, θ are equivalent:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to a root lattice of mixed type;*

(b) *either K is isomorphic to $\mathbb{Q}(\sqrt{2})$ and $\theta = \mathrm{id}$, or K is isomorphic to $\mathbb{Q}(\sqrt{-2})$ and θ is the complex conjugation.*

If (a), (b) *hold, then $(\mathscr{O}, \mathrm{tr}_{K,\theta}/2)$ is isometric to the lattice $\mathbb{Z}^1 \oplus \mathbb{A}_1$.*

Cubic fields K with lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to a root lattice of mixed type

Theorem

If K is a cubic (i.e., $n = 3$) totally real field and $\theta = \mathrm{id}$, then the following two properties of a pair K, θ are equivalent:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to a root lattice of mixed type;*

(b) K *is the maximal totally real subfield of a 9th cyclotomic field.*

If (a), (b) *hold, then* $(\mathscr{O}, \mathrm{tr}_{K,\theta}/3)$ *is isometric to the root lattice* $\mathbb{Z}^1 \oplus \mathbb{A}_2$.

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type: Examples

The following group of examples gives an infinite series of pairs K, θ, for which $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to a root lattice of mixed type.

The construction uses cyclotomic fields $\mathbb{Q}(\zeta_d)$, where ζ_d is a primitive root of 1 of degree d, and their maximal totally real subfields

$$\mathbb{Q}(\zeta_d)^+ := \mathbb{Q}(\zeta_d + \zeta_d^{-1}).$$

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type: Examples

Example (A. A. Andrade and J. C. Interlando)

Let $a \in \mathbb{Z}$, $a > 2$ and let

$$K = \mathbb{Q}(\zeta_{2^a})^+, \quad \theta = \mathrm{id}.$$

Then

$$m = n = 2^{a-2} \quad \text{and}$$

$(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is <u>isometric to the root lattice</u> $\mathbb{Z}^1 \oplus \mathbb{A}_1^{2^{a-2}-1}$.

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type: Examples

Example (E. Bayer-Fluckiger)

Let $b \in \mathbb{Z}$, $b > 1$ and let

$$K = \mathbb{Q}(\zeta_{3^b})^+, \quad \theta = \mathrm{id}.$$

Then

$$m = n = 3^{b-1} \quad \text{and}$$

$$(\mathscr{O}, \mathrm{tr}_{K,\theta}/m) \ \text{ is isometric to the root lattice } \mathbb{Z}^1 \oplus \mathbb{A}_2^{(3^{b-1}-1)/2}.$$

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type: Examples

Example (E. Bayer-Fluckiger and P. Maciak)

Let $a \in \mathbb{Z}$, $a > 2$ and let

$$K = \mathbb{Q}(\zeta_{2^a} - \zeta_{2^a}^{-1}) \subset \mathbb{Q}(\zeta_{2^a}),$$
$$\theta \text{ is the complex conjugation}$$

(this field K is a purely imaginary quadratic extension of the totally real field $\mathbb{Q}(\zeta_{2^{a-1}})^+$). Then

$$m = n = 2^{a-2} \quad \text{and}$$

$(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is <u>isometric to the root lattice</u> $\mathbb{Z}^1 \oplus \mathbb{A}_1^{2^{a-2}-1}$.

Lattices $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to root lattices of mixed type: Examples

Example

Let $a, b \in \mathbb{Z}$, $a > 1$, $b > 1$ and let

$$K = \mathbb{Q}(\zeta_{2^a}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_{3^b})^+ = \mathbb{Q}(\zeta_{2^a}(\zeta_{3^b} + \zeta_{3^b}^{-1})) \subset \mathbb{Q}(\zeta_{2^a 3^b}),$$

θ is the complex conjugation.

Then

$$m = n = 2^{a-1}3^{b-1} \quad \text{and}$$

$(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is <u>isometric to the root lattice</u> $\mathbb{Z}^{2^{a-1}} \oplus \mathbb{A}_2^{2^{a-2}(3^{b-1}-1)}$.