ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 319–329

JOURNAL OF PURE AND APPLIED ALGEBRA

Calculating the structure of a semisimple Lie algebra[1]

W.A. de Graaf

Faculty of Mathematics & Computer Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, Netherlands

Abstract

First we briefly describe two previously published algorithms: one that constructs a Cartan subalgebra and one that decomposes a semisimple Lie algebra L as a direct sum of simple ideals. Then, by reducing L modulo a prime we derive an algorithm to obtain the type of L (thereby solving the isomorphism problem for semisimple Lie algebras over $\bar{\mathbf{Q}}$ having structure constants in $\mathbf{Q}$). © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 17-08, 17B05, 17B20

1. Introduction

In this paper we deal with finite-dimensional Lie algebras from a computational point of view. Given a Lie algebra L, we would like to compute as much of its structure as possible. In some cases (e.g., when L is nilpotent) there is no elaborate structure theory available, and consequently this plan does not seem very promising. On the other hand, for the important class of semisimple Lie algebras the structure theory is very rich. Here we present some algorithms that calculate parts of this structure.

First we give a brief overview of parts of the existing theory for semisimple Lie algebras. For the proofs we refer to the standard monographs [4, 5].

Let L be an arbitrary Lie algebra. A Cartan subalgebra H of L is a nilpotent subalgebra that equals its own normaliser in L. Over ground fields of characteristic 0, Cartan subalgebras are known to exist (see Section 2). Now we transcribe a result from Jacobson's book:

[1] This research is supported by the technology foundation (STW).

PII S0022-4049(97)00016-9

Lemma 1. *Let A, B be linear transformations in a finite-dimensional vector space V satisfying*

$$[A,[A,\ldots,[A,B]\ldots]]=0 \ (n \text{ factors } A)$$

for some n. Let p be a polynomial and let $V_{p(A)}=\{v\in V \mid p(A)^m v=0 \text{ for some } m>0\}$. Then $V_{p(A)}$ is invariant under B.

Proof. See [5, p. 40]. □

Via the adjoint representation, H is viewed as a nilpotent Lie algebra of linear transformations of the vector space L. Since H is nilpotent, Lemma 1 applies to any pair of its elements. Hence L decomposes as a direct sum

$$L=L_0\oplus L_1\oplus\cdots\oplus L_s$$

of stable subspaces such that the restriction of any element to L_i has a minimum polynomial that is a prime power [5, p. 41]. The subspace L_0 corresponds to the polynomial X. It can be proved that it equals H [5, p. 58].

Now let L be a semisimple Lie algebra and let the ground field F be algebraically closed. Then it turns out that the matrices $\operatorname{ad} h$ for $h\in H$ are simultaneously diagonalisable. It follows that there are functionals $\alpha_i : H\to F$ such that

$$L=H\oplus L_{\alpha_1}\oplus\cdots\oplus L_{\alpha_m},$$

where $L_{\alpha_i}=\{x\in L \mid \operatorname{ad} h(x)=\alpha_i(h)x \text{ for all } h\in H\}$. These α_i are called *roots* and the L_{α_i} *root spaces*. It can be proved that the root spaces are all one dimensional. The set $R=\{\alpha_1,\ldots,\alpha_m\}$ is a root system in the vector space H^*. To a root system corresponds a matrix, called the *Cartan matrix*. The root systems are classified by their Cartan matrices (see, e.g., [4]) and as a consequence the classification of the simple Lie algebras over algebraically closed ground fields of characteristic 0 is obtained.

If L is semisimple rather than simple, then L is a direct sum

$$L=I_1\oplus\cdots\oplus I_t,$$

where the I_k are simple ideals of L [5, Theorem 3, p. 71]. There is a corresponding decomposition of the set of roots $R=R_1\cup\cdots\cup R_t$, where R_k is the root system of I_k. As a consequence also all semisimple Lie algebras over algebraically closed ground fields of characteristic 0 are classified.

Here we suppose that a Lie algebra L over the field F of dimension n is given by an array of n^3 structure constants $(c_{ij}^k)\in F^3$ for $1\le i,j,k\le n$ such that the Lie multiplication is described by

$$[x_i,x_j]=\sum_{k=1}^{n} c_{ij}^k x_k,$$

where $\{x_1,\ldots,x_n\}$ is a basis of L. Concerning the input field F, we assume throughout that it is of characteristic zero. For simplicity, we frequently assume $F=\mathbf{Q}$, the field

of rational numbers. However, all our methods work also over more general fields that admit efficient symbolic arithmetic.

For Lie algebras given by an array of structure constants it is easy to check whether L is semisimple (for instance, by using the fact that L is semisimple if and only if its Killing form is nondegenerate). If L happens to be semisimple then one would like to compute the structure described above. However, because we need to diagonalise the elements of a Cartan subalgebra, in general this theory is only valid over algebraically closed ground fields. And on a computer such fields are not feasible. In this paper we present some methods dealing with this problem. In Section 2 an algorithm for the computation of a Cartan subalgebra (central in the theory of semisimple Lie algebras) is described. Then in Section 3 we show a method to decompose a semisimple Lie algebra into a direct sum of simple ideals. Finally, in Section 4 we present an algorithm to obtain the type of a semisimple Lie algebra.

The algorithms described here have been implemented in GAP, inside a library of routines operating on Lie algebras called ELIAS (Eindhoven LIe Algebra System).

2. Calculating a Cartan subalgebra

In this section we treat the problem of finding a Cartan subalgebra of a Lie algebra L of characteristic 0. Several solutions have been given in the literature [1, 3, 10]. We follow [3] because we think it leads to the most elegant algorithm.

For an element x of L, we set

$$L_0(x) = \{y \in L \mid (\operatorname{ad} x)^m y = 0 \text{ for some } m > 0\}.$$

From Humphreys' book [4] we have the following lemma:

Lemma 2. *Let x be an element of L and set $K = L_0(x)$. Then K is a subalgebra and $N_L(K) = K$.*

Proof. See [4, pp. 78, 79]. □

From this it follows that a subalgebra of the form $L_0(x)$ is "almost" a Cartan subalgebra. We must only make sure that it is nilpotent. The idea is to start with a subalgebra $L_0(x)$ and then make it smaller until it is nilpotent. To do this we need to be able to find elements $x \in L$ such that $\operatorname{ad} x$ is not nilpotent (otherwise $L_0(x) = L$). To this end we have the following proposition.

Proposition 3. *Let L be a nonnilpotent Lie algebra over a field of characteristic 0 with basis $\{x_1, \ldots, x_n\}$, then the set*

$$\{x_1, \ldots, x_n\} \cup \{x_i + x_j \mid 1 \leq i < j \leq n\}$$

contains a nonnilpotent element.

Proof. If L is solvable but not nilpotent then by [5, Corollary 2, p. 45], we have that the nil radical of L is the set of all nilpotent elements of L. Hence, there must be a basis element x_i such that x_i is not nilpotent. On the other hand, if L is not solvable, then the Killing form of L cannot be identically zero (because it is nondegenerate on the semisimple part of L). It follows that there exist basis elements x_i and x_j for $1 \leq i \leq j \leq n$ such that $\mathrm{Tr}(\mathrm{ad}\, x_i \cdot \mathrm{ad}\, x_j) \neq 0$. From $\mathrm{Tr}((\mathrm{ad}\, x_i + \mathrm{ad}\, x_j)^2) - \mathrm{Tr}((\mathrm{ad}\, x_i)^2) - \mathrm{Tr}((\mathrm{ad}\, x_j)^2) = 2\,\mathrm{Tr}(\mathrm{ad}\, x_i \cdot \mathrm{ad}\, x_j) \neq 0$, we infer that the elements x_i, x_j and $x_i + x_j$ cannot be all nilpotent. □

Now using the following proposition, we can make a subalgebra $L_0(x)$ smaller until it is a Cartan subalgebra.

Proposition 4. *Suppose that L is not nilpotent over a field F. Let Ω be a subset of F of size* $\dim L + 1$. *Let x be a nonnilpotent element of L. Suppose that $L_0(x)$ is not a nilpotent subalgebra and let y be a nonnilpotent element of $L_0(x)$. Then there exists a $c_0 \in \Omega$ such that $L_0(x + c_0(y - x))$ is properly contained in $L_0(x)$.*

Proof. The proof can be obtained by a careful reformulation of the proof of Lemma 15.2 A in [4] (see also [3]). We omit it here.

This proposition implies that the following algorithm terminates:

Algorithm Cartan
Input: A Lie algebra L.
Output: A Cartan subalgebra of L.

Step 1: If L is nilpotent, then return L, otherwise go to Step 2.
Step 2: Let x be a nonnilpotent element of L. If $L_0(x)$ is nilpotent then return $L_0(x)$, otherwise go to Step 3.
Step 3: Let y be a nonnilpotent element of $L_0(x)$ and let c be a scalar such that $L_0(x+c(y-x))$ is properly contained in $L_0(x)$. Return to Step 2 with $x+c(y-x)$ in place of x.

Remark 5. This algorithm runs in polynomial time. For the details we refer to [3].

3. The decomposition into simple components

In this section we suppose that L is a semisimple Lie algebra and we try to find the decomposition of L into a direct sum of simple ideals. Here we follow [2]. Let H be a Cartan subalgebra of L. We will use the adjoint action of H on L to decompose L as a direct sum of simple ideals. Let $\{h_1, \ldots, h_l\}$ be a basis of H. A decomposition

$$L = L_1 \oplus \cdots \oplus L_s \oplus H$$

will be called a *generalised Cartan decomposition* of L with respect to H if for $1 \leq i \leq l$ and $1 \leq j \leq s$ we have the following:

(i) L_j is mapped into itself by $\operatorname{ad} h_i$,

(ii) the minimum polynomial of the restriction of $\operatorname{ad} h_i$ to L_j is irreducible.

Since the $\operatorname{ad} h_i$ are semisimple transformations, they all have a square free minimum polynomial. Hence, Lemma 1 gives an easy algorithm to compute a generalised Cartan decomposition of L with respect to H.

Proposition 6. *Let L be a semisimple Lie algebra over a field F of characteristic 0. Let H be a Cartan subalgebra of L. Suppose that*

$$L = L_1 \oplus \cdots \oplus L_s \oplus H$$

is a generalised Cartan decomposition of L with respect to H. Then the minimum polynomial of $\operatorname{ad} h$ for every $h \in H$ restricted to L_j is irreducible.

Proof. Let $h \in H$ and let f be the minimum polynomial of the restriction of $\operatorname{ad} h$ to L_j (for a certain $j \in \{1, \ldots, s\}$). Suppose f is reducible, i.e., $f = f_1 f_2$. Then L_j decomposes accordingly:

$$L_j = V_1 \oplus V_2,$$

where V_1 and V_2 are stable under H (by Lemma 1) and the minimum polynomial of the restriction of $\operatorname{ad} h$ to V_k is f_k for $k = 1, 2$. Now we tensor L with the algebraic closure of F. Then L splits as a direct sum of root spaces that are one dimensional. The roots are determined by their values on the basis elements of H. The minimum polynomial of the restriction of a basis element to L_j is irreducible. So the minimum polynomials of the restrictions of a basis element to V_1 and V_2 are the same. Hence in L_j there is at least one root space of dimension > 1. (For every eigenvalue there is an eigenvector in V_1, but also in V_2.) But this is impossible. Hence f is irreducible. □

The next theorem states that the generalised Cartan decomposition of L with respect to a Cartan subalgebra is compatible with the direct sum decomposition of L.

Theorem 7. *Let L and H be the same as in Proposition 6 and let*

$$L = L_1 \oplus \cdots \oplus L_s \oplus H$$

be a generalised Cartan decomposition of L with respect to H. Suppose that L decomposes as a direct sum of ideals, $L = I_1 \oplus I_2$. Then every L_i is contained in I_1 or in I_2.

Proof. We can write

$$L_i = L_i \cap I_1 \oplus W \oplus L_i \cap I_2.$$

We note that H decomposes as $H = H_1 \oplus H_2$ where H_l is a Cartan subalgebra of I_l for $l = 1, 2$. By Proposition 6 there is an element $h \in H_1 \cup H_2$ such that the restriction

of $\operatorname{ad} h$ to L_i is nonsingular. (Otherwise the minimum polynomial of the restriction of every element of a basis of H to L_i would be X. This implies that $[H, L_i] = 0$ and by definition of Cartan subalgebra we have $L_i \subset H$, a contradiction.)

First suppose that $h \in H_1$. Then also $h \in I_1$ so that $\operatorname{ad} h(L) \subset I_1$ and in particular $\operatorname{ad} h(L_i) \subset I_1$. Now the fact that $\operatorname{ad} h$ is nonsingular on L_i implies that $W \oplus L_i \cap I_2 = 0$. Hence L_i is contained in I_1. In the same way $h \in H_2$ implies that L_i is contained in I_2. □

This theorem implies that the following algorithm is correct.

Algorithm Decompose
Input: A semisimple Lie algebra L.
Output: A list of bases of the direct summands of L.

Step 1: Compute a generalised Cartan decomposition

$$L = L_1 \oplus \cdots \oplus L_s \oplus H.$$

Step 2: For $1 \leq i \leq s$ determine a basis of the ideal of L generated by L_i.
Step 3: Delete multiple instances from the list.

Remark 8. If L is defined over a field of characteristic $p \neq 2, 3$, then the statements of this section hold for L, provided that the Killing form of L is nondegenerate. In this case L behaves like a semisimple Lie algebra of characteristic 0 (see [9]).

Remark 9. The method runs in polynomial time except (maybe) for Step 1, where an oracle is called to factor polynomials. For the algorithmic problem of factoring polynomials many solutions have been given (see [7]). Some of these methods do not run in polynomial time, others use randomisation. So the running time as well as the nature (deterministic or randomized) of the algorithm depend on the specific factoring algorithm used.

4. Identifying a semisimple Lie algebra

Over algebraically closed fields (of characteristic 0) all semisimple Lie algebras have been classified. A simple Lie algebra is isomorphic either to an element of one of the "great" classes of simple Lie algebras (A_l, B_l, C_l, D_l) or to one of the exceptional Lie algebras (E_6, E_7, E_8, F_4, G_2). And the semisimple Lie algebras are sums of the simple ones. If a given Lie algebra L over $\mathbf{Q}$ is isomorphic to e.g. $A_2 + D_5 + G_2$ (when viewed over $\bar{\mathbf{Q}}$), then we call $A_2 + D_5 + G_2$ the *type* of L.

For a semisimple Lie algebra we would like to be able to obtain its type. This is equivalent to solving the isomorphism problem for semisimple Lie algebras over algebraically closed fields of characteristic 0, having structure constants in $\mathbf{Q}$. In general,

Table 1
Structure constants of a six-dimensional semisimple Lie algebra

	x_1	x_2	x_3	x_4	x_5	x_6
x_1	0	0	$2x_4$	$-2x_3$	$-2x_6$	$2x_4$
x_2	0	0	$2x_3$	$2x_4$	$-2x_5$	$-2x_6$
x_3	$-2x_4$	$-2x_3$	0	0	x_2	x_1
x_4	$2x_3$	$-2x_4$	0	0	x_1	$-x_2$
x_5	$2x_6$	$2x_5$	$-x_2$	$-x_1$	0	0
x_6	$-2x_5$	$2x_6$	$-x_1$	x_2	0	0

however, to calculate the root system and the corresponding Cartan matrix, we need arbitrary number fields. We have an example illustrating this.

Example 10. Let L be a six dimensional Lie algebra over the field of rational numbers with structure constants shown in Table 1. (It is the semisimple part of the Poincaré algebra.)

Then the determinant of the Killing form is -2^{20}, and hence L is semisimple. It is immediately seen that x_1 is not nilpotent and that $L_0(x_1) = \langle x_1, x_2 \rangle$ is a Cartan subalgebra. The transformations $\operatorname{ad} x_1$ and $\operatorname{ad} x_2$ have minimum polynomials $X^3 + 4X$ and $X^3 - 4X$, respectively. The decomposition of Section 3 is

$$L = L_{1,2} \oplus L_{3,4} \oplus L_{5,6}$$

where $L_{i,j}$ is the subspace of L spanned by x_i and x_j. From the multiplication table it follows that the ideals generated by $L_{3,4}$ and $L_{5,6}$ are both equal to L. Hence, by Theorem 7 we have that L is simple. However, over $\bar{\mathbf{Q}}$ there is only one six-dimensional semisimple Lie algebra, namely $A_1 + A_1$. In this case, to obtain a splitting of the Cartan subalgebra, we need the field $\mathbf{Q}(\sqrt{-1})$, a field of degree two. "Generically" the degree of the field needed is $k!$ if the degree of an irreducible factor of the minimum polynomial of an $\operatorname{ad} h$ is k.

The idea we pursue here is to avoid working over large number fields by reducing the Lie algebra modulo a prime number p. (Note that if we multiply all basis elements by a scalar λ, then the structure constants relative to this new basis are also multiplied by λ, so that we can get all structure constants to be integers.) The algebraic extensions of F_p are much easier to handle. If p does not divide the determinant of the matrix of the Killing form, then the reduced Lie algebra fits into a similar classification (see [9]). The only thing we have to prove is that both Lie algebras produce equivalent Cartan matrices.

Throughout we assume that L is a semisimple Lie algebra with structure constants in $\mathbf{Z}$ and with Cartan subalgebra H. The Killing form on L will be denoted by κ. Let $\{h_1, \ldots, h_l\}$ be a basis of H and let f_i be the characteristic polynomial of $\operatorname{ad} h_i$ for $1 \leq i \leq l$. Write $f_i = X^{m_i} g_i$ where $g_i(0) \neq 0$. If $p \geq 7$ is a prime number not dividing the determinant of the matrix of the Killing form and not dividing the numbers $g_i(0)$

for $1 \leq i \leq l$, then p is called *pleasant*. In the sequel we use a fixed pleasant prime number p.

Let F be the smallest number field containing all eigenvalues of the $\operatorname{ad} h$ for $h \in H$ and let $\mathcal{O}_F$ be the ring of algebraic integers of F. There exists a prime ideal P of $\mathcal{O}_F$ such that $P \cap Z = (p)$ (see [6, p. 9]). Let

$$\mathcal{O}_F^P = \left\{ \frac{x}{y} \mid x \in \mathcal{O}_F, \ y \in \mathcal{O}_F \backslash P \right\}$$

be the localization of $\mathcal{O}_F$ at P. Let M_p be the unique maximal ideal of $\mathcal{O}_F^P$. It follows that $\mathcal{O}_F^P / M_p = F_{p^m}$, the finite field of p^m elements. In the sequel we view L as a Lie algebra over $\mathcal{O}_F^P$ and we set

$$L_p = L \otimes F_{p^m}.$$

Let $\phi : \mathcal{O}_F^P \to F_{p^m}$ be the projection map. In the obvious way we extend ϕ to a map from L into L_p. Let $\{x_1, \ldots, x_n\}$ be a basis of L. Then

$$\phi\left(\sum_{i=1}^{n} a_i x_i \right) = \sum_{i=1}^{n} \phi(a_i) \bar{x}_i,$$

where $\{\bar{x}_1, \ldots, \bar{x}_n\}$ is a basis of L_p. Then the structure constants of L_p are the images under ϕ of the structure constants of L, and hence they lie in the prime field F_p. From this it follows that the Killing form κ_p of L_p satisfies

$$\kappa_p(\phi(x), \phi(y)) = \phi(\kappa(x, y)) \quad \text{for } x, y \in L.$$

Because p is pleasant, we have that κ_p is nondegenerate.

Let H_p be the image under ϕ of H. The map ϕ induces a map

$$\tilde{\phi} : H^* \to H_p^*.$$

If $\lambda : H \to \mathcal{O}_F^P$ is an element of H^*, then we set $\tilde{\phi}(\lambda)(\phi(h)) = \phi(\lambda(h))$. The image of a $\lambda \in H^*$ is denoted by $\bar{\lambda}$.

Since $\mathcal{O}_F^P$ contains all eigenvalues of $\operatorname{ad} h_i$ for $1 \leq i \leq l$, we have that the roots exist over $\mathcal{O}_F^P$ (though the root vectors need not exist, because $\mathcal{O}_F^P$ is not a field). Let $R \subset H^*$ be the set of roots and denote the image of R under $\tilde{\phi}$ in H_p^* by $\bar{R}$. Then the elements of $\bar{R}$ are the roots of L_p (since L_p is defined over a field the root vectors do exist in this case).

Lemma 11. *The subalgebra H_p of L_p is a Cartan subalgebra of L_p.*

Proof. Let α be a root of L. The fact that p is pleasant implies that the multiplicity of 0 as a root of f_i is the same as the multiplicity of 0 as a root of $\bar{f}_i$ and hence $\bar{\alpha}$ is nonzero. So if $x_{\bar{\alpha}}$ is a nonzero element of the root space of L_p belonging to $\bar{\alpha}$, then there is an index i such that $[\bar{h}_i, x_{\bar{\alpha}}] = \bar{\alpha}(\bar{h}_i) x_{\bar{\alpha}}$ is nonzero. Hence, if $[\bar{h}, \bar{x}] \in H_p$ for an $\bar{x} \in L_p$ and all $\bar{h} \in H_p$, then $\bar{x} \in H_p$. The fact that H_p is nilpotent is trivial. □

Lemma 12. *The restriction of κ_p to H_p is nondegenerate.*

Proof. Let h be an element of H and $\bar{h}$ be its image in H_p. Let $L = H \oplus L_1$ be the Fitting decomposition of L relative to H (see [5, p. 57]). Then from [5, p. 108], it is seen that $\kappa(h, x) = 0$ for all $x \in L_1$. Hence also $\kappa_p(\bar{h}, \bar{x}) = 0$. Because κ_p is nondegenerate there must be a $g \in H$ such that $\kappa_p(\bar{h}, \bar{g})$ is nonzero. □

It is well known that we can identify H and H^* because the Killing form is nondegenerate. Let λ be an element of H^*. Then the corresponding element $\theta(\lambda)$ of H is required to satisfy $\kappa(\theta(\lambda), h) = \lambda(h)$ for all $h \in H$. If $\{h_1, \ldots, h_l\}$ is a basis of H and $\theta(\lambda) = a_1 h_1 + \cdots + a_l h_l$, then we have the system of equations

$$(\kappa(h_i, h_j)) \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = \begin{pmatrix} \lambda(h_1) \\ \vdots \\ \lambda(h_l) \end{pmatrix}. \tag{1}$$

By Lemma 12 the determinant of the matrix of this system is an integer not divisible by p. Hence, by Cramer's rule, there exists a unique solution over $\mathcal{O}_F^P$. Also by Lemma 12 we have that in the case of L_p there is a similar map θ_p.

Lemma 13. *We have the following identity*:

$$\phi \circ \theta = \theta_p \circ \tilde{\phi}.$$

Proof. Choose $\lambda \in H^*$ and suppose that $\theta_p(\tilde{\phi}(\lambda)) = b_1 \bar{h}_1 + \cdots + b_l \bar{h}_l$, where $b_i \in F_{p^m}$. Then because $\tilde{\phi}(\lambda)(\bar{h}_i) = \phi(\lambda(h_i))$ we have that the equation system for the b_i is just the image under ϕ of the equation system (1). Hence, $b_i = \phi(a_i)$ and we are done. □

Using the map θ, an inner product $(\ ,\ )$ is defined on H^*, by

$$(\lambda, \mu) = \kappa(\theta(\lambda), \theta(\mu)).$$

In the same way there is an inner product $(\ ,\ )_p$ on H_p^*.

Lemma 14. *For $\lambda, \mu \in H^*$ we have $\phi((\lambda, \mu)) = (\bar{\lambda}, \bar{\mu})_p$.*

Proof. The proof is by straightforward calculation:

$$\begin{aligned} \phi((\lambda, \mu)) &= \phi(\kappa(\theta(\lambda), \theta(\mu))) \\ &= \kappa_p(\phi(\theta(\lambda)), \phi(\theta(\mu))) \\ &= \kappa_p(\theta_p(\tilde{\phi}(\lambda)), \theta_p(\tilde{\phi}(\mu))) \quad \text{by Lemma 13} \\ &= (\tilde{\phi}(\lambda), \tilde{\phi}(\mu))_p. \end{aligned}$$

□

Let α and β be two roots, then we set

$$\frac{2(\alpha,\beta)}{(\beta,\beta)} = \langle \alpha, \beta \rangle.$$

For the modular case we have a similar formula

$$\frac{2(\bar{\alpha},\bar{\beta})_p}{(\bar{\beta},\bar{\beta})_p} = \langle \bar{\alpha}, \bar{\beta} \rangle_p.$$

We remark that by [8, Theorem 5.6], it follows that $(\bar{\beta},\bar{\beta})_p$ is nonzero.

Following [9], we call a set of roots $\{\alpha_1,\ldots,\alpha_l\}$ a fundamental system if the following is satisfied:

(i) If α is a root, then one of the following holds:
  (a) α is a member of a sequence of the form α_{i_1}, $\alpha_{i_1}+\alpha_{i_2},\ldots$,
  (b) $-\alpha$ is a member of such a sequence,

(ii) Every diagonal minor of the matrix $(\langle \alpha_i, \alpha_j \rangle)$ is positive.

In the modular case the matrix in (2), will be an integer matrix (a_{ij}) such that $\phi(a_{ij}) = \langle \alpha_i, \alpha_j \rangle_p$ and $a_{ij} = 2, 0, -1, -2$ or -3. The matrix $(\langle \alpha_i, \alpha_j \rangle)$ is the Cartan matrix of the root system.

Proposition 15. *Let C be the Cartan matrix of R and let $\bar{C}$ be the Cartan matrix of $\bar{R}$. Then $\phi(C) = \bar{C}$.*

Proof. Let $\{\alpha_1,\ldots,\alpha_l\}$ be a fundamental system of roots in H^*. Then it is immediate that $\{\bar{\alpha}_1,\ldots,\bar{\alpha}_l\}$ is a fundamental system of roots in H_p^*. Hence Lemma 14 implies that

$$\langle \bar{\alpha}_i, \bar{\alpha}_j \rangle_p = \phi(\langle \alpha_i, \alpha_j \rangle). \qquad \square$$

Corollary 16. *From the Cartan matrix of $\bar{R}$ we can recover the Cartan matrix of R.*

Proof. The numbers $\langle \alpha_i, \alpha_j \rangle$ are known to be $2, 0, -1, -2$ or -3 [5, p. 121]. Because $p \geq 7$, we can recover those numbers from their images in F_p. Now Proposition 15 finishes the proof. $\square$

The above results lead to the following algorithm:

Algorithm Type
Input: A semisimple Lie algebra L over $\mathbf{Q}$.
Output: The type of L.

Step 1: Calculate a Cartan subalgebra H of L (Section 2).
Step 2: Extend a basis of H to a basis of L and multiply by an integer in order to ensure that all structure constants relative to this basis are integers.
Step 3: Determine a pleasant prime p.

Step 4: Consider the Lie algebra $L_p = L \otimes F_{p^m}$ where m is large enough to ensure that the characteristic polynomials of $\operatorname{ad} h_i$ for h_i in a basis of H_p split into linear factors.

Step 5: Decompose L_p into a direct sum of simple ideals (Section 3).

Step 6: For each component of L_p, determine a fundamental system inside the root system. Calculate the Cartan matrices which determine the type of L.

Remark 17. The integer m in Step 4 will be the least common multiple of the degrees of the irreducible factors of the minimum polynomial of $\operatorname{ad} h_i$, where h_i runs over a basis of H. We cannot prove that this number is polynomial in the dimension of L. However, this bound is much better than the bound on the degree of a splitting field of characteristic zero.

Remark 18. The number -3 will occur in the Cartan matrix only if there is a simple factor isomorphic to G_2. So if the semisimple Lie algebra L has no ideals of type G_2, then we can take $p \geq 5$. On the other hand, if a simple ideal I of L is of type G_2, then we can recognize it by inspection of the dimension and the rank. The conclusion is that we can always take $p \geq 5$.

References

[1] R.E. Beck, B. Kolman and I.N. Stewart, Computing the structure of a Lie algebra, in: R.E. Beck and B. Kolman, eds., Computers in Non-associative Rings and Algebras (Academic Press, New York, 1977) 167–188.

[2] W.A. de Graaf, An Algorithm for the decomposition of semisimple Lie algebras, preprint, 1996.

[3] W.A. de Graaf, G. Ivanyos and L. Rónyai, Computing Cartan subalgebras of Lie algebras, Applicable Algebra Eng., Comm. Comput., to appear.

[4] J.E. Humphreys, Introduction to Lie Algebras and Representation Theory (Springer, New York, 1972).

[5] N. Jacobson, Lie Algebras (Dover, New York 1979).

[6] S. Lang, Algebraic Number Theory (Springer, New York, 1994).

[7] A.K. Lenstra, Factorisation of polynomials, in: H.W. Lenstra Jr. and R. Tijdeman eds., Computational Methods in Number Theory, Mathematical Centre Tract, Vol. 154 (Mathematical Centre, Amsterdam, 1982) 169–198.

[8] G.B. Seligman, On Lie Algebras of Prime Characteristic, Memoirs of the American Mathematical Society, No. 19, 1956.

[9] G.B. Seligman, Modular Lie Algebras (Springer, New York, 1967).

[10] H. Zassenhaus, On the Cartan subalgebra of a Lie algebra, Linear Algebra Appl. 52/53 (1983) 743–761.