ROOT SYSTEMS IN NUMBER FIELDS

VLADIMIR L. POPOV[1,2] AND YURI G. ZARHIN[3]

Abstract. We classify the types of root systems R in the rings of integers of number fields K such that the Weyl group $W(R)$ lies in the group $\mathcal{L}(K)$ generated by $\mathrm{Aut}(K)$ and multiplications by the elements of K^*. We also classify the Weyl groups of roots systems of rank n which are isomorphic to a subgroup of $\mathcal{L}(K)$ for a number field K of degree n over $\mathbb{Q}$.

1. Introduction

In what follows, we call the type of a (not necessarily reduced) root system the type of its Dynkin diagram.

Let L be a free Abelian group of a finite rank $n > 0$. We shall consider it as a lattice of full rank in the n-dimensional linear space $V := L \otimes_{\mathbb{Z}} \mathbb{Q}$ over $\mathbb{Q}$. Since every root is a integer linear combination of simple roots, for every type R of the root systems of rank n, there is a subset R in L of rank n, which is a root system of type R. However, if the pair (V, L) is endowed with an additional structure, then the Weyl group $W(R)$ of such a realization may be inconsistent with this structure. Say, if the space V is endowed with a scalar product, then it may happen that the group $W(R)$ does not preserve it (for instance, if $n = 2$ and e_1, e_2 is an orthonormal basis in L, then $\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}$ is the root system of type A_2 in V, whose Weyl group does not consist of orthogonal transformations). Therefore, it is of interest only finding such realizations, the Weyl group of which is consistent with some additional structures on the pair (V, L).

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

[1] Steklov Mathematical Institute, Russian Academy of Sciences, Gubkina 8, Moscow 119991, Russia, *popovvl@mi.ras.ru*.

[2] National Research University Higher School of Economics, Myasnitskaya 20, Moscow 101000, Russia.

[3] Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA, *zarhin@math.psu.edu*.

The second named author (Y. Z.) is partially supported by Simons Foundation Collaboration grant # 585711. Part of this work was done during his stay in May–July 2018 at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

ring of integers. In this case, three subgroups are naturally distinguished in the group $\mathrm{GL}_{\mathbb{Q}}(K)$ of nondegenerate linear transformations of the linear space K over $\mathbb{Q}$. The first one is the automorphism group $\mathrm{Aut}(K)$ of the field K. The second is the image of the group monomorphism

$$\mathrm{mult}\colon K^* \hookrightarrow \mathrm{GL}_{\mathbb{Q}}(K), \tag{1}$$

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

$$\mathrm{mult}(a)\colon K \to K,\ x \mapsto ax. \tag{2}$$

The third one is the subgroup $\mathcal{L}(K)$ in $\mathrm{GL}_{\mathbb{Q}}(K)$ generated by $\mathrm{Aut}(K)$ and $\mathrm{mult}(K^*)$.

Definition 1. We say that *the type* R *of* (*not necessarily reduced*) *root systems admits a realization in the number field* K if

(a) $[K:\mathbb{Q}] = \mathrm{rk}(\mathsf{R})$;
(b) there is a subset R of rank $\mathrm{rk}(\mathsf{R})$ in $\mathscr{O}_K$, which is a root system of type R;
(c) $W(R)$ is a subgroup of the group $\mathcal{L}(K)$.

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

It is worth noting that if we replace $\mathscr{O}_K$ by K in (b), we do not obtain a broader concept. Indeed, if R is a subset of rank $\mathrm{rk}(\mathsf{R})$ in K, which is a root systen of type R such that (a) and (c) hold, then there is a positive integer m such that $m\cdot R := \{m\alpha \mid \alpha \in R\} \subset \mathscr{O}_K$. Clearly the set $m\cdot R$ has rank $\mathrm{rk}(\mathsf{R})$, it is a root system of type R, and $W(m\cdot R) = W(R)$.

In view of Definition 1, if a type R of root systems admits a realization in a number field K, then the group $\mathcal{L}(K)$ contains a subgroup isomorphic to the Weyl group of a root system of type R. Our first main result is the classification of all the cases when the latter property holds:

Theorem 1. *The following properties of the Weyl group $W(R)$ of a reduced root system R of type R and rank n are equivalent:*

(i) *$W(R)$ is isomorphic to a subgroup G of the group $\mathcal{L}(K)$, where K is a number field of degree n over $\mathbb{Q}$;*
(ii) *R is contained in the following list:*

$$\mathsf{A}_1,\ \mathsf{A}_2,\ \mathsf{B}_2,\ \mathsf{G}_2,\ 2\mathsf{A}_1,\ 2\mathsf{A}_1 \dotplus \mathsf{A}_2,\ \mathsf{A}_2 \dotplus \mathsf{B}_2. \tag{3}$$

The fact that a subgroup G of the group $\mathcal{L}(K)$ is isomorphic to the Weyl group of a root system of rank $n = [K:\mathbb{Q}]$ and of type R is not equivalent to the fact that $G = W(R)$, where R is a root system of type R in $\mathscr{O}_K$. This is seen from comparing Theorem 1 with our second main result. The latter answers the question of which of the types of root systems in list (3) are realized in number fields:

Theorem 2. *For every type* R *of root systems, the following properties are equivalent:*

(i) *there is a number field, in which* R *admits a relization;*
(ii) $\mathrm{rk}(\mathsf{R}) = 1$ *or* 2.

For $\mathrm{rk}(\mathsf{R}) = 1$ or 2, the specific realizations of R in number fields see in Section 2.

Terminology and notation

If R is the type of a root system R, then the type of the direct sum of m copies of R is denoted by $m\mathsf{R}$. We say that R is irreducible if R is.

All root systems of type R have the same rank denoted by $\mathrm{rk}(\mathsf{R})$.

A_1' is the unique type of nonreduced root systems of rank 1.

By a number field K we mean an extension of a finite degree of the field $\mathbb{Q}$.

μ_K is the multiplicative group of all roots of unity in K; it is a finite cyclic group.

$\mathscr{O}_K$ is the ring of all integers in K.

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

$\mathrm{ord}(g)$ is the order of an element g of a group

$\langle g \rangle$ is a cyclic group with the generating element g.

$[G, G]$ is the commutator subgroup of a group G.

For a prime number p and a non-zero integer n, the p-adic valuation of n is denoted by $\nu_p(n)$ (i.e., $\nu_p(n)$ is the highest exponent e such that p^e divides n).

φ is Euler's totient function, i.e., for every integer $d > 0$, the value $\varphi(d)$ is the number of positive integers $\leqslant d$ that are relatively prime to d.

2. Ranks 1 and 2

The following examples show that every type R of root systems of rank 1 or 2 admits a realization in an number field K.

Root systems of types A_1 *and* A_1'

In this case, $K = \mathbb{Q}$, $\mathscr{O}_K = \mathbb{Z}$ and $\mathcal{L}(K) = \mathrm{mult}(\mathbb{Q}^*)$. If $\alpha \in \mathbb{Z}$, $\alpha \neq 0$, then $R := \{\pm\alpha\}$ (respectively, $R := \{\pm\alpha, \pm 2\alpha\}$) is a realization of type A_1 (respectively, A_1') in the field K, because $W(R) = \langle \mathrm{mult}(-1) \rangle \subset \mathcal{L}(K)$.

Root systems of types A_2 *and* G_2

Let K be the third cyclotomic field: $K = \mathbb{Q}(\sqrt{-3})$. Then $\mathscr{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + i\sqrt{3})/2$, and $\mathrm{Aut}(K) = \langle c \rangle$, where c is the complex conjugation $a \mapsto \overline{a}$. The bilinear form

$$K \times K \to \mathbb{Q},\ (a, b) \mapsto \operatorname{trace}_{K/\mathbb{Q}}(a\overline{b}) = 2\mathrm{Re}(a\overline{b}), \tag{4}$$

defines on K a structure of Euclidean space over $\mathbb{Q}$. Any element of $\mathcal{L}(K)$, whose order is finite (in particular, any reflection), is an orthogonal (with respect to this structure) transformation.

Since $r_1 := \operatorname{mult}(-1)c \in \mathcal{L}(K)$ is a reflection with respect to 1, the transformation $\rho r_1 \rho^{-1}$ for every $\rho \in \mathrm{GL}_{\mathbb{Q}}(K)$ is a reflection with respect to $\rho(1)$. For $\rho = \operatorname{mult}(a)$, where $a \in K^*$, this yields the element

$$r_a := \operatorname{mult}(-a\overline{a}^{-1})c \tag{5}$$

of $\mathcal{L}(K)$, which is a reflection with respect to a.

The multiplicative group $\{\pm 1, \pm\omega, \pm\omega^2\}$ of all 6th roots of 1 coincides with $\mathscr{O}_K(1)$. Hence

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

Therefore, $\mathscr{O}_K(1)$ is the root system of type A_2 with the base α_1, α_2. If $a \in \mathscr{O}_K(1)$, then $r_a(\mathscr{O}_K(1)) = \mathscr{O}_K(1)$. Therefore, $r_a \in W(\mathscr{O}_K(1))$. Hence $W(\mathscr{O}_K(1)) \subset \mathcal{L}(K)$. This means that $\mathscr{O}_K(1)$ is the realization of type A_2 in the field K.

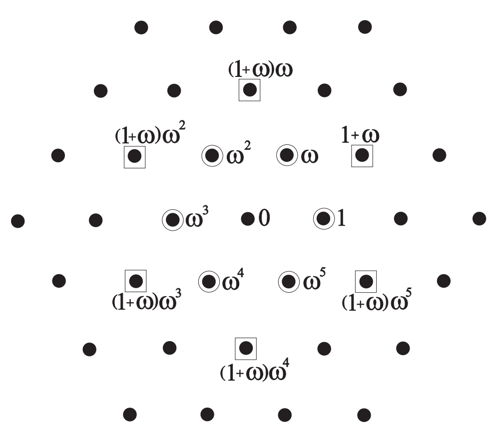
Since we have

$$\mathscr{O}_K(3) = (1 + \omega)\mathscr{O}_K(1),$$

the set $\mathscr{O}_K(3)$ is the root system of type A_2 with the base

$$\beta_1 = (1 + \omega)\alpha_1, \beta_2 = (1 + \omega)\alpha_2.$$

If $a \in \mathscr{O}_K(3)$, then $r_a(\mathscr{O}_K(3)) = \mathscr{O}_K(3)$. Therefore, $W(\mathscr{O}_K(3)) \subset \mathcal{L}(K)$. Hence $\mathscr{O}_K(3)$ is yet another realization of type A_2 in the field K.



Firure 1. Elements of $\mathscr{O}_K$, $\mathscr{O}_K(1)$, and $\mathscr{O}_K(3)$ are depicted respectively by $\bullet$, $\odot$, and $\boxdot$

Since we have

$$\begin{aligned}&\mathscr{O}_K(1)\bigcup\mathscr{O}_K(3)\\&\quad=\{\pm\alpha_1,\pm\beta_2,\pm(\alpha_1+\beta_2),\pm(2\alpha_1+\beta_2),\pm(3\alpha_1+\beta_2),\pm(3\alpha_1+2\beta_2)\},\end{aligned}$$

the set $\mathscr{O}_K(1)\bigcup\mathscr{O}_K(3)$ is the root system of type G_2 with the base α_1,β_2 (this is noted in [3, V, 16]). If $a\in\mathscr{O}_K(3)$, $b\in\mathscr{O}_K(1)$, then $r_a(\mathscr{O}_K(1))=\mathscr{O}_K(1)$, $r_b(\mathscr{O}_K(3))=\mathscr{O}_K(3)$. Therefore, $W\big(\mathscr{O}_K(1)\bigcup\mathscr{O}_K(3)\big)\subset\mathcal{L}(K)$. Hence $\mathscr{O}_K(1)\bigcup\mathscr{O}_K(3)$ is the realization of type G_2 in the field K.

Root systems B_2, $2\mathsf{A}_1$, BC_2, $2\mathsf{A}'$, *and* $\mathsf{A}\dotplus\mathsf{A}'$

Let K be the fourth cyclotomic field: $K=\mathbb{Q}(\sqrt{-1})$. Then $\mathscr{O}_K=\mathbb{Z}+\mathbb{Z}i$ and $\mathrm{Aut}(K)=\langle c\rangle$, where c is the complex conjugation $a\mapsto\overline{a}$. As above, (4) defines on K a structure of Euclidean space over $\mathbb{Q}$, and any element of $\mathcal{L}(K)$ of finite order (in particular, any reflection) is an orthogonal (with respect to this structure) transformation.

As above, for every $a\in K^*$, the element $r_a\in\mathcal{L}(K)$, given by formula (5), is a reflection with respect to a.

The multiplicative group $\{\pm1,\pm i\}$ of all 4th roots of 1 coincides with $\mathscr{O}_K(1)$. Therefore,

$$\mathscr{O}_K(1)=\{\pm\alpha_1,\pm\alpha_2\}$$

is the root system of type $2\mathsf{A}_1$ with the base $\alpha_1=1,\alpha_2=i$. If $a\in\mathscr{O}_K(1)$, then $r_a(\mathscr{O}_K(1))=\mathscr{O}_K(1)$. Hence $r_a\in W(\mathscr{O}_K(1))$; therefore, $W(\mathscr{O}_K(1))\subset\mathcal{L}(K)$. So, $\mathscr{O}_K(1)$ is the realization of type $2\mathsf{A}_1$ in K.

Since we have

$$\mathscr{O}_K(2)=(1+i)\mathscr{O}_K(1),$$

the set $\mathscr{O}_K(2)$ is the root system of type $2\mathsf{A}_1$ with the base

$$\beta_1=(1+i)\alpha_1,\ \beta_2=(1+i)\alpha_2.$$

If $a\in\mathscr{O}_K(2)$, then $r_a(\mathscr{O}_K(2))=\mathscr{O}_K(2)$. Therefore, $W\big(\mathscr{O}_K(2)\big)\subset\mathcal{L}(K)$. Hence $\mathscr{O}_K(2)$ is yet another realization of type $2\mathsf{A}_1$ in K.

Since we have

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

the set $\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)$ is the root system of type B_2 with the base α_1,β_2. If $a\in\mathscr{O}_K(2)$, $b\in\mathscr{O}_K(1)$, then $r_a(\mathscr{O}_K(1))=\mathscr{O}_K(1)$, $r_b(\mathscr{O}_K(2))=\mathscr{O}_K(2)$. Therefore, $W\big(\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)\big)\subset\mathcal{L}(K)$, hence $\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)$ is the realization of type B_2 in the field K.

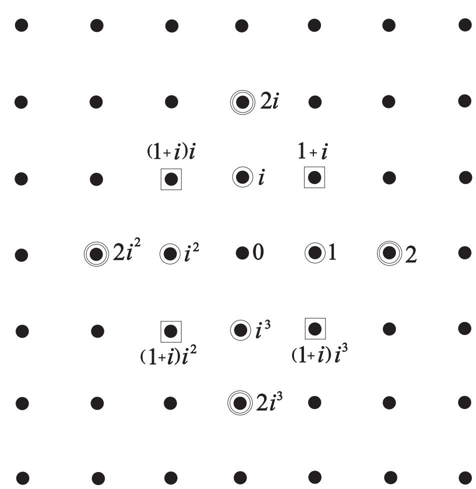
Since we have

$$\mathscr{O}_K(4)=2\mathscr{O}_K(1),$$

the group $W(\mathscr{O}_K(4))$ coincides with the group $W(\mathscr{O}_K(1))$. Therefore, $\mathscr{O}_K(4)$ is yet another realization of type $2\mathsf{A}_1$ in K. Since

$$\begin{aligned}\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)\bigcup\mathscr{O}_K(4)\\ &= \{\pm\alpha_1, \pm 2\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm 2(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2)\},\end{aligned}$$

the set $\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)\bigcup\mathscr{O}_K(4)$ is the root system of type BC_2 with the base α_1, β_2. In view of $W\big(\mathscr{O}_K(1)\bigcup\mathscr{O}_K(2)\bigcup\mathscr{O}_K(4)\big)\subset\mathcal{L}(K)$, it is the realization of type BC_2 in K.



Firure 2. Elements of $\mathscr{O}_K$, $\mathscr{O}_K(1)$, $\mathscr{O}_K(2)$, and $\mathscr{O}_K(4)$ are depicted respectively by $\bullet$, $\odot$, $\boxdot$, and $\circledcirc$

Finally, the realizations of types $2\mathsf{A}_1'$ and $\mathsf{A}_1\dotplus\mathsf{A}_1'$ in K are respectively

$$\mathscr{O}_K(1)\bigcup\mathscr{O}_K(4)\ \text{ and }\ \mathscr{O}_K(1)\bigcup\{\pm 2\}.$$

Summing up, we have the following

Proposition 1. *Every type of root systems of rank $\leqslant 2$ admits a realization in a number field.*

3. Group $\mathcal{L}(K)$ and its finite subgroups

Below K is a number field of degree n over $\mathbb{Q}$.

Theorem 3. *The group $\mathcal{L}(K)$ is a semidirect product of its normal subgroup* $\operatorname{mult}(K^*)$ *and the subgroup* $\operatorname{Aut}(K)$. *Therewith,*

$$g\operatorname{mult}(a)\,g^{-1}=\operatorname{mult}(g(a))\quad \textit{for any } a\in K^*,\ g\in\operatorname{Aut}(K). \tag{6}$$

Proof. First, check that the set of all products $\mathrm{mult}(a)g$, where $a \in K^*$, $g \in \mathrm{Aut}(K)$, is a subgroup of $\mathrm{GL}_{\mathbb{Q}}(K)$. Let $a_1, a_2 \in K^*$ and $g_1, g_2 \in \mathrm{Aut}\,(K)$. Then, for each $v \in K$,

$$\mathrm{mult}(a_1)g_1\mathrm{mult}(a_2)g_2(v) = a_1(g_1(a_2g_2(v))) = a_1(g_1(a_2))(g_1(g_2(v))).$$

This yields

$$\mathrm{mult}(a_1)g_1\mathrm{mult}(a_2)g_2 = \mathrm{mult}(a_1(g_1(a_2)))g_1g_2. \tag{7}$$

From (7) we infer that the inverse of $\mathrm{mult}(\alpha)g$ is $\mathrm{mult}(g^{-1}(a^{-1}))g^{-1}$. Thus the set of all products $\mathrm{mult}(\alpha)g$ is a subgroup of $\mathrm{GL}_{\mathbb{Q}}(K)$.

On the other hand,

$$\mathrm{mult}(a)g(1) = a(g(1)) = a1 = a,$$

hence the linear operator $\mathrm{mult}(a)g$ uniquely determines α, and therefore, g as well. This implies that the map

$$\psi\colon \mathcal{L}(K) \to \mathrm{Aut}\,(K), \quad \mathrm{mult}(\alpha)g \mapsto g, \tag{8}$$

is well defined. By (7), the map (8) is a group epimomorphism and

$$\ker(\psi) = \mathrm{mult}(K^*). \tag{9}$$

Finally, (6) straightforwardly follows from (7). ☐

Lemma 1. *For any finite subgroup G of $\mathcal{L}(K)$, there is a* (*cyclic*) *subgroup H of μ_K such that* $\mathrm{mult}(H) \subseteq G$ *and*

(i) *the sequence* $1 \to H \xrightarrow{\mathrm{mult}} G \xrightarrow{\psi} \psi(G) \to 1$ *is exact;*
(ii) $|G| = |H|{\cdot}|\psi(G)|$;
(iii) $|H|$ *divides* $|\mu_K|$;
(iv) $\varphi(|H|)$ *divides* n;
(v) $|\psi(G)|$ *divides* $|\mathrm{Aut}\,(K)|$, *which divides* n;
(vi) *if* $p \geqslant 2$ *is a prime integer, then* $\nu_p(|G|) \leqslant 2\nu_p(n) + 1$.

Proof. Since μ_K is the set of all elements of finite order in K^*, and (1) is a group monomorphism, the existence of H and (i) follow from (9). Since μ_K is cyclic, H is cyclic as well.

Statements (ii), (iii), (v) are clear.

Let θ be a generator of the cyclic group H. Then $[\mathbb{Q}(\theta) : \mathbb{Q}] = \varphi(\mathrm{ord}(\theta)) = \varphi(|H|)$. Whence (iv), because $\mathbb{Q}(\theta)$ is a subfield of K.

Let $\nu_p(|\mu_K|) = d$ and let $\zeta \in \mu_K$ be a primitive p^dth root of unity. From $\mathbb{Q}(\zeta) \subseteq K$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^d) = p^{d-1}(p-1)$ we infer that $p^{d-1}(p-1)$ divides n. Hence $\nu_p(n) \geqslant d - 1 = \nu_p(|\mu_K|) - 1$. This and (ii), (iii), (v) then imply $\nu_p(|G|) \leqslant \nu_p(|\mu_K|) + \nu_p(n) \leqslant 2\nu_p(n) + 1$, which proves (vi). ☐

Lemma 2. *Let $W(R)$ be the Weyl group of a root system R. Then*
$$\nu_2(|W(R)|) \geqslant [(\mathrm{rk}(R)+1)/2]\,. \tag{10}$$

Proof. First, note that, given an integer $m>0$, then
$$\nu_2(m!) \geqslant [(m+1)/2] \quad \text{if } m \neq 1, 3. \tag{11}$$
Indeed, let $s=[m/2]$. Then the product of all even integers between 1 and m is $2^s s!$, hence $\nu_2(m!) \geqslant s$. Therefore, (11) holds for m even, because then $[(m+1)/2]=s$. If m is odd, then we have $[(m+1)/2]=s+1$. If, moreover, $m\geqslant 5$, then $s!$ is even, hence $2^s s!$ is divisible by 2^{s+1}. Therefore, (11) holds in this case as well.

Next, suppose that R is irreducible of type R. By [1] we have

Tables 1

R	$\mathsf{A}_\ell,\ \ell\geqslant 1$	$\mathsf{B}_\ell,\ \ell\geqslant 2$	$\mathsf{C}_\ell,\ \ell\geqslant 2$	$\mathsf{D}_\ell,\ \ell\geqslant 4$
$\lvert W(R)\rvert$	$(\ell+1)!$	$2^\ell\cdot\ell!$	$2^\ell\cdot\ell!$	$2^{\ell-1}\cdot\ell!$

R	E_6	E_7	E_8	F_4	G_2
$\lvert W(R)\rvert$	$2^7\cdot3^4\cdot5$	$2^{10}\cdot3^4\cdot5\cdot7$	$2^{14}\cdot3^5\cdot5^2\cdot7$	$2^7\cdot3^2$	$2^4\cdot3$

Then (10) directly follows from Tables 1 and (11).

In the case of an arbitrary root system
$$R = R_1 \dotplus \cdots \dotplus R_d, \tag{12}$$
where R_i is an irreducible root system for every i, we have
$$\mathrm{rk}(R) = \mathrm{rk}(R_1) + \cdots + \mathrm{rk}(R_d) \tag{13}$$
and $W(R)$ splits into the product
$$W(R) = W(R_1) \times \cdots \times W(R_d) \tag{14}$$
where $W(R_i)$ is the Weyl group of R_i. It follows from (14) that, for every prime integer $p\geqslant 2$,
$$\nu_p(|W(R)|) = \sum_{i=1}^{d} \nu_p(|W(R_i)|). \tag{15}$$

Given that for every $W(R_i)$ the desired inequality is proved, we then deduce from (15) that
$$\nu_2(|W(R)|) \geqslant \sum_{i=1}^{d} [(\mathrm{rk}(R_i)+1)/2]\,. \tag{16}$$

Now (10) follows from (16) because of the inequality
$$[(a+b+1)/2] \leqslant [(a+1)/2] + [(b+1)/2], \tag{17}$$

which holds for all integers a and b. To prove (17), note that if we replace a by $a+2$ then the both sides of (17) would increase by 1. So it suffices to verify the cases $a=0$ and $a=1$. If $a=0$, then the first summand of the right-hand side of (17) is zero and we get the equality. If $a=1$, then, for the left-hand side of (17), we have

$$[(1+b+1)/2] = 1 + [b/2] \leqslant [(1+1)/2] + [(b+1)/2]\,,$$

which proves (17). $\square$

Below some of the arguments are based on the information that readily follows from Tables 1. It is convenient to collect it in Tables 2, where we use the same notation as in Tables 1 and, for every prime integer $p \geqslant 2$, put $\nu_p(\mathsf{R}) := \nu_p(|W(R)|)$.

Tables 2

$\mathsf{R} = \mathsf{A}_\ell$

ℓ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\nu_2(\mathsf{R})$	1	1	3	3	4	4	7	7	8	8	10	10	11	11	15	15
$\nu_3(\mathsf{R})$	0	1	1	1	2	2	2	4	4	4	5	5	5	6	6	6

$\mathsf{R} = \mathsf{B}_\ell$ and C_ℓ

ℓ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\nu_2(\mathsf{R})$	3	3	7	8	10	11	15	16	18	19	22	23	25	26	31
$\nu_3(\mathsf{R})$	0	1	1	1	2	2	2	4	4	4	5	5	5	6	6

$\mathsf{R} = \mathsf{D}_\ell$

ℓ	4	5	6	7	8	9	10	11	12	13	14	15	16
$\nu_2(\mathsf{R})$	6	7	9	10	14	15	17	18	21	22	24	25	30
$\nu_3(\mathsf{R})$	1	1	2	2	2	4	4	4	5	5	5	6	6

R	E_6	E_7	E_8	F_4	G_2
$\nu_2(\mathsf{R})$	7	10	14	7	4
$\nu_3(\mathsf{R})$	4	4	5	2	1

Below, for every type R of root systems, we put $\varnothing \dot{+} \mathsf{R} := \mathsf{R}$.

Proposition 2. *Let R be a root system of type R.*

(i) *If* $\mathsf{R} = \mathsf{S}_1 \dot{+} \mathsf{S}_2$, *then*

$$\nu_2(\mathsf{S}_1) \leqslant \nu_2(\mathsf{R}) - [(\mathrm{rk}(\mathsf{S}_2)+1)/2].$$

In particular, if R_i *is the type of* R_i *in* (12), *then*

$$\nu_2(\mathsf{R}_i) \leqslant \nu_2(\mathsf{R}) - [(n-\mathrm{rk}(\mathsf{R}_i)+1)/2] < \nu_2(\mathsf{R}).$$

(ii) *If* $\nu_2(\mathsf{R}) \leqslant 3$, *then*

$$\begin{gathered}\mathsf{R} = a_1\mathsf{A}_1 \dotplus a_2\mathsf{A}_2 \dotplus a_3\mathsf{A}_3 \dotplus a_4\mathsf{A}_4 \dotplus b_2\mathsf{B}_2 \dotplus b_3\mathsf{B}_3 \dotplus c_3\mathsf{C}_3,\\ a_1 + 2a_2 + 3a_3 + 4a_4 + 2b_2 + 3b_3 + 3c_3 = \mathrm{rk}(\mathsf{R}),\\ a_1 + a_2 + 3a_3 + 3a_4 + 3b_2 + 3b_3 + 3c_3 = \nu_2(\mathsf{R}),\\ a_2 + a_3 + a_4 + b_3 + c_3 = \nu_3(\mathsf{R}).\end{gathered}$$

(iii) *If* $\nu_3(\mathsf{R}) \leqslant 1$, *then*

$$\mathsf{R} = \mathsf{X} \dotplus a\mathsf{A}_1 \dotplus b\mathsf{B}_2, \quad \text{where} \tag{18}$$

$$\mathsf{X} \in \{\mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4, \mathsf{B}_3, \mathsf{B}_4, \mathsf{B}_5, \mathsf{C}_3, \mathsf{C}_4, \mathsf{C}_5, \mathsf{D}_4, \mathsf{D}_5, \mathsf{G}_2, \varnothing\}, \tag{19}$$

$$\begin{gathered}\mathrm{rk}(\mathsf{X}) + a + 2b = \mathrm{rk}(\mathsf{R}),\\ \nu_2(\mathsf{X}) + a + 3b = \nu_2(\mathsf{R}),\end{gathered}$$

and, by definition, $\mathrm{rk}(\varnothing) = \nu_p(\varnothing) = 0$ *for any* p.

Proof. This follows from Lemma 2, (13), (15), and Tables 2. □

Proposition 3. *Let K be a number field of degree n over $\mathbb{Q}$ and let m be a positive integer. If the group $\mathcal{L}(K)$ contains a subgroup G isomorphic to the Weyl group a root system of type $m\mathsf{A}_1$, then 2^{m-1} divides n. In particular, if $m = n$, then $n = 1$ or 2.*

Proof. In view of (14) and Tables 1, the group G is an elementary Abelian 2-group of order 2^m. From this, Lemma 1(i)(ii), and the cyclicity of H, we infer that $|H| = 1$ or 2, hence, respectively, $|\psi(G)| = 2^m$ or 2^{m-1}. The claim then follows from Lemma 1(v). □

Proposition 4. *Let K be a number field of degree n over $\mathbb{Q}$. If the group $\mathcal{L}(K)$ contains a finite subgroup G isomorphic to the Weyl group $W(R)$ of a root system R of type R and rank n, then $n \in \{1, 2, 4\}$.*

Proof. First, in Step 1, we shall show that $n \in \{1, 2, 4, 6, 8, 16\}$. Then, in Steps 2, 3, and 4, we shall consider respectively the cases $n = 6, 8$, and 16, and eliminate each of them.

Step 1

Lemma 1(vi) yields $\nu_2(|G|) \leqslant 2\nu_2(n) + 1$. By Lemma 2 we have $\nu_2(|G|) \geqslant [(n+1)/2]$. Therefore,

$$[(n+1)/2] \leqslant 2\nu_2(n) + 1. \tag{20}$$

Let $n \geqslant 3$. Then $2 \leqslant [(n+1)/2]$. In view of (20), this implies that $\nu_2(n) \geqslant 1$, i.e., n is even. Since $n/2 \leqslant [(n+1)/2]$, from (20) we infer

$$2^{n/2} \leqslant 2^{[(n+1)/2]} \leqslant 2^{2\nu_2(n)+1} \leqslant 2n^2. \tag{21}$$

In addition, if n is not a power of 2, then $2^{\nu_2(n)} \cdot 3 \leqslant n$, so (21) yields

$$2^{n/2} \leqslant 2^{2\nu_2(n)+1} \leqslant 2\,(n/3)^2\,. \tag{22}$$

If in (22) we replace n by $n+2$ then the left-hand side will be multiplied by 2 while the right-hand side will be multiplied by $(1+2/n)^2 < 2$, because $n > 4$. Taking into account that (22) becomes equality if $n = 6$, we conclude that $n = 6$ if $n \geqslant 3$ is not a power of 2.

Now suppose that $n = 2^s$, where $s \geqslant 2$. Then (20) yields

$$2^{s-1} \leqslant 2s+1$$

and therefore $s = 2, 3$ or 4, i.e., $n = 4, 8$ or 16 respectively.

Taking into account all $n < 3$, we conclude that $n \in \{1, 2, 4, 6, 8, 16\}$.

In Steps 2, 3, and 4, we use the notation of (12), (14) introduced in the proof of Lemma 2. The type of R_i is denoted by R_i.

Step 2

Arguing on the contrary, assume that $n = 6$. Since $\nu_2(n) = 1$, Lemma 1(vi) yields $\nu_2(\mathsf{R}) \leqslant 3$. From Proposition 2(ii) we then infer that $\mathsf{R} = a\mathsf{A}_1 \dot{+} b\mathsf{A}_2$, where $x = a, y = b$ is a solution of the system

$$\left.\begin{aligned} x + 2y &= 6,\\ x + y &\leqslant 3. \end{aligned}\right\} \tag{23}$$

It is easily seen that (23) has only one solution in non-negative integers, namely, $x = 0, y = 3$. Thus $\mathsf{R} = 3\mathsf{A}_2$. Hence, from Tables 1 and (14) we obtain

$$|G| = 2^3 \cdot 3^3. \tag{24}$$

Lemma 1(v) implies that $|\psi(G)| = 1, 2, 3$ or 6. From Lemma 1(ii) and (24) we then infer that $|H|$ is one of the integers $2^3 \cdot 3^3, 2^2 \cdot 3^3, 2^3 \cdot 3^2$ or $2^2 \cdot 3^2$. Hence, respectively, $\varphi(|H|) = 2^3 \cdot 3^2, 2^2 \cdot 3^2, 2^3 \cdot 3^1$ or $2^2 \cdot 3^1$. Since neither of these integers divides 6, this contradicts Lemma 1(iv). So we proved that $n \neq 6$.

Step 3

Arguing on the contrary, assume that $n = 8$. We have $\nu_2(n) = 3$, $\nu_3(n) = 0$. Therefore, Lemma 1(vi) yields $\nu_2(\mathsf{R}) \leqslant 7$ and $\nu_3(\mathsf{R}) \leqslant 1$. From Proposition 2(iii) we then deduce that (18), (19) hold, where

$$\operatorname{rk}(\mathsf{X}) + a + 2b = 8, \tag{25}$$

$$\nu_2(\mathsf{X}) + a + 3b \leqslant 7. \tag{26}$$

In turn, (25), (26) yield: $a + 3b \geqslant a + 2b \overset{(25)}{=} 8 - \operatorname{rk}(\mathsf{X}) \overset{(19)}{\geqslant} 8 - 5 = 3$, hence $\nu_2(\mathsf{X}) \overset{(26)}{\leqslant} 7 - (a + 3b) \leqslant 7 - 3 = 4$. This, (19), and Table 2 show that

$$\mathsf{X} \in \{\mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4, \mathsf{B}_3, \mathsf{C}_3, \mathsf{G}_2, \varnothing\}. \tag{27}$$

Next, from (25), (26) we obtain $b \leqslant \mathrm{rk}(\mathsf{X}) - \nu_2(\mathsf{X}) - 1$. Tables 2 imply that the right-hand side of the latter inequality is negative if $\mathsf{X} \in \{\mathsf{A}_3, \mathsf{B}_3, \mathsf{C}_3, \mathsf{G}_2, \varnothing\}$. Since this is impossible, from (27) we conclude that $\mathsf{X} = \mathsf{A}_2$ or A_4. In each of these cases, there is a unique pair (a, b) of non-negative integers satisfying (25), (26), namely, $(a, b) = (6, 0)$ for $\mathsf{X} = \mathsf{A}_2$, and $(a, b) = (4, 0)$ for $\mathsf{X} = \mathsf{A}_4$. So, $\mathsf{R} = 6\mathsf{A}_1 \dotplus \mathsf{A}_2$ or $4\mathsf{A}_1 \dotplus \mathsf{A}_4$. We now consider these possibilities.

Assume that $\mathsf{R} = 6\mathsf{A}_1 \dotplus \mathsf{A}_2$. Then G contains a subgroup isomorphic to the Weyl group of a root system of type $6\mathsf{A}_1$. Hence 2^{6-1} divides $n = 8$ by Proposition 3. This contradiction proves that, in fact, $\mathsf{R} \neq 6\mathsf{A}_1 \dotplus \mathsf{A}_2$.

Next, assume that $\mathsf{R} = 4\mathsf{A}_1 \dotplus \mathsf{A}_4$. Then Tables 1 and (14) yield

$$|G| = 2^7 \cdot 3 \cdot 5. \tag{28}$$

Hence, if $|\psi(G)| = 1, 2, 4$ or 8, then, respectively, $|H| = 2^7 \cdot 3 \cdot 5$, $2^6 \cdot 3 \cdot 5$, $2^5 \cdot 3 \cdot 5$ or $2^4 \cdot 3 \cdot 5$, and, accordingly, $\varphi(|H|) = 2^9, 2^8, 2^7$ or 2^6. Contrary to Lemma 1(iv), neither of the latter integers divides 8. This refutes our assumption thereby completing the proof that $n \neq 8$.

Step 4

Arguing on the contrary, assume that $n = 16$. We have $\nu_2(n) = 4$, $\nu_3(n) = 0$. Therefore, Lemma 1(vi) yields $\nu_2(\mathsf{R}) \leqslant 9$ and $\nu_3(\mathsf{R}) \leqslant 1$. By Proposition 2(iii) we then conclude that (18), (19) hold, where

$$\left.\begin{aligned} \mathrm{rk}(\mathsf{X}) + a + 2b &= 16,\\ \nu_2(\mathsf{X}) + a + 3b &\leqslant 9. \end{aligned}\right\} \tag{29}$$

But (29) implies $b \leqslant \mathrm{rk}(\mathsf{X}) - \nu_2(\mathsf{X}) - 7$, and, in view of (19) and Tables 2, the right-hand side of this inequality is negative. This refutes our assumption and proves that $n \neq 16$. □

4. Proofs of Theorems 1 and 2

Proof of Theorem 1.

(i)⇒(ii) Assume that (i) holds. In view of Proposition 4, we have to show that if $n = 4$, then R is either $\mathsf{A}_2 \dotplus \mathsf{B}_2$ or $2\mathsf{A}_1 \dotplus \mathsf{A}_2$.

So, let $n = 4$. Then Lemma 1(v) (whose notation we use) yields

$$|\psi(G)| = 1, 2, \text{ or } 4. \tag{30}$$

Next, we have $\nu_2(n) = 2$, $\nu_3(n) = 0$. Therefore, Lemma 1(vi) yields $\nu_2(\mathsf{R}) \leqslant 5$, $\nu_3(\mathsf{R}) \leqslant 1$. From Proposition 2(iii) and Tables 2 we then deduce that

$$\mathsf{R} \in \{\mathsf{A}_4, \mathsf{A}_1 \dotplus \mathsf{A}_3, \mathsf{A}_1 \dotplus \mathsf{B}_3, \mathsf{A}_1 \dotplus \mathsf{C}_3, 2\mathsf{A}_1 \dotplus \mathsf{A}_2, 2\mathsf{A}_1 \dotplus \mathsf{B}_2, 4\mathsf{A}_1, \mathsf{A}_2 \dotplus \mathsf{B}_2\}.$$

Assume that $\mathsf{R} = \mathsf{A}_4$. Then from Tables 1 we obtain

$$|G| = 2^3 \cdot 3 \cdot 5. \tag{31}$$

From Lemma 1(ii) and (31) we infer that, respectively to (30), we have $|H| = 2^3 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 5$, or $2 \cdot 3 \cdot 5$, and, accordingly, $\varphi(|H|) = 2^5, 2^4$, or 2^3. Contrary to Lemma 1(iv), neither of the latter integers divides 4. This contradiction show that, in fact, $\mathsf{R} \neq \mathsf{A}_4$.

Assume that $\mathsf{R} = \mathsf{A}_1 \dot{+} \mathsf{B}_3$ or $\mathsf{A}_1 \dot{+} \mathsf{C}_3$. Then Tables 1 and (14) yield

$$|G| = 2^5 \cdot 3. \tag{32}$$

From Lemma 1(ii) and (32) we infer that, respectively to (30), we have $|H| = 2^5 \cdot 3$, $2^4 \cdot 3$, or $2^3 \cdot 3$, and, accordingly, $\varphi(|H|) = 2^5, 2^4$, or 2^3. So, as above we conclude that, in fact, $\mathsf{R} \neq \mathsf{A}_1 \dot{+} \mathsf{B}_3$ or $\mathsf{A}_1 \dot{+} \mathsf{C}_3$.

Assume that $\mathsf{R} = \mathsf{A}_1 \dot{+} \mathsf{A}_3$. Then Tables 1 and (14) yield

$$|G| = 2^4 \cdot 3. \tag{33}$$

Lemma 1(ii) and (33) imply that, respectively to (30), we have $|H| = 2^4 \cdot 3$, $2^3 \cdot 3$, or $2^2 \cdot 3$, and, accordingly, $\varphi(|H|) = 2^4, 2^3$, or 2^2. Since only the last integer divides 4, by Lemma 1(iv) we conclude that $|\psi(G)| = 4$.

The latter equality implies that the group $\psi(G)$ is Abelian. From this and Lemma 1(i) we infer that $[G, G] \subseteq \ker(\psi) = H$. Since the group H is Abelian, we conclude that the group $[G, G]$ is Abelian as well. But G is isomorpic to $W(R) = W(R_1) \times W(R_2)$, where the types of R_1 and R_2 are respectively A_1 and A_3. Therefore, $[G, G]$ contains a subgroup isomorphic to $[W(R_2), W(R_2)]$. The latter is the alternating group on 4 letters, hence non-Abelian. This contradiction shows that, in fact, $\mathsf{R} \neq \mathsf{A}_1 \dot{+} \mathsf{A}_3$.

Assume that $\mathsf{R} = 2\mathsf{A}_1 \dot{+} \mathsf{B}_2$. Then $W(R) = W(R_1) \times W(R_2) \times W(R_3)$, where R_1 and R_2 are of type A_1, and R_3 is of type B_2. Tables 1 yield $|W(R_1)| = |W(R_2)| = 2$, $|W(R_3)| = 8$. Since $W(R_3)$ is non-Abelian, this implies that G does not contain an element of order $\geqslant 8$. On the other hand, as $|G| = 2^5$, Lemma 1(ii),(v) yields $|H| \geqslant 2^5/2^2 = 8$. As H is cyclic, this implies that G contains an element of order $\geqslant 8$. This contradiction means that, in fact, $\mathsf{R} \neq 2\mathsf{A}_1 \dot{+} \mathsf{B}_2$.

If $\mathsf{R} = 4\mathsf{A}_1$, then 2^{4-1} divides $n = 4$ by Proposition 3. This contradiction means that $\mathsf{R} \neq 4\mathsf{A}_1$.

The proof of (i)⇒(ii) is now completed.

(ii)⇒(i) If $\mathsf{R} \in \{\mathsf{A}_2, \mathsf{B}_2, \mathsf{G}_2, 2\mathsf{A}_1\}$, then (i) follows from Proposition 1 and Definition 1.

Consider the case $\mathsf{R} = \mathsf{A}_2 \dot{+} \mathsf{B}_2$.

Let K be the biquadratic field $\mathbb{Q}(\sqrt{-3}, \sqrt{-1})$. Then

$$K = \mathbb{Q}(\sqrt{-3}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}).$$

This equality determines the natural homomorphism

$$\mathcal{L}(\mathbb{Q}(\sqrt{-3})) \times \mathcal{L}(\mathbb{Q}(\sqrt{-1})) \to \mathcal{L}(K), \tag{34}$$

whose restriction to $\mathrm{Aut}(\mathbb{Q}(\sqrt{-3})) \times \mathrm{Aut}(\mathbb{Q}(\sqrt{-1}))$ is an isomorphism with $\mathrm{Aut}(K)$ (see [2, Chap. VIII, §1, Thm. 5]). Homomorphism (34) is surjective and its kernel is $\{(\mathrm{mult}(a), \mathrm{mult}(a^{-1})) \mid a \in \mathbb{Q}^*\}$.

Let R_1 and R_2 be respectively the realizations of type A_2 in $\mathbb{Q}(\sqrt{-3})$ and of type B_2 in $\mathbb{Q}(\sqrt{-1})$ constructed in the proof of Proposition 1. Since $-1 \notin W(R_1)$, the restriction of homomorphism (34) to the group $W(R_1) \times W(R_2)$ is an embedding. Therefore, its image is the subgroup of $\mathcal{L}(K)$ isomorphic to the Weyl group of a root system of type $\mathsf{A}_2 \dot{+} \mathsf{B}_2$. This proves that (i) holds if $\mathsf{R} = \mathsf{A}_2 \dot{+} \mathsf{B}_2$.

Now consider the case $\mathsf{R} = \mathsf{A}_2 \dot{+} 2\mathsf{A}_1$.

If R_3 is a subset of R_2, which is a realization of type $2\mathsf{A}_1$ in K, then the restriction of homomorphism (34) to $W(R_1) \times W(R_3)$ is the subgroup of $\mathcal{L}(K)$ isomorphic to the Weyl group of a root system of type $\mathsf{A}_2 \dot{+} 2\mathsf{A}_1$. Thus (i) holds if R is of this type.

This completes the proof of (ii)⇒(i) and that of Theorem 1. □

Proof of Theorem 2. (i)⇒(ii) In view of Theorem 1 and Definition 1, we have to show that if $\mathsf{R} = \mathsf{A}_2 \dot{+} \mathsf{B}_2$ or $\mathsf{A}_2 \dot{+} 2\mathsf{A}_1$, then R admits no realizations in the number fields. Arguing on the contrary, assume that this is not the case, so R admits a realization in a number field K.

The linear space K over $\mathbb{Q}$ is then a direct sum of two 2-dimensional linear subspaces L_1 and L_2 such that

(a) L_i is the linear span of $R_i := R \bigcap L_i$ over $\mathbb{Q}$ for every i;
(b) R_1 is a root system in L_1 of type A_2;
(c) R_2 is a root system in L_2 of type B_2 or $2\mathsf{A}_1$;
(d) $R = R_1 \bigsqcup R_2$.

Let $\iota\colon \mathrm{GL}_{\mathbb{Q}}(L_1) \times \mathrm{GL}_{\mathbb{Q}}(L_2) \hookrightarrow \mathrm{GL}_{\mathbb{Q}}(K)$ be the natural embedding. Then

$$W(R) = \iota(W(R_1)) \times \iota(W(R_2)). \tag{35}$$

In view of (b), the group $\iota(W(R_1))$ is isomorphic to the symmetric group on three letters, hence contains an element z of order 3. By (35), the fixed points set K^z of z has the property

$$L_2 \subseteq K^z. \tag{36}$$

According to Theorem 3, there are uniquely defined elements $a \in K^*$ and $g \in \mathrm{Aut}(K)$ such that $z = \mathrm{mult}(a)g$. From (6) we infer that ord(g) divides ord$(z)=3$. Since ord(g) divides $|\mathrm{Aut}(K)|$, which, in turn, divides $\dim_{\mathbb{Q}}(K)=4$, we conclude that

$$z = \mathrm{mult}(a). \tag{37}$$

As ord$(z) \neq 1$, we have $a \neq 1$. From this, (37), and (2) we infer that $K^z = 0$ contrary to (36). This completes the proof of (i)⇒(ii).

(ii)⇒(i) This follows from Proposition 1. □

References

[1] N. Bourbaki, *Groupes et Algébres de Lie*, Chaps. IV–VI, Hermann, Paris, 1968.
[2] S. Lang, *Algebra*, Addison-Wesley, Mass., 1965.
[3] J.-P. Serre, *Complex Semisimple Lie Algebras*, Berlin, Springer, 2001.