An integrality theorem of root systems

A. Bhattacharya, G.R. Vijayakumar

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 400 005, India

Received 23 September 2005; accepted 6 February 2006
Available online 30 August 2006

Abstract

Let $\Phi$ be an irreducible root system and $\Delta$ be a base for $\Phi$; it is well known that any root in $\Phi$ is an integral combination of the roots in $\Delta$. In comparison to this fact, we establish the following result: Any indecomposable subset $T$ of $\Phi$ is contained in the $\mathbb{Z}$-span of an indecomposable linearly independent subset of $T$.

© 2006 Elsevier Ltd. All rights reserved.

Throughout this paper, $\mathbb{R}$ and $\mathbb{Z}$ denote the set of reals and the set of integers respectively and $E$ is a finite dimensional vector space over $\mathbb{R}$ with usual inner product $(\ast, \ast)$. If $v_0, v_1, v_2, \ldots, v_n$ are vectors in $E$ such that $v_0 = \sum_{i=1}^n t_i v_i$ where $t_i \in \mathbb{Z}$ for $i = 1, \ldots, n$, then $v_0$ is called an integral combination of $v_1, v_2, \ldots, v_n$. Let $S$ and $T$ be two subsets of $E$. If $S$ is contained in the $\mathbb{Z}$-span of $T$ – or equivalently, if every vector of $S$ is an integral combination of vectors in $T$ – then we say that $S$ is generated by $T$.

For occasional graph theoretic terms used in this paper, we refer the reader to [1]. Let $S$ be any subset of $E$; we can associate a graph with $S$ as follows: its vertex set is $S$; two vertices are joined if their inner product is nonzero. If this graph is connected, then $S$ is called indecomposable; otherwise it is decomposable. Note that when $S$ is decomposable, it has a proper subset $T$ such that for all $x \in T$ and for all $y \in S \setminus T$, $(x, y) = 0$.

Definition 1. A subset $\Phi$ of $E$ is called a root system in $E$ if the following axioms are satisfied:

- (R1) $\Phi$ is finite and its linear span is $E$; it does not contain 0.
- (R2) If $\alpha \in \Phi$ and $t \in \mathbb{R}$, then $t \alpha \in \Phi$ only when $t = \pm 1$.
- (R3) If $\alpha, \beta \in \Phi$, then $\frac{2(\alpha, \beta)}{(\beta, \beta)}$ is an integer.
- (R4) For any $\alpha, \beta \in \Phi$, $\alpha - \frac{2(\alpha, \beta)}{(\beta, \beta)} \beta \in \Phi$.

E-mail addresses: amitava@math.tifr.res.in (A. Bhattacharya), vijay@math.tifr.res.in (G.R. Vijayakumar).

0195-6698/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2006.02.006
The elements of $\Phi$ are called roots. For any $\alpha \in \Phi$, $\|\alpha\|$ is called the length of $\alpha$. If $\Phi$ is indecomposable (decomposable) it is also called irreducible (reducible).

Henceforth, $\Phi$ stands for a root system. For any $\alpha, \beta \in \Phi$, we denote the integer $\frac{2(\alpha,\beta)}{\langle \beta, \beta \rangle}$ by $\langle \alpha, \beta \rangle$.

**Remark 2.** For any $\alpha, \beta \in \Phi$, the following hold.

1. $-\alpha \in \Phi$. [This follows from (R4) by putting $\beta = \alpha$.]
2. If $\alpha \neq \pm \beta$ and $\|\alpha\| \leq \|\beta\|$, then $\langle \alpha, \beta \rangle \in \{-1, 0, 1\}$; if $\|\alpha\| > \|\beta\|$, then $|\langle \alpha, \beta \rangle| \in \{0, 2, 3\}$.
3. If $\langle \alpha, \beta \rangle < 0$ and $\alpha \neq -\beta$, then $\alpha + \beta$ is a root. [If $\langle \alpha, \beta \rangle > 0$ and $\alpha \neq \beta$, then by (1), $\alpha - \beta$ is a root.]

(See Chapter 3 of [2] for proofs of (2) and (3) and other elementary facts about root systems.)

**Definition 3.** A subset $\Delta$ of $\Phi$ is called a base if the following conditions are satisfied.

1. $\Delta$ is a basis of $\mathbb{E}$.
2. Each root $\beta$ can be written as $\sum_{\alpha \in \Delta} k_{\alpha} \alpha$ where either all the $k_{\alpha}$’s are nonnegative integers or all of them are nonpositive integers.

Bases play the vital role in classifying the root systems. For showing the existence of a base in a root system and for other details the reader is referred to [2,4]. It has been shown that a root system is completely determined by a base. If a root system $\Phi$ has two bases, then there exists an automorphism of $\mathbb{E}$ fixing $\Phi$ and taking one base into another.

A natural question to ask in connection with (B2) is the following: If $S$ is a linearly dependent subset of $\Phi$, can there be a linearly independent subset of $S$ which generates $S$? We answer this question affirmatively in this paper:

**Theorem 4.** Any indecomposable subset $S$ of $\Phi$ is generated by an indecomposable linearly independent subset of $S$.

The above result for any irreducible root system of unique root length has been proved in [6]. (See Remark 18.)

**Outline of the proof of Theorem 4.** This result is settled in three stages. By using Dynkin diagrams (see Definition 6), we show that the conclusion of the result holds for circuits. (See Definition 5 and Proposition 15.) For a minimal linearly dependent set $S$ of $\Phi$ – i.e., $S$ is a linearly dependent subset of $\Phi$ but every proper subset of $S$ is linearly independent – by using a parameter defined for such subsets of $\Phi$ and Lemma 17, the result is proved; from this, the proof for any indecomposable linearly dependent subset of $\Phi$ can be easily derived.

A subset $S$ of $\Phi$ is called obtuse if for all distinct $\alpha, \beta \in S$, $(\alpha, \beta) \leq 0$; in other words, $S$ is obtuse if the angle between any two different roots of $S$ is not acute. It can be shown that any base of a root system is obtuse. (See [2, p. 47].)

**Definition 5.** A nonempty subset $\mathcal{C}$ of $\Phi$ is called a circuit if it satisfies the following:

1. $\mathcal{C}$ is obtuse.
2. $\mathcal{C}$ is a minimal linearly dependent set.
3. If a root $\alpha \in \mathcal{C}$, then $-\alpha \not\in \mathcal{C}$. 


Using these relations, it can be shown that of its graph in \( R \) Let \( S \) be as in Definition 6. It is not difficult to show that from the Dynkin diagram of any \( S \), \( (\alpha, \beta) \) for any \( \alpha, \beta \in S \) can be found (cf. [5, p. 291]). For example, the second Dynkin diagram drawn in Fig. 1 represents the set \( \{\alpha, \alpha_2, \alpha_3, \alpha_4\} \) where for all \( i, j \in \{1, 2, 3, 4\}, (\alpha_i, \alpha_j) \) is the \((i, j)\)-th entry of the matrix shown in that figure. (\( S \) is a base of a root system known as \( F_4 \) in the literature. The matrix just mentioned is called a Cartan matrix.)

In the literature, the root systems have been classified by finding the Dynkin diagrams of their bases. Any irreducible root system is determined by one of the Dynkin diagrams in Fig. 2.

**Definition 6.** Let \( S \) be an obtuse subset of \( \Phi \). The Dynkin diagram associated with \( S \) is a drawing of its graph in \( \mathbb{R}^2 \) as follows: If two vertices \( \alpha \) and \( \beta \) are adjacent – i.e., if \( (\alpha, \beta) < 0 \) – then the corresponding edge consists of \( (\alpha, \beta) \langle \beta, \alpha \rangle \) line segments; when \( \|\alpha\| > \|\beta\| \), then an arrow pointing towards \( \beta \) is put on this edge. The number of line segments in an edge is called the valency of that edge. The valency of a vertex \( \alpha \) is the sum of valencies of the edges incident with that vertex and it is denoted by \( \text{val} \alpha \).

If \( S = \{\alpha, \beta\} \) with \( (\alpha, \beta) = -3 \), then the corresponding Dynkin diagram is the first graph drawn in Fig. 1. (The root system for which \( S \) is a base is known as \( G_2 \).)

Let \( S \) be as in Definition 6. It is not difficult to show that from the Dynkin diagram of \( S, (\alpha, \beta) \) for any \( \alpha, \beta \in S \) can be found (cf. [5, p. 291]). For example, the second Dynkin diagram drawn in Fig. 1 represents the set \( \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \) where for all \( i, j \in \{1, 2, 3, 4\}, (\alpha_i, \alpha_j) \) is the \((i, j)\)-th entry of the matrix shown in that figure. (\( S \) is a base of a root system known as \( F_4 \) in the literature. The matrix just mentioned is called a Cartan matrix.)

In the literature, the root systems have been classified by finding the Dynkin diagrams of their bases. Any irreducible root system is determined by one of the Dynkin diagrams in Fig. 2.

**Lemma 7.** No obtuse subset of \( \Phi \) can have the graph drawn in Fig. 3 as its Dynkin diagram.

**Proof.** Otherwise, we have a set of roots \( \alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1} \) such that

\[
\frac{\langle \alpha_0, \alpha_0 \rangle}{2} = (\alpha_1, \alpha_1) = (\alpha_2, \alpha_2) = \cdots = (\alpha_n, \alpha_n) = 2(\alpha_{n+1}, \alpha_{n+1});
\]

\[
2\frac{(\alpha_0, \alpha_1)}{(\alpha_0, \alpha_0)} = 2\frac{(\alpha_1, \alpha_2)}{(\alpha_1, \alpha_1)} = \cdots = 2\frac{(\alpha_{n-1}, \alpha_n)}{(\alpha_{n-1}, \alpha_{n-1})} = 2\frac{(\alpha_n, \alpha_{n+1})}{(\alpha_n, \alpha_n)} = -1;
\]

and \( (\alpha_i, \alpha_j) = 0 \) if \( 0 \leq i < j - 1 \leq n \).

Using these relations, it can be shown that \( \|\alpha_0 + 2\beta\|^2 = 0 \) where \( \beta = \alpha_1 + \alpha_2 + \cdots + \alpha_n + \alpha_{n+1} \). However by using (3) of Remark 2 repeatedly, it can be seen that \( \beta \in \Phi \); thus we have \(-2\beta \in \Phi \), contradicting Axiom (R2) of Definition 1. \( \square \)

**Remark 8.** If the arrows in Fig. 3 have different directions, then it can be verified that \( \alpha_0 + \alpha_{n+1} + t \sum_{i=1}^{n} \alpha_i = 0 \) where \( t \) is 1 or 2; thus any one of \( \alpha_0, \alpha_{n+1} \) is an integral combination of other roots.

**Remark 9.** It has been shown that in an irreducible root system at most two root lengths can occur. (See [2, p. 53].) Thus from this result also, Lemma 7 follows. In an irreducible root sys-
tem with two distinct root lengths, the roots of longer length are called *long roots* and the remains are called *short roots*. If all roots have same length, it is conventional to call all of them long.
The following result gives a condition which is sufficient for a linearly dependent subset of \( \Phi \) to be minimal.

**Proposition 10.** If \( S \) is a linearly dependent subset of \( \Phi \) such that its graph is a tree, then \( S \) is minimal.

**Proof.** Let \( A \) be a minimal linearly dependent subset of \( S \). Then the graph of \( A \) is connected. If \( A \neq S \), then for some \( \alpha \in S \setminus A \) and \( \beta \in A \), \( (\alpha, \beta) \neq 0 \) implying that \((\alpha, \gamma) \neq 0 \) for some \( \gamma \in A \setminus \{\beta\} \) (because by minimality of \( A \), \( \beta \) is in the linear span of \( A \setminus \{\beta\} \)) and therefore the graph of \( A \cup \{\alpha\} \) contains a cycle—a contradiction. This establishes the minimality of \( S \). \( \blacksquare \)

**Proposition 11.** If the Dynkin diagram \( \mathcal{D} \) of a circuit \( \mathcal{C} \) contains a cycle, then \( \mathcal{D} \) itself has to be that cycle and every vertex of \( \mathcal{D} \) has valency 2.

**Proof.** Let \((\alpha_1, \ldots, \alpha_n, \alpha_{n+1} = \alpha_1)\) be a cycle of \( \mathcal{D} \).

Now \( \left\| \sum_{i=1}^{n} \alpha_i \right\|^2 = \sum \left\| \alpha_i \right\|^2 + 2 \sum (\alpha_i, \alpha_{i+1}) \)
\[ = \sum \left\| \alpha_i \right\|^2 + 2 \sum \langle \alpha_i, \alpha_{i+1} \rangle \left\| \alpha_{i+1} \right\|^2 \]
\[ \leq \sum \left\| \alpha_i \right\|^2 + \sum (-1) \left\| \alpha_{i+1} \right\|^2 = 0. \]

Therefore \( \sum \alpha_i = 0 \) and by minimality of \( \mathcal{C} \), \( \mathcal{D} \) is a cycle; further for each \( i = 1, 2, \ldots, n \), \( \langle \alpha_i, \alpha_{i+1} \rangle = -1 \) implying that \( \left\| \alpha_i \right\| \leq \left\| \alpha_{i+1} \right\| \). Therefore all roots of \( \mathcal{C} \) have the same length and hence every vertex of \( \mathcal{D} \) is of valency 2. \( \blacksquare \)

**Lemma 12.** If \( \alpha \) is a root in a circuit \( \mathcal{C} \) and \( \mathcal{D} \) is the Dynkin diagram of \( \mathcal{C} \), then \( \text{val} \alpha \leq 4 \); when equality holds, every vertex of \( \mathcal{D} \) other than \( \alpha \) is joined to \( \alpha \) and any root of minimum valency is an integral combination of the remaining roots of \( \mathcal{C} \).

**Proof.** By Proposition 11, we can assume that \( \mathcal{D} \) is a tree. Let \( \beta_1, \beta_2, \ldots, \beta_k \) be the vertices of \( \mathcal{D} \) which are joined to \( \alpha \). We can write \( 2\alpha = \sum_{i=1}^{k} t_i \beta_i + \gamma \) where \( \gamma \) is a vector orthogonal to \( \beta_1, \beta_2, \ldots, \beta_k \) and \( t_j, i = 1, \ldots, k \), are scalars.

For any \( j \leq k \), \( 2\langle \alpha, \beta_j \rangle = \sum_{i=1}^{k} t_i \langle \beta_i, \beta_j \rangle = 2t_j \). Thus we have \( 2\alpha = \sum_i \langle \alpha, \beta_i \rangle \beta_i + \gamma \). Therefore \( 4\langle \alpha, \alpha \rangle = \sum \langle \alpha, \beta_i \rangle^2 < \beta_i, \beta_i > + \langle \gamma, \gamma \rangle \) implying that \( \sum \langle \alpha, \beta_i \rangle^2 \frac{\langle \beta_i, \beta_i \rangle}{\langle \alpha, \alpha \rangle} \leq 4 \).

Simplifying we have \( \sum \langle \alpha, \beta_i \rangle \langle \beta_i, \alpha \rangle \leq 4 \); i.e., \( \text{val} \alpha \leq 4 \). When equality holds, we have \( 2\alpha = \sum \langle \alpha, \beta_i \rangle \beta_i \); by minimality, \( \mathcal{C} = \{\alpha, \beta_1, \beta_2, \ldots, \beta_k\} \) and it can be seen that any \( \beta_j \) of minimum valency is an integral combination of the remaining roots of \( \mathcal{C} \). \( \blacksquare \)

**Remark 13.** Let \( \Phi \) be irreducible and \( \Delta \) be a base of \( \Phi \). Define a relation ‘\(<\)’ on \( \Phi \) as follows: for any two roots \( \alpha, \beta \in \Phi \), \( \alpha \prec \beta \) if \( \beta - \alpha \) is a sum of positive roots relative to \( \Delta \). (A root is called positive relative to \( \Delta \) if it can be expressed as a sum of roots in \( \Delta \), in which repetition of any root can occur.) It can be verified that ‘\(<\)’ is a partial order on \( \Phi \). The following have been proved in the literature (cf. [2, Chapter 3]).

(1) \( \Phi \) has a unique maximal root.
(2) If \( \Phi \) admits two distinct root lengths (see Remark 9), then the maximal root is long. \( \Phi \) also has a unique maximal root among the short roots.
The highest long and short roots also have been computed (cf. [2, p. 66]). In any Dynkin diagram in Fig. 4, the vertex starred is the negative of either the highest long root or the highest short root of the base determined by the Dynkin diagram formed by the rest of the vertices. (The type concerned is superscribed with \( s \) if the starred root is short; otherwise it is superscribed with \( * \).)

**Proposition 14.** For any circuit \( C \), its Dynkin diagram \( D \) is one of those types drawn in Fig. 4.

**Proof.** If \( D \) contains a cycle, then by Proposition 11, \( D \) is of the first type given in Fig. 4. So let us assume that \( D \) is a tree. By minimality of \( C \), removal of any end vertex of \( D \) gives a Dynkin diagram of some type drawn in Fig. 2. Thus \( D \) can be recovered from a Dynkin diagram in that figure by adding a vertex and joining it to one of vertices of the latter. Any such choice is restricted by the following obvious conditions:

- The valency of the vertex to which the new one is joined cannot be more than 4 (by Lemma 12).
- When the valency of the new edge is more than 1, then the arrow on that is set according to Lemma 7.

It can be seen that such a choice for any one of the types in Fig. 2 is either again of some type in that figure or contains one of those types drawn in Fig. 4. Thus it follows that any circuit is given by one of those in Fig. 4. Since it can be verified that no graph of Fig. 4 is a subgraph of any other one, it follows that the collection of all Dynkin diagrams drawn in Fig. 4 are precisely those associated with the class of all circuits. ■

Combining Remark 13 and Proposition 14, we have the following:

**Proposition 15.** Let \( B \) be an indecomposable subset of \( \Phi \) which is also linearly independent and obtuse. (In other words \( B \) is a base of some root system.) If \( B \) has at least two elements and \( p \) is either the highest long root or the highest short root relative to \( B \), then \( B \cup \{-p\} \) is a circuit of \( \Phi \). Conversely any circuit \( C \) can be put in this form.

The second part of the above proposition can be proved directly: We can assume, by Proposition 11, that the Dynkin diagram of \( C \) is a tree. If there is any edge of valency > 1 in this tree, let \( x \) be one of them; otherwise let \( x \) be a vertex of maximum degree. Let \( p \) be the (end) vertex which is at maximum possible distance from \( x \). It can be shown that \(-p\) is a highest root of the root system with base \( C \setminus \{p\} \).

In the classification process of the root systems described in Chapter 3 of [2], Dynkin diagrams of both types – those in Figs. 2 and 4 – have been considered and, discarding those Dynkin diagrams which correspond to linearly dependent sets of roots, the list of graphs in Fig. 2 has been constructed. (See also [4,5].) Here also by a similar process which discards Dynkin diagrams which correspond to linearly independent sets, the graphs in Fig. 4 can be constructed. A sketch of such a method is as follows:

Let \( C \) be a circuit and \( D \) be its Dynkin diagram. If \( D \) contains a cycle, then by Proposition 11, \( D \) is of the first type drawn in Fig. 4; so let \( D \) be a tree. If \( D \) has an edge of valency 3, then by Lemma 12, \( D \) has to be either \( G^*_2 \) or \( G^*_3 \). So, suppose \( D \) has no edge of valency 3. If \( D \) has two edges of valency 2, then by Remark 8, \( D \) has to be either \( B^*_n \) or \( C^*_n \).

Now suppose \( D \) has exactly one edge of valency 2. If \( D \) has any vertex of degree > 2, then \( D \) is either \( B^*_n \) or \( C^*_n \). So, assume that the degree of every vertex of \( D \) is \( \leq 2 \). Then the (unique)
Fig. 4. The Dynkin diagrams of circuits.
edge of valency 2 cannot be a pendant edge of \( D \) for the reason that \( D \) can be neither \( B_n \) nor \( C_n \). Thus \( F_4 \) has to be a subgraph of \( D \) and the latter has to be either \( F_4^* \) or \( F_4^\ast \).

Now assume that every edge of \( D \) has valency 1. Since \( D \) is not of the type \( A_n \), there should be at least one vertex of degree \( \geq 3 \). If \( D \) has either a vertex of degree \( \geq 3 \) or two vertices of degree \( \geq 2 \), then \( D \) is of the type \( D_n^* \). So, we can assume that \( D \) has exactly one vertex of degree 3. Then \( D \) has to be one of those types in \( \{ D_n, E_6, E_7, E_8, E_6^*, E_7^*, E_8^* \} \). \( E \) being linearly dependent, it follows that \( D \) is of one of the latter three types given above.

**Remark 16.** By studying ‘generalized Cartan matrices’ and using a fundamental fact from ‘the theory of linear inequalities’, the Dynkin diagrams of bases of root systems and also those of circuits have been computed in [3].

**Lemma 17.** If \( \{ \alpha_1, \alpha_2, \ldots, \alpha_n \} \) is a linearly dependent subset of \( \Phi \), then there exist integers \( t_1, t_2, \ldots, t_n \), not all zero, such that \( t_1\alpha_1 + t_2\alpha_2 + \cdots + t_n\alpha_n = 0 \).

**Proof.** It can be verified that \( \det([\langle \alpha_i, \alpha_j \rangle]) = 0 \) where \( [\langle \alpha_i, \alpha_j \rangle] \) is the \( n \times n \) matrix in which for \( 1 \leq i, j \leq n \), the \( (i, j) \)-th entry is \( \langle \alpha_i, \alpha_j \rangle \). (Taking \( \alpha_1, \alpha_2, \ldots, \alpha_n \) as vectors in \( \mathbb{R}^n \) yields \([\langle \alpha_i, \alpha_j \rangle]\) = \( MM' \) where \( M \) is the \( n \times n \) matrix whose rows are \( \alpha_1, \alpha_2, \ldots, \alpha_n \) and its transpose is \( M' \).) Therefore \( \det \left( \frac{2\langle \alpha_i, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} \right) = 0 \). Since the entries of the latter matrix are integers, there exist integers \( t_1, t_2, \ldots, t_n \), not all zero, such that

\[
(t_1, t_2, \ldots, t_n) \begin{bmatrix} \frac{2\langle \alpha_i, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} \end{bmatrix} = (0, 0, \ldots, 0);
\]

i.e., for \( j = 1, 2, \ldots, n \), \( \sum_t t_i \frac{\langle \alpha_i, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} = 0 \);

i.e., for \( j = 1, 2, \ldots, n \), \( \left( \sum t_i \langle \alpha_i, \alpha_j \rangle \right) = 0 \).

Therefore \( \left( \sum t_i \alpha_i, \sum t_i \alpha_i \right) = 0 \). ■

Now we are in the position to prove the main result of this paper.

**Proof of Theorem 4.** First let \( S \) be any minimal linearly dependent subset of \( \Phi \). We can assume the following.

(a) The conclusion of the theorem holds for any minimal linearly dependent subset of \( \Phi \) with cardinality \( < |S| \).

Let \( X = \{ x_1, x_2, \ldots, x_k \} \) be any minimal linearly dependent subset of \( \Phi \). By Lemma 17 we can choose integers \( t_1, t_2, \ldots, t_k \) without any common divisor such that \( \sum t_i x_i = 0 \). Define \( \rho(X) = -\sum |t_i| \). (Note that by minimality, \( \rho(X) \) is independent of the choice of the integers \( t_1, t_2, \ldots, t_k \), since the only other choice is \( \{-t_1, -t_2, \ldots, -t_k\} \).) Since \( \Phi \) is finite [by (R1)] we can also assume the following.

(b) If \( X \) is any minimal linearly dependent subset of \( \Phi \) such that \( |X| = |S| \) and \( \rho(X) < \rho(S) \), then the conclusion holds for \( X \).

Let \( \alpha_1, \alpha_2, \ldots, \alpha_n \) be the elements of \( S \). Let \( t_1, t_2, \ldots, t_n \) be a set of relatively prime integers such that

(c) \( t_1\alpha_1 + t_2\alpha_2 + \cdots + t_n\alpha_n = 0 \).
For any \( i \leq n \), we can assume that \( t_i > 0 \), for otherwise \( t_i \) and \( \alpha_i \) can be replaced by \(-t_i\) and \(-\alpha_i\) respectively. We can also assume that (3) of Definition 5 holds (with \( S \) in place of \( \emptyset \)), for otherwise the conclusion holds for \( S \). If \( S \) is obtuse, then \( S \) is a circuit and by Proposition 15, again the conclusion follows. So we can assume the existence of two roots, say \( \alpha_1, \alpha_2 \), in \( S \) which have positive inner product. Then by (3) of Remark 2, \( \alpha_1 - \alpha_2 \in \Phi \). Now consider the set \( S' = \{ \alpha_1 - \alpha_2, \alpha_2, \alpha_3, \ldots, \alpha_n \} \). If \( S' \) is not a minimal linearly dependent set, then obviously \( \{ \alpha_1 - \alpha_2, \alpha_3, \ldots, \alpha_n \} \) has to be a (minimal) linearly dependent set; then by (a), the theorem holds for this subset and it can be verified that it holds for \( S \) also. So, let \( S' \) be a minimal linearly dependent set.

Now by (c), we have

\[
(t_1(\alpha_1 - \alpha_2) + (t_1 + t_2)\alpha_2 + t_3\alpha_3 + \cdots + t_n\alpha_n = 0.
\]

Since \( \rho(S') < \rho(S) \), by (b) the conclusion holds for \( S' \). Now it can be verified that for \( S \) also the same holds.

Now let \( S \) be any indecomposable linearly dependent subset of \( \Phi \) and assume that for any indecomposable linearly dependent subset of \( \Phi \) with cardinality \( < |S| \), the conclusion holds. By what has been proved earlier, there exists a root in \( S \) and an indecomposable subset of \( S \setminus \{ \alpha \} \) by which \( \alpha \) is generated. It is easy to verify that \( S \setminus \{ \alpha \} \) is also indecomposable and by the last assumption, \( S \setminus \{ \alpha \} \) is generated by one of its indecomposable subsets; obviously the latter also generates \( S \). ■

Remark 18. The method used above is based on a simpler variation of a technique employed in [6]; there the above theorem for root systems of unique root length, viz., \( A_n \), \( D_n \) and \( E_k \) where \( n \geq 2 \) and \( k = 6, 7, 8 \), has been proved.

Acknowledgements

The authors are grateful to the referee for suggestions for improving the exposition of the paper and for pointing out some minor mistakes. The first author’s work was partially supported by Kanwal Rekhi Career Development Scholarship of the TIFR Endowment Fund.

References