Chapter 4

Symmetries and Lie algebras

4.1 Introduction

Symmetry is a characteristic of geometrical shapes, equations and other objects; we say that such an object is symmetric with respect to a given operation if this operation, when applied to the object, does not appear to change it. The three main symmetrical operations are reflection, rotation and translation. A reflection "flips" an object over a line, inverting it as if in a mirror. A rotation rotates an object using a point as its center. A translation "slides" an object from one area to another by a vector. Even more complex operations on a geometric object, like shrinking or shape warping, can be reduced to the operation of translation of every point within the object. Symmetry occurs in geometry, mathematics, physics, biology, art, literature (palindromes), etc[1].

Although two objects with great similarity appear the same, they must logically be different. For example, if one rotates an equilateral triangle around its center 120 degrees, it will appear the same as it was before the rotation to an observer. In theoretical Euclidean geometry, such a rotation would be un recognizable from its previous form. In reality however, each corner of any equilateral triangle composed of matter must be composed of separate molecules in separate locations. Symmetry therefore, is a matter of similarity instead of sameness. The difficulty for an intelligence to differentiate such a seemingly exact similarity might for a responsible for the mild altered state of consciousness one gets by observing intricate patterns based on symmetry.

4.1.1. Symmetry in Geometry

The object with the most symmetry is empty space because any part of it can be rotate, reflected or translated without apparent change.

The most familiar and conventionally taught type of symmetry is the left-right or mirror image symmetry exhibited for instance by the letter T: when this letter is reflected along a vertical axis, it appears the same. An equilateral triangle exhibits such a reflection symmetry along three axes, and in addition it shows rotational symmetry: if rotated by 120 or 240 degrees, it remains unchanged. An instance of a shape which exhibits only rotational but no reflectional symmetry is the swastika. The German geometer Felix Klein enunciated a very influential Erlangen programme in 1872, suggesting symmetry as unifying and organizing principle in geometry (at a time when that was read 'geometries'). This is a broad rather than

[1] " file:localhost/Noether's 20%/Symmetric group/Wikipedia/20%/free/com" Wikipedia paper.

deep principle. Initially it led to interest in the group attached to geometries, and the slogan transformation geometry (an aspect of the New Math, but hardly controversial in modern mathematical practice). By now it has been applied in numerous forms, as kind of standard attack on problems.

A fractal, coined by Mandelbrot is symmetry involving scale. For example an equilateral triangle can be shrunk so that each of its sides is one third the length of the original's sides. These smaller triangles can be rotated and translated until they are adjacent and in the center of each of the larger triangle's lines. The smaller triangles can repeat the process, resulting in even smaller triangle's on their sides. Fascinating intricate structures can be created by repeating such scaling symmetrical operations many times.

4.1.2. Symmetry in Mathematics

An example of a mathematical expression exhibiting symmetry is $a2c + 3ab + b2c$. If a and b are exchanged, the expression remains unchanged due to the commutatively of addition and multiplication.

In mathematics, one studies the symmetry of a given object by collecting all the operations that leave the object unchanged. These operations form a group. For a geometrical object, this is known as its symmetry group; for an algebraic object one uses the term auto Orphism group. The whole subject of galios Theory deals with well-hidden symmetries of fields.

4.1.3. Generalization of Symmetry

If we have a given set of objects with some structure, then it is possible for symmetry to merely convert only one object into another instead of acting upon all possible objects simultaneously. This requires a generalization from the concept of symmetry groups to that of a groupoid.

4.1.4. Symmetry in Physics

The generalization of symmetry in physics to mean invariance under any kind of transformation has become one of the most powerful tools of theoretical physics. See Noether's theorem for more details. This has led to group theory being one of the areas of mathematics most studied by physicists.

4.1.5. Symmetry in the arts and crafts

You can find the use of symmetry across a wide variety of arts and crafts. Symmetry has long been a predominant design element in architecture; prominent examples include the Leaning

Tower of Pisa, Monticello, the Astrodome, the Sydney Opera House, Gothic church windows, and the Pantheon. Symmetry is used in the design of all overll floor plan of buildings as well as the design of individual building elements such as doors, windows, floors, frieze work, and ornamentation; many facades adhere to bilateral symmetry.

4.1.6. Symmetry Group

The symmetry group of an object **(image, signal,etc)** is the group of all isometries under which it's invariant with composition as the operation. It's a subgroup of the isometry group of the space concerned. If not stated otherwise; this article considers symmetry groups in Euclidean geometry.

The symmetry group is sometimes also called full symmetry group in order to emphasize that it includes the orientation-reversing isometries like reflections, glide reflections and improper rotations under which the figure is invariant.

The subgroup of orientation-preserving isometries (i.e. transformations, rotations, and composition of these) which leave the figure invariant is called its proper symmetry group. The proper symmetry group of an object is equal to it's full symmetry group if and only if the object is chiral (and thus there are no orientation-reversing isometries under which it's invariant). Any symmetry group whose elements have a common fixed point, which is true for all finite symmetry groups and also for the symmetry groups of bounded figures, can be represented as a subgroup of orthogonal $O(0)$ by choosing the origin to be a fixed point. The proper symmetry group is a subgroup of the special orthogonal group $SO(n)$ then, and therefore also called rotation group of the figure.

4.1.7. Discrete symmetry groups

Finite point groups, which include only rotations, reflections, inversion and roto inversion- they are in fact just the finite subgroups of $O(0)$.

Infinite lattice groups which include only translations, and infinite space groups which combines elements of both previous types, and may be also include extra transformations like screw axis and glide reflection . There are also continuous symmetry groups, which contains of arbitrary small angles or translations of arbitrary small distance.

The group of all symmetries of a sphere $O(3)$ is an example of this, and in general such continuous symmetry groups are studied a Lie groups. With a categorization of subgroups of the Euclidean group corresponds a categorization of symmetry groups.

Two geometry figures are considered to be of the same symmetry type if their symmetry groups are conjugate subgroups of the Euclidean group $E(n)$ (the isometry group of R^2). Where two subgroups H_1, H_2 of a group G are conjugate, if there exists $g \in G$ such that

$H_1 = g^{-1} H_2\, g$

Examples 4.1.1.

i. Two $3D$ figure have mirror symmetry, but with respect to different mirror planes.

ii. Two $3D$ figures have 3-fold rotational symmetry, but with respect to different axes.

iii. Two $2D$ patterns have translational symmetry,each in one direction; the two translation vectors have the same length but a different direction.

4.2 Symmetric Group

In Mathematics, the symmetric group on a set is the group consisting of all bijections of the set (all one-to-one and on to functions from the set to itself) with function composition as the group operation.

Definition 4.2.1.

The symmetric group on a set X is the group whose underlying set is the collection of all bijections from X to X and whose group operation is that of function composition. The symmetric group of degree n is the symmetric group on the set $[X = 1,2, \dots \dots, n]$.

The symmetric group on a set X is dented in various ways including S_X , G_X , Σ_X and $sym(x)$. If X is the set $[1,2, \dots \dots, n]$ when the symmetry group on X is also dented S_n , G_n , Σ_n and $sym(n)$.

i. Elements

The elements of symmetric group on a set X are the permutations of X.

ii. Multiplication:

The group operation in a symmetric group is function composition,deonted by juxtaposition of the permutations. The composition $f \circ g$ of permutations f and g, pronounced f after g, maps any element x of X to $F(g(x))$. Concretely, let

$$f = (1 \quad 3)(4 \quad 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

And

$$g = (1 \quad 2 \quad 5)(3 \quad 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

Applying f and g maps 1 first to 2 and then 2 to it self. 2 to 5 and then to 4,3 to 4 and then to 5, and so on. So composing f and g gives

$$fg = f \circ g = (1 \quad 2 \quad 4)(3 \quad 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

A cycle of length $L = K.m$, taken to k-th power, will decompose into k cycles of length m. For example : $(k = 2, m = 3)$

$$(1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6)^2 = (1 \quad 3 \quad 5)(4 \quad 5 \quad 6)$$

4.3 Symmetry Sets

Reflections and Symmetries

Let G [2]be a group with identity 1 and let R be a subset of G containing 1. Then R has a partial product $\pi(a, b) = ab$ defined on $D = \{(a, b) \in R \times R | ab \in R\}$, and R together with π is a product set in the sense of the following definition.

Definition 4.3.1.

A product set is a set R together with a function π from a subset D of $R \times R$ to R, denoted $\pi(a, b) = ab$ and called the partial product of R, such that :

1. R has an identity element 1 such that $(1, a)$, $(a, 1) \in D$ and $1a = a1 = a$ for all $a \in R$;

2. $ab = ac$ implies $b = c$ for all (a, b), $(a, c) \in D$.

If $(a, b) \in D$ implies $(b, a) \in D$ and $ab = ba$ for all , $b \in R$, R is abelian.

Here we will denote R as a finite product set with identity 1, partial product π and the domain D of π. The motivating example is that of a subset R of a group G, such as the set R of roots of a Lie algebra.

We define $a^i b$ for $a, b \in R$, $i \in \mathbb{Z}$ as follows:

1. $a^\circ b = b$

2. $a^i b = a\left(a^{i-1} b\right)$ for all $i \geq 1$ for which $a^{i-1} b$ and $a\left(a^{i-1} b\right)$ are defined:

[2] Symmetry sets – David J. Winter- Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109 communicated by Walter Feit – April 16,1980.

3. $a^{-i}b = d$ if $= a^i d$ $(i \geq 0)$.

We let $a^i b \in R$ indicate that $a^i b$ is defined, and we let $a^i b \notin R$ indicate that $a^i b$ is not defined (an abuse of language). Note that $a^i\left(a^j b\right) = a^{i+j} b$ for all $i, j \in \mathbb{Z}$ for which $a^j b$, $a^i\left(a^j b\right) \in R$.

4.4 Homomorphisms of product sets

Definition 4.4.1.

Let R_1, R_2 are mapping $f: R_1 \longrightarrow R_2$ such that $f(ab) = f(a)f(b)$ for all $a, b\, ab \in R_1$. A homomorphism of product sets $f: R_1 \longrightarrow R_2$ is an isomorphism (automorphism $R_1 = R_2$) if f is bijective and both f and f^{-1} are homomorphism. The set of homomorphisms from $R_1$to R_2 is denoted $Hom(R_1, R_2)$, and $Aut\ R$ denotes the group of automorphism of R.

Note that $f\left(a^i b\right) = f(a)^i b$ for $f \in Hom(R_1, R_2)$, $i \in \mathbb{Z}$, $a, b\, ab \in R_1$.

For $a \in R$ and $\boldsymbol{S} \subset R$, the relation $\{(x, y) \in \boldsymbol{S} |\ y = ax\}$ generates an equivalence relation on $\boldsymbol{S}$. The corresponding equivalence class of $b \in \boldsymbol{S}$ is the string $\boldsymbol{S}_b(a) = \{a^{-r} b, \dots, b, \dots, a^q b\}$. If $a^{-(r+1)} b, a_{q+1} b \notin \boldsymbol{S}$**,** we say that the string $\boldsymbol{S}_b(a)$ is bounded of length $q + r$.

If all strings $\boldsymbol{S}_b(a)$ $(b \in \boldsymbol{S})$ are bounded, we introduce the reflection $r_a: \boldsymbol{S} \longrightarrow \boldsymbol{S}$**,** which is the bijection from $\boldsymbol{S}$ to itself reversing each string $\boldsymbol{S}_b(a) = \{a^{-r} b, \dots, a^q b\} : r_a\left(a^i b\right) = a^{q-r-i}\, b$.

In particular, $r_a(b) = a^{-a*(b)}\, b$, where $a * (b) = r - q$, the Cartan integer of b at a. Clearly, r_a is a symmetry of $\boldsymbol{S}$ at a in the following sense.

Definition 4.4.2.

A symmetry of $\boldsymbol{S}$ at a is a bijection $s : \boldsymbol{S} \longrightarrow \boldsymbol{S}$ such that

(i) $s\, \boldsymbol{S}_b(a) = \boldsymbol{S}_b(a)$ for all $b \in \boldsymbol{S}$

(ii) $s\left(a^i b\right) = a^{-i}\, s(b)$ for all $b \in \boldsymbol{S}$ and all $a^i b \in \boldsymbol{S}_b(a)$ $(-r \leq i \leq q)$.

Clearly, a symmetry s of $\boldsymbol{S}$ at a has period 2. Moreover, if all strings $\boldsymbol{S}_b(a)$ $(b \in \boldsymbol{S})$ are bounded, r_a is the only symmetry of $\boldsymbol{S}$ at a.

4.5 Reflection Sets and Symmetry Sets

Definition 4.5.1.

A reflection set is a finite product set R such that :

1. The strings $R_b(a)$ $(a, b \in R\ , a \neq 1)$ are all bounded

2. The reflections $r_a(a \in R\ , a \neq 1)$ are automorphisms of R.

3. The subgroup $W(R)$ of $Aut\ R$ generated by the reflections $r_a(a \in R\ , a \neq 1)$ is called the Weyl group of R.

Clearly, a reflection set is a symmetry set in the following sense,

Definition 4.5.2.

A symmetry set is a finite product set R such that $Aut\ R$ contains a symmetry s_a of R at a for all $a \in R\ , a \neq 1$.

In a symmetry set R, each element $a \in R$ has a unique inverse $b \in R$ such that $ab = ba = 1$. This follows from the equations

$s_a(a) = s_a(a1) = a^{-1}s_a(1) = a^{-1}\ 1,$

$1 = a(a^{-1}\ 1)$

$1 = s_a\big(a(a^{-1}\ 1)\big) = s_a(a)\ s_a(a^{-1}\ 1) = (a^{-1}\ 1)\big(as_a(1)\big) = (a^{-1}\ 1)a$

Clearly, the inverse of a is $a^{-1}\ 1$, which we denote henceforth by a^{-1} . Clearly, $s_a(a) = a^{-1}$

If s_a is the reflection $r_a(b) = a^{-a*(b)}\ b$, we have $a * (a) = 2$. For example ,

$R_a(a) = \{a^{-r}a, \ldots., a^q a\} = \{a^{1-r}1, \ldots., a^{-1}1, 1.a1, \ldots., a^{q+1}1\}$

And $r_a(1) = 1$, implies that $-(1 - r) = q + 1$ and $a * (a) = r - q = 2$. This is needed for (Theorem 4.5.1)

Definition 4.5.3.

a root system is a finite product set R such that for all $a \in R$, $a \neq 1$, there exists

$a \in Hom(R, \mathbb{Z})$ such that $a\cdot(a) = 2$ and $s_a(b) = a^{-a\cdot(b)}\ b$ defines an automorphism and symmetry s_a of R at a.

Theorem 4.5.1.

The following conditions are equivalent:

1. R is a root system

2. R is a symmetry set and $Hom(R,\mathbb{Z})$ separates R

3. R is reflection set and $a^* \in Hom(R,\mathbb{Z})$ for all $a \in R$, $a \neq 1$

4. R is isomorphic to a system of roots in the sense of Bourbaki with 0 added.

Proof:

We show that $(\mathbf{1}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{3}) \Longrightarrow (\mathbf{4}) \Longrightarrow (\mathbf{1})$. Suppose first that R is a root system, $b,c \in R$, $b \neq c$ and $a\cdot(b) = a\cdot(c)$ for all $a \in R$, $a \neq 1$. Consider, first the possibility that $c^{-1}b \in R - \{1\}$. Then $c \in R$, $c^{-1}b \in R$ and $c(c^{-1}b) = b \in R$ implies that

$$a\cdot(b) = a\cdot\big(c(c^{-1}b)\big) = a\cdot(c) + a\cdot(c^{-1}b),$$

so that $a\cdot(c^{-1}b) = a\cdot(b) - a\cdot(c) = 0$ for all $a \in R$, $a \neq 1$.

In particular, $2 = (c^{-1}b)\cdot(c^{-1}b) = 0$, a contradiction.

Thus, $c^{-1}b \notin R - \{1\}$, so that $R_b(c) = \{b, \dots, c^q b\}$ and $R_b(c)$ is bounded of length q. It follows that $s_c(b) = c^q b$, so that $s_c(b) = c^{-c\cdot(b)}b$ implies that $-q = c\cdot(b) = c\cdot(c) = 2$, a contradiction. We must conclude that $\{c\cdot|a \in R, a \neq 1\}$ separates R, so that $(\mathbf{1}) \Longrightarrow (\mathbf{2})$.

For $(\mathbf{2}) \Longrightarrow (\mathbf{3})$, suppose that R is symmetry set and $Hom(R,\mathbb{Z})$, let R^{**} be the group $Hom(R^*,\mathbb{Z})$ and define $\hat{a} \in R^{**}$ for $a \in R$ by $\hat{a}(f) = f(a)(f \in R^*)$:

$$\hat{a}(f+g) = (f+g)(a) = f(a) + g(a) = \hat{a}(f) + \hat{a}(g)$$

Then $\wedge: a \mapsto \hat{a}$ is a homomorphism from R to $\hat{R} = \{\hat{a}|a \in R\}$ which is bijective, since $Hom(R,\mathbb{Z})$ separates R. Since $\hat{R}$ is contained in the torsion free group R^{**}, the strings $\hat{R}_{\hat{b}}(\hat{a})$ are bounded for all $\hat{a},\hat{b} \in \hat{R}$, $\hat{a} \neq \hat{1}$. It follows that the strings $R_b(a)$ are bounded for all $a,b \in R$, $a \neq 1$, so that the symmetries s_a are the reflection set. Finally, for $b,c\,, bc \in R$ we have $a^{-a^*(bc)}\,bc = r_a(bc) = r_a(b)r_a(c) = \big(a^{-a^*(b)}\,b\big)\big(a^{-a^*(c)}\,c\big)$, so that

$\hat{b} + \hat{c} - a^*(bc)\hat{a} = \hat{b} - a^*(c)\hat{a}$, and $a^*(b) = a^*(b) + a^*(c)$, since the additive group R^{**} is torsion free. Thus, $a^* \in Hom(R,\mathbb{Z})$ for all $a \in R$, $a \neq 1$. Clearly, $(\mathbf{4}) \Longrightarrow (\mathbf{1})$. It remains to show that $(\mathbf{3}) \Longrightarrow (\mathbf{4})$. For this assume that R is a reflection set and $a^* \in Hom(R,\mathbb{Z})$ for all $a \in R$, $a \neq 1$. As in $(\mathbf{1}) \Longrightarrow (\mathbf{2})$, $\{a^*|a \in R, a \neq 1\}$ separates R. Therefore, as in $(\mathbf{2}) \Longrightarrow (\mathbf{3})$, $R \longrightarrow \hat{R}$ is a bijective homomorphism with $\hat{R}$ abelian. But his homomorphism is an isomorphism by (Theorem **4.5.2**) below, and $\hat{R}$ is isomorphisc to a system of roots with 0 added by the discussion below.

The strategy in the above is to pass from a symmetry set R to its image R under the closure homomorphism $\wedge: R \longmapsto R^{**}$ where $\hat{a}$ is defined by $\hat{a}(f)(f \in R^*)$ for $a \in R$. Here $R^* = Hom(R, \mathbb{Z})$ and $R^{**} = Hom(R, \mathbb{Z})$ are torsion free additive groups. Since automorphisms s of R determine adjoints $s^* \in Aut\ R^*$ and $s^{**} = (s^*)^* \in Aut\ R^{**}$ such that

$s^{**}(\hat{a}) = \widehat{s(a)}$, the image $\hat{R}$ of the symmetry set R is a reflection set called the closure of R . here s^* is defined, as one would expect, by $s^*(f) = f \circ s$ for $f \in R^*$. More specifically, a symmetry $s_a \in Aut\ R$ of R at $a \neq 1$ determines a symmetry $\hat{s}_a = (s_a)^{**}|_{\hat{R}} \in Aut\ \hat{R}$ of $\hat{R}$ at $\hat{a}$ which, since R^{**} is torsion free, is the reflection of R^* at $\hat{a} : \hat{s}_a = r_{\hat{a}}$. As in the above proof, we have $\hat{a}^* \in Hom(\hat{R}, \mathbb{Z})$ for all $\hat{a} \in R$, $\hat{a} \neq 0$. Since $r_{\hat{a}} = \hat{b} - \hat{a}^*(\hat{b})\hat{a}(\hat{a} \in \hat{R}, \hat{a} \neq 0)$, $\hat{R}$ is isomorphic to a system of roots in the sense of Bourbaki[3] with 0 added, the system of roots being the subset $(\hat{R} - \{0\})\otimes 1$ of the subspace V which it generates in $R^{**}\otimes_{\mathbb{Z}}\mathbb{R}$.

The closure homomorphism $\longrightarrow \hat{R}$ is an isomorphism if and only if it is injective, that is if and only if $Hom(R, \mathbb{Z})$ separates points, by the following theorem .

Theorem 4.5.2.

Let $s: R \longrightarrow R'$ be a surjective homomorphism of product sets, denoted $s(b) = b'$. Suppose that all strings $R_b(a)(a, b \in R, a \neq 1\ )$ and $R'_{b'}(a')(a', b' \in R', a' \neq 1')$ are bounded and $r_{a'}(b') = r_a(b')$ for all $a, b \in R, a \neq 1, a' \neq 1'$. Then

$a'^*(b) = a^*(b)$ for all $a, b \in R, a \neq 1, a' \neq 1'$

For any $a \in R\ , c' \in R', a' \neq 1'$, there exists $b \in R$ such that $b' = c'$ and s maps $R_b(a)$ bijectively to $R_{b'}(a')$. s is an isomorphism if and only if s is bijective

Proof:

For (**1**), we have $r_{a'}(b') = r_a(b)' = \left(a^{-a^*(b)}\, b\right)' = a'^{\,-a^*(b)}\, b'$ and $r_{a'}(b') = a'^{\,-a^*(b')}\, b'$. Since s is a homomorphism, we have $-r' \leq -r \leq -a^*(b) \leq q \leq q'$, where $R_b(a) = \{a^{-r}b, \dots, a^q b\}$ and $R_{b'}(a') = \{a^{1-r'}b', \dots, a'^{q'}b'\}$. This implies that $a^*(b) = a'^*(b')$, proving (**1**). For (**2**), let $R'_{c'}(a') = \{a^{1-r'}c', \dots, a'^{q'}c'\} = \{c'_0, \dots., c'_n\}$ with $n' = q' + r'$ and $c'_i = a'^i c'_0$ for $0 \leq i \leq n'$.

Let $R_{c_0}(a) = \{b_0, \dots, b_n\}$, where $b_j = a^j b_0$ $(0 \leq j \leq n)$, and note that $c_0 = b_0$, since $c_0 = a^j b_0$ for some j and $a'^{-1}c'_0 \notin R'$. Then

[3] N.Bourbaki. "Groupes et alge'bres de Lie" Chaps 4-6, Hermann, Paris, 1968.

$c_{n'}^{'} = r_{a'}(c_0^{'}) = r_a(c_0)^{'} = r_a(b_0)^{'} = b_n^{'} = (a^n b_0)^{'} = a'^n b_0^{'} = a'^n c_0^{'} = c_n^{'}$

Thus, $n^{'} = n$ and $b_j^{'} = \left(a^j b_0\right)^{'} = a'^j c_0^{'} = c_j^{'}$ for $0 \leq j \leq n$, so that s maps $R_{c_0}(a) = \{b_0, \ldots, b_n\}$ bijectively to $\{c_0^{'}, \ldots., c_n^{'}\} = R_{c'}^{'}(a^{'})$. Clearly, $R_{c_0}(a) = R_b(a)$, where $b = b_i$, and i is chosen with $1 \leq i \leq n$ so that $b_i^{'} = c'$ and $b^{'} = c'$.

For (**3**), let s be bijective and $a, b \in R, a \neq 1$ such that $a'b' \in R'$. With notation as in (**2**) above, we then have $R_a(a)^{'} = \{b_0, \ldots, b_n\}^{'} = \{b_0^{'}, \ldots., b_n^{'}\} = R_{b'}(a^{'})$, $b = b_r = a^r b_0$ for some r, $0 \leq r \leq n$, $b^{'} = (a^r b_0)^{'} = a'^r b'_0$ and

$a^{'} b^{'} = a'^{r+1} b_0^{'} = b_{r+1}^{'} = (a^{r+1} b_0)^{'} = (aa^r b_0)^{'} = (ab)^{'}$

Thus, $ab \in R$ and $s^{-1}(a^{'} b^{'}) = ab = s^{-1}(a^{'}) s^{-1}(b^{'})$. This shows that $s^{-1} \in Hom(R^{'}, R)$, so that s is an isomorphism.

Definition 4.5.4. (Direct Sums)

Let $R_1, \ldots, R_n$ be product sets. Resituate them (up to isomorphism) so that their identities all coincide (call it 1) and $R_i \cap R_j = \{1\}$ for all $i \neq j$. Then the outer direct sum

$R = R_1 \oplus \ldots \oplus R_n$ of $R_1, \ldots, R_n$ is the product set $R = R_1 \cup \ldots \cup R_n$ such that $ab = c$ in R if and only if there exists i such that $a, b, c \in R_i$ and $ab = c$ in R_i .

Conversely, for any product set R with identity 1, R is the inner direct sum $R = R_1 + \cdots + R_n$ of subsets $R_1, \ldots, R_n$ of R if $R = R_1 \cup \ldots \cup R_n$, $R_i \cap R_j = \{1\}$ for all $i \neq j$ and $ab = c$ in R_i . note that if R is an inner direct sum $R = R_1 + \cdots + R_n$, then $R_1, \ldots, R_n$ are product sets whose outer direct sum is R .

$R_b(a) = R_{jb}(a)$ for $a \in R$, $b \in R_j$, and $R_b(a) = \{b\}$ if $b \in R_j$ and $a \in R - R_j$.

R is symmetry set (respectively reflection set) if and only if the $R_1, \ldots, R_n$ are also a symmetry (respectively reflection) s_a of R at $a \in R_i$ is the same as a symmetry (respectively reflection) s_{ia} of R_i at extended to R by fixing the elements of $R - R_j$.

Let R be a symmetry set and let S , $T \subset R$. We let $= \{ab | a \in S, b \in T, ab \in R\}$,

$S^{-1} = \{a^{-1} | a \in S\}$ and $\dot{S} = S - \{1\}$. We say that S is π −closed if $S\,S \subset S$ and symmetric if $S^{-1} \subset S$.

A subset $\dot{S}$ of $\dot{R}$ is closed in $\dot{R}$ if $R = S + \tilde{S}$ (inner direct sum), where $S = \dot{S} \cup \{1\}$ and $\tilde{S} = R - \dot{S}$. For $\dot{S}$ is closed, S and $\tilde{S}$ are clearly π −closed and symmetric, and they can

viewed as symmetry sets. Moreover, $\tilde{S}$ is closed and $\tilde{\tilde{S}} = S$. For $\dot{S}$ and $\dot{T}$ closed in R, the inner direct sum.

$R = (S \cup \tilde{S}) \cap (T \cup \tilde{T}) = S \cap T + S \cap \tilde{T} + \tilde{S} \cap T + \tilde{S} \cap \tilde{T}$, can be used to show that $\dot{S} \cap \dot{T}$ and $\dot{S} \cup \dot{T}$ are closed in $\dot{R}$. Thus, the set $\mathfrak{D} = \{\dot{S} | \dot{S}$ is closed in $\dot{R}\}$ is a topology for $\dot{R}$. Since $\dot{S}$ is closed if and only if $\dot{S}$ is open, the connected components of $\dot{R}$ are the minimal elements $\dot{S}_1, \ldots\ldots, \dot{S}_n$ of $\mathfrak{D}$ and $R = S_1 + \cdots + S_n$ is the unique inner direct sum decomposition of R which cannot further be refined. If $n = 1$, we say that R is irreducible. The irreducible symmetry sets S_i are the components of R.

If R is a subset of a group, then the topology $\mathfrak{D}$ introduced here for $\dot{R}$ coincides with the symmetric $G-$topology. For any finite subset $\dot{R}$ of a group G by the $S \subset \dot{R}$ is closed if S and $\dot{R} - S$ are both $\pi-$closed and symmetric.

Examples of Symmetry sets 4.5.1.

1. Symmetry sets which are not root systems are symmetry sets having a component which is a nonzero finite vector space $V = (\mathbb{Z}_p)^d$, a symmetry $s_a(v)$ at a being defined for any $\dot{a} \in Hom(V, \mathbb{Z}_p)$ such that :

$\dot{a}(a) = \bar{2}$ by $s_a(v) = v - \dot{a}(v)a \quad (a \in V, a \neq 0)$

2. Any two symmetries s_{1a}, s_{2a} are conjugate in $Aut\, V$ by a unipotent $u_a \in Aut\, V$ of V at $a: u_a(a + b) = a + u_a(b)$ for all $b \in V$ $(p > 2)$. In fact, it the conjugate of $2-$ Sylow groups in the dihedral group $\langle s_{1a}, s_{2a} \rangle$. This unicity can be generalized along the lines of Winter[4].

Definition 4.5.4. (Reduced Symmetry Sets in an Abelian Group)

Let R be a sub set containing 0 of an additive abelian group G having no 2,3,5,7 torsion, and assume that R is a symmetry set which is reduced, that is $2a \notin R$ for all a$\in R$, $a \neq 0$.

Using simple modifications of techniques of Seligman, we show that R is root system. We first note that a string $R_b(a)$ can not contain $b, b + a, b + 2a, b + 3a, b + 4a$. For suppose otherwise.

Since $\pm 2a \notin R$, the elements $b, b + a, b + 2a, b + 3a, b + 4a$ are nonzero. Since $2(b + a) \notin R$ and $-2a \notin R$, $R_b(b + 2a) = \{b\}$, so that $s_{b+2a}(b) = b$. Since $2(b + 3a) \notin R$

[4] D.J.Winter, A combinatorial theory of symmetry and applications to Lie algebras, in "Algebra Carbondale 1980" Lecture Notes in Matematics No.848, Spring-Verlag, Berlin/ New York,1981.

and $2a \notin R$, $R_{b+4a}(b+2a) = \{b+4a\}$ so that $s_{b+2a}(b+4a) = b+4a$. Letting $s = s_{b+2a}$, we then have $b+4a = s(b+4a) = s(b) + 4s(a) = b + 4s(a)$. Thus, $4a = 4s(a)$ and $a = s(a)$. But then $-(b+2a) = s_{b+2a}(b+2a) = s(b+2a) = b+2a$, so that $2(b+2a) = 0$ and $-2a \notin R$, a contradiction.

It follows that the strings $R_b(a)$ are bounded of length at most 3. Therefore, the symmetries $s_a(b)$ are the reflections $r_a(b) = b - a^*(b)a$, $a^*(b) = r - q$.

Since $r_a(b+c) = r_a(b) + r_a(c)$, we have $a^*(b+c)a = \big(a^*(b) + a^*(c)\big)a$ for all $b, c, b+c \in R$. Since G has no 2,3,5,7 torsion, the order of a is at least 11, so that the restrictions on the Cartan integers $r-q$ that $r, q \geq 0$ and $r+q \leq 3$ lead us to conclude that $a^*(b+c) = a^*(b) + a^*(c)$. It follows that $a^* Hom(R, \mathbb{Z})$ for all $a \in R$, $a \neq 0$, so that R is a root system.

4.6 Classical Lie Algebras

Let $\mathfrak{g}$ be a classical Lie algebra with classical Cartan subalgebra H and corresponding set of roots $R = R(\mathfrak{g}, H)$. Suppose that the characteristic of $\mathfrak{g}$ is not 2,3,5,7. Then $R = R(\mathfrak{g}, H)$ is a reduced reflection set with reflections $r_a(b) = b - 2(b(h_a)/a(h_a))a$, by the beautiful results of Lemma II2.2, II3.1, IIe.2, II4.2 of Seligman[5]. Thus, $R = R(\mathfrak{g}, H)$ is isomorphic to a reduced system of roots with 0 added, by (Theorem 4.1). since $\mathfrak{g}$ together with H is determined uniquely up to isomorphism by $R = R(\mathfrak{g}, H)$, by a version of (Theorem 3.7.4.9) of winter, the classical Lie algebras $\mathfrak{g}$ with H are classified by systems of roots in the sense of Bourbaki with zero added by the correspondence $(\mathfrak{g}, H) \mapsto R(\mathfrak{g}, H)$. In this approach to the classification, we transfer R together with its combinatorial structure from the hostile environment of characteristic p to real Euclidean space by passing to $\hat{R} \subset R^{**}$ rather than classify R "on the spot" using orderings, fundamental systems of roots and their Cartan matrices.

Definition 4.6.1. (Relation Sets and Symmetry Sets)

A relation set is a set R and a subset π of R^3, such that R has an identity element 1 such that $(x,1,x), (1,x,x) \in R$ for all $x \in R$. We let $ax = y$ indicate that $(a,x,y) \in \pi$. Note that y need not be uniquely determined by a and x.

Clearly, a product set is just a relation set such that **:**

1. $ax = y$ and $ax = z$ implies $y = z$

[5] G.Seligman, "Modular Lie algebras" Ergebnisse der Mathematik u. ihrer Grenzegbeite Bd 40, Spring – Verlag, Berlin 1967.

2. $ay = x$ and a$z = x$ implies $y = z$ for all $a, x, y, z \in R$.

In this section we let R be a finite relation set. Our objective is to **:**

i. Indicate briefly how the above theory of symmetries generalizes from product sets to relation sets

ii. Describe the root system $\widehat{S(R)}$ which R determines.

A homomorphism of relation sets R_1, R_2 is a mapping $f: R_1 \longrightarrow R_2$ such that $ax = y$ implies $f(a)f(x) = f(y)$ for all $a,, x, y \in R$. And f is an isomorphism (automorphism if $R_1 = R_2$) if f is bijective and f, f^{-1} are homomorphisms. We let $Hom(R_1, R_2)$ denote the set of homomorphism from R_1 to R_2 and we let $Aut\ R$ denote the automorphism group of R.

For $a \in R$ and $S \subset R$, a determines the equivalence relation on S generated by the relation $\{(x, y) \in S \times S | ax = y\}$. We let $S_b(a)$ denote the corresponding equivalence class of $b \in S$.

A symmetry of S at a is a bijection $s_a: S \longrightarrow S$ such that **:** $s_a S_b(a) = S_b(a)$ for all $b \in S$

$ax = y$ implies $a\ s_a(y) = s_a(x)$ for all $x, y \in S$

Note that if R is a product set, condition (2) is equivalent to $s_a(a^i x) = a^{-i} s_a(x)$ for all $a^i x \in R$.

A symmetry set is a finite relation set R such that $Aut\ R$ contains a symmetry s_a of R at a fro every $a \in R$. Clearly, this coincides with our earlier definition if R is a product set.

Consider the additive group $R^* = Hom(R, \mathbb{Z})$, where $f + g = h$ is the function defined by $h(a) = f(a) + g(a)(a \in R)$ for $f, g \in R^*$. Similarly, consider the additive group

$R^{**} = Hom(R^*, \mathbb{Z})$. As in previous section we get the closure homomorphism $\bigwedge: R \longrightarrow R^{**}$ with $\hat{a}(f) = f(a)(f \in R^*)$ for $a \in R$:

$$xy = z \text{ in } R \Longrightarrow f(x) + f(y) = f(z) \qquad \forall f \in R^*$$

$$\Longrightarrow \hat{x}(f) + \hat{y}(f) = \hat{z}(f) \qquad \forall f \in R^*$$

$$\Longrightarrow \hat{x} + \hat{y} = \hat{z} \qquad \text{in } R^{**}$$

The subset $\hat{R} = \{\hat{a} | a \in R\}$ of torsion free additive group R^{**} is a product set called the closure of R.

If R is a symmetry set in the sense of this section, then the product set $\hat{R}$ is a symmetry set since, as one easily checks, the double adjoint s_a^{**} of s_a restricted to a symmetry $\hat{s}_a = s_a^{**}|_{\hat{R}}$ of $\hat{R}$ at $\hat{a}$ in $Aut\,\hat{R}$. In fact, $\hat{R}$ is a system of roots with 0 added, as we now show in greater generality.

For any relation set R we let $S(R) = \{a \in R|$there exists a symmetry $s_a \in Aut\,R$ of R at $a\}$. Clearly, $S(R)$ is stable under $Aut\,R$, so that $s_a S(R) = S(R)$ for all $a \in S(R)$. Thus, $S(R)$ is a symmetry set in R in the following sense.

Definition 4.6.2.

A symmetry set in R is a subset S of R containing 1 such that for each $a \in S$, there exists a symmetry $s_a \in Aut\,R$ of R at a such that $s_a(S) = S$. The closure of S in R is the image $\hat{S} = \{\hat{s}|s \in S$ of under the closure mapping $\wedge: R \longrightarrow \hat{R}$ of R. For $a \in S(R)$, the double adjoint s_a^{**} is an automorphism of the torsion free group R^{**} and $\bar{s}_a = s_a^{**}|_{\langle R\rangle} \in Aut\,\langle\hat{R}\rangle$ satisfies $\bar{s}_a(b) \equiv b(mod\ \mathbb{Z}\hat{a})$ for $b \in \langle\hat{R}\rangle$. Thus, there exists $a^{\cdot} \in Hom(\langle\hat{R}\rangle, \mathbb{Z})$ such that $\bar{s}_a(b) = b - a^{\cdot}(b)a\ \left(b \in \langle\hat{R}\rangle\right)$. Clearly, $a^{\cdot}(\hat{a}) = 2$ since $-\hat{a} = \bar{s}_a(\hat{a})$.

Theorem 4.6.1.

$\widehat{S(R)}$ is a system of roots with 0 added[6].

Proof:

By the above discussion, $\widehat{S(R)}$ has the required reflections $r_{\hat{a}}(\hat{b}) = \hat{b} - a^{\cdot}(\hat{b})\hat{a}$ $(\hat{a} \in SR, a \neq 0$.

In taking the closure $S(R)$ of $S(R)$ in R rather than in $\widehat{S(R)}$ in the above discussion, we assure the validity of the otherwise unwarranted step $\bar{s}_a(b) \equiv b(mod\ \mathbb{Z}\hat{a})$ for b in the closure of $S(R)$ in $S(R)$. (the symmetry s_a might not preserve the sets $S(R)_a$ (a)) .

4.7 Root Systems

Definition 4.7.1.

A root system[7] is a pair (V, R), where V is a vector space and R is a finite subset of V containing 0 which has a symmetry $r_a(v) = v - a^0(v)a$ $(v \in V)$ for each $a \in R - \{0\}$: $a^0 \in Hom_k(V, k)$ and $a^0(a) = 2$

[6] Symmetry sets – David J. Winter- Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109 communicated by Walter Feit – April 16,1980.

$r_a(R_b(a)) = R_b(a)$ for every bounded a-orbit $R_b(a)$ $(b \in R)$

We also assume that R spans V.

The rank of (V, R) is the dimension of the span $V = kR$ of R. The $\mathbb{Z}$-rank of R is the rank of the groupoid dual $Hom(R, \mathbb{Z})$.

We let $Ra = R \cap \mathbb{Z}a$ and define the set $R^{\cdot} = \{a \in R - \{0\} | Ra = R^0 \cup R^{\cdot}$ and $R_b(a)$ has 1 or $p-1$ or p elements for every $a \in R^0 - \{0\}$, $b \in R$.

We call the orbits $R_b(a)$ $(a \in R^{\cdot}\ b \in R)$ classical orbits, and the orbits $R_b(a)$ $(a \in R^0 - \{0\}, b \in R)$ Witt orbits. Accordingly, a root system is a Lie root system if all are roots are either classical or Witt and every Witt orbit has 1 or $p-1$ or p elements.

Note that if $2a, 2(b+a), 2(b+3a) \notin R$. Then $R_b(a)$ doesnot contain $a, b+a, b+2a, b+3a, b+4a$ and therefore, is bounded of length at most 3. Thus, orbits $R_b(a)$ of length greater than there exist only when R^0 contains one of $a, b+a, b+2a, b+3a$. It follows that if R^0 is a group, that is , $R^0 + R^0 = R^0$. Then $R_b(a)$ with $b \in R^0$ has length greater than three only for $a \in R^0$.

Proposition 4.7.1.

Let R^0 be a group, $b \in R^0$ and $R_b(a) \neq \{b]$. Then :

For $p > 5$, $a \in R^0$ if and only if $R_b(a)$ has $p-1$ or p elements,For $p = 5$, $a \in R^0$ if $R_b(a) = \mathbb{Z}a + b$.

By the same argument, it follows that $R = R^{\cdot} \cup \{0\}$ if and only if every orbit

$R_b(a)$ $(a \in R - \{0\}, b \in R)$is bounded, in which case the Lie root-system R is a reduced symmetry set.

Definition 4.7.2.

A classical root system is a Lie root system all of whose nonzero roots are classical, that is $R = R^{\cdot} \cup \{0\}$.

Theorem 4.7.2.

A root system (V, R) is classical if and only if R is isomorphic as groupoid to a reduced root system in the sense of Bourbaki with 0 added.

---

[7]David. J.Winter, Symmetric Lie algebras, Depatement of Mathematics, University of Mishigan, Ann Arbor, Michigan 48109, Communicated by N.Jacobson, Received April 10, 1982.

In the next section, we classify the rank two Lie root systems $Rab = R \cap (\mathbb{Z}a + \mathbb{Z}b)$ up to isomorphism. All turn to be symmetry sets. At the same time, only two rank 1 Lie root system are symmetry sets, namely A_1 and W_1 as the Lie root systems of rank 1 defined over $\mathbb{Z}_p$. The general situation for rank one is as follows.

Theorem 4.7.3.

Let R be a rank one Lie root system. Then either $R = R^0$ and R is a group, or $R = \{-a, 0, a\}$.

Proof:

Let $a \in R^0 - \{0\}$, $b \in R - \{0\}$ and write $b = ma$, where $m \in k$ (which is possible since R is of rank 1). If $R_b(a)$ is bounded, then $a^0(b) = 2m$ is in the prime field $\mathbb{Z}_p = \mathbb{Z}1$, so that $b = ma$ is in $\mathbb{Z}1 = R_0(a)$.

But then $R_b(a) = R_0(a) = \mathbb{Z}a$ and $R_b(a)$ is not bounded, acontradiction.

Thus, $R_b(a) = \mathbb{Z}a + b$. Iterating, we have $R^0 + R \subset R$, $R^0 + R^0 + R \subset R, \ldots.$, $G = R^0 + \cdots + R^0$ (n times) $\subset R$. Since R is finite , G isb a group for some n.

Since every subgroup of R is in R^0, $G = R^0$ and R^0 is a group. Next, let $a \in R^0 - \{0\}$, $b \in R - \{0\}$ and consider $R_a(b)$. If it is unbounded, we have $b \in R^0$, by (Prop 4.7.1) Suppose that it is bounded : $R_a(b) = \{a - rb, \ldots., a + qb\} = R_c(b) = \{c, \ldots, c + (r + q)b\}$. Then $b^0(c) = -(r + q) \in \mathbb{Z}_p$. We may write $c = sb$ with $s \in k$, by invoking " rank 1", so that $2s = r + q$ and $s \in \mathbb{Z}_p$. Then we have $b \in R^0 : c = sb \in \mathbb{Z}_p\, b \Longrightarrow a = c + rb \in \mathbb{Z}_p b = \mathbb{Z}_p a \subset R^0 \Longrightarrow b \in R^0$. Thus, an element $b \in R - \{0\}$ is in R^0 in all cases, so that $R = R^0$ if and only if R^0 is nonzero. Suppose, finally that $R^0 = \{0\}$, so that $R = R^{\cdot} \cup [0]$. By the remarks preceding (Def 4.7.2) , each orbit $R_b(a)$ is bounded :

$R_b(a) = \{b - ra, \ldots., b + qa\}\ (a \in R^{\cdot}) = R - \{0\}, b \in R)$.

Then $b + qa = r_a(b - ra)$, $a^0(b) = r - q$ and $2s = a^0(sa) = a^0(b) = r - q$, where $b = sa$ $(s \in k)$, so that $s \in \mathbb{Z}_p$ and $b \in s \cap \mathbb{Z}_p = ra = \{-a, 0, a\}$. It follows that $R = \{-a, 0, a\}$.

Any finite subgroup G of k^+ determines the Lie root system (k, G). For the others, define $S \vee T = \{(s, t) \in S \times T | s = 0$ or $t = 0\}$ and $S \oplus T = \{(s, t) | s \in S, t \in T\}$, where S and T are sets with a distinguished element : $0 \in S, 0 \in T$. Identify $s = (s, 0)$, $t = (0, t)$ and write $s + t = (s, t)$. Let $A = \{-a, 0, a\} \subset ka$ and $W = \{-a, 0, \ldots, p - 2\} \subset ka$, the rank 1 Lie root systems defined over $\mathbb{Z}_p$.

Next construct $A\vee A, A\vee W, W\vee W$, the reducible rank 2 Lie root systems defined over $\mathbb{Z}_p$.

Let $A_2 = \{(0,0), \pm(1,0), \pm(0,1), \pm(1,1)\}$, $B_2 = \{(0,0), \pm(1,0), \pm(0,1), \pm(1,1), (1,-1)\}$, $G_2 = \{(0,0), \pm(1,0), \pm(0,1), \pm(1,1), \pm(1,2), \pm(2,1), \pm(1,-1)\}$, which are symmetry sets in $\mathbb{Z}_p^2$ whose groupoid reflections $r_a(b) = b - a^*(b)a$ determine $a^* \in Hom(R, \mathbb{Z})$ and $a^0 \in Hom(\mathbb{Z}_p^2, \mathbb{Z}_p)$ (a^* reduced modulo p) for $a \in R - \{0\}$ and $B = A_2, B_2, G_2$. These are the irreducible rank 2 classical root systems. Note that the irreducible nonreduced classical symmetry sets
$2A = \{0, \pm a, \pm 2a\}$,$BC_2 = \{(0,0), \pm(1,0), \pm(0,1), \pm(1,1), \pm(1,-1), \pm(0,2), \pm(2,0)\}$ are not Lie root systems, due to the occurrence of $a, 2a \in R, 3a \notin R$.

Finally, construct $W_2 = W \oplus W$, $W \oplus A$, $S_2 = \{(i,j) \in \mathbb{Z}_p^2 | i,j \neq 0\} \cup \{(0,0)\}$, $T = T_2(n) = S_2 \cup \{\pm(n,-n)\} = S_2 \cup A = S_2 + A$, where $A = \{(0,0), \pm(n,-n)\}(1 \leq n \leq p-1)$, the irreducible rank 2 nonclassical Lie root systems defined over $\mathbb{Z}_p$.

To see that $W \oplus A = \mathbb{Z}a - b \cup \mathbb{Z}a + 0 \cup \mathbb{Z}a + b$, S_2 and $T_2(n)$ are Lie root systems, we define the symmetries $r_c(b) = b - c^0(b)c$ in the three cases $W \oplus A$. S_2, $T_2(n)$ by specifying the appropriate Cartan function $c^0 \in Hom(\mathbb{Z}_p^2, \mathbb{Z}_p)$:

$(ia)^0(ia) = 2$, $(ia)^0(b) = 0$

$(\pm b + ja)^0(\pm b + ja) = 2$ $(\pm b + ja)^0(a) = 0$

$(i,j)^0(r,s) = 2\frac{r+s}{i+j}$ $\left((i,j) \in S_2, (r,s) \in \mathbb{Z}_p^2\right)$

$(n,-n)^0(n,-n) = 2$ $(n,-n)^0(1,0) =$ anything

Definition 4.7.3.

A root system (V, R) is defined over $\mathbb{Z}_p$ if R is contained in some $\mathbb{Z}_p$-form $V_{\mathbb{Z}_p}$ of V: any $\mathbb{Z}_p$-basis for $V_{\mathbb{Z}_p}$ is a k-basis for V.

The following propositions are straight fro ward. In the first proposition, $Ra_1, \ldots, a_n = R \cap (\mathbb{Z}a_1, \ldots, \mathbb{Z}a_n)$.

Proposition 4.7.2.

A Lie root system R of rank n is defined over $\mathbb{Z}_p$ if and only if $R = Ra_1, \ldots, a_n$ for some $a_1, \ldots, a_n \in R$.

4.8 Classification of Lie Root System of Rank

We now determine Recognition properties for all possible for all possible k-independent pairs a, b of roots in a Lie root system R, and classify all corresponding Lie root systems Rab of rank 2 up to isomorphism. The results are given in Table 1, the irreducible root systems of rank 2 defined over $\mathbb{Z}_p$ being A_2, B_2.

TABLE I

Possibilities for Pairs of Independent Roots a, b, Up to Change of Signs

No.	Diagram	Recognition conditions on a and b	Type of Rab	$a^0(b)$ $b^0(a)$
1.	a b	$a, b \in R^{\cdot}$, $R_b(a) = \{b\}$	$A \vee A$	0 0
2.	a b	$a, b \in R^{\cdot}$, $a^*(b)\, b^*(a) = 1$	A_2	-1 -1
3.	a b	$a, b \in R^{\cdot}$, $a^*(b)\, b^*(a) = \dfrac{a^*(b)}{b^*(a)} = 2$	B_2	-2 -1
4.	a b	$a, b \in R^{\cdot}$, $a^*(b)\, b^*(a) = \dfrac{a^*(b)}{b^*(a)} = 3$	G_2	-3 -1
5.	a b	$a \in R^0$, $b \in R^{\cdot}$, $R_b(a) = \{b\}$	$W \vee A$	0 0
6.	a b	$a, b \in R^0$, $R_b(a) = \{b\}$	$W \vee W$	0 0
7.	mn a b	$a, b \in R^0$, $R_b(a) = \mathbb{Z}a + b$	W_2	$-m$ $-n$
8.	a b	$a \in R^0$, $b \in R^{\cdot}$, $a + b \in R^{\cdot}$	$W \oplus A$	$-m$ 0
9.	a b	$a, b \in R^{\cdot}$, $a^*(b)\, b^*(a) = 4, \dfrac{a^*(b)}{b^*(a)} = 1$	$W \oplus A$	-2 -2
10.	a b	$a, b \in R^0$, $a^0(b)\, b^0(a) = 4$	S_2	$-m$ $-4/m$
11.	a b	$a \in R^0$, $b \in R^{\cdot}$, $a + b \in R^0$	T_2	0 $-m$

$G_2, W_2, W \oplus A, S_2, T_2$. In this table, diagrams are introduced to represent each of the 11 classes of k-independent root pairs a, b. Classical and Witt roots are denoted by black and white nodes, respectively. The number of solid lines is the product $a^0(b)b^0(a)$. No lines indicates that a and b are orthogonal : $a \pm b$ are not roots and $a^0(b)b^0(a) = 0$. A dotted line indicates that a and b are not orthogonal and $a^0(b)b^0(a) = 0$, which occurs for types S_2, T_2 and for type W_2 if $m = 0$ or $n = 0$.

Orientation indicats which root is shorter, for types B_2, B_2. Orientation indicates that $a + b$ is classical or Witt, for types $W \oplus A$ and T_2, depending on whether the black or white nodes is "less" (which suffices to distinguish between types $W \oplus A$ and T_2). Actual values for m, n in 7,8,10,11 are suppressed in the diagrams. Adjustments in a, b would lead to default values $-1, -1$ in 7, $-1,0$ (or $-p$) in 8, -2 , -2 in 10 and 0 (or $-p$), -1 in 11, which bring the use of orientation (or lack thereof) in these diagrams in line with its conventional use in the diagrams of the classical root systems 1,2,3,4.

Here and in the sequel, we decompose a root system into its irreducible components as follows. We say that $S \subset R$ is closed if $0 \in S$, $S = -S$ and $a + b \in S$ whenever $a, b \in S$ and $a + b \in R$. If $(R - S) \cup \{0\}$ is closed, we say that $S \subset R$ is open. Then $\{S - \{0\} | S$ is open and closed in $R\}$ is a topology for $R - \{0\}$,whose connected components $R_1 - \{0\}, \dots, R_n - \{0\}$ determine the irreducible components $R_1, \dots, R_n$ of R:

$R = R_1 \cup \dots \cup R_n$ with $R_i \cap R_j = \{0\}$ for $i = j$

$a = a_1 + \cdots + a_n \in R$ with $a_i \in R_i$ $(1 \leq i \leq n)$ implies $a = a_i \in R_i$ for some i

We use the notation $R = S \cup R = S \cup T = \{0\}$, where S, T are open and closed in R. Then R is irreducible if only if $R = R_1$ if and only if $R = \{0\}$ is connected if and only if $R = S \cup$ implies $R = S$ or $R = T$.

Proposition 4.8.1.

The irreducible components R_i of a Lie root system are Lie root systems.

We begin with the following theorem, which establishes Recognition Conditions 1,5,6. It is proved in the cases of $a \in R^0, b \in R$ needed for the ensuing rank 2 classificaation. The case $a \in R^{\cdot}$ then follows from the classification.

Theorem 4.8.1.

Let R be a Lie root system and let $a, b \in R - \{0\}$. Then $Rab = Ra \cup Rb$ with

$Ra \cup Rb = \{0\}$ if only if $R_b(a) = \{b\}$.

Proof:

For one direction, note that $a \pm b \in R_b(a) \subset Ra \subset \mathbb{Z}a$, say implies that $Rab = \{-a, 0, a\}$ or $\mathbb{Z}a$ and $R_b(a) = Rab$.

For the other direction, suppose first that $a \in R^0, b \in R^{\cdot}$ and $R_b(a) = \{b\}$. Thus, we know that $a \pm b \notin R$. We claim that $= Ra \cup Rb$, $Ra \cup Rb = \{0\}$. Suppose, otherwise that there exist $b' = ra + sb \in R$ with $r, s \neq 0$. We claim that $s \in \{(p-1)/2, (p+1)/2\}$, and that $R = s\big((Ra + Rb) - Rb\big) \cup Rb = s((W + A) - A) \cup A$. Where $Ra = W = \mathbb{Z}a$, $Rb = A = \{-b, 0, b\}$. For this, note first that $r_a(b) = b$ and $a^0(b) = 0$, so $a^0(b') \neq 0$ and $r_a(b') \neq b'$. It follows that $R_{b'}(a) \neq \{b'\}$ and therefore, has p or $p - 1$ elements, by (Def 4.7.1), since $a \in R^0$. We refer to Table II in what follows.

Note that $R_{b'}(a)$ is contained in Column C_s, among the columns C_0 =Column $0, \ldots, C_{-1} = C_{p-1}$ =Column $p-1$ of Table II, each of which has at most p-elements. Since $R \cap C_{\pm 1}$ exclude $\pm(b-a), \pm(b+a)$, we must have $s \neq \pm 1$. Thus, since $b \in R^{\cdot}$, we have $sb \notin R_{b'}(a)$. These constraints force $R_{b'}(b) = \mathbb{Z}(a) + sb - \{sb\}$. Moreover, the constraint $s \neq \pm 1$ forces $R_{b'}(b)$ to have fewer than p-elements, so that $b'' =_{def} r_b(b') = ra - sb \in R$. repeating the above argument, we have $R_{b''}(a) = \mathbb{Z}(a) - sb - \{-sb\}$. Thus,

$$R \supset \big((\mathbb{Z}a + s\{-b, 0, b\}) - s\{-b, 0, b\}\big) \cup \{-b, 0, b\} = \big((W + sA) - sA\big) \cup A$$

$$= s\big((W + A) - A\big) \cup A.$$

It follows that $s(b-a) \in R$. Since $(b-a) \notin R, s$ can take on only two values, by (Prop **4.7.1**). It follows that $R = s\big((W + A) - A\big) \cup A$. Interchanging signs, if necessary we have $2 \leq s \leq \cdots \leq (p-1)s \leq \cdots \leq p-2$. It follows that $R_{sb+a} = \{sb + a,\ (s+1)\ \ b + a\}$ and , therefore that $s + 1 = -s$ and $s = -\frac{1}{2}$, as asserted. Now compute $R_b(sb + a) = \left\{b, \frac{1}{2}\ b + a, 0 + 2a, -\frac{1}{2}b + 3a\right\}$.Then$(sb + a)^0(sb + a) - (sb + a)^0(b) = -3$ and $(sb + a)^0(sb) = \frac{2}{3}$. Thus,

$$(sb + a)^0(a) = (sb + a)^0(sb + a) - (sb + a)^0(sb) = 2 - \frac{2}{3} = \frac{1}{2}$$

But $R_a(sb + a) = \{a, sb + 2a\}$ implies , to the contrary that $(sb + a)^0(a) = -1$. We must therefore conclude that $R = Ra \cup R_b$ for $b \in R^{\cdot}$ and $R_b(a) = \{b\}$.

Next, suppose that $b \in R^0$ and $R_b(a) = \{b\}$. We begin claim that $Rab = Ra \cup Rb$,

$R\,a \cup Rb = [0\}$. Note that $C_1 \cap R$ exclude $b \pm a$ and therefore no $b' = b + ra\ (r = 0)$ is in R: $b' \in R \Longrightarrow R_{b'}(a) = \{b'\} \Longrightarrow a^*(b') = 0 \Longrightarrow 0 = a^*(ra) = 2r \Longrightarrow r = 0$

TABLE II

The Roots of $W_2 \supset T_2(n) \supset S_2$ as Successively Generated in a-orbits from the Nonroots $m(b-a)$ of S_2

	0	1	2	3	$p-1$
0	0	$\underline{b-a}$	$\underline{2b-2a}$	$\underline{3b-3a}$	$\underline{(p-1)\,b+a}$
1	a	b	$2b-a$	$3b-2a$	$(p-1)\,b+2a$
2	$2a$	$b+a$	$2b$	$3b-a$	$(p-1)\,b+3a$
3	$3a$	$b+2a$	$2b+a$	$3b$	$(p-1)\,b+4a$
4	$4a$	$b+3a$	$2b+2a$	$3b+a$	$(p-1)\,b+5a$
5	$5a$	$b+4a$	$2b+3a$	$3b+2a$	$(p-1)\,b+6a$
6	$6a$	$b+5a$	$2b+4a$	$3b+3a$	$(p-1)\,b+7a$
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	$(p-1)\,a$	$b+(p-2)\,a$	$2b+(p-3a)$	$3b+(p-4)\,a$	$(p-1)\,b$

Similarly, no $a^{'} = a + sb$ $(s \neq 0)$ is in R. But then every column C_s excludes $sb \pm a$, so that each $R_{b'}(a)$ is $\{b^{'}\}$ for $b^{'} \in C_s - \{sb\}$, which is impossible since :

$0 = a^*(b^{'}) = a^*(sb + ra) = 2r$ implies $r = 0$. Thus, $= Ra \biguplus Rb$.

The remaining case $a, b \in R^{\cdot}$ is not needed for the rank 2 classification given below. Applying this classification, we need only observe that one of the conditions $R_b(a) = \{b\}$ or $a^*(b) = 0$ is not met for each pair 2,3,4,9, to complete the proof.

Theorem 4.8.2.

Let R be a Lie root system and let $a \in R^0, b \in R^{\cdot}$ with Rab irreducible. Then $b - a \in R$ and $Rab \supset Ra + Rb = W \oplus A$.

Proof:

Suppose that $b - a \notin R$. Since Rab is irreducible, $b + a \in R$, by (Theorem 4.8.1). Thus, $R_b(a) = b, \ldots, b + (p-2)a$, by (Def 4.7.1). It follows that $a^0(b) = 2 = a^0(a)$ and $a^0(b - a) = 0$. Thus, $a^0(2b - 4a) = 2a^0(b - a) - 2a^0(a) = -4$ and

$r_a(2b - 4a) = 2b - 4a - a^0(2b - 4a)a = 2b \notin R$. It follows that $2b - 4a \notin R$. Since $2b, 2b - 4a \notin R$ and $-2b, -2b + 4a \notin R$, R contains no root $\pm(2b + ra)$ otherwise $R_{2b+ra}(a)$, say has fewer than $p - 1$ elements, so $R_{2b+ra}(a) = \{2b + ra\}$, which contradicts the irreduciblility of Rab. It follows that $R_a(b) = \{a, a + b\}$, whereas $R_{2a}(b) = \{-b + 2a, 2a, b + 2a\}$. Thus, $-1 = b^0(a)$ and $-2 = b^0(-b + 2a) = -2 + 2b^0(a) = -1$ and $2 = 0$, a contradiction. We conclude that $b - a \in R$ for all $b \in R^{\cdot}$. If $\mathbb{Z}a + b \subset Rab$, we are done.

Otherwise, choose r such that $b^{'} = b - ra \in R$ and $b^{'} - a \notin R$. From our discussion above, we conclude that $b^{'} \in R^0$. But then the classification below, which does not depend on this case, implies that Rab' is $W_2, S_2,$ or T_2: Nos. $7, 10, 11$ of Table I. But then $Rab^{'} = T_1$, since $R^{\cdot}$ is empty for $R = W_2$ or S_2 in which case $b \in T_2$ and $T_2 = R \supset Ra + Rb = W \oplus A$ as asserted.

Theorem 4.8.3.

Every non classical irreducible rank 1 or 2 Lie root system defined over $\mathbb{Z}_p$ R is one of $W, W \oplus A, W_2, S_2, T_2$.

Proof:

Let R be non classical, irreducible and not one of $W, W\oplus A, W_2$. We claim that R is S_2, or T_2, as asserted. Since R is not classical it is not reduced, so that there exist $a \in R^0$ by (Def 4.7.1). We know that R is an irreducible rank 2 root system defined over $\mathbb{Z}_p$. Letting V be the $\mathbb{Z}_p$-span of R, we have $R \subset \mathbb{Z}a + \mathbb{Z}b = V$ for any $b \in V - \mathbb{Z}a$.

Suppose first that $(b + \mathbb{Z}a) \cap R = \phi$ for some $b \in V - \mathbb{Z}a$. Then $c \in R - \mathbb{Z}a$ implies that $c \notin R^0$, so that $c \in R^{\cdot}$. But then it follows from the proven part of (Theorem 4.8.2) that $c + \mathbb{Z}a \subseteq R$, so that $R \supseteq \mathbb{Z}a + \{-c, 0, c\} = W\oplus A$. Moreover, any element $d \in R - \mathbb{Z}a$ has the form $d = r(c + ta)$ with $c + ta \in R^{\cdot}$ (just as in the above case $r = 1, t = 0$), so that $r = \pm 1$ and $d \in \pm c + \mathbb{Z}a$. It follows that $R = W\oplus A$.

Suppose next that $(b + \mathbb{Z}a) \cap R \neq \phi$ for every $b \in V - \mathbb{Z}a$. Then $(b + \mathbb{Z}a) \cap R$ has more than one element for every $b \in V - \mathbb{Z}a$, by (Theorem 4.8.1) and the irreducibility of R. But then $(b + \mathbb{Z}a) \cap R$ has at least $p - 1$ elements for every $b \in V - \mathbb{Z}a$, by (Def 4.7.1). Take $c \in V - \mathbb{Z}a$ with $\mathbb{Z}c \cap R$ as small as possible. Then $R \subseteq \mathbb{Z}a + \mathbb{Z}c$ and $\mathbb{Z}c \cap R$ has one or three or p elements. If $\mathbb{Z}c \cap R$ has p elements, then $R = W_2$. If $\mathbb{Z}c \cap R$ has only one element, namely 0, then each set $(\mathbb{Z}a + jc) \cap R$ $(j \neq 0)$ has exactly $p - 1$ elements in it and $R = \big((\mathbb{Z}a + \mathbb{Z}c) - \mathbb{Z}c\big) \cup \{0\} = S_2$. In the remaining case, $\mathbb{Z}c \cap R$ has three elements, which we may take to be $\{-c, 0, c\}$ with no loss in generality. Then R contains $ia + jc$ when $i \neq 0$ and $j \neq \pm 1$. It follows that R contains four or more, hence all p, multiples of every $b \in V - \mathbb{Z}c$. Thus, $R = (\mathbb{Z}a + \mathbb{Z}c - \mathbb{Z}c) \cup \{-c, 0, c\} = T_2$.

4.9 Base and Closure

Let $(V, R), (W, S)$ be root systems and consider $R\oplus S = \{a\oplus b | a \in R, b \in S\} \subset V\oplus W$.

Introduce

$r_{a\oplus b}(c\oplus d) = c\oplus d - (a\oplus b)^0(c\oplus d)\ (a\oplus b)$b specifying$(a\oplus b)^0 \in Hom(V\oplus W, \mathbb{Z}_p)$ as follows:

$(a\oplus 0)^0(c \oplus d) = a^0(c)$

$(a\oplus b)^0(c \oplus d) = b^0(d) \qquad (b \neq 0)$

Note that $R + S_{c\oplus d}(a\oplus 0) = R_c(a)\oplus d$ and $r_{a\oplus 0}(c\oplus d) = c\oplus d - a^0(c)\ (a\oplus 0) = r_a(c)\oplus d$. Next, suppose that R is a group, that is , $R + R = R$, and note that

$R + S_{c\oplus d}(a\oplus b) = \{c\oplus d - r(a\oplus b), \dots, c\oplus d + q(a\oplus b)\}$, where

$S_d(b) = \{d - rb, \ldots, d + qb\}$, so that $d + qb = r_b(d - rb) = (d - rb) - b^0(d - rb)b$ implies $c \oplus d + q(a \oplus b) = r_{a+b}(c \oplus d - r(a \oplus b))$. It follows that $V \oplus W, R \oplus S$ is a root system, provided that R is a group (**TableIII**).

Next, let $V = \mathbb{Z}_p^n$ with basis $a_1, \ldots, a_n$. Consider $S_n = \{0\} \cup \{r_1 a_1 + \cdots . + r_n a_n | r_1 + \cdots . + r_n \neq 0\}$ and note that $S_n = \{v \in V | f(v, v) \neq 0\}$, where f is the symmetric bilinear form $f(a_i, a_j) = 1$ for all i, j. Then S_n is a Lie root system

TABLE III

Rootsystems Constructed from a Given Rootsystem R

$G \oplus R$	(G finite subgroup of k^+)
$W_n \oplus R$	($W_n = \mathbb{Z}_p^n$)
$S_n + R = S_n \cup R = S_n(R) \subset \mathbb{Z}_p^n$	($n >$ rank R)

With the symmetries $r_a(b) = b - 2(f(a, b)/f(a, a))a = b - 2(\sum s_i / \sum r_i)a$ for $a = \sum r_i a_i$, $b = \sum s_i a_i$. The condition $0 = f(a, b) = (\sum r_i)^2$ defines the hyper-plane $V - S_n = W$ of dimension $n - 1$. Let (W, R) be any Lie root system in W. Then $S_n + R = S_n \cup R$ is a Lie root system:

$(S_n + R)_b(a) = \mathbb{Z}a + b$ and $a^*(b) = 0$ for $a \in S_n - \{0\}$, $b \in R$

$(S_n + R)_a(b) = a + \mathbb{Z}b$ for $a \in S_n - \{0\}$, $b \in R - [0\}$

$(S_n + R)_c(b) = R_c(b)$ for $\in R$, $b \in R - \{0\}$,

$(S_n + R)_b(a) = (S_n)_b(a)$ or $b + \mathbb{Z}a$ for $a, b \in S_n - \{0\}$, (use the latter if $b + ia \in R$ for some i).

Definition 4.9.1.

We define base for a Lie root system (V, R) to be a basis $\pi = \{a_1, \ldots, a_n\}$ for V contained in R such that

1. If $Ra_i a_j$ is type A_2, B_2 or G_2 then the diagram for a_i, a_j is

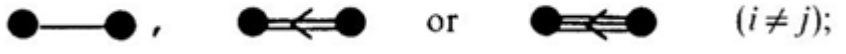


Fig (4.1)

2. $R = R^-(\pi) \cup \{0\} \cup R^+(\pi)$, where $R^-(\pi) = -R^+(\pi)$ and $R^+(\pi)$ is the set of those $a \in R$ for which there exist $a_{i_1}, \ldots, a_{i_s} \in \pi$ such that $\sum_{j=1}^{r} a_{i_j} \in R$ for $1 \leq r \leq s$ and $= \sum_{j=1}^{s} a_{i_j}$.

In characteristic 0, this is the usual concept of base, since condition (**1**) implies that $(a_i, a_j) \leq 0$ for all $i \neq j$ and condition (**1**) implies condition (**2**).

If R has base $a_1, \ldots., a_n$, then $W_m \oplus R$ has base $b_1, \ldots., b_m, a_1, \ldots., a_n$, where $b_1, \ldots., b_m$ is a basis for W_m as a group. And $S_m + R(m > n)$ has base $a_1, \ldots., a_n, a_{n+1}, \ldots., a_m$ obtained by taking any $\in S_m$, forming the independent set $a + a_1, \ldots., a + a_n, a$, showing that it is part of a base $a + a_1, \ldots., a + a_n, a = a_{n+1}, \ldots., a_m$ for S_m and then returning to $a_1, \ldots., a_n, a_{n+1}, \ldots., a_m$.

Definition 4.9.2:

A Lie root system (V, R) which has a base is said to be regular. A Lie root system (V, R) need not be regular. In fact, a classical root system (V, R) of type A_r where $p|(r+1)$ need not be regular, since it is possible that $\dim V' < r$. We illustrate this by describing two root systems $(V, R), (V', R')$ of type A_r $(p|(r+1))$ with (V, R) regular and (V', R') not regular.

For this , let k be a field of characteristic $p > 0$, let $e_0, \ldots., e_r$ be the basis of k^{r+1} with coordinate conditions $(e_i)_j = \delta_{ij}$, let $R = \{e_i - e_j \,|\, i \neq j, 0 \leq i, j \leq r\}$, let $\pi = \{a_j \,|\, 1 \leq i \leq r\}$ with $a_j = e_{j-1} - t_j$ and let V be the k-span of R. Then (V, R) is a root system of type A_r,π is a basis for (V, R) in the sense of (Def **4.9.1**) and (V, R) is regular.

Next assuming that $p|r+1$, note that V contains $e_0 + \cdots . + e_r$ and pass to quotients of V modulo $k(e_0 + \cdots . + e_r)$. Let $f(v) = v + k(e_0 + \cdots . + e_r)$ be the quotient map and define $v' = f(v)$, $V' = \{v' | v \in V\}$, $V' = \{a' | a \in R\}$. Then (V', R') is a root system of type A_r and $f: R \longrightarrow R'$ is an isomorphism of groupoids. Since a dimension is lost in passing from V to V', π' is not a basis for V' and (V', R') is not regular.

To by pass this pathology for classical root systems (V, R), we pass to their k-closures (H^*, R), described below. This passage corresponds, for certain Lie algebras $\mathfrak{g}$ to passage certain Lie algebras $H^* + \text{ad}\, \mathfrak{g}^\infty$ of derivations, $H^* = Hom(R, k)$, where $[h^*, x] = h^*(a)x$ for $a \in R$, $x \in \mathfrak{g}_a$, $h^* \in H^*$. When $\mathfrak{g}$ is classical, this Lie algebra is Der $\mathfrak{g} = H^* + \text{ad}\, \mathfrak{g}$, which since $\mathfrak{g}$ is center less and idempotent.

Definition 4.9.3.

$H = Hom(R, K) = \{f: R \to K | f(a + b) = f(a) + f(b)$ for all $a, d, a + b \in R\}$ iscalled the Cartan space of (V, R) and H_∞ denotes the k-span of its subset $\{a^0|_R | a \in R - \{0\}\}$. The groupoid homomorphism $R \to H^* = Hom_k(H, k)$ which sends $a \in R$ to $\bar{a} \in H^*$ defined by

$\bar{a}(f) = f(a)$ is called the k-closure homomorphism, and $\bar{R} = \bar{a}|a \in R$ is the set of roots of the Cartan space H.

We identify a^0 and a^0/R. Then the k-closure $(H^*, \bar{R})$ of (V, R) is a root system with Cartan functions $\bar{a}^0(\bar{b}) = a^0(b)$ and symmetries$r_a(\bar{b}) = \overline{r_a(b)}$ $(a, b \in R, \bar{a} \neq \bar{0})$.

Using k-closures and regular functions, we show in (Theorem 4.9.2) that we can pass from a classical root system (V, R) that may not be regular to an isomorphic root system $(H^*, \bar{R})$ which is regular .

If the k-closure homomorphism $R \to \bar{k}$ is an isomorphism of groupoids, and if it can be extended to an isomorphism of vector-spaces from V to H^*, then we say that (V, R) coincides, up to identification, with its k-closures.

Definition 4.9.4

(V, R) is k-closed if (V, R) coincides, up to identifications, with its k-closure. It is convenient to have passed from a root system (V, R) to its k-closure $(H^*, \bar{R})$, in order to have realized all latent independence among roots, as in the case of passage from $A_r(k)(p|r+1)$ covered by (Theorem **4.9.2**) below.

Moreover, R is isomorphic to $\bar{R}$ in the absence of the root system S_2, in which case we may simplify notation and work with the closed root system (H^*, R) with $R \subset H^*$,

$a^0 =_{def} h_a \in H_\infty$ and $a^0(b) = b(h_a) \in k$ for all $a \in R - \{0\}$..

We recall from Winter, the $\mathbb{Z}$-closure homomorphism $R \to \hat{R} = \{\hat{a}|a \in R\}$ from R into $H_{\mathbb{Z}} = Hom(R, \mathbb{Z}) \subset H_Q = Hom(R, Q) \subset H_{\mathbb{R}} = Hom(R, \mathbb{R})$, defined by $\hat{a}(f) = f(a)$, is an isomorphism of groupoids to a $\mathbb{Z}$-root system, provided that R is reduced. Thus, there exists a regular function on R that is a function $f \in H_{\mathbb{R}}$ such that $f(a) \neq 0$ for all $a \in R - \{0\}$, and we then define $R^{\pm} = R^{\pm}(f) = \{a \in R| \pm f(a) > 0\}$ and $\pi^{\pm} = \pi^{\pm}(f) = \{a \in R^{\pm}(f)\big|a$ is not contained in $R^{\pm}(f) = R^{\pm}(f)\}$. Conversely, let there exist a regular function $f \in H_{\mathbb{R}}$ for R. Then $f|_{Rab}$ is a regular function on the rank 2 root system Rab. A look at the possibilities for Rab,

Theorem 4.9.1.

A root system (V, R) is classical if and only if there is a regular function $f \in H_{\mathbb{R}}$ on R. For any regular function $f \in H_{\mathbb{R}}, \pi^+(f)$ is base for R if and only if $\pi^+(f)$ is linearly independent.

We observe that the closure $(H^*, \bar{R})$ of a classical root system R is a regular root system $\bar{R}$ isomorphic to R as groupoid such that:

$\overline{\pi^+(f)} = \{\bar{a}_1, \ldots\ldots, \bar{a}_r\}$ is a base for $\bar{R}$ for any regular function $f \in H_{\mathbb{R}}$ on R. For this, define $\hat{d}_i \in Hom(\hat{R}, \mathbb{Z})$ such that $\hat{d}_i(\hat{a}_j) = \delta_{ij}$ $(1 \leq i, j \leq r)$. This is possible since $\pi^+(\hat{f}) = \{\hat{a}_1, \ldots\ldots, \hat{a}_r\}$ is a base for $\hat{R}$, where $\hat{f} \in Hom(\hat{R}, \mathbb{Z})$ is defined by $\hat{f}(\hat{a}) = f(a)(a \in R)$. Then define $d_i : R \to K$ by taking $d_i(a)$ to be $\hat{d}_i(\hat{a})$ reduced modulo p. Then $d_i(\bar{a}_j) = \delta_{ij}$, so that

$\overline{\pi^+(f)}$ is a basis for $\bar{R}$ and $\bar{R}$ is a regular root system isomorphic to R.

Theorem 4.9.2.

The closure $(H^*, \bar{R})$ of a classical root system (V, R) is a regular root system with R isomorphic to $\bar{R}$ as groupoid and base $\bar{\pi} = \overline{\pi^+(f)}$.

4.10 Rigidity and Collapse under Core

In studying a root system R of Lie algebra $\mathfrak{g}$, it is important to understand the passage from R to Core R and from $\mathfrak{g}$ to Core $\mathfrak{g} = \mathfrak{g}^{\infty}/Nil\,\mathfrak{g}^{\infty}$. For this, we further develop concepts introduced in (Def **4.3.1**).

Definition 4.10.1

The core of a root system (V, R) is $(H_{\infty}^*, R_{\infty})$, where core $R = R_{\infty} = \{a_{\infty} | a \in R\}$ and $a_{\infty} = \bar{a}|_{H_{\infty}}$. Here, $a \longmapsto \bar{a}$ is the closure map and H_{∞} is the k-span o$\{a^0 | a \in R - \{0\}\}$. We call $R \longmapsto R_{\infty}$, sending a to $a_{\infty}(a \in R)$, the core map. If the core map is bijective, we say that R is rigid.

The following proposition is evident.

Proposition 4.10.1.

If R is rigid, the closure mapping is an isomorphism.

We say that a set $\{a_1, \ldots\ldots, a_n\}$ $(n \geq 2)$ of n distinct roots collapse if $a_{1_{\infty}} = \cdots = a_{n_{\infty}}$. The following theorem on collapse shows that R is rigid (has no collapse) if R has no root system Rab of type S_2.

Theorem 4.10.1.

Let $\{a_1, \ldots\ldots, a_n\}$ collpase. Then $Ra_1 \ldots a_n = R \cap (\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n)$ is a root system of type S_m for some m.

Proof:

Without loss of generality, take $a_1, \ldots, a_n$ linearly independent.

First, take distinct elements $a, b \in \{a_1, \ldots, a_n\}$. Note that $b - a \notin R$: for otherwise

$2 = (b-a)^0(b-a) = (b-a)^0(b_\infty - a_\infty) = 0$. Thus, $R_b(a) = \{b, \ldots, b + qa\}$, where $-q = a^0(b) = a^0(b_\infty) = a^0(b_\infty) = a^0(b) = 0$, and $R_b(a) = \{b, \ldots, b - 2a\}$.

Similarly, $R_b(a) = \{a, \ldots, a - 2b\}$.As in section 4.8, we now proceed to cogenerate roots and non-roots of S_2, as in Table II. Note that no difference $mb - ma = m(b-a)$ is a root.

For this, observe that $2b - a, a \in R$ with $2b - a \notin R$: for otherwise

$(2b-2a)^0(2b-2a) = (2b-2a)^0(2b_\infty - 2a_\infty) = 0$. Similarly, $2a - b, b \in R$ with $2a - 2b \notin R$. This generalizes easily to $mb - (m-1)a, a \in R$, with $m(b-a) \notin R$. Therefore, this cogeneration leads to $Rab = \{ra + sb | r + s \neq 0\} = S_2$. Next, suppose that we have $m \geq 2$ such that $a = \sum_1^m r_i a_i \in R$ for $\sum_1^m r_i \neq 0$. For any such a,consider $b = (\sum_1^m r_i)\, a_{m+1}$ and note that $b - a \notin R$; otherwise

$2 = (b-a)^0(b-a) = (b-a)^0(b_\infty - a_\infty) = \sum_1^m r_i\, (b-a)^0(b_{m+1\infty} - a_{i\infty}) = 0.$

Thus, $R_b(a) = \{b, \ldots, b + qa\}$, where $-q = a^0(b) =$ etc.$= a^0(b) = 2$, and

$R_b(a) = \{b, \ldots, b - 2a\}$. Similarly, $R_b(a) = \{a, \ldots, a - 2b\}$. It follows that

$a = \sum_1^m r_i a_i \in R$, provided that $\sum_1^{m+1} r_i \neq 0$. By induction, therefore, R contains S_n. Finally, let $a = \sum_1^n r_i a_i \in R$ and suppose that $\sum_1^n r_i = 0$. Then $a_\infty = 0$, which is impossible:

$2 = (a)^0(a) = (a)^0(a_\infty) = 0$. it follows that $Ra_1 \ldots \ldots a_n = S_n$.

4.11 Lie Root System Excluding T_2

A Lie root system R has a closure $\hat{R} = \{\hat{a} | a \in R\}$ over the field $\mathbb{R}$ of real numbers, and a closure homomorphism $R \to \hat{R}$ sending $a \in R$ to $\hat{a} \in H^* = Hom_{\mathbb{R}}(H, \mathbb{R})$, where $\hat{a}$ is defined by $\hat{a}(f) = f(a)$ for $f \in H = Hom_{Groupoid}\ (H, \mathbb{R}^+)$, $\mathbb{R}^+ = (\mathbb{R}, +)$: $\widehat{a+b} = \hat{a} + \hat{b}$ for $a, b, a + b \in R$. We let $\mathbb{R}\hat{R}$ denote the $\mathbb{R}$-sapn of $\hat{R}$ in H^*. The closure $\left(\mathbb{R}\hat{R}, \hat{R}\right)$ of (V, R) is a root system over $\mathbb{R}$ in the sense of Winter :

1. Each $\hat{a} \in \hat{R} - \{\hat{0}\}$ has an associated $\hat{a}^0 \in Hom_{\mathbb{R}}\left(\mathbb{R}\hat{R}, \mathbb{R}\right)$, with $\hat{a}^0(\hat{a}) = 2$ defined by the condition $r_{\hat{a}}\left(\hat{b}\right) = \hat{b} - \hat{a}^0\left(\hat{b}\right)\hat{a}$, where $r_{\hat{a}}$ is defined as in (2) below;

2. Each $\hat{a} \in \hat{R} - \{\hat{0}\}$ has an associated symmetry $r_{\hat{a}} \in Aut_{\mathbb{R}}(\mathbb{R}\hat{R})$ defined as $r_{\hat{a}} = \hat{r}_a$, where $\hat{s} \in Aut_{\mathbb{R}}(\mathbb{R}\hat{R})$ is as defined below for $s \in Aut\ R$.

Here, we define $\hat{s} = s^{**}|_{\mathbb{R}\hat{R}}$, where $s^* \in Aut_{\mathbb{R}}\ H$ and $s^{**} \in Aut_{\mathbb{R}}\ H^*$ are the adjoints of $s, s^*(f) = f \circ s(f \in h), s^{**}(g) = g \circ s^*(g \in H^*), \hat{s}(\hat{a}) = s^{**}(\hat{a}) = \hat{a} \circ s^*,$

$\hat{s}(\hat{a})(f) = \hat{a} \circ s^*(f) = \big(s^*(f)\big)9a\big) = (f \circ s)(a) = f\big(s(a)\big) = \widehat{s(a)}(f)(a \in R, f \in H).$

Thus, $\hat{s}(\hat{a})\widehat{s(a)}$ and $r_{\hat{a}}(\hat{b}) = \widehat{r_a(b)}$.

Note that $\hat{a} \in \hat{R} - \{\hat{0}\}$ implies that $\hat{R}_{\hat{b}}(\hat{a})$ is bounded, thus that $R_b(a)$ is bounded and $a^0(b) = a^*(b)$ mod p, where $a^*(b)$ is the Cartan integer in the sense of Bouraki with 0 added. The following theorem is needed for the proof of the main theorem. It is a variation of (Theorem **4.5.2**).

Theorem 4.11.1.

Let R be a Lie root system. Then

1. $R_a(b)$ is bounded and $\hat{a}^*(\hat{b}) = a^*(b)$ for all $a, b \in R, \hat{a} \neq \hat{0}$;

2. For any $a, b \in R, \hat{a} = \hat{0}$, there exists $c \in R$ such that the closure mapping maps $R_c(a)$ bijective onto $R_{\hat{b}}(\hat{a})$;

3. The closure mapping $R \to \hat{R}$ is an isomorphism (of groupoids) if and only if it is bijective.

$R_a(b)$ is bounded for $\hat{a} \neq \hat{0}$, as noted above, so that r_a can be written in terms of the Cartan integers $a^*(b) = r_a(b) = b - a^*(b)a$. Hence forth, we assume that no pair of type T_2 occurs in R. We then proceed to prove the Decomposition Theorem announced in the introduction.

Theorem 4.11.2.

Let R be a Lie root system excluding T_2 and let $\hat{a}_1, \ldots., \hat{a}_r$ be a base for the classical root system $\hat{R}$. Then $S = \{n_1 a_1 + \cdots + n_r a_r | n_i \in \mathbb{Z}, \hat{n}_1 \hat{a}_1 + \cdots + \hat{n}_r \hat{a}_r \in \hat{R}\}$ is a classical root system isomorphic to $\hat{R}$ and $R \subset R_0 + S$, where R_0 is a Witt root system given by

$R_0 = \{a \in R | \hat{a} = \hat{0}\}$.

Proof:

From Table I, $b^*(a) = 0, -1, -1, -1, -2, -3, 0, 0, -2$ in types $A \vee A, A_2, B_2$ long G_2 long B_2 short B_2 short, $W \vee A, W \oplus A$, mixed $W \oplus A$ classical, since R excludes T_2. These are the

Cartan integers, up to sign, for all classical b and all classical or Witt a. Since $b^0(c+d) = b^0(c) + b^0(d)(c,d \in kR)$, it follows that $b^*(c+d) = b^*(c) + b^*(d)$ $(c,d \in kR)$ for $b \in R^{\cdot}$. this verified for $p > 7$ by considering the integers $b^*(c)$ modulo p:

$b^*(c+d) = b^*(c) + b^*(d)$ $(c,d \in kR)$modulo p with $-3 \leq b^*(c), b^*(d), b^*(c+d) \leq 3$ implies $b^*(c+d) = b^*(c) + b^*(d)$. For $p = 5$ and 7, it follows from the characteristic 5 and 7 theory developed in (Section **4.1**).

Consequently, the groupoid dual $H = Hom\,(R, \mathbb{R})$ of R over $\mathbb{R}$ contains $b^*(b \in R^{\cdot})$.

Consider the $\mathbb{Z}$-closure mapping $R \longrightarrow \hat{R} = \{\hat{a} | a \in R\}$ described in (section **4.9**), which a groupoid homomorphism from R to the classical root system $\hat{R}$. Note that $\hat{a} = \hat{b} \Leftrightarrow f(a) = f(b)$ for all $f \in H = Hom\,(R, \mathbb{R})$. We claim that $R^0 = \{a \in R | a$ is Witt root $\}$ is the kernel $\{a \in R | \hat{a} = \hat{0}\}$ of $R \longrightarrow \hat{R}$. Since $\hat{a}, 2\hat{a}, \ldots, (p-1)\hat{a} \in \hat{R}$ for $a \in R^0$, and since $\hat{R}$ is classical, we have $\hat{a} = \hat{0}$ for $a \in R^0$.

Next, let $b \in R^{\cdot}$. then $b^* \in H = Hom\,(R, \mathbb{R})$, as observed above , so that $\hat{b}(b^*) = b^*(b) = 2$.

It follows that $\hat{b} \neq \hat{0}$. Thus, $R^0 = R - R^{\cdot}$ is the kernel $\{a \in R | \hat{a} = \hat{0}\}$ is a Lie root system, R^0 is Witt Lie root system. We now construct a copy S of the classical root system $\hat{R}$ in R such that $R \subset R^0 + S$. A part of this construction was done in collaboration with M. Let $\hat{f} \in H = Hom_{\mathbb{R}}\left(\mathbb{R}\hat{R}, \mathbb{R}\right)$ be regular on the root system $\hat{R}$, that is $\hat{f}(\hat{a}) \neq \hat{0}$ for $\hat{a} \in \hat{R} - \{0\}$.

Define $f: R \to \mathbb{R}$ by $f(a) = \hat{f}(\hat{a})$. Let $\langle \hat{a}, \hat{b} \rangle$ be a positive definite symmetric bilinear form on $\mathbb{R}\hat{R}$ such that $\hat{a}^*(\hat{b}) = 2(\langle \hat{a}, \hat{b} \rangle / \langle \hat{a}, \hat{a} \rangle \left(\hat{a}, \hat{b} \in \hat{R} - \{\hat{0}\}\right)$, define $\langle a, b \rangle = \langle \hat{a}, \hat{b} \rangle$ $(a \in R^{\cdot}, b \in R)$ and note that $a^*(b) = \hat{a}^*(\hat{b}) = \langle \hat{a}, \hat{b} \rangle = \langle a, b \rangle$ $(a \in R^{\cdot}, b \in R)$.

Observe, accordingly that if $\langle a, b \rangle > 0$, then $b - a \in R$ $(a \in R^{\cdot}, b \in R)$.

Let $\hat{R}^+ = \{a \in \hat{R} | \hat{f}(\hat{a}) > 0\}$ and $R^+ = \{a \in R | f(a) > 0\}$.

Let $a_1, \ldots\ldots, a_r$ be any elements of R such that $\hat{\pi} = \{\hat{a}_1, \ldots\ldots, \hat{a}_r\}$ is the set of simple roots $\hat{R}^+$ in the classical root system $\hat{R}$. We claim first that $S^+ = \{n_1 a_1, \ldots\ldots, n_r a_r | n_i \in \mathbb{Z}, n_1\,\hat{a}_1, \ldots\ldots, n_1 \hat{a}_r \in \hat{R}^+\}$ is contained in R^+ and that

$\widehat{R_b(a_j)} = R_{\hat{b}}(\hat{a}_j)$ for $\hat{b} = \sum n_i \hat{a}_i \in \hat{R}^+$. We proceed by induction on the height $h(\hat{b}) = \sum n_i$ of $\hat{b}$. If $h(\hat{b}) = 1$, $\hat{b} = \hat{a}_i$ and $a_i \in S^+$ for some i. Moreover, $a_i - a_j \notin R$, since $\hat{a}_i - \hat{a}_j \notin \hat{R}$: $a_i - a_j \in R \Longrightarrow \hat{a}_i - \hat{a}_j = \hat{a}_i + \left(\widehat{-a_j}\right) - \widehat{a_i - a_j} \in R$. Since $a_j^*(a_i) = \hat{a}_j^*(\hat{a}_i)$ and

$R_{a_i}\ (a_j) = \{a_i, \ldots., a_i - a_j^*(a_i)a_j\}$ maps onto $\hat{R}_{\hat{a}_i}\ (\hat{a}_j) = \{\hat{a}_i, \ldots., \hat{a}_i - \hat{a}_j^*(\hat{a}_i)\hat{a}_j\}$, which establishes over assertion for $\hat{b} = \hat{a}_i$ and $h(\hat{b}) = 1$

Next, let $h(\hat{b}) > 1$ and suppose that our assertion has been establish for $h - 1$. Since $\widehat{a_1}, \ldots, \widehat{a_r}$, $\hat{b}$ are lineary dependent elements of $\hat{R}^+$ and $\langle \widehat{a_i}, \widehat{a_j} \rangle < 0$ for all $i \neq j$, we have $\langle \hat{b}, \widehat{a_j} \rangle > 0$ for some i. But then $\hat{b} - \widehat{a_j} = \sum_n j\, \widehat{a_j} - \widehat{a_i} \in \hat{R}^+$. With $h(\hat{b} - \widehat{a_i}) = h(\hat{b}) - 1$. By induction, therefore $c = \sum n_j a_j - a_i$ is in R and

$$\widehat{R_c(a_i)} = R_{\hat{c}}(\widehat{a_i}) = R_{\hat{b}-\widehat{a_i}}\ (\widehat{a_i}) = R_{\hat{b}}(\widehat{a_i}) \ni \hat{b} = \hat{c} + \widehat{a_i}.$$

We do not yet know that $\sum n_j a_j \in R$. However, we know that some element of $R_c(a_i)$ maps to $\hat{c} + \widehat{a_i}$, and this element, by virtue of its f-value, must be $c + a_i = \sum n_j a_j =_{def} b$. This said, we may conclude that $b = \sum n_j a_j \in R^+$ and moreover, that

$\widehat{R_b(a_i)} = R_{\widehat{b-a_i}}(a_i) = \widehat{R_c(a_i)} = R_{\hat{b}}(\widehat{a_i})$ by what are shown above.

It remains to show that $R_b(a_j) = R_{\hat{b}}(\widehat{a_j})$ for $j \neq i$. If $\hat{b} - \widehat{a_j} \in \hat{R}^+$, we argue by induction, just as in the case $j = i$ above. We conclude, by induction that $S^+ \subset R^+$ and

$R_b\widehat{(a_j)} = R_{\hat{b}}(\widehat{a_j})$, since $a_j^*(\hat{b}) = \hat{a}_j * (\hat{b})$, with details as in the similar case encountered above. We conclude, by induction that $S^+ \subset R^+$ and $R_b\widehat{(a_j)} = R_{\hat{b}}(\widehat{a_j}) = R_b(a_j)$ for $b \in S^+$, as asserted.

Implicitly derived in the above considerations is the decisive identity $\hat{b} = \sum n_i\, \widehat{a_i}$, valid for any $\sum n_i\, a_i \in \hat{R}^+$ and $b = \sum n_i\, \widehat{a_i} \in S^+$. This is based on the implicit iterative construction/ reconstruction of elements $b \in S^+/\hat{b} \in \hat{R}^+$ as $b = a_{i_1}, \ldots., a_{i_k}$ and $\hat{b} = \hat{a}_{i_1}, \ldots., \hat{a}_{i_k}$, where all partial sums are roots in S^+, respectively in $\hat{R}^+$.

We claim next that $R \subset R^0 + S$. Suppose not, and take $b \in R^+ - (R^0 + S)$ with $f(b)$ minimal, noting that $\hat{b} \in \hat{R}^+$. We claim, firstly that $b - a_i \in R$ for some $1 \leq i \leq r$. For this, note that $\hat{a}_1, \ldots., \hat{a}_r\ , \hat{b} \in \hat{R}^+$ are linearly dependent and $\langle \widehat{a_i}, \widehat{a_j} \rangle < 0$ for all $1 \leq i \neq j \leq r$, so that $\langle \hat{b}, \widehat{a_i} \rangle > 0$ for some i. But then $\langle b, a_i \rangle > 0$ for some i, so that $b - a_i \in R$.

Next, we observe that $b \in R^0 + S$, contrary to assumption. In the case $\hat{b} = \hat{a}_i$, we have $b - a_i \in R$ (see above) and $\hat{b} - \hat{a}_i = \hat{0}$, so that $b - a_i \in R^0$ and $b = (b - a_i) + a_i \in R^0 + S$. In the case $b \neq a_i$, $b - a_i \in R$, we have $b - a_i \in R$ (as above), $\hat{b} - \widehat{a_i} \in \hat{R}^+$. But then

$b - a_i \in R^+$ with $f(b - a_i) < f(b)$. By minimality of $f(b)$, $b - a_i \in R^0 + S$. But then $b \in R^0 + S$.

To see this, write $b - a_i = a + \sum n_j a_j$, where $a \in R^0$ and $\sum n_i a_i \in \hat{R}^+$.

Then $\hat{b} - \hat{a}_i = \sum n_i \hat{a}_i \in \hat{R}^+$ and $\hat{b} = n_1\hat{a}_1 + \cdots + n_{i-1}\hat{a}_{i-1} + (n_i + 1)\hat{a}_i + n_{i+1}\hat{a}_i + \cdots + n_r\hat{a}_r$. Thus, $b = a + n_1a_1 + \cdots + n_{i-1}a_{i-1} + (n_i + 1)a_i + n_{i+1}a_i + \cdots + n_ra_r$.

And $b \in R^0 + S$, by the definition of S, contrary to assumption. Thus, $R \subset R^0 + S$ as asserted.

Finally, S has at most as many elements as $\hat{R}$, by its constructional definition, and $\hat{R} \subset \widehat{R^0 + S} = \hat{S}$, so that $S \longrightarrow \hat{S}$ is surjective from S to $\hat{R}$. It follows that $S \longrightarrow \hat{S}$ is bijective from S to $\hat{R}$, so that $S \longrightarrow \hat{R}$ is an isomorphism ,by (Theorem **4.11.1**) , which completes the proof of (Theorem **4.11.2**), since the root system $\hat{R}$ is classical.

Finally, we briefly consider subsystems. Consider a subset σ of $\pi = \{a_1, \dots, a_r\}$, where $\hat{\pi} = \{\hat{a}_1, \dots, \hat{a}_r\}$ is a simple system of $\hat{R}$, $\sigma = \{a_1, \dots, a_k\}$. Construct $R_\sigma = R_{a_1 \dots a_k} = \{n_1a_1 + \cdots + n_ka_k | n_1\hat{a}_1 + \cdots + n_k\hat{a}_k \in \hat{R}\}$. Then $\hat{R}_\sigma = \hat{R} \cap (\mathbb{Z}\hat{a}_1 + \cdots + \mathbb{Z}\hat{a}_k) = R\hat{a}_1 \dots \hat{a}_k$ is a classical root system and $\hat{R}_\sigma^{-1} =_{def} \{a \in R | \hat{a} \in \hat{R}_\sigma\}$ is a root system R^σ. Relative to the global closure maps $R \longrightarrow \hat{R}$, the same arguments as above show that $R^\sigma \subset R^{\sigma^0} + R_\sigma$, where R_σ, as defined above is a classical subsystem of R^σ. Both the global closure map and the closure map defined relative to R^σ map R_σ isomorphically to the image (closure in either sense) of R^σ.

Taking $\hat{\pi} = \hat{\pi}_1 \cup \dots \cup \hat{\pi}_n$ to be the decomposition of $\hat{\pi}$ into connected components, and letting $R^i = R^{\pi_i}$ and $R_i = R_{\pi_i}$, one now easily sees that :

1. $R = R^1 \cup \dots \cup R^n$

2. $a, b \in R^i, a + b \in R \Longrightarrow a + b \in R^i$

3. $R^i \subset R^{i0} + R_i$ with R_i irreducible and classical and R^{i0} Witt.

Next, take any $b \in R - R^0$, so that $\hat{b} \neq \hat{0}$, and take a simple system $\hat{\pi} = \{\hat{a}_1, \dots, \hat{a}_r\}$ for $\hat{R}$ such that $\hat{b} = \hat{a}_1$. This is possible, since $\hat{R}$ is reduced and a classical root system. In this case, R_b as define above is $R_b = \{-b, 0, b\}$.

We write $R^b = R^{\{b\}} = \hat{R}_b^{-1} = \{a \in R | \hat{a} \in \hat{R}_b\}$. Then $R^b \subset R^{b0} + R_b$.

Let $a \in R^{b0}$. If $a + b \in R$, then $Rab = R \cap (\mathbb{Z}a + \mathbb{Z}b)$ is type $W \oplus A$, by the exclusion of T_2 and consequently, $a - b$ is in R^b as well. It follows that $a + R_b \subset R^{b0}$ if $a + b \in R$, so that $R^b = U_{a \in R^0, b \in R\ ; a+b \in R}\ a + R_b$, where $R^1 = R_\pi$ and $a + R_b = a + [-b, 0, b\}$

By the above arguments and the inclusion $R \subset R^0 + R^1$ established in (Theorem **4.11.2**).

4.12 Lie Algebras

i. Preliminaries

Throughout previous part of this chapter, k denotes a field of characteristic $p > 3$. The following results of part I on Lie root systems (V, R) and Cartan functions $a^0 \in Hom_k(V, k)$ play key roles in part II.

Proposition 4.12.1.

A reduced nonzero symmetry set in $\mathbb{Z}_p$ whose symmetries are the reversals $r_a(b) = -b$ must be $\{-a, 0, a\}$ for some $a \in \mathbb{Z}_p$.

Theorem 4.12.1.

Let R be a classical Lie symmetry system or reduced symmetry set. Then R is isomorphic as groupoid to a root system in the sense of Bouraki.

Theorem 4.12.2.

Let R have rank 1. Then $R = \{-a, 0, a\}$ or R is a subgroup of k^+.

Theorem 4.12.3.

Let $c, b \in R$ be k-linearly independent. Then $R \subset D$ is classical or one of W (irreducible rank), $W \biguplus A\ , W \biguplus W$ (reducible rank 2), $W \oplus A, W \oplus W$, S_2, T_2 (irreducible rank 2), there $W = \{0, a, \ldots., (p-1)a\} = \mathbb{Z}a$, $A = \{-b, 0, b\}$, $W \oplus A = \{ia + jb | j = \pm 1\ or\ 0\}$, $W \oplus W = \mathbb{Z}_p^2$, $S_2 = \{(i, j) | i + j \neq 0\}$, $T_2 = S_2 \cup \{(m, -m), (0,0), (-m, m)\}$.

Theorem 4.12.4.

Let $R \to R|_{H_\infty} = R_\infty$ be the core map and let $a_1, \ldots., a_n$ $(n \geq 2)$ be k-independent elements of R such that $a_{1_\infty} = \cdots . = a_{n_\infty}$. Then $Ra_1 \ldots . a_n = R \cap (\mathbb{Z}a_1 + \cdots . + \mathbb{Z}a_n)$ is type of S_n.

We need the following theorems on representations of 3 dimensional Lie algebra $L = ke + kh + kf$ with $[e, f] = h$, $[h, e] = e$, $[h, f] = -f$. Suppose that the set of characteristic roots is $\{b, b+1, \ldots., b+j\}$. Then $j = p - 1$ or $2b = -j$.

In any $\mathfrak{g}$-module $V, \mathfrak{g}$ a Lie algebra over k, we define $(x-a)v = xv - av$ and $(x-a)^{n+1}v = (x-a)(x-a)^i v$ recursively for $x \in \mathfrak{g}, a \in k, v \in V$; and we let $V_a^i(x) = \{x \in V | (x-a)^i v = 0\}$.

Theorem 4.12.5.

Let $\mathfrak{g} = ke + kh + kf$, where $[e,f] = h$ and $[h,\mathfrak{g}] = 0$. Let V be an $\mathfrak{g}$-module such that $e^{p-1}V = 0$. Then $h^n V = 0$ for some n.

Proof:

Let $b \in k$, be an eigen value for h on V. Choose $v \in V - \{0\}$ satisfying $hv = bv$, subject to the constraint that the corresponding integer n such that $e^n v \neq 0$ and $e^{n+1}v = 0$ is maximal. Note that $n+1 \leq p-1$. Define $[e^n, f]v = e^n(fv) - f(e^n v)$, and note that $[e^n, f]v = 0$, since $f(fv) = bv$ and consequently, $e^{n+1}(fv) = 0$ by the constraint on v. Once can show, by induction, that $0 = [e^{n+1}, f]v = (n+1)b\, e^n v$. Thus, $0 = (n+1)b$ and $b = 0$. Consequently, h is nilpotent on V.

ii. Reductive Lie algebras

Let $\mathfrak{g}$ be a Lie algebra. Let $\mathfrak{g} = \mathfrak{g}_1 \supsetneq \mathfrak{g}_2 \supsetneq \cdots \supsetneq \mathfrak{g}_{n+1} = 0$ be a maximally refined chain of ideals of $\mathfrak{g}$ and $\mathfrak{g}_2 \oplus \ldots \oplus \mathfrak{g}_n$ where $\bar{\mathfrak{g}}_i = \mathfrak{g}_i/\mathfrak{g}_{i+1}$ $(1 \leq i \leq n)$. Then the ideal Nil

$\mathfrak{g} = \{x \in \mathfrak{g} | [x, \mathfrak{g}_1] \subset \mathfrak{g}_{n+1}\ (1 \leq i \leq n)\}$ consists of nilpotent elements and is called the nil radical of $\mathfrak{g}$. Note that $\mathfrak{g}/\text{Nil}\,\mathfrak{g}$ has the faithful completely reducible module $\bar{\mathfrak{g}} = \bar{\mathfrak{g}}_2 \oplus \ldots \oplus \bar{\mathfrak{g}}_n$ it follows, as in the proof of (Theorem **4.12.6**) below, that Nil $\mathfrak{g}$ contains every other ideal I of $\mathfrak{g}$ such that $ad_{\mathfrak{g}} I$ consist of nilpotent elements : $I\bar{\mathfrak{g}} = \{\bar{0}\}$ and therefore $I \subset$ Nil $\mathfrak{g}$. That is Nil $\mathfrak{g}$ is the unique maximal ideal such that ad Nil $\mathfrak{g}$ consists of nilpotent elements.

Definition 4.12.1.

$\mathfrak{g}$ is reductive if Nil $\mathfrak{g}$ is central in $\mathfrak{g}$.

Theorem 4.12.6.

$\mathfrak{g}$ is reductive if and only if ad $\mathfrak{g}$ has a faithful completely reducible representation which preserves nilpotency of elements of ad L.

Proof :

If $\mathfrak{g}$ is reductive, the representation afforded to ad $\mathfrak{g}$ by the $\mathfrak{g}$-module $\bar{\mathfrak{g}} = \bar{\mathfrak{g}}_2 \oplus \ldots \oplus \bar{\mathfrak{g}}_n$ is such a faithful completely reducible representation. Conversely, let $V = N_1 \oplus \ldots \oplus V_n$ be a

representation for ad $\mathfrak{g}$ with nonzero irreducible submodules $V_1, \dots, V_n$. Let ad N be an ideal of ad $\mathfrak{g}$ consisting of nilpotent elements, and assume that ad N acts by nilpotent transformations on V. Since ad N is an ideal of ad $\mathfrak{g}$, $V_{io} = \{v \in V_i | \text{ad } N, v = 0\}$ is a nonzero ad $\mathfrak{g}$-submodule of V_i, so that $V_i = V_{io}$ for $1 \leq i \leq n$. Thus, $(\text{ad } N)V = 0$. It follows that $N = \{0\}$ and N is central in $\mathfrak{g}$ if V is faithful. Thus, $\mathfrak{g}$ is reductive.

Theorem 4.12.7.

$\mathfrak{g}$ is reductive if and only if every solvable ideal is central in $\mathfrak{g}$.

Proof:

One direction is trivial, since Nil $\mathfrak{g}$ is nilpotent and therefore solvable. For the other, suppose that $\mathfrak{g}$ is reductive and let I be a solvable ideal of $\mathfrak{g}$. We show by induction on the dimension of I that I is central.

Suppose first that I is nilpotent. Then ad I is an ideal consisting of nilpotent elements since $[I, \dots . [I, \mathfrak{g}] \dots] \subset I^n = \{0\}$. Thus, I is central, by (Def 4.12.1). Next suppose that the assertion is true for solvable ideals of lower dimension than that of I and let J be the ideal $J = [I, I]$ by induction, J is central in $\mathfrak{g}$. Thus, I is nilpotent. But then I is central, as shown above.

Definition 4.12.2.

$\mathfrak{g}$ is semisimple if every solvable ideal of $\mathfrak{g}$ is 0.

Corollary 4.12.1.

$\mathfrak{g}$ is semisimple if and only if $\mathfrak{g}$ is reducible with center 0 if and only if Nil $\mathfrak{g} = 0$.

Proof:

One direction of the first implication is clear. For the other, suppose that $\mathfrak{g}$ is reductive with center 0, and let I be a solvable ideal of $\mathfrak{g}$. Then I is central , by ,(Theorem **4.12.7**). Thus, $I = \{0\}$. The remaining implication follows easily.

Definition 4.12.3.

Core $\mathfrak{g} = \mathfrak{g}^{\infty}/\text{Nil } \mathfrak{g}^{\infty}$, where $\mathfrak{g}^{\infty} = \bigcap_{i=1}^{\infty} \mathfrak{g}^i$. Since Center $\mathfrak{g}$ is the kernel of ad : $\mathfrak{g} \to \text{Der } \mathfrak{g}$, and since $[\text{d}, \text{ad } x] = \text{ad } d(x)$ for $d \in \text{Der } \mathfrak{g}$, $x \in \mathfrak{g}$, C = Center $\mathfrak{g}$ is stabilized by Der $\mathfrak{g}$. It follows that $\text{Der } (\mathfrak{g}, C) = \{d \in \text{Der } \mathfrak{g} | d(\mathfrak{g}) \subset C\} = Hom\,(\mathfrak{g}/\mathfrak{g}^{(1)}, C)$ is an ideal in Der $\mathfrak{g}$: $d \in \text{Der } (\mathfrak{g}, C)$, $e \in \text{Der}\mathfrak{g} \Rightarrow [d, e] = de - ed$ maps $\mathfrak{g}$ to 0. Note that $\text{Der } (\mathfrak{g}, C) \cap$

ad $\mathfrak{g} =$ Center ad $\mathfrak{g}$: ad $x\ (\mathfrak{g}) \subset C \Leftrightarrow [x, \mathfrak{g}] \subset C \Leftrightarrow [\text{ad}\ x, \text{ad}\ \mathfrak{g}] = 0$. We can now easily prove the following theorem.

Theorem 4.12.8.

Let $\mathfrak{g}$ be reductive. Then the solvable radical of Der $\mathfrak{g}$ is contained in Der $(\mathfrak{g}, C)$.

Proof:

Let I be a solvable ideal of Der $\mathfrak{g}$, so that $[I, \text{ad}\ \mathfrak{g}\ ] = \text{ad}\ I\ (\mathfrak{g}) \subset I \cap \text{ad}\ \mathfrak{g}$ is solvable ideal of ad $\mathfrak{g}$. Then $I(\mathfrak{g}) + C$ is central in $\mathfrak{g}$, since $\mathfrak{g}$ is reductive, so that $I(\mathfrak{g}) \subset C$ and $I \subset \text{Der}\ (\mathfrak{g}, C)$.

Corollary 4.12.2.

Suppose that $\mathfrak{g}$ is semisimple or that $\mathfrak{g}$ is reductive and idempotent in the sense that $\mathfrak{g} = \mathfrak{g}^2$. Then Der $\mathfrak{g}$ is semisimple.

Proof :

In either case, Der $(\mathfrak{g}, C) = Hom\left(\mathfrak{g}/\mathfrak{g}^{(1)}, C\right) = 0$.

Now consider Cartan decomposition $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ of $\mathfrak{g}$ with Cartan sub-algebra $H = \mathfrak{g}_0$. Note that $H_\infty = H \cap \mathfrak{g}^\infty = \sum_{a \in R - \{0\}} [\mathfrak{g}_{-a}, \mathfrak{g}_a]$ is a Cartan sub-algebra of $\mathfrak{g}^\infty$ if and only if $[H_\infty, \mathfrak{g}_b] = \mathfrak{g}_b$ for all $b \in R - \{0\}$, in which case ad $_L\ H_\infty$ contains Center ad $_{\mathfrak{g}}\ \mathfrak{g}^\infty$.

Theorem 4.12.9.

Let Der $(\mathfrak{g}^\infty, C)$ denote the set of derivatives of $\mathfrak{g}$ mapping $\mathfrak{g}^\infty$ into C. Then Der $(\mathfrak{g}^\infty, C)$ is deal of Der $\mathfrak{g}$ and Der $(\mathfrak{g}^\infty, C) \cap \text{ad}\ \mathfrak{g}^\infty =$ Center ad $\mathfrak{g}^\infty$.

Proof:

We have Der $\mathfrak{g} = D \rhd \text{ad}\ \mathfrak{g} > ad\ H$ with $[D, \text{ad}\ H\ ] \subset \text{ad}\ \mathfrak{g}$, so that $D = D_0\ \text{ad}\ \mathfrak{g}^\infty$ where $D_0 = D_0(\ \text{ad ad}\ H)$. We then have $D = \text{Der}\ \mathfrak{g} = \sum_{b \in R} D_b$ with $D_b = \text{ad}\ \mathfrak{g}_b\ (b \in R - \{0\})$.

It suffices to show that $[D_0, \text{Der}\ (\mathfrak{g}^\infty, C)\ ] \subset$ Der $(\mathfrak{g}^\infty, C)$, since $[\text{ad}\ \mathfrak{g}^\infty,$ Der $(\mathfrak{g}^\infty, C)] = 0$. Thus, take $d_0 \in D_0, d \in \text{Der}\ (\mathfrak{g}^\infty, C)$ and observe that $[d_0, d] = d_0 d - d d_0$ maps :

$\mathfrak{g}_a (a \in R - \{0\})$ to C: $d_0 d(\mathfrak{g}_a) \subset d_0(C) \subset C$ and $d d_0(\mathfrak{g}_a) \subset d(\mathfrak{g}_a) \subset C$. Thus, $[d_0, d]$ maps $\mathfrak{g}^\infty$ to C and $[d_0, d] \in \text{Der}\ (\mathfrak{g}^\infty, C)$.

Definition 4.12.4.

A Lie algebra $\mathfrak{g}$ is complete if $\mathfrak{g}$ has center 0 and Der $\mathfrak{g} =$ ad $\mathfrak{g}$.

Theorem 4.12.10.

Let $\mathfrak{g}$ be a Lie algebra over any field such that $\mathfrak{g} = \mathfrak{g}^2$ and Center $\mathfrak{g} = 0$. Then Der L is complete semisimple.

Corollary 4.12.3.

Let $\mathfrak{g}$ be semisimple with $\mathfrak{g} = \mathfrak{g}^2$. Then Der $\mathfrak{g}$ is complete semisimple.

Corollary 4.12.4.

Let $\mathfrak{g}$ be simple. Then Der $\mathfrak{g}$ is complete semisimple.

Theorem 4.12.11.

Let $\mathfrak{g}$ be semisimple. Then Der I is complete semisimple and Der $I \geq \mathfrak{g} \geq I$ (up to identifications) for $I = \mathfrak{g}^{(\infty)}$, in fact, for any idempotent ideal I of $\mathfrak{g}$ containing Scole $\mathfrak{g}$. If I is Der $\mathfrak{g}$ $-$ stable, then Der $\mathfrak{g}$ is normalize of $\mathfrak{g}$ in Der I.

4.13 Reflective and Toral Lie Algebras

Let L be a finite dimensional Lie algebra over k with split Cartan sub-algebra $H = L_0$ and root space decomposition $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$. Thus, $\mathfrak{g}_a = \{x \in \mathfrak{g} \nmid \big(ad\ h - a(h)\big)^{\dim L} x = 0$ for all $h \in H\}$ for a in the additive group H^* of functions from H to k, and $R = R(\mathfrak{g}, H) = \{a \in H^* | \mathfrak{g}_a \neq \{0\}\}$ is the set of roots of H on $\mathfrak{g}$.

Let V be an $\mathfrak{g}$-module, $V_b = \{v \in V | \big(h - b(h)\big)^{\dim V}, v = 0$ for all $h \in H\}$ and $S(V, H) = \{b \in H^* | V_b = \{0\}\}$, the set of weights of H in V.

Theorem 4.13.1.

Let $a \in R$ and let $S_b(a) = \{b - ra, \dots, b + qa\}$ be a bounded a-orbit in $S = S(V, H)$. Suppose that $h = [e, f]$, $[h, e] = a(h)\, e$, $[h, f] = -a(h) f$ with $e \in \mathfrak{g}_a$, $f \in \mathfrak{g}_{-a}$. Then

$2b(h) = (r - q)a(h)$. If $a(h) \neq 0$, then the reflection r_a reversing $S_b(a)$ is given by $r_a(c) = c - 2(c(h)/a(h))\, a (c \in S_b(a))$.

Proof:

First suppose that $a(h) \neq 0$ and let $h' = a(h)^{-1} h$. Then $2(b(h)^{-1} - r = -(q + r))$, so that $2b(h)^{-1} = r - q$ and $2b(h) = (r - q)a(h)$. Suppose next that $a(h) = 0$. Then $[e, f] = h$, $[h, e] = 0, [hf] = 0$ and $W = \sum_{c \in S_b(a)} V_c$ is a module for $N = ke + kh + kf$ such that $e^{p-1} W = 0$. It follows from theorem 7.7 that $h^n W = 0$ for some n, so that $b(h) = 0$,for $a(h) = 0$.

Let $c = b + ia$ and observe that: $c - 2(c(h)/a(h))\, a = (b + ia) - 2\big((b(h)/a(h)) + i\big)a$. Since $2(b(h)/a(h)) = r - q$, it follows that $c - 2(c(h)/a(h))\, a = b + (q - r - i)a = r_a(b + ia)$.

We let R_* be the set of those $a \in R$ such that $R_b(a)$ is bounded for all $b \in R$. We also define $\mathfrak{g}_a^1 = \{x \in \mathfrak{g}_a | [h, x] = a(h)x$ for all $h \in H\}$.

Theorem 4.13.2.

Let $a \in R_*$ and suppose that $h = [e, f]$ with $e \in \mathfrak{g}_a^{'}$, $\in \mathfrak{g}_{-a}^1$. Then

1. If $a(h) = 0$, ad h is nilpotent

2. If $a(h) \neq 0$, then $r_a(c) = c - 2(b(h)/a(h))\, a$ is symmetry of R at a;

3. If $a(h) \neq 0$, then $2a \notin R$.

Proof:

For (**1**), suppose that $a(h) = 0$. Since the $R_b(a)$ are bounded $(b \in R), k$ has characteristic $p \neq 2$. Since $2b(h) = (r - q) \quad a(h) = 0$, by (Theorem **4.13.1**), $b(h) = 0$ for all $b \in R$. Thus, ad h is nilpotent. Note that (2) follows directly from (Theorem **4.13.1**). For (**3**), consider $= kf + H + \mathfrak{g}_a + \cdots \mathfrak{g}_{qa}$, where $a, \ldots., qa \in R$ and $(q + 1)a \notin R$. Let $S = S(V, H)$, so that $S_0(a) = \{-a, 0, a, \ldots., qa\}$. Then $qa = r_a(-a) = a$, by (**2**). Thus, $S_0(a) = \{-a, 0, a\}$ and $2a \notin R$.

We recall the definition of classical Lie algebra.

Definition 4.13.1.

A Lie algebra $\mathfrak{g}$ with split Cartan subalgebra H is classical if $\mathfrak{g}$ has center 0, $\mathfrak{g}^{(1)} = \mathfrak{g}$, ad H is diagonalizable on $\mathfrak{g}$, $[\mathfrak{g}_a\ \mathfrak{g}_{-a}]$ is one dimensional and $R_b(a)(b \in R)$ is bounded for all $a \in R - \{0\}$.

We now introduce the reflective Lie algebra as diagonalizations of classical Lie algebras. In our definition, $[\mathfrak{g}_a^1\ , \mathfrak{g}_a^1\ ]$ denotes the span of $\{e, f | e \in \mathfrak{g}_a^1, f \in \mathfrak{g}_{-a}^1\ \}$.

Definition 4.13.2.

A Lie algebra $\mathfrak{g}$ with split Cartan subalgebra H is reflective if ad $[\mathfrak{g}_a^1\ , \mathfrak{g}_{-a}^1]$ has some nonnilpotent element and $R_b(a)(b \in R)$ is bounded for all $a \in R - \{0\}$.

Note that there are no reflective Lie algebra in characteristics 2 and 3, by the boundedness condition.

We let $\mathfrak{g}^{\infty} = \bigcap_{i=1}^{\infty} \mathfrak{g}^{i}$ and Core $\mathfrak{g} = \mathfrak{g}^{\infty}/\text{Nil}\,\mathfrak{g}^{\infty}$. If $\mathfrak{g} = \mathfrak{g}^{(1)} = \mathfrak{g}^{\infty}$, Recall that $\mathfrak{g}$ is idempotent. For any Cartan subalgebra H of $\mathfrak{g}$, we let $H_{\infty} = H \cap \mathfrak{g}^{\infty}$. Then $\mathfrak{g} = H + \mathfrak{g}^{\infty}$ and

$H_{\infty} = \sum_{a \in R-\{0\}} [\mathfrak{g}_a , \mathfrak{g}_{-a}]$, where $\mathfrak{g} = \sum_{a \in R-\{0\}} \mathfrak{g}_a$ is the Cartan decomposition of $\mathfrak{g}$ with $\mathfrak{g}_0 = H$.

The following theorem shows that reflective Lie algebras $(\mathfrak{g}, H)$ are roughly classified by corresponding classical root systems $R(\mathfrak{g}, H)$, defined and described before. For classical Lie algebras $(\mathfrak{g}, H)$ this classification $(\mathfrak{g}, H) \to R(\mathfrak{g}, H)$ is "up to isomorphism" e.g., by version Theorem 3.7.4.9 of Winter : $(\mathfrak{g}_1, H_1) \cong (\mathfrak{g}_2, H_2)$ if and only if $R(\mathfrak{g}_1, H_1) \cong R(\mathfrak{g}_2, H_2)$ for $(\mathfrak{g}_1, H_1), (\mathfrak{g}_2, H_2)$ classical.

Theorem 4.13.3.

Let $\mathfrak{g}$ be a reflective Lie algebra with split Cartan sub-algebra $\mathfrak{g}_0 = H$ and Cartan decomposition $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$. Then

R is a classical root system and $dim \mathfrak{g}_a = \dim[\mathfrak{g}_a , \mathfrak{g}_{-a}] = 1$ for all $a \in R - \{0\}$ and $[\mathfrak{g}_a , \mathfrak{g}_b] = \mathfrak{g}_{a+b}$ for all $a, b, a + b \in R - \{0\}$;

Proof:

Consider the set $\{[e, f] | e \in \mathfrak{g}_a^1 , e \in \mathfrak{g}_{-a}^1\}$ and note that W is commutative :

$$\big[[x, y], [e, f]\big] = \Big[\big[[x, y], e\big], f\Big] + \Big[e, \big[[x, y], f\big]\Big] = a([x, y])[e, f] - a([x, y])[e, f] = 0.$$

Since the span ad $[\mathfrak{g}_a^1 , \mathfrak{g}_{-a}^1]$ of ad W has dome non-nilpotent element, ad W must therefore contain a non-nilpotent element ad h_a. Let $h_a = [e_a , f_a]$ with $e_a \in \mathfrak{g}_a^1$, $f_a \in \mathfrak{g}_{-0}^1$. When the context is clear, we abbreviate $h = h_a$, $= e_a$, $f = f_a$. Note that $a(h) \neq 0$, (byTheorem **4.13.2**), so that $r_a(c) = c - 2(c(h)/a(h))\, a$ is a symmetry of R at a by the same (Theorem **4.13.2**). Note that $[H, f] = kf$, since $f \in \mathfrak{g}_{-a}^1$ and $[h, f] = a(h)f \neq 0$. It follows that $2a \notin R$. thus, R is reduced symmetry set . Since R is reduced with bounded orbits, the characteristic of k is not 2 or 3. Thus, R is reduced root system by (Theorem **4.12.1**).

Consider $\mathfrak{g}^{\infty} = H_{\infty} + \sum_{a \in R-\{0\}} \mathfrak{g}_a$ and $H_{\infty} = H \cap \mathfrak{g}^{\infty} = \sum_{a \in R-\{0\}} [\mathfrak{g}_a, \mathfrak{g}_{-a}]$. Note that $[\mathfrak{g}_a, \mathfrak{g}_a] = \{0\}$, since $2a \notin R$. Take $h_a = h = [e, f] \in [\mathfrak{g}_a^1, \mathfrak{g}_{-a}^1]$ as above , with $a(h) \neq 0$. For

$\in L_a^1$, note that $-a(h)u = [u,h] = \big[u,[e,f]\big] = \big[e,[u,f]\big] + 0 = -a([u,f])e$ and $u = (a([u,f])/a(h))\, e \in ke$.

Thus, $\mathfrak{g}_a^1 = ke$,We claim that $\mathfrak{g}_a = ke$. Suppose that $\mathfrak{g}_a \supsetneq ke$.

Since $(\text{ad}\, h - a(h))^{\dim L}\mathfrak{g}_a = 0$

There exists $u \in \mathfrak{g}_a - ke$ such that $\big(\text{ad}\, h - a(h)\big)u = ce$ and $[h,u] - a(h)u = ce$ for some $c \in k$. But then $-a(h)u - ce = [u,h] = \big[u,[e,f]\big] = \big[e,[u,f]\big] + 0 = -a([u,f])e$ and $u = (a([u,f]) - c/a(h))\ e \in ke$, a contradiction.

Thus, $\mathfrak{g}_a = ke$. This establishes that $\mathfrak{g}_a$ and $[\mathfrak{g}_a, \mathfrak{g}_{-a}]$ are one dimensional for all $a \in R - \{0\}$.

Now let $a, b, a+b \in R - \{0\}$, $S_b(a) = \{b - ra, \dots, b + qa\}$, $T = \{b - ra, \dots, b\}, V = \sum_{c \in T} \mathfrak{g}_c$. If $[\mathfrak{g}_a, \mathfrak{g}_b] = 0$, then V is a module for $ke + kh + kf = \mathfrak{g}_a + [\mathfrak{g}_a, \mathfrak{g}_{-a}] + \mathfrak{g}_{-a}$, so that $r_a(b - ra) = b + qa$ with $q \geq 1$. Thus $[\mathfrak{g}_a, \mathfrak{g}_b] \neq 0$, so that $[\mathfrak{g}_a, \mathfrak{g}_{-a}] = \mathfrak{g}_{a+b}$.

Next, we introduce toral Lie algebras as generalizations of reflective Lie algebras.

Definition 4.13.3.

A Lie algebra $\mathfrak{g}$ with split Cartan sub algebra H is toral if $\dim \mathfrak{g}_a = 1$ and $a([\mathfrak{g}_a, \mathfrak{g}_{-a}]) \neq 0$ for all $a \in R - \{0\}$.

The algebras of Block are those toral Lie algebras $(\mathfrak{g}, H)$ which are idempotent, have center 0 and have ad H diagonalizable. The algebras of Block are classified in Block[8] for $p > 5$.

Proposition 4.13.1.

Let $\mathfrak{g}$ be toral. Then $\mathfrak{g}^\infty \cap$ Center $\mathfrak{g}$ = Center $\mathfrak{g}^\infty \cap$ Center H, and H_∞ is a Cartan sub algebra of $\mathfrak{g}^\infty$. Moreover, ad $_{\mathfrak{g}} H_\infty$ is diagonalizable.

Proof:

Each ad $h \in$ ad H is diagonalizable on the $\mathfrak{g}_a (a \in R - \{0\})$, therefore on the algebra $\mathfrak{g}^\infty$

generated by them. Thus, $[H, H_\infty] = 0$. But then ad H_∞ is diagonalizable on $\mathfrak{g}^\infty$ and 0 on H.

We now determine Nil $\mathfrak{g}$. For this , observe that Kern $R = \{h \in H | a(h) = 0\ \forall a \in R\}$ is contained in the centralizer $C_{\mathfrak{g}}(\mathfrak{g}^\infty) = \{x \in \mathfrak{g} | [x, \mathfrak{g}^\infty] = 0\}$. For Kern R centeralizes the

[8] R.Block, On the Mills-Seligman axioms for Lie algebras of classical type, Trans.Amer.Math. Soc. 121 (1966), 378-392.

generators $\mathfrak{g}_a$ $(a \in R - \{0\})$ for $\mathfrak{g}^\infty$, so that Kern $R \subset C_{\mathfrak{g}}(\mathfrak{g}^\infty)$. Conversely, any $x \in C_{\mathfrak{g}}(\mathfrak{g}^\infty)$ centralizes the $\mathfrak{g}_a$ $(a \in R - \{0\})$ .Writing $x = \sum_{b \in R} x_b$ with $x_b \in \mathfrak{g}_b$,

$0 = [x, e_a] = \sum_{b \in R} [x_b , e_a]$, which implies that $0 = [x_b, \mathfrak{g}_a]$ for $\mathfrak{g}_a = ke_a$ $(a \in R - \{0\}, b \in R)$. Thus, $[x_b , \mathfrak{g}_{-a}] = 0$, which implies that $x_b = 0$ $(b \in R - \{0\})$ and , therefore, that $x = x_0 \in H$. Thus, $C_{\mathfrak{g}}(\mathfrak{g}^\infty) \subset H$ and, therefore, $C_{\mathfrak{g}}(\mathfrak{g}^\infty) \subset$ Kern R. Thus, Kern $R = C_{\mathfrak{g}}(\mathfrak{g}^\infty)$ is an ideal of $\mathfrak{g}$ contained in H centralizing $\mathfrak{g}^\infty$. As such, Kern $R \subset$ Nil $\mathfrak{g}$. Conversely, Nil $\mathfrak{g}$ is ad H- stable and is , therefore, a sum of $(\text{Nil } \mathfrak{g}) \cap H$ and certain of the one dimensional spaces $\mathfrak{g}_a$. But $[\mathfrak{g}_a , \mathfrak{g}_{-a}] \not\subset$ Nil $\mathfrak{g}$, since a $([\mathfrak{g}_a , \mathfrak{g}_{-a}]) \neq 0$, whereas $[(\text{Nil } \mathfrak{g}), \mathfrak{g}_{-a}] \subseteq$ Nil $\mathfrak{g}$ for $a \in R - \{0\}$.it follows that Nil $\mathfrak{g} \subset H$ and therefore, that Nil $\mathfrak{g} \subset$ Kern R. This establishes the following theorem.

Theorem 4.13.4.

Let $\mathfrak{g}$ be toral. Then Nil $\mathfrak{g} =$ Kren $R = C_{\mathfrak{g}}(\mathfrak{g}^\infty)$, where Kern $R = \{H \in H | a(h) = 0 \; \forall a \in R\}$ and $C_{\mathfrak{g}}(\mathfrak{g}^\infty)$ is centralizer in $\mathfrak{g}$ of $\mathfrak{g}^\infty$.

Corollary 4.13.1.

Let $\mathfrak{g}$ be toral and idempotent. Then $\mathfrak{g}$ is reductive .

Corollary 4.13.2.

Let $\mathfrak{g}$ be toral and H abelian . Then $\mathfrak{g}$ is reductive .

Proposition 4.13.2.

Let $\mathfrak{g}$ be toral with center 0. Then H is abelian, $\mathfrak{g}$ is reductive and Core $\mathfrak{g} = \mathfrak{g}^{(1)}$, that is $\mathfrak{g}^{(1)} = \mathfrak{g}^\infty$ and $\mathfrak{g}^{(1)}$ has center 0.

Proof:

Suppose that H is not abelian, and choose a nonzero element $h \in H^{(1)} \cap$ Center H. Then $[h, \mathfrak{g}_a] = 0$ for all $a \in R$ and $h \in$ Center $\mathfrak{g}$, so Center $\mathfrak{g} \neq \{0\}$ in contradiction to the hypothesis. Thus, H is abelian. It follows that $\mathfrak{g}$ is reductive, by (Corollary 4.13.2). Finally $\mathfrak{g}^\infty$ has center 0, since $\mathfrak{g} = H + \mathfrak{g}^\infty$ has center 0 and H is abelian. Thus, $\mathfrak{g}^{(1)} = H^{(1)} + \mathfrak{g}^\infty = \mathfrak{g}^\infty$.

Proposition 4.13.3.

Let $\mathfrak{g}$ be toral and reductive. Then Core ad $=$ $(\text{ad } \mathfrak{g})^{(1)}$.

Proof:

Since $H^{(1)} \subset \text{Kern } R = \text{Nil } \mathfrak{g}$ and $\text{Nil } \mathfrak{g}$ is central, $0 = \text{ad } H^{(1)} = [\text{ad } H, \text{ad } H]$. Thus, $\text{ad } H$ is abelian and $(\text{ad } \mathfrak{g})^{(1)} = \text{ad } H^{(1)} + \text{ad } \mathfrak{g}^{\infty} = \text{ad } \mathfrak{g}^{\infty}$. Since $\text{ad } \mathfrak{g}^{\infty}$ is idempotent, it suffices to show that it had center 0.

Let $\text{ad } h$ be central in $\text{ad } \mathfrak{g}^{\infty}$, so that $h \subset \text{Kern } R \subset \text{Nil } \mathfrak{g} \subset \text{Center } \mathfrak{g}$. Then $\text{ad } h = 0$.

The following theorem shows that the rough classification of reflective Lie algebras $(\mathfrak{g}, H)$ by their root systems, discussed in the paragraph preceding is equivalent to a rough classification of reflective Lie algebras $\mathfrak{g}$ by their (classical) cores. The latter classification is independent of a split Cartan sub algebra H of $\mathfrak{g}$.

Theorem 4.13.5.

Let $\mathfrak{g}$ be reflective. Then $\text{Core } \mathfrak{g} = \mathfrak{g}^{\infty}/\text{Nil } \mathfrak{g}^{\infty}$ is classical and isomorphic to $(\mathfrak{g}/\text{Nil } \mathfrak{g})^{(1)}$, and the root systems of $\mathfrak{g}$ and $\text{Core } \mathfrak{g}$ are canonically isomorphic.

Proof:

Let $\tilde{\mathfrak{g}} = \mathfrak{g}/\text{Nil } \mathfrak{g}, \tilde{H} = (H + \text{Nil } \mathfrak{g})/\text{Nil } \mathfrak{g}$.Then $\tilde{H}$ is a split Cartan sub algebra of $\tilde{\mathfrak{g}}, \dim \tilde{\mathfrak{g}}_a = 1$ and $a([\tilde{\mathfrak{g}}_a, \tilde{\mathfrak{g}}_{-a}]) \neq 0$ for all nonzero roots a of $\tilde{\mathfrak{g}}$ and $\tilde{\mathfrak{g}}$ is toral, by (Theorem **4.13.3**) and (Def **4.13.3**). By (Theorem **4.13.4**) $\tilde{\mathfrak{g}}$ has center 0, since any central element x would lie in $\{\tilde{x} \in \tilde{H} | a(x) = 0, \forall \text{ roots } a\} \subset \text{Nil } \mathfrak{g}/\text{Nil } \mathfrak{g} = \{\tilde{0}\}$. Thus, Core $\tilde{\mathfrak{g}} = \tilde{\mathfrak{g}}^{(1)}$, by (Prop **4.13.2**).

Since $\mathfrak{g}^{\infty}$ is idempotent, the homomorphism $\mathfrak{g}^{\infty} \longrightarrow \tilde{\mathfrak{g}}$ has image $\tilde{\mathfrak{g}}^{(1)} = \text{Core } \tilde{\mathfrak{g}}$ and therefore, Kernel $\text{Nil } \mathfrak{g}^{\infty}$. Thus, Core $\mathfrak{g}$ is isomorphic to $R_{\mathfrak{g}^{\infty}} \longrightarrow R_{\text{Core } \mathfrak{g}}$ (reduction mod Nil), where $R_{\mathfrak{g}}$, $R_{\mathfrak{g}^{\infty}}$, $R_{\text{Core } \mathfrak{g}}$ are sets of roots for $(\mathfrak{g}, H), (\mathfrak{g}^{\infty}, H_{\infty}), (\text{Core } \mathfrak{g}, H_{\infty}/\text{Nil } \mathfrak{g}^{\infty})$, respectively. We know, that $\{a^{\oplus} | a \in R - \{0\}\}$ separates R. Since $a^{\oplus}(b) = 2(b(h_a)/a(h_a))$ with $h_a \in \mathfrak{g}^{\infty}$, it follows that $\{a^{\oplus} | a \in R - \{0\}\}$ separates R_{∞} and , moreover, $\mathfrak{g}^{\infty}$ is reflective and Core $\mathfrak{g}$classical, since $a(h_a) \neq 0$ $(a \in R - \{0\})$. Thus, the mappings $R_{\mathfrak{g}} \to R_{\mathfrak{g}^{\infty}} \to R_{\text{Core } \mathfrak{g}}$ are bijections. It therefore follows from Winter[9], (Theorem **4.5.2**) , that they are isomorphisms of groupoids.

We say that $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ is weakly reflective if $R_b(a)$ is bounded and $[\mathfrak{g}'_{-a}, \mathfrak{g}'_a]$ has a non nilpotent element for all $a, b \in R$ such that $\mathfrak{g}_a \not\subset \text{Nil } \mathfrak{g}^{\infty}$ and $\mathfrak{g}_b \not\subset \text{Nil } \mathfrak{g}^{\infty}$. The above results lead easily to the following version of part of them which, by the conjugacy of Cartan sub

[9] D.JWinter, Symmetry sets, J.Algebra 73, No.1(1981), 238-247.

algebras of classical Lie algebras is an " invariant characterization". The proof is based on passage from $\mathfrak{g}$ to $\mathfrak{g}^{\infty}$.

Theorem 4.13.6.

A Lie algebra $\mathfrak{g}$ is weakly reflective with respect to some split Cartan sub algebra H if and only if Core $\mathfrak{g}$ is classical.

4.14 The Nilpotent Roots of $\mathfrak{g}$

For a Lie algebra $\mathfrak{g} = \sum_{a\in R} \mathfrak{g}_a$ with orbits $R_b(a)\ (a \in R - \{0\}, b \in R)$ bounded, $\mathfrak{g}$ is reflective if and only if the set $\mathrm{Nil}^1 R =_{\mathrm{def}} \{c \in R - \{0\} | [\mathfrak{g}'_{-c}, \mathfrak{g}'_c]$ consists of ad − nilpotent elements$\cup\{0\}$ of nilpotent roots of g,H is $\{0\}$. Note, in this connection, that $0 \in \mathrm{Nil}^1 R$ is not an anomaly, since $[\mathfrak{g}_0^1, \mathfrak{g}_0^1] = 0$. For adL_0 diagonalizable $\mathrm{Nil}^1 R = \mathrm{Nil}\, R$, where $\mathrm{Nil}^1 R =_{\mathrm{def}} \{c \in R - \{0\} | [\mathfrak{g}_{-c}, \mathfrak{g}_c]$ consists of ad − nilpotent elements$\} \cup \{0\}$.

Without assuming a condition that ad L_0 be diagonalizable, we now show that the sub algebra $\mathfrak{g}_{\mathrm{Nil}\ R}$ generated by $\{\mathfrak{g}_c | c \in \mathrm{Nil}\, R - \{0\}$ is ad − nilpotent on $\mathfrak{g}\}$ provided that the orbits $R_b(a)\ (a \in R - \{0\}, b \in R)$ are bounded. Note in this connection, that $0 \in \mathrm{Nil}\, R$ is an anomaly for certain Lie algebras $\mathfrak{g}$, even when $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}^{\infty} = \mathfrak{g}_0 \oplus \mathfrak{g}_a$, where $\mathfrak{g}^{\infty}$ is abelian and ad $\mathfrak{g}_0$ is irreducible on $\mathfrak{g}^{\infty} = \mathfrak{g}_a$: $[\mathfrak{g}_0, \mathfrak{g}_0]$ need not be ad-nilpotent .

Theorem 4.14.1.

Suppose that the orbits $R_b(a)\ (a \in R - \{0\}, b \in R)$ are bounded. Then $\mathfrak{g}_{\mathrm{Nil}\ R}$ is ad-nilpotent on $\mathfrak{g}$.

Proof:

Let $S =$ Nil $R - \{0\}$, Observe that the sub algebra $H_{\mathrm{Nil}\ R}$ generated by the "weakly closed" st $\bigcup_{c\in S} [\mathfrak{g}_{-c}, \mathfrak{g}_c]$ is ad-nilpotent on $\mathfrak{g}$, by the Jacobson-Engel theorem (Jacobson)[10].

We claim that the "weakly closed" set $W = \bigcup_{n=1}^{\infty} W_n$ of commutators $[x_1, \ldots, x_n] \in W_n$ (with any legal arrangements of brackets) $(n = 1,2, \ldots, c_i \in S, x \in \mathfrak{g}_{c_i})$ consists of ad-nilpotent elements. Consider $x = [x_1, \ldots, x_n] \in W_n$ of weight $\sum_1^n c_i = 0$, $x_i \in \mathfrak{g}_{c_i}$, $c_i \in S$. After successive factorizations $x = [[x_1, \ldots, x_m], [x_{m+1}, \ldots, x_n]]$ of x and generated terms thereof , and successive use of the Jacobi identity in conjunction there with x can be written as a linear combination of terms of W_n of the form $x' = [x'_1, [x'_2, \ldots, x'_n]]$ of weight

[10] N.Jacobson,"Lie algebras" Wiley-Interscience, New York,1962.

$0 = \sum_1^n c'_i$, $x_i \in \mathfrak{g}_{c_i}$, $c'_i \in S$. But then $x' \in [\mathfrak{g}_{c'_i}, \ldots, \mathfrak{g}_{-c'_i}] \subset H^S$, so that $x \in H^S$ as a linear combination of the generated terms x', and ad x is nilpotent on $\mathfrak{g}$, as an element of ad H^S.

Finally, consider an element $x = [x_1, \ldots, x_m] \in W_n$ of weight $c = \sum_1^n c_i \neq 0$. Then ad x is nilpotent on $\mathfrak{g}$, by the boundedness of orbits $R_b(c)(b \in R)$. Since ad W is a weakly closed set of nilpotent linear transformations of $\mathfrak{g}$, it follows that ad $\mathfrak{g}^S$ is nilpotent on $\mathfrak{g}$, by the Jacobson-Engle Theorem .

We now identify Nil R precisely in the case of Lie algebras $\mathfrak{g}$ of characteristic 0 .

Theorem 4.14.2.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be a Lie algebra of characteristic 0. Then:

Nil $R = \{c \in R - \{0\} | \mathfrak{g}_c \subset \text{Nil } \mathfrak{g}\} \cup \{0\}$.

Proof :

Since $\mathfrak{g}/\text{Nil } \mathfrak{g}$ is reductive, the theory of reductive Lie algebras of characteristic 0 implies that $\mathfrak{g}_c \subset \text{Nil } \mathfrak{g}$ of $c \in \text{Nil } R$. For the other direction, let $h \in [\mathfrak{g}_{-c}, \mathfrak{g}_c]$, where ad h is not nilpotent on $\mathfrak{g}$. By (Theorem **3.5.1**) of Winter[11] we have $c(h) \neq 0$, Tr $(\text{ad } h)^2 \neq 0$ and $h \notin \mathfrak{g}^\perp$ when $\mathfrak{g}^\perp$ is the radical of the killing form on $\mathfrak{g}$. It follows that $\bar{h} = h + \text{Rad } \mathfrak{g}$ is non zero in $\bar{\mathfrak{g}} = \mathfrak{g}/\text{Rad } \mathfrak{g}$, where Rad $\mathfrak{g}$ is the solvable radical of $\mathfrak{g}$. Since $\bar{h} \in [\bar{\mathfrak{g}}_{-c}, \bar{\mathfrak{g}}_c]$ and $c(h) \neq 0$, we have shown that $c \notin \text{Nil } R$ implies that $\mathfrak{g}_c \not\subset \text{Nil } \mathfrak{g}$.

The following corollary to (Theorem **4.14.2**) is straightforward. In it, $\langle \mathfrak{g}_{\text{Nil } R} \rangle$ denotes the ideal of $\mathfrak{g}$ generated by $\mathfrak{g}_{\text{Nil } R}$ and Core $R = R - \text{Nil } R \cup \{0\}$.

Corollary 4.14.1.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be a split Lie algebra of characteristic 0. Then $\mathfrak{g}/\langle \mathfrak{g}_{\text{Nil } R} \rangle$ is reductive with root system canonically isomorphic to Core R.

Definition 4.14.1.

Given a Lie algebra $= \sum_{a \in R} \mathfrak{g}_a$, we let $\mathfrak{g}_a^1 = \{x \in \mathfrak{g}_a | [h, x] = a(h)x \text{ for all } h \in \mathfrak{g}_0\}$ $(a \neq 0)$ and $\mathfrak{g}_0^1 = \mathfrak{g}_0$, and we let $\mathfrak{g}^1$ be the sub algebra $\mathfrak{g}^1 = \sum_{a \in R} \mathfrak{g}_a^1$. we say that $\mathfrak{g}$ is symmetric if $a([\mathfrak{g}_{-a}^1, \mathfrak{g}_a^1]) \neq 0$ for all $a \in R - \{0\}$.

[11] D.J.Winter, "Abstract Lie Algebras" MIT Press, Cambridge, Mass, 1972.

Proposition 4.14.1.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be symmetric and let $a \in R - \{0\}$, $b \in R$ with $R_b(a)$ bounded. Then $+b \in R \Longrightarrow \left[\mathfrak{g}_a^1 , \mathfrak{g}_b^1\right] \neq 0$.

Proof:

Let $R_b(a) = \{b - ra , \ldots . , b + qa\}$ and suppose that $\left[\mathfrak{g}_a^1 , \mathfrak{g}_b^1\right] = 0$. Let $T = \{b - ra , \ldots , b\}$ and consider $= \sum_{c \in T} \mathfrak{g}_c^1$. Then V is a module for $\mathfrak{g}^{(1)} = kf_a + kh_a + ke_a$ with $0 \neq h_a = [e_a, f_a] \in [\mathfrak{g}_a^1 , \mathfrak{g}_{-a}^1]$, so that $r_b(c) = c - (c(h_a)/a(h_a))$ a maps $b - ra$ to $b + qa$ and to b. Thus, $q = 0$ and $a + b \notin R$.

Theorem 4.14.3.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be symmetric**.** Then $\mathbb{Z}_p a \cap R$ is either $\{-a, 0, a\}$ or $\{-a, 0, a, \ldots , (p-2)a\}$ for any $a \in R - \{0\}$, that is , $R = R^{\circ} \cup R^{\cdot}$.

Proof:

Suppose that $S = \mathbb{Z}_p a \cap R$ is not $\{-a, 0, a, \ldots , (p-2)a\}$. Then $S_b(c) = R_a(c)$ is bounded for all $b \in S - \{0\}$, $c \in S$.

Let $b \in S - \{0\}$. Then the orbits $R_b(c)$ are stable under the reversal

$$R_c(b) = b - 2\ (b(h_c)/c(h_c))c = ic - 2(ic(h_c)/c(h_c))c = -ic = -b.$$

Thus, S is symmetry set in $\mathbb{Z}_p$, all of whose orbits $S_b(a)$ are bounded. Let $a \in S - \{0\}$ and consider the module $\mathfrak{g}_{ra} + \cdots + \mathfrak{g}_0 + ke_a$ for $f_a + kh_a + ke_a$, where $S_0(a) = \{-ra, \ldots , ra\}$. Then $T = \{-ra, \ldots ,0, a\}$ is stable under r_a , so that $a = r_a(-ra) = ra$ and $r = 1$. It follows that S is reduced. But then $S = \{-a, 0, a\}$.

Theorem 4.14.4.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be symmetric and let $= \mathfrak{g}_0$. Then :

1. $R \subset \mathrm{Hom}_k(H, k)$

2. ad H is triangulable on $\mathfrak{g}$

3. $\mathfrak{g}^{\infty}$ is symmetric with Cartan aub algebra H_{∞}

4. Core $\mathfrak{g}$ is symmetric

5. $\mathfrak{g}/(\text{Nil})\,\mathfrak{g}$ has center 0

6. $\mathfrak{g}^1 = \sum_{a\in R}\mathfrak{g}_a^1$ is symmetric and the Cartan sub algebra $\bar{H}^1$ of $\bar{\mathfrak{g}}^1 = \mathfrak{g}^1/\text{Nil}\,\mathfrak{g}^1$ is ad-diagonalizable.

Proof :

For (**1**) and (**2**), observe that $\sum_{a\in R-\{0\}}\mathfrak{g}_a^1$ is a module for ad H which is annihilated by $(\text{ad}\,H)^{(1)}$. Thus, $(\text{ad}\,H)^{(1)}$ is upper triangulable with only zeros on the diagonal, by Engle's Theorem. It follows that $\text{ad}\,H$ is triangulable on $\mathfrak{g}$. For (**3**), note that $[H_\infty, \mathfrak{g}_a] = \mathfrak{g}_a$, so that H_∞ is a Cartan sub algebra of $\mathfrak{g}^\infty$. For (**4**) , note that if $h \in [\mathfrak{g}_{-a}^1, \mathfrak{g}_a^1]$ with $a(h) \neq 0$, then $h \in \mathfrak{g}^\infty - \text{Nil}\,\mathfrak{g}$; for otherwise Nil $\mathfrak{g}$ contains $\mathfrak{g}_{-a}^1 + kh + \mathfrak{g}_a^1$, since Nil $\mathfrak{g}$ is an ideal which would contain h, contradicting the nilpotence of Nil $\mathfrak{g}$. Similarly, $h \in \mathfrak{g}^\infty - \text{Nil}\,\mathfrak{g}^\infty$.

Thus, $\text{Core}\,\mathfrak{g} = \mathfrak{g}^\infty/\text{Nil}\,\mathfrak{g}^\infty$ is symmetric. If $\mathfrak{g}$ is toral, $\mathfrak{g}^\infty \to \mathfrak{g}/\text{Nil}\,\mathfrak{g}$ has image $(\mathfrak{g}/\text{Nil}\,\mathfrak{g})^{(1)}$ and kernel Nil $\mathfrak{g}^\infty$, by a straightforward verification. For (5), let $h + \text{Nil}\,\mathfrak{g} \in \text{Center}\,\mathfrak{g}/\text{Nil}\,\mathfrak{g}$.

Then $[h, \mathfrak{g}_a] \subset \text{Nil}\,\mathfrak{g}$ $(a \in R - \{0\})$. Since $\mathfrak{g}$ is symmetric, $\mathfrak{g}_a \not\subset \text{Nil}\,\mathfrak{g}$ $(a \in R - \{0\})$. Thus, $a(h) = 0$, for otherwise, $\mathfrak{g}_a = [h, \mathfrak{g}_a] \subset \text{Nil}\,\mathfrak{g}$ $(a \in R - \{0\})$.

It follows that the ideal $kh + \text{Nil}\,\mathfrak{g}$ is ad-nilpotent on $\mathfrak{g}$, so that $h \in \text{Nil}\,\mathfrak{g}$, by the maximality of Nil $\mathfrak{g}$. Thus, $\mathfrak{g}/\text{Nil}\,\mathfrak{g}$ has center 0.

For (**6**), note that if $\mathfrak{g}$ has center 0 and ad H is diagonalizable on the $\mathfrak{g}_a$ $(a \in R - \{0\})$, then ad H is diagonalizable since H is then abelian :

$h \in H^{(1)} \cap \text{Center}\,H \Rightarrow h$ central in $\mathfrak{g} \Rightarrow h = 0$.

Theorem 4.14.5.

Let $\mathfrak{g} = \sum_{a\in R}\mathfrak{g}_a$ be symmetric with $0 \neq \mathbb{Z}_p\, a \subset R$. Then $\mathfrak{g}_1(a)/\text{Solv}\,\mathfrak{g}^{1(a)}$ is the Witt algebra W_1 for $\mathfrak{g}^{1(a)} = H + \sum_{i=1}^{p-1}\mathfrak{g}_{ai}^1$.

Proof :

Since $\mathfrak{g}^{1(a)}$ is symmetric $\bar{\mathfrak{g}} = \mathfrak{g}^{1(a)}/\text{Nil}\,\mathfrak{g}^{1(a)}$ is symmetric with center 0, by (Theorem **4.14.4**). Let $\bar{H}$ be the image of H in $\bar{\mathfrak{g}}$. It follows that $\bar{H}$ is abelian, for otherwise any $h \in \bar{H}^{(1)} \cap \text{Center}\,\bar{H}$ is central in $\bar{\mathfrak{g}}$. But then $\bar{H}$ is ad-diagonalizable on $\bar{\mathfrak{g}}$. Since Center $\bar{\mathfrak{g}} = 0$, it follows that $\bar{H}$ has dimension 1.

Let S be a maximal proper ideal of $\mathfrak{g}^{1(a)}$ containing Nil $\mathfrak{g}^{1(a)}$. If $\bar{H} \cap \bar{S}$, then $\bar{\mathfrak{g}} = \bar{\mathfrak{g}}_0(\text{ad}\,\bar{H}) + \bar{S} = \bar{H} + \bar{S} = \bar{S}$ and $\mathfrak{g} = S$. Thus, $\bar{H} \not\subset \bar{S}$. Since $\dim \bar{H} = 1$, it follows that $\bar{H} \cap \bar{S} = \bar{0}$ and

$\bar{S} = \sum_{i=1}^{p-1} \bar{S}_{ia}$, where $\bar{S}_{ia} = \bar{S}_{ia}(\text{ad}\,\bar{H})$. it then follows that $\text{ad}_{\bar{S}}\,\bar{S}_{ia}$ is nil $(1 \le i \le p-1)$ and $\bar{S}$ is nilpotent. Thus, $S = \text{Solv}_{\mathfrak{g}}\ 1(a)$. It follows that $\mathfrak{g}^{1(a)}/\text{Solv}_{\mathfrak{g}}\ \mathfrak{g}^{1(a)}$ is simple of rank 1 and toral rank1, so that it is W_1,by Kaplansky[12].

Theorem 4.14.6.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be symmetric Lie algebra. Then $(\mathfrak{g}_0^*, R)$ is a Lie root system.

Proof:

Let $a \in R - \{0\}$ and choose $h_a \in [\mathfrak{g}_{-a}^1, \mathfrak{g}_a^1]$ with $a(h_a) \neq 0$. Define $a^0 \in \text{Hom}_k(\mathfrak{g}_0^*, k)$ by $a^0(v) = 2(v(h_a)/a(h_a))$, let $r_a(v) = v - a^0(v)\ a$ $(v \in \mathfrak{g}_0^*)$, and note that $a^0(a) = 2$ and $r_a\ R_b(a) = R_b(a)$ for every bounded a-orbit $R_b(a)(b \in R)$, by (Theorem **4.8.1)**. thus, $(\mathfrak{g}_0^*, R)$ is a root system in the sense of (section **4.7**), and it remains to verify the supplemental "Lie conditions that $R = R^0 \cup R^{\cdot}$ and each "Witt orbit" $R_b(a)$ $(a \in R^0 - \{0\}, \text{b} \in \text{R})$ has 1 or $p-1$ or p elements. The condition $R = R^0 \cup R^{\cdot}$ was proved in (Theorem **4.10.1**).

Next, consider a "Witt orbit" $R_b(a)$ $(a \in R^0 - \{0\}, \text{b} \in \text{R})$. we must show that $R_b(a)$ has 1 or $p-1$ or p elements. Accordingly, we may, without loss of generality, assume that $1 < |R_b(a)| \le p-1$. To show that $|R_b(a)| = p-1$, we may replace $\mathfrak{g} = \sum_{c \in R} \mathfrak{g}_c$ by another symmetric Lie algebra having corresponding $a \in R^w, b \in R$ and $R_b(a)$ of the same length. It follows that we can, successively, replace $\mathfrak{g}$ by $\sum_{i,j=0}^{p-1} \mathfrak{g}_{ia+jb}^1$ with $\mathfrak{g}_0^1 =_{\text{def}} \sum_{i,j=0}^{p-1} [\mathfrak{g}_{ia+jb}^1, \mathfrak{g}_{-ia-jb}^1]$, $\mathfrak{g}/\text{Center}\ \mathfrak{g}$. Consequently, we may assume, with no loss of generality, that $\mathfrak{g} = \sum_{i,j=0}^{p-1} \mathfrak{g}_{ia+jb}^1$ and $\text{Center}\ \mathfrak{g} = \{0\}$.

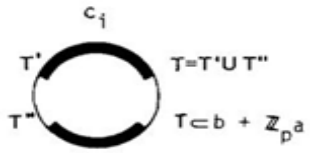
For each $1 \le i \le p-1$, choose $e_i \in \mathfrak{g}_{ia}^1, f_i \in \mathfrak{g}_{-ia}^1$, $h_i = [e_i, f_i]$ such that $a(h_i) = 1$ and define $r_{ia}(v) = v - 2(v(h_i)/ia(h_i))\ ia = v - 2v(h_i)\ a (v \in L_0^*)$.

Note that $r_i(a) = -a (1 \le i \le p-1)$. By (Theorem **4.13.1**) and the assumption $|R_b(a)| \le p-1$, the ia-orbits $T_{b'}(ia)(b' \in T)$ of $T = R \cap (b + \mathbb{Z}_p\ a)$ are $r_{\bar{i}}$ stable for any $1 \le i \le p-1$. It follows, in particular, that T contains $r_i(b) = b - 2b(h_i)a$, so that $\mathbb{Z}_p$ contains $b(h_i)$. Define $r_i = b - b(h_i)\ a \in b + \mathbb{Z}_p\ a$ and note that $r_{ia}(c_i) = c_i$ since $c_i(h_i) = 0$, for $1 \le i \le p-1$. Since, for $1 \le i \le p-1$, we have $r_i(c_i) = c_i$ and $r_i T_{b'}(ia) = T_{b'}(ia)$ $(b' \in T)$, one can easily verify that :

1. T has either 1 or 2 ia-orbits ,

[12] I.Kaplansky. Lie algebras of characteristic p, Trans. Amer.Math. Soc.89 (1958), 149-183.

2. If T has 2 ia-orbits $T^{'}, T^{''}$, then an odd number of elements and $T^{''} = T - T^{'}$, and then one of $T^{'}, T^{''}$ has an odd number of elements and contains c_i, and the other has an even number of elements.



Fig(2.4)

We claim, for each $1 \leq i \leq p-1$ and each $b^{'} \in T$, that the ia-orbit $T_{b'}(ia)$ is stable under each $r_i (1 \leq j \leq p-1)$. By (**1**) and (**2**) above, $T = T_{b'}(ia)$ (case of one ia-orbit) or $T^{'} = T_{b'}(ia)$ and the ia-orbits of T are T' and $T^{''} = T - T'$, where one of T', T'' has odd number of elements and the other has an even number of elements. Since $T = r_j(T) = r_j(T') \cup r_j(T'')$ and since $r_i(ia) = -ia$, one can easily verify that $r_j(T'), r_j(T'')$ are ia-orbits of T, thus that

They are $T^{'}, T''$ in one of the orders $T^{'}, T''$ or $T^{''}, T'$. But r_j preserves "odd" and "even" numbers of elements. It follows that $r_j(T') = T'$ and $r_j(T'') = T''$ for $1 \leq j \leq p-1$.

Take one fixed ia-orbit $T_{b'}(a)$ of T. Since it is stable under $r_1, \ldots, r_{p-1}$ and $r_j(a) = -a$ $(1 \leq j \leq p-1)$, each of the $r_1, \ldots, r_{p-1}$ reverse the a-orbit $T_{b'}(a)$.

It follows that $r_1(b') = \cdots = r_{p-1}(b')$ and $b^{'}(h_1) = \cdots = b^{'}(h_{p-1})$ forsuppose that all $b^{'} \in T$. Consequently, we have $b(h_i - h_j) = b(h_i - h_j) = 0$ for all $1 \leq j \leq p-1$.

Since $\mathfrak{g} = \sum_{i,j=0}^{p-1} \mathfrak{g}^1_{ia+jb}$ with $\mathfrak{g}^1_0 =_{\text{def}} \sum_{i,j=0}^{p-1} [\mathfrak{g}^1_{ia+jb}, \mathfrak{g}^1_{-ia-jb}]$, it follows that :

$h_i - h_j \in \text{Center}\, \mathfrak{g} = \{0\}$ and $h_i = h_j$ for all $1 \leq i, j \leq p-1$.

Finally, we let h denote h_1 , so that $h = h_i$ for $1 \leq i \leq p-1$ and $a(h) = 1$. By the flexibility in the choice of h_i above , it follows that $e \in \mathfrak{g}_{ia}, f \in \mathfrak{g}_{-ia}$ with $a[e,f] = 1$ implies that $h = [e, f]$, for $1 \leq i \leq p-1$. We claim that :

$e^{'} \in \mathfrak{g}_{ia}, f^{'} \in \mathfrak{g}_{-ia}, a([e^{'}, f^{'}]) = 0$ implies that $[e^{'}, f^{'}] = 0$ for $1 \leq i \leq p-1$.

To see this, let $1 \leq i \leq p-1$, choose $e \in \mathfrak{g}_{ia}, f \in \mathfrak{g}_{-ia}$ such that $h = [e, f]$ and $e^{'} \in \mathfrak{g}_{ia}, f^{'} \in \mathfrak{g}_{-ia}, h' = [e', f], a(h') = 0$. We claim that $h^{'} = 0$.

To see this ,let $h^{''} = [e^{'}, f], h^{'''} = [e, f']$. Consider first the case where $a(h^{''}) = a(h^{'''}) = 0$ then $1 = a(h + h'') = a([e + e^{'}, f])$, so that $h = [e + e^{'}, f]$ as observed above. But then

$h = h + h''$ and $h^{''} = 0$. Similarly, $h^{'''} = 0$. It follows that $[e + e^{'}, f + f'] = h + h^{'} + h^{''} + h^{'''} = h + h'$ and $h^{''} = 0$. Since $1 = a(h) = \big(a(h + h')\big) = a([e + e^{'}, f + f'])$, it follows from the discussion above that $h = h + h'$ and $h^{'} = 0$. Thus, $[e^{'}, f^{'}] = 0$ in the present case. Next, consider the case where one of $a(h^{''}), a(h^{'''})$ is not zero. We may then assume with no less of generality that $a(h^{''}) \neq 0$, for otherwise we can interchange $h^{''}, h^{'''}$. By replacing $e^{'}$ by $(1/a(h^{''}))\, e^{'}$, we may also assume that $1 = a(h^{''}) = a[e', f]$. But then $h'' = h$, by our earlier discussion. But then $h + h^{'} = [e', f] + [e', f'] + [e^{'}, f + f']$ and $1 = a([e^{'}, f + f'])$ implies that $[e^{'}, f + f'] = h$, by our earlier discussion, so that $h + h^{'} = h$ and $h = 0$.

By the preceding paragraph, we have $\mathfrak{g}_0^1 =_{\text{def}} \sum_{i,j=0}^{p-1} \mathfrak{g}_{ia+jb}^1 = kh$, that is, the Cartan sub algebra $H = \mathfrak{g}_0^1$ of $\mathfrak{g}$ is one dimensional. Let $\mathfrak{g} = \sum_{i=0}^{p-1} \mathfrak{g}_{ia} = \sum_{i=0}^{p-1} \mathfrak{g}_{ia}^1$ and let $S = \operatorname{Solv} \mathfrak{g}^a$. We observed in (Theorem **4.14.5**) that $\mathfrak{g}/S$ is the Witt algebra W_1. Since S is a proper ideal of $\mathfrak{g}$, we have $H \not\subset S$. Since $\dim H = 1$, it follows that $H \cap S = \{0\}$. Consequently, $= \sum_{i=0}^{p-1} S_{ia}$.

Regard $V = \sum_{c \in T} \mathfrak{g}_c$ as $\mathfrak{g}$-module via adjoints, where $T = R \cap \big(b + \mathbb{Z}_p\, a\big) \not\subseteq b + \mathbb{Z}_p\, a$. Let $f: \mathfrak{g} \longrightarrow \operatorname{Hom} V$ be the associated representation. Since $\not\subseteq b + \mathbb{Z}_p\, a$, $f(S_{ia})$ consists of nilpotent transformations of V for $1 \leq i \leq p - 1$. By the theorem of Jacobson[13] on weakly closed sets of linear transformations, it follows that $f(S)$ consists of nilpotent linear transformations of V. Letting $\bar{V}$ be any irreducible sub quotient $\bar{V} = V_i/V_{i+1}$, where $V_1, \ldots., V_r$ is a composition series for V, and letting $\bar{f}: \mathfrak{g} \longrightarrow \operatorname{Hom} \bar{V}$ be the associated representation of $\mathfrak{g}$, we claim that $\bar{f}(S)\bar{V} = \{0\}$. We use the notation $\bar{v} = v + V_{i+1} \in \bar{V}$ for $v \in V_i$.

Note that since $\bar{f}(S)$ is a Lie algebrs of nilpotent linear transformations of $\bar{V}$,

$\bar{V} = \big\{v \in \bar{V} | \bar{f}(S)\bar{v} = 0\big\}$ is nonzero. One sees easily that $\bar{V}_0$ is an $\mathfrak{g}$- sub module of $\bar{V}$, since S is an ideal of $\mathfrak{g}$:

$\bar{f}(S)\bar{v} = 0 \Longrightarrow \bar{f}(S)\big[\bar{f}(\mathfrak{g})\bar{v}\big] = 0.$

Since $\bar{V}$ is irreducible , $\bar{V} = \bar{V}_0$ and $\bar{f}(S)\bar{V} = \{0\}$.

Since $\bar{f}(S)\bar{V} = \{\bar{0}\}$, we may regard $\bar{V}$ as a module for $W_1 = \mathfrak{g}/S$ where the module action given by

$(x + s)\bar{v} = \overline{[x, v]}$

For $x + S \in \mathfrak{g}/S$, $\bar{v} = v + V_{i+1} \in \bar{V}$, $\overline{[x, v]} = [x, v] + V_{i+1} \in \bar{V}$. We let $\bar{V} = \sum_{c \in T'} \bar{V}_c$ be the root decomposition of $\bar{V}$ with respect to $H \subset \mathfrak{g}$ and $H + S/S = \bar{H}$ in $\mathfrak{g}/S = W_1$, and regard

[13] N.Jacobson,"Lie algebra" Wiley-Interscience, New York,1962.

T' as a sub set of R. The restricted irreducible W_1-modules have dimensions $1, p-1$ or p and one-dimensional weight spaces. It follows that $|T'| = 1, p-1$ or p. Since $1 < |R_b(a)|$, one of $b-a, b+a$ is in R. Consequently, we can choose $\bar{V}$ such that $\bar{V}_c \neq \{\bar{0}\}$ or $V_{b+a} \neq \{\bar{0}\}$, by (Prop 4.14.1). for this, $\bar{V}, |T'| \neq 1$, so that $|T'| = p-1$ or $|T'| = p$. But then $p-1 \leq |T'| \leq |R_b(a)| \leq p-1$, so that $|R_b(a)| = p-1$ as was to be proved.

Corollary 4.14.2.

Let $\mathfrak{g}$ be a symmetric Lie algebra. Then $\mathfrak{g}$ is reflective if and only if $\mathbb{Z}_p a \not\subset R$ for all

$a \in R - \{0\}$ if and only if R is classical : $R = R^{\cdot} \cup \{0\}$.

Proof:

The latter condition is equivalent, by theorem 11.6, to the condition that the Lie root system R is classical, that is $R = R^{\cdot} \cup \{0\}$, which in turn is equivalent, by the results stated Section 4.12, to the condition that the orbits $R_b(a)$ ($a \in R - \{0\}, b \in R$) of the Lie root system R are all bounded.

Corollary 4.14.3.

Let $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ be symmetric. Then $\dim \mathfrak{g}_a = 1$ for all $a \in R^{\cdot}$.

4.15 Exclusion of sub types of R and $\mathfrak{g}$

Let R be a Lie root system and / or $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ a symmetric Lie algebra. We have observed that $\mathfrak{g}$ is reflective and Core $\mathfrak{g}$ is classical if and only if R is classical : R has no $Ra = R \cap \mathbb{Z}a$ of type W_1. The latter condition can be restricted "R excludes W_1" in the following language.

Definition 4.15.1.

Let S be a root system of rank r. Then R excludes S if $Ra_1, \ldots\ldots, a_r = R \cap (\mathbb{Z}a_1, \ldots\ldots, \mathbb{Z}a_r)$ is not isomorphic to S for any $a_1, \ldots\ldots, a_r \in R$. $\mathfrak{g} = \sum_{a \in R} \mathfrak{g}_a$ excludes S if R excludes S.

Theorem 4.15.2.

Let R be an irreducible Lie root system. Then **:**

1. R is classical or $R = R^0$ if and only if R excludes $W \oplus A$ and T_2;

2. R is classical or rank 1 if and only if R excludes $W \oplus A$, $W \oplus W$ and S_2 .

Proof:

One direction for both (**1**) and (**2**) is clear. For the other, suppose that R excludes $W \oplus A$ and T_2. Suppose that $a \in R^0, b \in R^{\cdot}$ and consider Rab. If a$\neq$ 0, then $Rab = W \cup A$ and $a + b \notin R$, since the possibilities $W \oplus A, T_2$ are exclude. It follows that $a, a' \in R^0$ and $a + a' \in R$ implies $a + a' \in R^0$: $a + a' =_{\text{def}} -b \in R^{\cdot} \Longrightarrow a + b \in R \Longrightarrow a = 0 \Longrightarrow a + a' = a' \in R^0$.

Similarly, $b, b' \in R^{\cdot}$ and $b + b' \in R$ implies $b + b' \in R \cup \{0\}$: $b + b' = -a \in R^0 \Longrightarrow a + b \in R \Longrightarrow a = 0 \Longrightarrow b + b' = 0 \in R^{\cdot} \cup \{0\}$. since R is irreducible, it follows that $R = R^0$ or $R = R^{\cdot} \cup \{0\}$. this proves (**1**).

For (**2**), suppose that R excludes $W \oplus A$, $W \oplus W$ and S_2. Then R also excludes T_2, so that R is classical or $R = R^0$. Let $a \in R - \{0\}$ and defines $S = R \cap ka$, $T = (R - S) \cup \{0\}$. Take $b \in T$ and note that $b \neq 0$ implies $Rab = W \cup W$ and $a + b \notin R$, by exclusion of $W \oplus W$. It follows that $, a' \in S$, $a + a' \in R$ implies $a + a' \in S$ and $b, b' \in T$, $b + b' \in R$ implies $b + b' \in T$, as in earlier arguments.

By irreducibility of R, therefore, $R = S$ and R has rank 1.