JOURNAL OF ALGEBRA 97, 166–180 (1985)

Rootsystems of Simple Lie Algebras

DAVID J. WINTER

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109

Communicated by Walter Feit

Received June 13, 1983

Rootsystems of nonclassical simple Lie algebras $L=\sum_{a\in R} L_a$ such that $a([e,f])\neq 0$ for some $e\in L'_a, f\in L'_{-a}$ for each $a\in R-\{0\}$ either contain T_2-sections or are irreducible *Witt rootsystems.* The irreducible Witt rootsystems of prime ranks 1, 2, 3 are W, W_2, S_2, W_3, $W\oplus(W\vee W)$, $W\oplus S_2$, S_3, $S_3\oplus(W\vee W)$, $S_3(S_2)$. Witt rootsystems having no sections S_2, $W\oplus(W\vee W)$ are classified as those rootsystems whose irreducible components are finite vector space subgroups. Since the latter are rootsystems of generalized Albert–Zassenhaus Lie algebras, it follows that the rootsystems of nonclassical simple Lie algebras $L=\sum_{a\in R} L_a$ such that $([e,f])\neq 0$ for some $e\in L'_a, f\in L'_{-a}$ for each $a\in R-\{0\}$ which contain no section of type T_2, S_2, or $W\oplus(W\vee W)$ are classified up to isomorphism by finite vector space subgroups.

INTRODUCTION

In this paper, we discuss the rootsystem of a simple Lie algebra L with respect to a split Cartan decomposition $L=\sum_{a\in R} L_a$ such that for each $a\in R-\{0\}$, there exist $e\in L'_a$, $f\in L'_{-a}$ such that $a([e,f])\neq 0$. Here, L'_a is the eigenspace $L'_a=\{x\in L \mid [h,x]=a(h)x \text{ for all } h\in L_0\}$ of L_0 corresponding to the root a. The class of such simple Lie algebras $L=\sum_{a\in R} L_a$ includes, relative to the appropriate Cartan subalgebra, the simple classical Lie algebras, the Albert–Zassenhaus algebras, and the Kaplansky algebras $W(m,n)$ (also called generalized Witt algebras).

When the condition of simplicity is dropped, one has the larger class of *symmetric Lie algebras* studied in Winter [3]. The rootsystems of 2-sections $L^{(a,b)}=\sum_{i,j=0}^{p-1} L_{ia+jb}$ of symmetric Lie algebras L are classified up to isomorphism by types A, W, $A\vee A$, $A\vee W$, $W\vee W$, A_2, B_2, G_2, $A\oplus W$, $W\otimes W$, S_2, T_2. The rootsystem R of L decomposes as $R\subset R^w+S$ (S classical) if and only if no 2-section is of type T_2. For L simple, we now show that if L has no 2-section T_2, then either L is classical or R is a *Witt*

0021-8693/85 $3.00

rootsystem, that is, $R = R^w$. We then classify the Witt rootsystems of prime rank 3. Using the prime rank 3 classification, we classify all Witt rootsystems having no sections S_2, $W \oplus (W \vee W)$. Specifically, the following theorems are proved.

THEOREM 2.1. *Let $L = \sum_{a \in R} L_a$ be a simple nonclassical Lie algebra such that there exists, for each $a \in R - \{0\}$, $e \in L'_a$, $f \in L'_{-a}$ such that $a([e,f]) \neq 0$. Suppose that L has no 2-section of type T_2. Then either L is classical or R is an irreducible Witt rootsystem.*

THEOREM 3.7. *Let R be an irreducible Witt rootsystem. Then R is one of W, W_2, S_2, W_3, $W \oplus (W \vee W)$, $W \oplus S_2$, S_3, $S_3 \oplus (W \vee W)$, $S_3(S_2)$.*

THEOREM 3.15. *Let R be a Witt rootsystem. Then R has no sections S_2, $W \oplus (W \vee W)$ if and only if the irreducible components of R are vector space subgroups.*

Theorems 3.7 and 3.15 are the basis for the classification of rootsystems of generalized classical–Albert–Zassenhaus Lie algebras in Winter [2].

1. PRELIMINARIES

Throughout this paper, Lie algebras L over a field k of characteristic p are considered relative to a split Cartan decomposition $L = \sum_{a \in R} L_a$. Notation and conventions follow Seligman [1] and Winter [3].

We regard R as subsets of its k-span $V = kR$. Then L is *graded* by the additive group V with *support* R in the sense that $L = \sum_{a \in V} L_a$ (direct) with $L_a \neq \{0\}$ if and only if $a \in R$ and $[L_a, L_b] \subset L_{a+b}$ $a, b \in V$. This grading of L by V is a *Cartan grading* with *rootspaces* L_a $(a \in R)$ in the sense that the subalgebra L_0 is a Cartan subalgebra of L and the L_a $(a \in R)$ are the eigenspaces $L_a = \{x \in L \mid (\mathrm{ad}\, h - a(h)I)^{\dim L} x = 0 \text{ for all } h \in L_0\}$ of $\mathrm{ad}\, L_0$. Each rootspace L_a is nonzero and contains the *linear rootspace* $L'_a = \{x \in L \mid \mathrm{ad}\, h(x) = a(h)x \text{ for all } h \in L_0\}$. If $\mathrm{ad}\, L_0$ is triangulable, then each linear rootspace L'_a $(a \in R)$ is nonzero.

Following Winter [3], L is *symmetric* if a $([L'_{-a}, L'_a]) \neq 0$ for all $a \in R - \{0\}$. And (R, V) is a *Lie rootsystem* over k if

LRS 1. $0 \in R = -R$ and R is a finite subset of the vector space V over k;

LRS 2. for all $a \in R - \{0\}$, there exists $a^0 \in \mathrm{Hom}_k(V, k)$ such that $a^0(a) = 2$ and the *reflection* $r_a(b) = b - a^0(b)a$ at a^0 stabilizes all bounded a-orbits $R_b(a)$;

LRS 3. each nonzero root a is classical or Witt;

LRS 4. each Witt orbit has 1, $p-1$, or p elements.

Here, the *a-orbit* of b is the translational orbit $\{b-ra,..., b+qa\}$ with $b+ia \in R$ $(-r \leqslant i \leqslant q)$ and either $q+1=-r$ modulo p, in which case $R_b(a)=\mathbb{Z}a+b$ and $R_b(a)$ is *unbounded*, or $b-(r+1)a \notin R$ and $b+(q+1)a \notin R$, in which case $R_b(a)$ is *bounded*. An element $a \in R$ is *classical* (respectively *Witt*) if the subsystem $R_a = \mathbb{Z}a \cap R$ is $\{-a, 0, a\}$ (respectively $\mathbb{Z}a$); and an orbit $R_b(a)$ is *classical* (respectively *Witt*) if a is classical (respectively Witt). The set of Witt roots is denoted R^w, and the set of classical roots is denoted R^c. It is observed in Corollary 1.6 below that, in the absence of 2-sections of type T_2 (see below), R^w is a Lie rootsystem.

Any Lie rootsystem R decomposes as $R = R_1 V \cdots V R_n$ where R_i are the *irreducible component* Lie rootsystems of R, following Winter [3].

A *classical rootsystem* is a Lie rootsystem R such that $R = R^c$, and a *Witt rootsystem* is a Lie rootsystem R such that $R = R^w$. Clearly, R is classical (respectively Witt) if and only if its irreducible components R_i are classical (respectively Witt).

The present paper depends on the following results.

1.1. THEOREM (Winter [3]). *For $L = \sum_{a \in R} L_a$ symmetric, (R, V) is a Lie rootsystem. Moreover, L_a is one dimensional for every $a \in R^c$.*

1.2. THEOREM. (Winter [3]). *The irreducible classical rootsystems are those of type $A_n (n \geqslant 1)$, $B_n (n \geqslant 2)$, $C_n (n \geqslant 3)$, $D_n (n \geqslant 4)$, $E_n (n = 6, 7, 8)$, F_4, G_2.*

1.3. THEOREM (Winter [3]). *A Lie algebra $L = \sum_{a \in R} L_a$ is classical if and only if L is symmetric with R classical and $L^2 = L$, Center $L = \{0\}$.*

Given $\mathbb{Z}_p$-independent $a_1,..., a_n$ in R, $Ra_1 \cdots a_n =_{\text{def}} R \cap (\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n)$ is a Lie rootsystem of *prime rank n* called an *n-section* of R. The 1-sections and 2-sections are of special importance. They are classified as follows.

1.4. THEOREM (Winter [3]). *For (R, V) a Lie rootsystem, the* 1*-sections R_a and* 2-sections *Rab are of the following types:*

A_1 *or* W_1 *(if $a = b$),*
$A_1 \vee A_1$, $A_1 \vee W_1$, $W_1 \vee W_1$ *(if R is reducible),*
A_2, B_2, G_2 *(if R is irreducible and classical),*
W_2, $W_1 \oplus A_1$ *(if R is irreducible, nonclassical, and no Witt orbits of $p-1$ elements occur),*
S_2, T_2 *(if Witt orbits of $p-1$ elements occur).*

In particular, Rab is of type T_2 if $a \in R^w - \{0\}$, $b \in R^c - \{0\}$, and $b^0(a) \neq 0$.

Letting $\hat{}: R \to \hat{R}$ be the *closure homomorphism* from R to its double

$\mathbb{Z}$-dual $\hat{R}$, $\hat{R}$ is a classical rootsystem and R^w is the kernel of $\hat{}$ if R has no 2-section of type T_2, by Winter [3].

1.5. THEOREM (Winter [3]). *Let R be a Lie rootsystem having no 2-sections Rab of type T_2. Then every classical complement S of R^w is a classical rootsystem such that $R \subset R^w + S$ and S is isomorphic to $\hat{R}$ under $b \mapsto \hat{b}$.*

Here, a *classical complement* of R^w is any subset S of R which is constructed by taxing a base $\hat{a}_1, ..., \hat{a}_r$ for the classical rootsystem $\hat{R}$, taking preimages $a_1, ..., a_r \in R$ and forming S as

$$S = \{n_1 a_1 + \cdots + n_r a_r \mid n_1 a_1 + \cdots + n_r a_r \in \hat{R}\}.$$

We call $b \mapsto \hat{b}$ the *canonical isomorphism* from S to $\hat{R}$.

We also need the following corollary.

1.6. COROLLARY. *Let R be a Lie rootsystem having no subsystem Rab of type T_2 and let c be a nonzero root in R. Then*

1. *c is a Witt root if and only if $\hat{c} = \hat{0}$, and R^w is a Lie rootsystem consisting of Witt roots;*

2. *c is classical if and only if $c \in S$ for some classical complement S of R^0.*

Proof. For (1), take a classical complement S of R^0 and write $c = a + b$ with $a \in R^0$, $b \in S$. Then $\hat{c} = \hat{a} + \hat{b} = \hat{0} + \hat{b} = \hat{b}$. Thus, it suffices to show that $\hat{b} \neq \hat{0}$ for every $b \in S - \{0\}$. But this is a consequence of the fact that $b \mapsto \hat{b}$ maps S isomorphically onto $\hat{R}$. The remaining assertion is now evident, $a, b \in R^0$ with $a + b \in R \Rightarrow \widehat{a+b} = \hat{a} + \hat{b} = \hat{0} \Rightarrow a + b \in R^0$.

For (2), let c be classical. Then $\hat{c} \neq \hat{0}$ by (1). It follows that $\hat{R}$ has a base $\hat{a}_1, ..., \hat{a}_r$ which includes $\hat{c}$, so that R has a classical complement S containing c. ▌

Finally, we need the following theorem on collapse. In the theorem, H_∞ is the k-span of $\{a^0 \mid a \in R - \{0\}\}$ and $a_\infty : H_\infty \to k$ is defined by $a_\infty(f) = f(a)$ $(f \in H_\infty)$. Note that $a_\infty = b_\infty$ if and only if $c^0(a) = c^0(b)$ for all $c \in R - \{0\}$.

1.7. THEOREM. *Let $a_{1\infty} = ... = a_{n\infty}$. Then $Ra_1 \cdots a_n$ is of type S_m for some m.*

2. The Rootsystem of a Simple Symmetric Lie Algebra

Let $L = \sum_{a \in R} L_a$ be a symmetric Lie algebra. We show in this section that if L is simple, then L is classical, R is Witt, or R has a 2-section Rab of type T_2. This is done using the results of Winter [3] collected in Section 1.

2.1. Theorem. *Suppose that R is a simple nonclassical having no 2-section of type T_2. Then R is an irreducible Witt rootsystem.*

Proof. Let S be a classical complement of R_w, so that $R \subset R^w + S$ by Theorem 1.5. If $R^w = \{0\}$, then R is classical and L is a classical Lie algebra by Theorem 1.3. Thus, $R^w \neq \{0\}$. Observe that the subalgebra $I = \sum_{b \in R^c - \{0\}} (L_b + [L_b, L_c])$ generated by $\{L_b \mid b \in R^c - \{0\}\}$ is an ideal. For this, we must use the result $R^c - \{0\} = \{b \in R \mid \hat{b} \neq \hat{0}\}$ of Corollary 1.6. That I is, indeed, the subalgebra generated by $\{L_b \mid \hat{b} \neq \hat{0}\}$ is then easily verified. Next, consider any L_a with $a \in R - (R^c - \{0\}) = R^w$, so that $\hat{a} = \hat{0}$. If $[L_a, L_b] \neq \{0\}$ then $a + b \in R$ and $\hat{a} + \hat{b} = \hat{0} + \hat{b} = \hat{b} \neq \hat{0}$ implies that $a + b \in R^c - \{0\}$ and $[L_a, L_b] \subset I$. Similarly, $[L_a, [L_b, L_c]] = [[L_a, L_b], L_c] + [L_b, [L_a, L_c]]$ with $\hat{b}, \hat{c} \neq 0$ implies that $[L_a, [L_b, L_c]] \subset I$. Thus, I is an ideal of L. If $I = \{0\}$, then $R^c = \{0\}$ and $R = R^w$, and we are done. Suppose that $I \neq 0$. Then $L = I$, by simplicity of L. We now show that it is impossible, thereby completing the proof. Since $R^w \neq \{0\}$, we may take $a \in R^w - \{0\}$. Since $L = I$, we have

$$L_a = \sum_{\substack{a = b + c \\ \hat{b} \neq \hat{0}}} [L_b, L_c].$$

Consequently

$$[L_{-a}, L_a] = \sum_{\substack{a = b + c = d + e \\ \hat{b} \neq \hat{0} \neq \hat{d}}} [[L_{-b}, L_{-c}], [L_d, L_e]]$$

$$= \sum_{\hat{b} \neq \hat{0} \neq \hat{d}} [[L_{-b}, L_{-a+b}], [L_d, L_{a-d}]].$$

Since $[[L_{-b}, L_{-a+b}], [L_d, L_{a-d}]] \subset [L_{a-b}, L_{-a+b}] + [L_{-b}, L_b]$, by a straightforward calculation, we conclude that $[L_{-a}, L_a] \subset \sum_{\hat{b} \neq \hat{0}} \{L_{a-b}, L_{-a+b}] + \sum_{\hat{b} \neq \hat{0}} \{L_{-b}, L_b]$. Take $h_a \in [L'_{-a}, L'_a] - \{0\}$ such that $a(h_a) \neq 0$. For $b, a - b \in R$ with $\hat{b} \neq \hat{0}$, $\dim L_b = \dim L_{a-b} = 1$ since $b, a - b \in R^c$, by Theorem 1.1. Thus, $[L_{-b}, L_b] = kh_b$, $[L_{a-b}, L_{-a+b}] = kh_{a-b}$ for $b \in R$, $\hat{b} \neq \hat{0}$. Writing $h_a = \sum_{\hat{b} \neq \hat{0}} c_b h_b$, we must have $a(h_b) \neq 0$ for some $\hat{b} \neq \hat{0}$, since $a(h_a) \neq 0$. For such b, we have $b^0(a) = a(h_b) \neq 0$ and $b \in R^c - \{0\}$. Since $a \in R_w$, it follows from Theorem 1.4 that Rab is of type T_2. But that is impossible, by hypothesis. ▮

Witt rootsystems are studied in detail in the next section.

3. Witt Rootsystems

We now assume that R is a Witt rootsystem. We know from Theorem 1.4. that the Witt rootsystems of prime ranks 1 and 2 are $W_1 = W$, $W \vee W$, W_2, S_2. We show in Theorem 3.7 that the irreducible Witt rootsystems of prime rank 3 are W_3, $W \oplus (W \vee W)$, $W \oplus S_2$, S_3, $S_3 \oplus (W \vee W)$, $S_3(S_2)$ where the Witt rootsystems of the form $S_3(R)$ are introduced below. This is then used to show, in Theorem 3.15, that the irreducible Witt rootsystems having no section S_2 or $W \oplus (W \vee W)$ are the finite subgroup of vectorspaces.

We begin by constructing and studying an infinite family U_n $(n \geqslant 3)$ of irreducible Witt rootsystems.

3.1. Definition. $U_{n+1} = \{(i_1, \cdots, i_n, i_{n+1}) \in \mathbb{Z}_p^{n+1} \mid i_1 + \cdots + i_n \neq 0$ or $i_{n+1} \neq 0\}$ for $n \geqslant 2$.

Let $a_1, \ldots, a_{n+1}$ denote the standard basis for $\mathbb{Z}_p^{n+1}$, let $R = U_{n+1}$, and let $c = a_{n+1}$. Observe that $Ra_1 \cdots a_n = R \cap (\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n)$ is a Witt rootsystem of type S_n.

To establish that U_{n+1} is a Witt rootsystem and determine its symmetries, we introduce $d^0(e)$ for $d = i_1 a_1 + \cdots + i_{n+1} a_{n+1}$, $e = j_1 a_1 + \cdots + j_{n+1} a_{n+1} \in U_{n+1}$ as follows:

$$d_0(e) = 2\,\frac{j_1 + \cdots + j_n}{i_1 + \cdots + i_n} \qquad \text{if} \quad i_1 + \cdots + i_n \neq 0;$$

$$d_0(e) = 2\,\frac{j_{n+1}}{i_{n+1}} \qquad \text{if} \quad i_1 + \cdots + i_n = 0 \text{ and } i_{n+1} \neq 0.$$

Remarkably, U_{n+1} is a Witt rootsystem with symmetries $r_d(e) = e - d_0(e)\, d$, the $d^0(e)$ being defined by the above conditions. Since $Ra = \mathbb{Z}a$ for all $a \in R$, verification that $R = U_{n+1}$ is a Witt rootsystem amounts to showing that $d_0(d) = 2$ (obvious); and that every bounded d-orbit $R_e(d)$ has 1 (clearly impossible) or $p-1$ elements and is stabilized by r_d. For this, consider any bounded d-orbit $R_e(d) = \{e - rd, \ldots, e + qd\}$ and the nonroots $e + (q+1)\, d$, $e - (r+1)\, d$. Since the latter are not contained in U_{n+1}, we must have $(q+1) i_{n+1} + j_{n+1} = 0$ and $(q+1)(i_1 + \cdots + i_n) + j_1 + \cdots + j_n = 0$. Thus, $q + 1 = -j_{n+1}/i_{n+1}$, if $i_{n+1} \neq 0$, and $q+1 = -(j_1 + \cdots + j_n))/(i_1 + \cdots + i_n)$ if $i_1 + \cdots i_n \neq 0$. Similarly, we have, $-(r+1) = -j_{n+1}/i_{n+1}$, if $i_{n+1} \neq 0$, and $-(r+1) = -(j_1 + \cdots + j_n)/(i_1 + \cdots + i_n)$ if $i_1 + \cdots + i_n \neq 0$. In particular, we have $-(r+1) = q+1$ and $q = p - 2 - r = -2 - 4$, which implies that any bounded d-orbit $R_e(d)$ has $p-1$ elements, that is, $R_e(d) = \{e - rd, \ldots, (e - rd + (p-2)d\}$. To show that $R_e(d)$ is stable under r_d, we observe, first, that $e + \mathbb{Z}d$ is r_d-stable, since $r_d(e + id) = e - d^0(e)\, d - id$ with $d^0(e) \in \mathbb{Z}_p$. Thus, it suffices to show that r_d

stabilizes the singleton set $(e+\mathbb{Z}d)-R_e(d)=\{e+(q+1)\,d\}$. Equivalently, it suffices to show that $0=d^0(e+(q+1)d)=d^0(e)-2(q+1)$ or $d^0(e)=2(q+1)$. But this follows from our earlier calculation of $q+1$:

$$q+1=-\frac{j_{n+1}}{i_{n+1}} \qquad \text{if } k\neq 0 \text{ and } i_1+\cdots+i_n=0;$$

$$q+1=-\frac{j_1+\cdots+j_n}{i_1+\cdots+i_n} \qquad \text{if } i_1+\cdots+i_n\neq 0.$$

This completes the proof of the following proposition, the assertions of irreducibility and rank being clear.

3.2. PROPOSITION. *U_n $(n\geqslant 3)$ is an irreducible Witt rootsystem of prime rank n.*

The Witt rootsystem U_n can also be expressed as $U_n=S_n(R)$ for $R=\{(i_1,..., i_n)\in\mathbb{Z}_p^n \mid i_1+\cdots+i_n=0 \text{ and } i_n\neq 0\}$, a Witt rootsystem of type S_{n-1}. Here, $S_n(R)$ is the Lie rootsystem $S_n+R=S_n\cup R$ defined in Section 1, where $S_n=\{(i_1,..,i_n)\in\mathbb{Z}_p^n \mid i_1+\cdots+i_n\neq 0\}\cup\{0\}$ and R is any Lie rootsystem in the vector space $\mathbb{Z}_p^n-S_n$. We therefore have $U_n=S_{n,n-1}$ in the sense of the following definition.

3.3. DEFINITION. Let $n=(n_1,..., n_r)$ where the n_i are integers $n_1>\cdots>n_r$ $(r>1)$. Then $S_{\mathbf{n}}=S_{n_1,...,n_r}$ is the Lie rootsystem defined by the recursive construction $S_{n_1,...,n_r}=S_{n_1}(R)$ where R is a Lie rootsystem of type $S_{n_2,...,n_r}$ in the vector space $\mathbb{Z}_p^{n_1}-S_{n_1}$.

Note that there is a canonical choice for R in the above definition, generated by the choice $S_{n,m}=S_n\cup R$ where $R=\{(i_1,...,i_n)\in\mathbb{Z}_p^n \mid i_1+\cdots+i_n=0, i_{m+1}\neq 0, i_{m+2}=\cdots=i_n=0\}$ in the case $r=2$. It can be shown that $S_n(R)$ and $S_n(R')$ are isomorphic if and only if R and R' are isomorphic, so that $S_{n^1,...,n_r}$ is well defined even when not specified as the canonical choice.

We introduce explicitly two more Witt rootsystems $S_3(W)$, $S_3(W\vee W)$ needed for the rank 3 classification.

3.4. DEFINITION. $S_3(W)$ and $S_3(\mathrm{W}\vee\mathrm{W})$ are defined as $S_3(R)$ where $R=\mathbb{Z}(1,-1,0)$ and $R=\mathbb{Z}(1,-1,0)\vee\mathbb{Z}(0,1,-1)$, respectively.

It is a simple exercise to prove that $S_3(W)$ is isomorphic to $W\oplus S_2$, which explains the omission of $S_3(W)$ from the list given in Theorem 3.7.

For the sequel, we need the following definition and proposition, which naturally extend the concept of connectivity for Dynkin diagrams of complex semisimple Lie algebras. The proof is straightforward.

3.5. DEFINITION. We let $a \sim b$ (read *a adjoins b*) be the statement that $a+b \in R$ or $a-b \in R$ for $a, b \in R-\{0\}$.

3.6. PROPOSITION. *The equivalence classes of the equivalence relation on* $R-\{0\}$ *generated by* $\sim$ *are the irreducible components of* R *with* 0 *removed.*

We say that a and b are *connected* if a and b are nonzero elements of the same irreducible component of R, that is, if $a \sim b_1 \sim \cdots b_n \sim b$ for suitable $b_i \in R-\{0\}$.

We now proceed to classify the Witt rootsystems of prime rank at most three, in the following theorem. This leads to the classification in Section 3 of all rank three subsystems $Rabc$ of a Lie rootsystem R excluding T_2, which in turn leads to strong structural results for Lie rootsystems excluding T_2. The classification is, of necessity, combinatorial, the strategy being to search systematically among statements describing rank 2 features of R; and then to abandon those statements defining sets which are not Witt rootsystems.

3.7. THEOREM. *Let* R *be an irreducible Witt rootsystem of prime rank* 3. *Then* R *is isomorphic to exactly one of* W_3, $W \oplus (W \vee W)$, $W \oplus S_2$, S_3, $S_3 \oplus (W \vee W)$, $S_3(S_2)$.

Proof. In what follows, scalars i, , k, etc., are assumed to come from $\mathbb{Z}_p$, and we write $\mathbb{Z}_a$ (set of sums 0, $\pm(a+\cdots+a)$) and $\mathbb{Z}_p a$ (set of scalar multiples of a) interchangeably, depending on context and notational expedience.

Since R is irreducible of prime rank 3, we may assume with no loss generality that $R = Rabc$ with $a \sim b \sim c$. We first consider the case where R excludes S_2, that is, where no subsystem Ruv $(u, v \in R)$ is of type S_2. We then show, as follows, that R is of type W_3 if and only if $a \sim c$; and that R is of type $W \oplus (W \vee W)$ if and only if $a \not\sim c$. Suppose first that $R = Rab \cup Rbc \cup Rac$, so that $R = \mathbb{Z}a + \mathbb{Z}b \cup \mathbb{Z}b + \mathbb{Z}c \cup Rac$ with $Rac = \mathbb{Z}a + \mathbb{Z}c$ or $\mathbb{Z}a \cup \mathbb{Z}c$, by Theorem 1.4 and the exclusion of S_2. If $a \not\sim c$, it then follows that, $R = \mathbb{Z}a + \mathbb{Z}b \cup \mathbb{Z}b + \mathbb{Z}c = \mathbb{Z}b \oplus (\mathbb{Z}a \cup \mathbb{Z}c) = W \oplus (W \vee W)$ and $Rabc = Rb \oplus (Ra \vee Rc)$. Conversely, $Rabc = Rb \oplus (Ra \vee Rc)$ clearly implies $a \not\sim c$. Next, suppose that $a \sim c$, so that $Rac = \mathbb{Z}a + \mathbb{Z}c$. Then $R_{ib+jc}(a+b) = \{ib+jc\}$ and $0 = (a+b)^0(ib+jc) = i(a+b)^0(b) + j(a+b)^0(c)$ for all $i \neq \pm 1, j \neq 0$, so that $(a+b)^0(b) = 0$. Similarly, $(a+b)^0(a) = 0$, so that $2 = (a+b)^0(a+b) = (a+b)^0(a) + (a+b)^0(b) = 0$, a contradiction. We conclude that $R \supsetneqq Rab \cup Rbc \cup Rac$, that is, R contains some $d = ra + sb + tc$ where $r, s, t \neq 0$. Since R contains $ra + sb \in Rab = \mathbb{Z}a + \mathbb{Z}b$ and $sb + tc \in Rbc = \mathbb{Z}b + \mathbb{Z}c$, by the assumed exclusion of S_2, R contains $Rd \oplus (ra+sb) = \mathbb{Z}(ra+sb) + \mathbb{Z}c$ and $Rd \oplus (sb+tc) = \mathbb{Z}a + \mathbb{Z}(sb+tc)$, by the exclusion of S_2. Since R contains

$\mathbb{Z}a + qab + qtc$ and $\mathbb{Z}a + qsb$ for all $qsb \in \mathbb{Z}b$, it follows that R contains $\mathbb{Z}a + qsb + \mathbb{Z}c$, by the exclusion of S_2, for all $qsb \in \mathbb{Z}b - \{0\}$. Thus, R contains $(\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}c) - (\mathbb{Z}a + \mathbb{Z}c)$. To show that $R = W_3$, it suffices, therefore, to show that R contains $\mathbb{Z}a + \mathbb{Z}c$, that is, that $a \sim c$ and $Rab = \mathbb{Z}a + \mathbb{Z}c$. Suppose, to the contrary, that $a \not\sim c$ and $Rac = \mathbb{Z}a \cup \mathbb{Z}c$. Then $R_{a+b+c}(b)$ has $p-1$ elements, that is, $Rb(a+b+c) = S_2$, by Theorem 1.4, which contradicts our assumption that R excludes S_2. We conclude that $Rab = \mathbb{Z}a + \mathbb{Z}c$ and $R = W_3$. From the discussion, it is also clear that $a \not\sim c$ if and only if $Rabc = Rb \oplus (Ra \vee Rb)$, for Witt rootsystems R excluding S_2 and $a \sim b \sim c$.

Next, we consider the case where some subsystem Ruv is of type S_2, in which case we may assume with no loss of generality that Rab is $\{ia + jb \mid i + j \neq 0\} \cup \{0\}$, of type S_2. Suppose that $R = Rab \cup Rbc \cup Rac$. Then we have $R_{b \pm 2c}(a) = \{b \pm 2c\}$ and $0 = a^0(b \pm 2c) = a^0(b) + 2a^0(c) = 2 \pm 2a^0(c)$, which implies that $a^0(c) = -1$ and $a^0(c) = 1$, a contradiction. Thus, $R \supsetneqq Rab \cup Rbc \cup Rac$, so that R contains some $d = ra + sb + tc$ with $r, s, t \neq 0$.

We now proceed to show that $a \sim c$ for any Witt rootsystem $R = Rabc$ where $a \sim b \sim c$ with Rab of type S_2. This *transitivity* plays an important role in the proof, both now and later. As observed in the preceding paragraph, we may take $a^0(b) = 2$, $Rab = \{ia + jb \mid i + j \neq 0\} \cup \{0\}$. Moreover, there exists $d = ra + sb + tc \in R$ with $r, s, t \neq 0$. Suppose first that $a \not\sim c$. And then suppose next that some such d adjoins b, that is, $b \sim d$. We then proceed, in the next few paragraphs, to explicitly determine the set R and show that it is not a Witt rootsystem, a contradiction. We then can assume that no such d adjoins b.

Since $b \sim d$, Rbd is of type S_2. It follows that $Rbd = \{ra + jb + tc \mid j \neq 0\}$, since $ra + tc \in (\mathbb{Z}b + \mathbb{Z}d) - R$. In particular, Rbd contains $ra - rb + tc$. Moreover, we have $ra + jb \in R$ and $(ra + jb) \sim c$ for all $j \neq 0$, $r + j \neq 0$. It follows that, for $j \neq 0$, $r + j \neq 0$, $R(ra + jb)c$ is of type S_2 or W_2 and R contains $ra + jb + kc$, at least for all values of k for which the element c of $R(ra + jb)c$ is not *orthogonal* to $ra + jb + kc$, that is, for which $0 \neq c^0(ra + jb + kc) = 0 + jc^0(b) + 2k$ or $k \neq -jc^0(b)/2$.

We first consider the case $c^0(b) = 0$, in which case it follows that $ra + jb + kc \in R$ for all $j \neq 0$, $r + j \neq 0$, k $(r, j, k \in \mathbb{Z}_p)$. Then $R \supset S = (Rab - \mathbb{Z}a) \oplus \mathbb{Z}c \cup Rab \cup R(ra - rb + tc)c$. Since $c^0(ra - rb + tc)$ then equals $0 + 0 + 2t \neq 0$, we see that $R(ra - rb + tc)c$ is of type S_2 and equals $\{j(a - b) + kc \mid j, k \in \mathbb{Z}_p, k \neq 0\}$. Since $a \not\sim c$ and $Rac = \mathbb{Z}a \cup \mathbb{Z}c$, it follows that any element $ia + jb + kc$ of R must be in $Rab \cup Rbc \cup \{j(a - b) + kc \mid k \neq 0, \; j \in \mathbb{Z}_p\} \cup \{ia + jb + kc \mid j \neq 0, \; i + j \neq 0, k \in \mathbb{Z}_p\} \subset S$. Thus, we have $R = S = \{ia + jb + kc \mid (k = 0$ and $i + j \neq 0)$ or $(k \neq 0$ and $i + j = 0)$ or $(j \neq 0$ and $i + j \neq 0)\} \cup \{0\} = ((\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}c) - (\mathbb{Z}(a - b) \cup \{ia + kc \mid ik \neq 0\})) \cup \{0\}$ where the i, j, k come from $\mathbb{Z}_p$. But this set S is not a Witt rootsystem, because it has an orbit $S_d(e)$ of cardinality $|S_d(e)| \neq 1, p-1, p$:

1. S contains $d = -2b - c$ and $e = a + b + c$;
2. $S_d(e)$ contains d and $d - e = -a - 3b - 2c$;
3. $S_d(e)$ does not contain $d + e = a - b$, $d + 2e = 2a + c$.

Thus, the assumption $c^0(b) = 0$ leads to a contradiction.

Accordingly, we now may assume that $c^0(b) \neq 0$. Replacing a and b by a suitable scalar multiple (the same for both), we may assume that $c^0(b) = 2$. Thus, by the foregoing, R contains $ra + jb + kc$ for all $j \neq 0$, $r + j \neq 0$ and $k \neq -jc^0(b)/2 = -j$. Since R contains all scalar multiples of its elements, R contains $ia + jb + kc$ for all i, j, k for which $j \neq 0$, $i + j \neq 0$, $j + k \neq 0$. If $c \not\sim ra - rb + tc$, then $0 = c^0(ra - rb + tc) = 0 - rc^0(b) + tc^0(c) = 2(t - r)$ implies that $t = r$, so that $R \cap \{ia - ib + kc \mid i, k \in \mathbb{Z}_p\} = \mathbb{Z}(a - b + c)$. It follows that R does not contain $r_b(a - b + kc) = a - b + k(c - b^0(c)b) = a - (1 + kb^0(c)b + kc)$ for, $k \neq 1$. Since R contains $ia + jb + kc$ whenever $j \neq 0$, $i + j \neq 0$, $j + k \neq 0$, it follows that $b^0(c) = 0$. But then $b^0(a - b + c) = 0$ which, since $b \sim (a - b + c)$ by the assumption $b \sim d$ with $d = ra + sb + rc$, implies that $Rb(a - b + c)$ is of type W_2. But then $a + c \in R$, a contradiction. Accordingly, we must conclude that $c \sim (ra - rb + tc)$, so that R contains $\{i(a - b) + kc \mid i \in \mathbb{Z}_p, k \neq 0\}$.

We now determine the elements $ia + jb + kc = e$ of R explicitly. For $j = 0$, we have $\mathbb{Z}a \cup \mathbb{Z}c \subset R$. For $k = 0$, we have $S_{ab} = \{ia + jb \mid i + j \neq 0\} \cup \{0\} \subset R$. For $i = 0$, we have $\mathbb{Z}b + \mathbb{Z}c \subset R$, since Rbc contains $\mathbb{Z}b \cup \mathbb{Z}c \cup \{jb + kc \mid j \neq 0$ and $j + k \neq 0\}$. For $j \neq 0$, we already know that $\{i(a - b) + kc \mid i \in \mathbb{Z}_p$, $k \neq 0\} \cup \{ia + jb + kc \mid j \neq 0$, $i + j \neq 0$, $j + k \neq 0\}$. Suppose next that $j \neq 0$, $i + j \neq 0$, and $j + k \neq 0\}$. Suppose next that $j \neq 0$, $i + j \neq 0$, and $j + k = 0$, so that $e = ia + jb - jc$. Then $e \in R$ for $i = 0$ and $i = -j$. It follows that $Ra(b - c)$ is of type S_2 or W_2, so that it contains e unless $0 = a^0(e) = 2(i + j)$. Since $i + j \neq 0$, we have $e \in R$. Since R contains $ia + jb - jc$ $(j \neq 0$, $i + j \neq 0)$ and $i(a - b) + kc$ $(k \neq 0)$, R contains $\mathbb{Z}a + \mathbb{Z}(b - c)$. We conclude that $R = \{ia + jb \mid i + j \neq 0\} \cup \mathbb{Z}_b + \mathbb{Z}_c \cup \{i(a - b) + kc \mid k \neq 0$, any $i\} \cup \{ia + jb + kc \mid j \neq 0$, $i + j \neq 0$, any $k\}$. But then $R = S$ where S is the set $((\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}c) - (\mathbb{Z}(a - b) \cup \{ia + kc \mid ik \neq 0\})) \cup \{0\}$ which was shown above not to be a Witt rootsystem, a contradiction. We must conclude, therefore, that no $d = ra + sb + tc \in R$ with $r, s, t = 0$ adjoins b.

We next consider the case where $a \not\sim c$ and $b \not\sim d$ for all $d = ra + sb + tc \in R$ with $rst \neq 0$. Take some such d (shown above to exist). Then $Rbd = Rb \vee Rd$ and $0 = b^0(d) = d^0(b)$. We claim that $sb + tc \notin R$. For otherwise, $a \sim (sb + tc)$ implies that R contains some $d' = r'a + sb + tc$ with $r' = r, 0$, in which case we also have $b \not\sim d'$, by our assumption, so that $0 = b^0(d) = b^0(d')$ and $0 = b^0(d - d') = b^0((r - r')a) = (r - r')b^0(a) =$

$2(r-r')$, a contradiction. Thus, $sb+tc \notin R$. Normalizing d so that $s=1$, we have $d=ra+b+tc$ with $b+tc \notin R$. Since $b \sim c$ with $b+tc \notin R$, we must have $Rbc=S_2$. Choosing c such that $b^0(c)=2$, we then have $t=-1$ and $d=ra+b-c$. It follows that $ra+b \notin R$; for otherwise $(ra+b) \sim c$ implies that R contains some $d'=ra+b+t'c$ with $t' \neq -1$, in which case we also have $b \not\sim d'$ and $0=b^0(d'-d)=b^0((t'+1)c)=2(t'+1)$, a contradiction. But $ra+b \notin R$ with $b^0(a)=2$ implies that $r=-1$, so that $d=-a+b-c$. From this, we conclude from our supposition $a \not\sim c$ that $R=\{ia+jb \mid i+j \neq 0\} \cup \{ib+jc \mid i+j \neq 0\} \cup \mathbb{Z}(-a+b-c)$, given the normalization of c introduced above. But then $d \not\sim a$, $d \not\sim b$, and $d \not\sim c$, and in fact there is no chain $a \sim e_1 \sim \cdots \sim e_n \sim d$ $(e_i \in R-\{0\})$, which contradicts the irreducibility of R. (And, moreover, this particular $S_2 \cup S_2 \cup W_1$ with $S_2 \cap S_2 \neq \{0\}$, S_2 is not even a Lie rootsystem.) Thus, we must conclude that $a \sim c$.

By the foregoing, we now have $Rab=\{ia+jb \mid i+j \neq 0\}$, $b \sim c$, $a \sim c$, and $d=ra+sb+tc \in R$ with $r, s, t \neq 0$. We first consider the case where one of Rbc, Rac is of type W_2; and we then take Rbc to be of type W_2, with no loss of generality. After a few paragraphs, we then consider the general case. Suppose that Rac is of type S_2, and normalize c so that $a^0(c)=2$. We then have $a \sim b \sim (b-c)$ with Rab, $Rb(b-c)$ of types S_2, W_2, respectively. As in the foregoing, we may conclude that $a \sim (b-c)$. Since $a^0(b-c)=a^0(b)-a^0(c)=2-2=0$, $Ra(b-c)$ is of of type W_2, by Theorem 1.4.

Since we may replace c by $b-c$, we may assume with no loss of generality that Rac is of type W_2.

We claim that $a^0(c), b^0(c) \in \mathbb{Z}_p$, without loss of generality. Suppose to the contrary that, say, $a^0(c) \notin \mathbb{Z}_p$. Consider any $jb+kc \in Rbc=\mathbb{Z}b+\mathbb{Z}c$ with $k \neq 0$. Then $a^0(jb+kc) \notin \mathbb{Z}_p$ implies that $Ra(jb+kc)=\mathbb{Z}_a+\mathbb{Z}(jb+kc)$. It follows that $R=Rab \cup \{ia+jb+kc \mid k \neq 0,\ i, j \in \mathbb{Z}\}=\{ia+jb+kc \mid k \neq 0$ or $(k=0$ and $i+j \neq 0)\}=S_3 \cup \{ia+jb-(i-j)c \mid i+j \neq 0\}=S_3(S_2)$, which is among the Witt rootsystems listed in the theorem. Thus, we may assume that $a^0(c), b^0(c) \in \mathbb{Z}_p$.

We claim next that $a^0(c)=0$, with no loss of generality. We have seen above that we may assume $a^0(c) \in \mathbb{Z}_p$. If $a^0(c) \neq 0$, replace c by $c'=c-(a^0(c)//2)b \in \mathbb{Z}b+\mathbb{Z}c=Rbc$. Then $a^0(c')=0$, as desired, and $Rac'=W_2$ as before, $Rac'=W \vee W$ being ruled out as in the foregoing exclusion of $Rac=W \vee W$, since $b \sim c'$; and $Rac'=S_2$ being ruled out by $a^0(c')=0$. We therefore have $Rab=S_2$, $Rbc=W_2$, $Rac'=W_2$ as before, as well as $a^0(c')=0$. Thus, we may assume with no loss of generality that $a^0(c)=0$.

We now show, using $a^0(c)=0$, that $R=\{ia+jb \mid i+j \neq 0\}+\mathbb{Z}c=S_2 \oplus W$. Note first that $a \sim (jb+kc)$ for all k and all $j \neq 0$, since $a^0(jb+kc)=a^0(jb)=2j$. If $Ra(jb+kc)$ is of type W_2, then R contains

$ia+jb+kc$ for all i. Otherwise, $Ra(jb+kc)$ is of type S_2, in which case the condition that $ia+(jb+kc)$ be in this S_2 is that $0 \neq a^0(ia+jb+kc) = 2(i+j)+a^0(kc) = 2(i+j)$. It follows that R contains $ia+jb+kc$ for all $i, j, k \in \mathbb{Z}_p$ with $i+j \neq 0$, that is, $R \supset \{ia+jb \mid i+j \neq 0\} + \mathbb{Z}c = S_2 \oplus W$. If $R = S_2 \oplus W$, we are done. Otherwise, R contains $\mathbb{Z}\,d$ with $d = a-b+kc$ for some $k \neq 0$. We may therefore assume, with no loss of generality, that $a-b+c \in R$. If $c \sim d$, then Rcd is of type S_2 with $a-b \notin R$, so that R contains $i(a-b)+kc$ for all $i, k \in \mathbb{Z}_p$ with $k \neq 0$. It then follows that $R = \{ia+jb+kc \mid i+j \neq 0, \text{ any } k\} \cup \{i(a-b)+kc \mid k \neq 0, \text{ any } i\} = \{ia+jb+kc \mid (i+j+k \neq 0) \text{ or } (i+j = -k \neq 0)\} = S_3(S_2) = S_{3,2}$. If $c \not\sim d$, then Rcd is of type $W \vee W$ and $Rcd = \mathbb{Z}c \cup \mathbb{Z}(a-b+c)$. Furthermore, $R = S_2 \oplus W \cup Rcd = Rab \oplus \mathbb{Z}c \cup \mathbb{Z}(a-b+c) = S_2 \oplus W \vee W$ with $Rab = \{ia+jb \mid i+j \neq 0\} \cup \{0\}$. Counting, we see that $|R| = p^3-p^2+2p-1$. Let $x=a$, $y=a+c$, $z=b$ and note that $x-y=-c$, $y-z=d$. Then R contains $\{ix+jy+kz \mid i+j+k \neq 0\} \cup \mathbb{Z}(x-y) \cup \mathbb{Z}(y-z) = S_3(W \vee W)$, since $ix+jy+kz = (i+j)a+kb+jc \in R$ for $i+j+k \neq 0$. Since $|S_3(W \vee W)| = |S_3 \cup W \cup W| = |S_3|+|W|+|W|-2 = p^3-p^2+1+p+p-2 = p^3-p^2+2p-1$, it follows that $R = S_3(W \vee W)$.

Finally, given that $Rab = S_2$, we drop the hypothesis that one of Rbc, Rac be of type W_2. Suppose that some subsystem Ruv $(u, v \in R)$ is of type W_2, and take a chain $a = e_1 \sim b = e_2 \sim \cdots \sim e_{n-1} = u \sim e_n = v$. Since Rab is of type W_2, and since each Re_ie_{i+1} is of type S_2 or W_2, there exists $1 < i < n$ such that $Re_{i-1}e_i$ is of type S_2 and Re_ie_{i+1} is of type W_2. Thus, we may assume with no loss of generality that $n=3$, $i=2$, $e_1=a$, $e_2=b=u$, $e_3=v=c$, that is, that Rab is of type S_2 and Rbc is of type W_2. But this is the case which we considered above.

We now may assume that Ruv is of type S_2 or $W \vee W$ or W for all $u, v \in R-\{0\}$. Since $a \sim b \sim c$ with Rab and Rac of type S_2, we may assume with no loss of generality that $a^0(b)=2$ and $b^0(c)=2$. After preliminary observations, we now show that $R = \{ia+jb+kc \mid i+j+k \neq 0\}$, so that R is of type S_3.

Consider any $\mathbb{Z}_p$-independent elements $u, v \in R-\{0\}$. With our present assumptions, Ruv is of type $W \vee W$ if and only if $u^0(v)=0$; and Ruv is of type S_2 if and only if $u^0(v) \neq 0$. Moreover, it is clear that $u^0(v) \in \mathbb{Z}_p$, and that $Ruv = \{iu+jv \mid i+j \neq 0\}$ if and only if $u^0(v)=2$.

We proved the transitivity $u \sim v \sim w$ implies $u \sim w$ $(u, v, w \in R-\{0\})$, under the assumption that Ruv be of type S_2, earlier in this proof. In the present context, the condition that Ruv be of type S_2 is always satisfied when $u \sim v \sim w$. Consequently the relation $\sim$ is transitive on $R-\{0\}$. We now use this transitivity to prove that $R = \{ia+jb+kc \mid i+j+k \neq 0\} = S_3$. For this suffices, by Theorem 1.7, to show that, $d^0(a) = d^0(b) = d^0(c)$ for all $d \in R-\{0\}$. By symmetry, we need only show that $d^0(a) = d^0(b)$ for all $d \in R-\{0\}$. Suppose, to the contrary, that $d^0(a-b) \neq 0$ for some

$d \in R - \{0\}$. If $d^0(a) = 0$, it follows that $d^0(b) \neq 0$ and $a \sim b \sim d$. But then $a \sim d$, by transitivity, so that $d^0(a) \neq 0$, a contradiction. Similarly, if $d^0(b) = 0$, then $d^0(a) \neq 0$ and $b \sim a \sim d$. Thus, $b \sim d$, by transitivity, so that $d^0(b) \neq 0$, a contradiction. We conclude that $d^0(a) \neq 0$, $d^0(b) \neq 0$. Consequently, $d^0(ia - b) = 0$ for some $i \in \mathbb{Z}_p$. Since $d^0(a - b) \neq 0$, we have $i \neq 1$ and $ia - b \in R - \{0\}$. But then $a^0(ia - b) = 2(i - 1) \neq 0$ and $d \sim a \sim (ia - b)$. By transitivity, we then have $d \sim (ia - b)$, so that $d^0(ia - b) \neq 0$, a contradiction. We conclude that $d^0(a - b) = 0$ and $d^0(a) = d^0(b)$ for all $d \in R - \{0\}$. By symmetry, we also have $d^0(b) = d^0(c)$ for all $d \in R - \{0\}$. By symmetry, we also have $d^0(b) = d^0(c)$ for all $d \in R - \{0\}$. Thus, $R = \{ia + jb + kc \mid i + j + k \neq 0\}$, by Theorem 1.7.

It remains only to verify that no two distinct Witt rootsystems from among W_3, $W \oplus (W \vee W)$, $S_3(S_2)$ are isomorphic. But this is clear by inspection of cardinalities:

$$|W_3| = p^3$$
$$|W \oplus (W \vee W)| = 2p^2 - p$$
$$|W \oplus S_2| = p^3 - p^2 + 2$$
$$|S_3| = p^3 - p^2 + 1$$
$$|S_3(W \vee W)| = p^3 - p^2 + 2p - 1$$
$$|S_3(S_2)| = p^3 - p + 1.$$

It is clear from the proof of Theorem 3.7 that $a \sim b \sim c$ with Rab of type S_2 implies $a \sim c$ for any nonzero elements a, b, c of Witt rootsystem R. We next suppose that $a \sim b \sim c$ and $a \not\sim c$ where a, b, c are nonzero elements of a Witt rootsystem R. It follows from inspection of the possibilities for $Rabc$ given in Theorem 3.7 that either $Rabc$ is of type $W \oplus (W \vee W)$, in which case $Rabc = Rb \oplus (Ra \vee Rc)$, or $Rabc$ is of type $S_3(W \vee W) = \{ix + jy + kz \mid (i + j + k \neq 0) \text{ or } (i + j + k = 0 \text{ and } ik = 0)\}$. In the latter case, let $a = ix + jy + kz$, $c = rx + sy + tz$. Since $a \not\sim c$, it follows that $a \pm c \notin R$. Consequently, we have $(i + j + k) + (r + s + t) = (i + j + k) - (r + s + t) = 0$. But then $i + j + k = r + s + t = 0$, so that a and c are in the subspace $\{ix + jy + kz \mid i + j + k = 0\}$. It follows easily that $x, y, z \in S_3(W \vee W)$ can be chosen such that $a = x - y$ and $c = y - z$. This establishes the following transitivity theorem for Witt rootsystems.

3.8. THEOREM. *Let R be a Witt rootsystem and let $a \sim b \sim c$ with $a \not\sim c$. Then Rab and Rbc are both of type W_2. Moereover, $Rabc$ is either $Rb \oplus (Ra \vee Rc)$ of type $W \oplus (W \vee W)$ or $S_3(Ra \vee Rc)$ of type $S_3(W \vee W)$ where $S_3(R_a \cup R_c) = \{ix + jy + kz \mid (i + j + k \neq 0)$ or $(i + j + k = 0$ and $ik = 0)\}$ with $a = x - y$, $b = y - z$.*

3.9. DEFINITION. A Witt rootsystem R is *transitive* if R excludes $W \oplus (W \vee W)$ and $S_3(W \vee W)$.

Theorem 3.8 shows that a Witt rootsystem R is transitive if and only if $\sim$ is a transitive relation on $R - \{0\}$. Clearly $W \oplus R$ is transitive if and only if R is transitive. Therefore, the determination of all transitive Witt rootsystems reduces to the determination of those which are *compact* in the following sense.

3.10 DEFINITION. A Lie rootsystem is *compact* if it is not of the form $W \oplus R$ where R is a Lie rootsystem.

3.11. PROPOSITION. *A Witt rootsystem R is compact if and only if there exists no $x \in R$ such that Rxy is type W_2 for all $x \in R - Rx$.*

Proof. Suppose that there exists $x \in R$ such that Rxy is of type W_2 for all $y \in R - \mathbb{Z}_p x$, and take $\mathbb{Z}_p$-independent elements $x_1, \ldots, x_r$ with r maximal such that $x \notin Rx_1 \cdots x_r$. Then $y \in Rx_1 \cdots x_r$ implies $\mathbb{Z}x + \mathbb{Z}y \subset R$, so that $R \supset \mathbb{Z}x \oplus Rx_1 \cdots x_r$. We claim equality. Thus, let $y \in R - Rx_1 \cdots x_r$. Then $x \in Ryx_1 \cdots x_r$, so that $x = cy + \sum_1^r c_i x_i$. But then $\sum_1^r c_i x_i \in \mathbb{Z}x + \mathbb{Z}y \subset R$ and $y = (1//c)(x - \sum_1^r c_i x_i) \in \mathbb{Z}x + \mathbb{Z} \sum_{i=1}^r c_i x_i \subset R$. Thus, $R = \mathbb{Z}x \oplus Rx_1 \cdots x_r$ and R is not compact. The other direction is trivial.

3.12. PROPOSITION. *$R = S_n = (R')$ is transitive and irreducible for any $n \geqslant 3$ and any transitive irreducible Witt rootsystem R' of prime rank less than n.*

Proof. We have $R = \{(a_1, \ldots, a_n) \in \mathbb{Z}_p^n \mid \sum_{i=1}^n a_i \neq 0$ or $\sum_{i=1}^n a_i = 0$ and $(a_1, \ldots, a_n) \in R'\}$ where R' is a transitive irreducible Witt rootsystem in the vector space $\mathbb{Z}_p^n - \{(a_1, \ldots, a_n) \mid \sum_{i=1}^n a_i \neq 0\}$. Let $x = \sum_{i=1}^n x_i a_i$, $y = \sum_{i=1}^n y_i a_i \in R - \{0\}$ and suppose that $x \not\sim y$. Then $x + y,\ x - y \notin R$, so that $\sum_{i=1}^n x_i + \sum_{i=1}^n y_i = \sum_{i=1}^n x_i - \sum_{i=1}^n y_i = 0$. It follows that $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i = 0$, so that $x, y \in R'$. But then $x \sim y$ since R' is transitive and irreducible, a contradiction. We must conclude that $x \sim y$ for any two $x, y \in R - \{0\}$, so that R is transitive and irreducible as asserted.

3.13. *Conjecture.* The transitive irreducible Witt rootsystems are those of the form W_m, S_n, or $W_m \oplus S_n(R')$ for $m \geqslant 1$, $n \geqslant 2$, and R' a transitive irreducible Witt rootsystem of prime rank less than n.

The above propositions reduce the above conjecture to the following conjecture.

3.14. *Conjecture.* A transitive irreducible Witt rootsystem R having no element $x \in R - \{0\}$ such that Rxy is of type W_2 for all $x \in R - Rx$ has the form $R = S_b(R')$ for some $n \geqslant 2$ and some transitive irreducible Witt rootsystem R' of prime rank less than n.

The following theorem determines the transitive Witt rootsystems which exclude S_2.

3.15. THEOREM. *The irreducible components of a Witt rootsystem R are groups if and only if R excludes* S_2 *and* $W \oplus (W \vee W)$.

Proof. We assume with no loss of generality that R is irreducible. One direction is clear. For the other, assume that R excludes S_2 and $W \oplus (W \vee W)$. Then $\sim$ is a transitive relation on $R - \{0\}$, by Theorem 3.8. By the irreducibility of R, we have $a \sim b$ and Rab is of type S_2 or W_2 for all $\mathbb{Z}_p$-independent $a, b \in R$. Since R excludes S_2, we conclude that $a, b \in R \Rightarrow \mathbb{Z}a + \mathbb{Z}b \subset R$, so that R is a group. ▌

ACKNOWLEDGMENT

The author takes this opportunity to thank the University of Chicago for its hospitality during his visit there, where this paper was written.

REFERENCES

1. G. SELIGMAN, Modular Lie algebras, *Ergeb. Math. Grenzgeb.* **40** (1967).
2. D. J. WINTER, Generalized classical Albert–Zassenhaus Lie algebras, *J. Algebra* **97** (1985), 181–200.
3. D. J. WINTER, Symmetric Lie algebras, *J. Algebra* **97** (1985), 130–165.