18.745 Introduction to Lie Algebras November 1, 2010

Lecture 16 — Root Systems and Root Lattices

Prof. Victor Kac *Scribe: Michael Crossley*

Recall that a root system is a pair (V, Δ), where V is a finite dimensional Euclidean space over $\mathbb{R}$ with a positive definite bilinear form $(\cdot, \cdot)$ and Δ is a finite subset, such that:

1. $0 \notin \Delta; \mathbb{R}\Delta = V$;
2. If $\alpha \in \Delta$, then $n\alpha \in \Delta$ if and only if $n = \pm 1$;
3. (String property) if $\alpha, \beta \in \Delta$, then $\{\beta + j\alpha | j \in \mathbb{Z}\} \cap (\Delta \cup 0) = \{\beta - p\alpha, \dots, \beta, \dots, \beta + q\alpha\}$where $p - q = 2\frac{(\alpha,\beta)}{(\alpha,\alpha)}$.

(V, Δ) is called indecomposable if it cannot be decomposed into a non-trivial orthogonal direct sum. $r = dimV$ is called the rank of (V, Δ) and elements of Δ are called roots.

Definition 16.1. An isomorphism of an indecomposable root system (V, Δ) and (V_1, Δ_1) is a vector space isomorphism $\varphi : V \to V_1$, such that $\varphi(\Delta) = \Delta_1$, and $(\varphi(\alpha), \varphi(\beta))_1 = c(\alpha, \beta)$ for all $\alpha, \beta \in \Delta$, where c is a positive constant, independent of α and β. In particular, replacing $(\cdot, \cdot)$ by $c(\cdot, \cdot)$, where $c > 0$, we get, by definition, an isomorphic root system.

Example 16.1. Root systems of rank 1: $(\mathbb{R}, \Delta = \{\alpha, -\alpha\})$, $\alpha \neq 0$, $(\alpha, \beta) = \alpha\beta$. This root system is isomorphic to that of $sl_2(\mathbb{F})$, $so_3(\mathbb{F})$, and $sp_2(\mathbb{F})$.

Proposition 16.1. *Let (V, Δ) be an indecomposable root system with the bilinear form $(\cdot, \cdot)$. Then*

1. *Any other bilinear form $(\cdot, \cdot)_1$ for which the string property holds is proportional to $(\cdot, \cdot)$, i.e. $(\alpha, \beta)_1 = c(\alpha, \beta)$ for some positive $c \in \mathbb{R}$, independent of α and β.*
2. *If $(\alpha, \alpha) \in \mathbb{Q}$ for some $\alpha \in \Delta$, then $(\beta, \gamma) \in \mathbb{Q}$ for all $\beta, \gamma \in \Delta$.*

Proof. Fix $\alpha \in \Delta$. Since (V, Δ) is indecomposable, for any $\beta \in \Delta$ there exists a sequence $\gamma_0, \gamma_1, \dots, \gamma_k$ such that $\alpha = \gamma_0$, $\beta = \gamma_k$, $(\gamma_i, \gamma_{i+1}) \neq 0$ for all $i = 0, \dots, k-1$. Define c by $(\alpha, \alpha)_1 = c(\alpha, \alpha)$. By the string property $p - q = 2\frac{(\alpha,\gamma_1)}{(\alpha,\alpha)} = 2\frac{(\alpha,\gamma_1)_1}{(\alpha,\alpha)_1}$. Hence $(\alpha, \gamma_1)_1 = c(\alpha, \gamma_1)$. Likewise, by the string property, $\frac{2(\alpha,\gamma_1)}{(\gamma_1,\gamma_1)} = \frac{2(\alpha,\gamma_1)_1}{(\gamma_1,\gamma_1)_1}$. Hence $(\gamma_1, \gamma_1) = c(\gamma_1, \gamma_1)$. Continuing this way, we show that $(\gamma_2, \gamma_2)_1 = c(\gamma_2, \gamma_2), \dots (\beta, \beta)_1 = c(\beta, \beta)$. Since $\frac{2(\alpha,\beta)}{(\alpha,\alpha)} = \frac{2(\alpha,\beta)_1}{(\alpha,\alpha)_1}$, we conclude that $(\alpha, \beta)_1 = c(\alpha, \beta)$ for all $\alpha, \beta \in \Delta$. Since Δ spans V, we conclude that (1) holds. The same argument proves (2).

□

Definition 16.2. A lattice in an Euclidean space V is a discrete subgroup $(Q, +)$ of V, which spans V over $\mathbb{R}$, i.e. $\mathbb{R}Q = V$. For example, $\mathbb{Z}^n \subset \mathbb{R}^n$.

Proposition 16.2. *If Δ is a finite set in an Euclidean space V, spanning V over $\mathbb{R}$, such that $(\alpha, \beta) \in \mathbb{Q}$ for all $\alpha, \beta \in \Delta$, then $\mathbb{Z}\Delta$ is a lattice in V.*

Proof. The only thing to prove is that $\mathbb{Z}\Delta$ is a discrete set. Choose a basis $\beta_1, \ldots, \beta_r$ of V among the vectors of Δ. Then for any $\alpha \in \Delta$, we have $\alpha = \sum_{i=1}^r c_i\beta_i$, $c_i \in \mathbb{R}$. Hence, $(\alpha, \beta_j) = \sum_{i=1}^r c_i(\beta_i, \beta_j)$. But $((\beta_i, \beta_j))_{i,j=1}^r$ is a Gramm matrix of a basis, hence it is non-singular. Hence the c_i's can be computed by Cramer's rule, so all $c_i \in \mathbb{Q}$. So $\mathbb{Z}\Delta \subset \mathbb{Q}\{\beta_1, \ldots, \beta_r\}$. But since Δ is finite, we conclude that $\mathbb{Z}\Delta \subset \frac{1}{N}\mathbb{Z}\{\beta_1, \ldots, \beta_r\}$ where N is a positive integer. But $\frac{1}{N}\mathbb{Z}\{\beta_1, \ldots, \beta_r\}$ is discrete, hence $\mathbb{Z}\Delta$ is discrete. □

Example 16.2. $\{1, \sqrt{2}\} \subset \mathbb{R}$, then $\mathbb{Z}\{1, \sqrt{2}\}$is not a discrete set.

Corollary 16.3. *If (V, Δ) is a root system, then $Q := \mathbb{Z}\Delta$ is a lattice, called the root lattice.*

Proof. By the two propositions, the corollary holds if (V, Δ) is indecomposable, hence holds for any root system (V, Δ). □

We will list four series of root systems of rank r known to us. In all cases $(\epsilon_i, \epsilon_j) = \delta_{ij}$.

Type	$\mathfrak{g}$	V	Δ	Q
A	$sl_{r+1}(\mathbb{F})$	$\{\sum_{i=1}^{r+1} a_i\epsilon_i \mid a_i \in \mathbb{R}, \sum_{i=1}^{r+1} a_i = 0\}$	$\{\epsilon_i - \epsilon_j \mid 1 \le i, j \le r+1\}$	$\{\sum_{i=1}^{r+1} a_i\epsilon_i \mid a_i \in \mathbb{Z}, \sum_{i=1}^{r+1} a_i = 0\}$
B	$so_{2r+1}(\mathbb{F})$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{R}\}$	$\{\pm\epsilon_i \pm \epsilon_j, \pm\epsilon_i \mid 1 \le i, j \le r, i \ne j\}$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{Z}\}$
C	$sp_{2r}(\mathbb{F})$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{R}\}$	$\{\pm\epsilon_i \pm \epsilon_j, \pm 2\epsilon_i \mid 1 \le i, j \le r, i \ne j\}$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{Z}, \sum_{i=1}^{r} a_i \in 2\mathbb{Z}\}$
D	$so_{2r}(\mathbb{F}), r \ge 3$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{R}\}$	$\{\pm\epsilon_i \pm \epsilon_j \mid 1 \le i, j \le r, i \ne j\}$	$\{\sum_{i=1}^{r} a_i\epsilon_i \mid a_i \in \mathbb{Z}, \sum_{i=1}^{r} a_i \in 2\mathbb{Z}\}$

Remark Explanation: in case A, V is a factor space of $\widetilde{V} = \sum_{i=1}^{r+1} a_i\epsilon_i$ by a 1-dimensional subspace $\mathbb{R}(\epsilon_1 + \ldots + \epsilon_{r+1})$. Notice that $(\epsilon_1 + \ldots + \epsilon_{r+1})^\perp = V$ in the table, so $\widetilde{V} = V \oplus \mathbb{R}(\epsilon_1 + \ldots + \epsilon_{r+1})$ with direct sum. Secondly, why is $\Delta_A = \{\sum_{i=1}^{r+1} a_i\epsilon_i \mid a_i \in \mathbb{Z}, \sum_{i=1}^{r+1} a_i = 0\}$. Clearly, $\mathbb{Z}\{\epsilon_i - \epsilon_j \mid i \ne j\}$ is included in this set. To show the reverse inclusion, write

$$Q \ni \sum_{i=1}^{r+1} a_i\epsilon_i = a_1(\epsilon_1-\epsilon_2)+(a_1+a_2)(\epsilon_2-\epsilon_3)+\ldots+(a_1+a_2+\ldots+a_r)(\epsilon_r-\epsilon_{r+1})+(a_1+\ldots+a_{r+1})(\epsilon_{r+1}),$$

where the coefficient of the last term is zero. So the reverse inclusion is also true. For case B, the form of the root lattice is clearly correct.

Exercise 16.1. Explain the root lattices in cases C and D.

Proof. C. $\mathbb{Z}\Delta_{C_r} \subset Q_{C_r}$ as each member of Δ_{C_r} is of the form $a_1\epsilon_i + a_2\epsilon_j$ with $a_1 = \pm 1$, $a_2 = \pm 1$. So each element of $\mathbb{Z}\Delta_{C_r}$is of the form $\sum_{i=1}^r a_i\epsilon_i$ where $a_i \in \mathbb{Z}$, $\sum_{i=1}^r a_i \in 2\mathbb{Z}$. $Q_{C_r} \subset \mathbb{Z}\Delta_{C_r}$ as any $\sum_{i=1}^r a_i\epsilon_i$ with $a_i \in \mathbb{Z}$, $\sum_{i=1}^r a_i \in 2\mathbb{Z}$ can be written in the form

$$\sum_{i=1}^{r} a_i\epsilon_i = a_1(\epsilon_1-\epsilon_2)+(a_2+a_1)(\epsilon_2-\epsilon_3)+\ldots+(a_r+a_{r-1}+\ldots+a_1)(\epsilon_r-\epsilon_1)+(a_r+\ldots+a_1)\epsilon_1.$$

All these coefficients belong to $\mathbb{Z}$ and the final coefficient of $\epsilon_1$belongs to $2\mathbb{Z}$ so can be written as $\frac{a_r+\ldots+a_1}{2}2\epsilon_1$, hence $\sum_{i=1}^r a_i\epsilon_i \in \mathbb{Z}\Delta_{C_r}$.

D. The proof for Q_{D_r} is identical except $2\epsilon_i \in \Delta_{D_r}$, so write

$$\sum_{i=1}^{r} a_i\epsilon_i = a_1(\epsilon_1 - \epsilon_2) + (a_2 + a_1)(\epsilon_2 - \epsilon_3) + \\ \ldots + \frac{a_r + \ldots + a_1}{2}(\epsilon_r - \epsilon_1) + \frac{a_r + \ldots + a_1}{2}(\epsilon_r - \epsilon_2) + \frac{a_r + \ldots + a_1}{2}(\epsilon_1 + \epsilon_2)$$

as $r \geq 3$, and this belongs to $\mathbb{Z}\Delta_{D_r}$.

□

Definition 16.3. A lattice Q is called integral (respectively even) if $(\alpha, \beta) \in \mathbb{Z}$ (respectively $(\alpha, \alpha) \in 2\mathbb{Z}$) for all $\alpha, \beta \in Q$. Note that an even lattice is always integral: if $\alpha, \beta \in Q$, Q even, then $(\alpha + \beta, \alpha + \beta) = (\alpha, \alpha) + (\beta, \beta) + 2(\alpha, \beta)$, $(\alpha, \alpha), (\beta, \beta) \in 2\mathbb{Z}$. Hence $2(\alpha, \beta) \in 2\mathbb{Z}$, so $(\alpha, \beta) \in \mathbb{Z}$.

Example 16.3. For a positive integer r let

$$E_r = \{\sum_{i=1}^{r} a_i\epsilon_i | \text{ either all } a_i \in \mathbb{Z} \text{ or all } a_i \in \mathbb{Z} + \frac{1}{2}, \text{ and } \sum_{i=1}^{r} a_i \in 2\mathbb{Z}\},$$

with $E_r \subset \mathbb{R}^r$,$(\epsilon_i, \epsilon_j) = \delta_{ij}$.

Proposition 16.4. *E_r is an even lattice if and only if r is divisible by 8.*

Proof. We use that $a^2 \pm a \in 2\mathbb{Z}$ if $a \in \mathbb{Z}$. Let $\alpha = \sum_{i=1}^{r} a_i\epsilon_i \in E_r$. Case 1: all $a_i \in \mathbb{Z}$, then $(\alpha, \alpha) = \sum_{i=1}^{r} a_i^2 = \sum_{i=1}^{r} a_i \bmod 2 \equiv 0 \bmod 2$ by the condition of E_r, so $(\alpha, \alpha) \in 2\mathbb{Z}$. Case 2: write $\alpha = \rho + \beta$ where $\rho = (\frac{1}{2}, \ldots, \frac{1}{2})$ and β has integer coefficients b_i. Then $(\alpha, \alpha) = (\rho, \rho) + 2(\rho, \beta) + (\beta, \beta) = (\rho, \rho) + \sum_{i=1}^{r}(b_i^2 + b_i) = \frac{r}{4} + n$, $n \in 2\mathbb{Z}$. So (α, α) is even if and only if r is a multiple of 8. □

Theorem 16.5. *Let Q be an even lattice in an Euclidean space V, and assume the subset $\Delta = \{\alpha \in Q | (\alpha, \alpha) = 2\}$ spans V over $\mathbb{R}$. Then $(V, \Delta)$is a root system.*

Proof. Axiom (1) of a root system is clear, as is axiom (2): if $(\alpha, \alpha) = 2$, then $(n\alpha, n\alpha) = 2$ iff. $n = \pm 1$. It remains to show the string property. Reversing the sign of α if necessary, we may assume $(\alpha, \beta) \geq 0$. Note that for $\alpha, \beta \in \Delta$ we have:

$$0 \leq (\alpha - \beta, \alpha - \beta) = (\alpha, \alpha) - 2(\alpha, \beta) + (\beta, \beta) = 4 - 2(\alpha, \beta),$$

where $(\alpha, \beta) \in \mathbb{Z}$, $(\alpha, \beta) \geq 0$. So the only possibilities are $(\alpha, \beta) = 0, 1$ or 2. In the last case, hence $q = 0$, $p = 2$, so $p - q = (\alpha, \beta) = 2$ and the string property is satisfied. □

Exercise 16.2. Complete the proof, for $(\alpha, \beta) = 0$ or 1.

Proof. For $(\alpha, \beta) = 1$, $\alpha - \beta \in \Delta$, $\alpha + \beta \notin \Delta$, so $p = 1$, $q = 0$, and $p - q = (\alpha, \beta)$. For $(\alpha, \beta) = 0$, $\alpha + \beta \notin \Delta$, $\alpha - \beta \notin \Delta$, $p = 0$, $q = 0$, and $p - q = (\alpha, \beta)$. So the string property holds generally, and the theorem holds. □

The most remarkable lattice is E_8 (which is even by proposition.)

Exercise 16.3. Show that

$\Delta_{E_8} := \{\alpha \in E_8 | (\alpha, \alpha) = 2\} = \{\pm\epsilon_i \pm \epsilon_j | i \neq j\} \cup \{\frac{1}{2}(\pm\epsilon_1 \pm \ldots \pm \epsilon_8) |$ even number of minus signs$\}$,

that $|\Delta_{E_8}| = 240$, and that $\mathbb{R}\Delta_{E_8}$=V.

Proof.

$$E_8 = \{\sum_{i=1}^{8} a_i\epsilon_i | \text{ all } a_i \in \mathbb{Z}, \sum_{i=1}^{8} a_i \in 2\mathbb{Z}\} \cup \{\sum_{i=1}^{8} a_i\epsilon_i | \text{ all } a_i \in \mathbb{Z} + \frac{1}{2}, \sum_{i=1}^{8} a_i \in 2\mathbb{Z}\}.$$

The elements from the first set satisfying $(\alpha, \alpha) = 2$ are clearly $\{\pm\epsilon_i \pm \epsilon_j | i \neq j\}$ as $(\epsilon_i, \epsilon_j) = \delta_{ij}$, and the second set must have all $a_i = \pm\frac{1}{2}$ else $(\alpha, \alpha) > 2$, and as $\sum_{i=1}^{8} a_i \in 2\mathbb{Z}$, there must be an even number of minus signs.

$$\begin{aligned}|\Delta_{E_8}| &= |\{\epsilon_i + \epsilon_j | i \neq j\}| + |\{-\epsilon_i - \epsilon_j | i \neq j\}| + |\{\epsilon_i - \epsilon_j | i \neq j\}| + \left|\{\frac{1}{2}(\pm\epsilon_1 \pm \ldots \pm \epsilon_8) | \text{ even number of minus signs}\}\right| \\ &= \frac{8.7}{2} + \frac{8.7}{2} + 8.7 + 2^7 = 240.\end{aligned}$$

Clearly $\epsilon_i = \frac{\epsilon_i + \epsilon_j}{2} + \frac{\epsilon_i - \epsilon_j}{2} \in \mathbb{R}\Delta_{E_8}$, and $\{\epsilon_i\}$ form a basis of V, hence $\mathbb{R}\Delta = V$.

□

So $(\mathbb{R}^8, \Delta_{E_8})$ is a root system by the theorem, which is called the root system of type E_8.

Exercise 16.4. Consider the following subsystem of the root system of type E_8 : take $\rho = (\frac{1}{2}, \ldots, \frac{1}{2})$ and let $\Delta_{E_7} = \{\alpha \in \Delta_{E_8} | (\alpha, \rho) = 0\}$, $Q_{E_7} = \{\alpha \in Q_{E_8} | (\alpha, \rho) = 0\}$, $V_{E_7} = \{v \in V_{E_8} | (v, \rho) = 0\}$. Show that (V_{E_7}, Δ_{E_7}) is a root system of rank 7, and that $|\Delta_{E_7}| = 126$.

Proof. Clearly $\Delta_{E_7} = \{\alpha \in Q_{E_7} | (\alpha, \alpha) = 2\}$. Q_{E_7} is an even lattice in V_{E_7} as it is a subgroup of Q_{E_8} and clearly $\mathbb{R}Q_{E_7} = V_{E_7}$, so $(V_{E_7}, \Delta_{E_7})$is a root system of rank 7 as $V_{E_8} = V_{E_7} \oplus \mathbb{R}(\frac{1}{2}, \ldots, \frac{1}{2})$, $V_{E_7} = (\frac{1}{2}, \ldots, \frac{1}{2})^{\perp}$, and $dimV_{E_8} = 8$.

$$\Delta_{E_7} = \{\epsilon_i - \epsilon_j | i \neq j\} \cup \{\frac{\pm\epsilon_1 \pm \ldots \pm \epsilon_8}{2} | \text{ 4 minus signs.}\}$$

Hence,

$$|\Delta_{E_7}| = 56 + \binom{8}{4} = 126$$

□

Exercise 16.5. Let $\Delta_{E_6} = \{\alpha \in \Delta_{E_7} | (\alpha, \epsilon_7 + \epsilon_8) = 0\}$, $Q_{E_6} = \{\alpha \in Q_{E_7} | (\alpha, \epsilon_7 + \epsilon_8) = 0\}$, $V_{E_6} = \{v \in V_{E_7} | (v, \epsilon_7 + \epsilon_8) = 0\}$. Show that (V_{E_6}, Δ_{E_6}) is a root system of rank 6, and that $|\Delta_{E_6}| = 72$.

Proof. Clearly $\Delta_{E_6} = \{\alpha \in Q_{E_6} | (\alpha, \alpha) = 2\}$. Q_{E_6} is an even lattice in V_{E_6} as it is a subgroup of Q_{E_7} and clearly $\mathbb{R}Q_{E_6} = V_{E_6}$, so (V_{E_6}, Δ_{E_6}) is a root system of rank 6 as $V_{E_7} = V_{E_6} \oplus \mathbb{R}(\epsilon_7 + \epsilon_8)$, $V_{E_6} = (\epsilon_7 + \epsilon_8)^{\perp}$, and $dimV_{E_7} = 7$.

$\Delta_{E_6} = \{\epsilon_i - \epsilon_j | \text{ if } i = 7, j = 8, \text{ if } i = 8, j = 7\} \cup \{\frac{\pm\epsilon_1 \pm \ldots \pm \epsilon_8}{2} | \text{ 4 minus signs and } \epsilon_{7,}\epsilon_8 \text{ have opposite signs}\}$

Hence,

$$|\Delta_{E_6}| = 6.5 + 2 + 2\binom{6}{3} = 72.$$

□