Modular Lie Algebras

Dmitriy Rumynin*

March 11, 2010

How to use these notes

The lecture notes are split into 3 chapters, further split into 30 sections. Each section will be discussed on a separate lecture. There will be a cutoff point for the exam: a few of the last lectures will not appear on the exam.

Each section consists of subsections. Regular subsection are examinable. Vista and background subsections are not. Vista subsections contain blue-sky material for further contemplation. Background sections contain material that should be known to students but is still included to make the notes self-contained. I have no intention to examine background subsections but they are useful for understanding of the course. If you are missing some background, please, ask me and I could add a background subsection to remedy it.

Exercise sections contain exercises that you should attempt: they may appear on the exam. Proofs of propositions are examinable as soon as the proof is written or covered in class. Overall, 100% of the exam will be covered by these lecture notes and in-class proofs. Consult these written notes because my planning may not be perfect and some material in a section could be skipped during the lecture. You should still learn it because it could appear on the exam.

It is worth mentioning that I don't follow any particular book. Furthermore, no book is relevant enough. The lecture notes are not fully ready yet. All the updates will be available on the website. Check whether you have got the latest version. The final version will be available from the general office.

If you see any errors, misprints, oddities of my English, send me an email. Also write me if you think that some bits require better explanation. If you

want to contribute by writing a proof, an example, a valuable observation, please, do so and send them to me. Just don't use WORD. Send them as text files with or without LATEX: put all the symbols you want me to latex between $ $. All the contributions will be acknowledged and your name will be covered with eternal (sh)fame.

Introduction

We study modular Lie algebras, that is, Lie algebras over fields of positive characteristic in this course. After careful thinking I have chosen the following three topics to discuss:

- classification of simple Lie algebras,
- restricted Burnside problem,
- irreducible representations of classical simple Lie algebras.

The reasons to choose these three is my perception of what constitutes an important development in the area. Complete proofs are often long and complicated and the emphasis is definitely on understanding the concepts instead of proving all the results. The aim is to introduce various concepts from Algebra, Algebraic Geometry and Representation Theory and see how they are useful for solving mathematical problems.

Contents

1 Basics

We recall some basic definitions in this lecture. If you know how to associate Lie algebra to a Lie group, then all of this should be quite transparent.

1.1 Algebras and multiplications

Recall that an algebra over a field $\mathbb{K}$ of characteristic p is a vector space A with a $\mathbb{K}$-bilinear multiplication operation $\mu : A \times A \to A$, which we usually write in the standard shorthand notation $a * b$ or even ab instead of the long notation $\mu(a, b)$.

To an element $a \in A$ one can associate two linear operators $L_a, R_a : A \to A$ where $L_a(b) = ab$ and $R_a(b) = ba$. The names of this operators are intuitive: L_a is the left multiplication operator and R_a is the right multiplication operator.

These operators are useful for many things. One is that the algebra axioms can be reformulated in their terms. For instance, we need *associative algebras* that are characterised by the associativity identity $a(bc) = (ab)c$ for all $a, b, c \in A$ and the presence of identity element $1 \in A$ such that $L_1 = R_1 = \mathrm{Id}_A$. The associativity can be reformulated as $L_a \circ L_b = L_{ab}$ for all $a, b \in A$ in terms of the left multiplication. Equivalently, it says $R_c \circ R_b = R_{bc}$ for all $b, c \in A$ in terms of the right multiplication.

Another important class of algebras we use is *commutative algebras*. These are associative algebras which satisfy the commutativity identity $ab = ba$ for all $a, b \in A$. In terms of multiplication operators, it says that $L_a = R_a$ for all $a \in A$.

Our main protagonist is *Lie algebras*. They satisfy the anticommutativity and Jacobi identity. Both identities have subtle points which require some discussion. We define the anticommutativty as $a * a = 0$ for all $a \in A$. Notice that this implies that $0 = (a + b) * (a + b) - a * a - b * b = a * b + b * a$ and, consequently, $a * b = -b * a$ for all $a, b \in A$. This property can be reformulated as $L_a = -R_a$ for all $a \in A$. Notice that if $p \neq 2$ then this is equivalent to anticommutativity: $a * a = -a * a$ implies that $2a * a = 0$ and $a * a = 0$.

On the other hand, if $p = 2$ then $2a * a = 0$ always holds for trivial reasons. Moreover, $a * b = -b * a$ is the same as $a * b = b * a$ since $1 = -1$. This identity is commutativity. The anticommutativity is $a * a = 0$. One unintended consequence of this terminology is that anticommutativity implies commutativity.

The Jacobi identity is $(a * b) * c + (b * c) * a + (c * a) * b = 0$. We are going to reformulate it twice in the coming two subsections.

1.2 Endomorphisms and Derivations

The following terminology should be familiar to you from *Algebra-II*, although we are going to apply it to general algebras. *A homomorphism* of algebras is a linear map $f : A \to B$ such that $f(xy) = f(x)f(y)$. If A contains identity, we also require $f(1_A) = 1_B$. As a consequence the zero map is a homomorphism of associative algebras if and only if $B = 0$.

An isomorphism is a bijective homomorphism. *An endomorphism* is a homomorphism $f : A \to A$. Finally, *an automorphism* is an isomorphism $f : A \to A$.

A new notion, which you may have seen in *Lie Algebras* is a derivation. *A derivation* is a linear map $d : A \to A$ such that $d(ab) = d(a)b + ad(b)$, i.e. it satisfies Leibniz identity.

Proposition 1.1 *For an anticommutative algebra A the Jacobi identity is equivalent to the fact that each L_a is a derivation for each $a \in A$.*

PROOF: We rewrite Jacobi identity as $(a * b) * c + (c * a) * b = -(b * c) * a$. Using anticommutativity we rewrite further as $(a*b)*c+b*(a*c) = a*(b*c)$ that is exactly the fact that L_a is a derivation. □

Notice that it is also equivalent to all right multiplications R_a being derivations.

1.3 Modules and Representations

These notions are usually interchangeable but we make an artificial distinction that we will follow through in the lecture notes. Let A be an algebra (no axioms assumed). We consider vector spaces V equipped with bilinear actions maps $A \times V \to V$ (denoted by $(a, v) \mapsto av$). Such a vector space can be *a module* or *a representation* if certain axioms are satisfied.

The module axiom is $(a * b)v = a(bv)$ for all $a, b \in A$, $v \in V$. If A contains 1, we also require $1v = v$ for all $v \in V$.

The representation axiom is $(a * b)v = a(bv) - b(av)$ for all $a, b \in A$, $v \in V$.

The way we set the distinction up ensures that it only makes sense to talk about modules for associative algebras and representations for Lie algebras. The notions of subrepresentation, quotient representation, submodule and quotient module are standard. Homomorphisms, isomorphisms, direct sums and isomorphism theorems work in the same way for modules and representations. Following the convention a representation V is *irreducible* if $V \neq 0$ and 0, V are the only subrepresentations, while a module with the similar property is called *simple*.

Proposition 1.2 *For an anticommutative algebra A the Jacobi identity is equivalent to the fact that A with the multiplication map is a representation of A.*

PROOF: A is a representation if and only if L_a is a derivation for each $a \in A$. One does not even need anticommutativity for this as $(a*b)*c+b*(a*c) = a*(b*c)$ is rewritten as $(a*b)c = a(bc) - b(ac)$. Now use Proposition 1.1. □

1.4 Simple algebras

A vector subspace I of an algebra A is *an ideal* if it is stable under all multiplications, i.e., $L_a(I) \subseteq I \supseteq R_a(I)$ for all $a \in A$. The significance of ideals is that they are kernels of homomorphisms. Besides they allow to define quotient algebras A/I.

An algebra A is simple if $A \neq 0$ and 0 and A are the only ideals. Simple algebras do not have non-trivial quotients. In particular, any homomorphism from a simple algebra is injective.

It is a popular problem in Algebra to classify simple algebras in a certain class of algebras. It often leads to interesting mathematics. For instance, in *Rings and Modules* you have seen Artin-Wedderburn theorem that states that simple associative artinian algebras are matrix algebras over division rings. In *Lie Algebras* you have seen the Cartan-Killing classification of simple finite dimensional Lie algebras over an algebraically closed field of characteristic zero. Our goal is to understand the following classification theorem, whose complete proof is beyond the scope of the present course.

Theorem 1.3 *Let $\mathbb{K}$ be an algebraically closed of characteristic $p \geq 5$. Then a finite dimensional simple Lie algebra over $\mathbb{K}$ is either of classical type or of Cartan type or of Melikian type.*

1.5 Commutation

If A is an algebra we define a new algebra $A^{[-]}$ as the same vector space with *the commutator product*: $[a, b] = a*b-b*a$. We call it *the commutator algebra* of A. Apriori, it is not clear why the commutator algebra is particularly significant, why the commutator product leads to more interesting mathematics than $a*b+b*a$ or $a*b-2010b*a$. The following proposition gives some explanation.

Proposition 1.4 *Let A be an associative algebra. Then $A^{[-]}$ is a Lie algebra.*

PROOF: The anticommutativity is obvious: $[a,a] = a*a - a*a = 0$. The Jacobi identity can be done by a straightforward check but we use a slightly more conceptual method. Let us check that L_a in $A^{[-]}$ is a derivation of A: $L_a(b)c + bL_a(c) = (ab-ba)c + b(ac-ca) = abc - bca = L_a(bc)$. It follows that it is a derivation of $A^{[-]}$: $L_a([b,c]) = L_a(bc) - L_a(cb) = L_a(b)c - cL_a(b) + bL_a(c) - L_a(c)b = [L_a(b), c] + [b, L_a(c)]$. Now use Proposition 1.1. □

Notice that $A^{[-]}$ can be a Lie algebra without A being associative (see the vista subsection below).

If M is an R-module then we denote $\mathrm{End}_R(M)$ the set of all R-module endomorphisms. It is an algebra under the composition of morphisms. In particular, if A is a vector space then $\mathrm{End}_{\mathbb{K}}(A)$ is the algebra of linear maps from A to A. It is irrelevant if A is an algebra itself: we still consider all linear operators.

Proposition 1.5 *Let A be an algebra. Derivations form a Lie subalgebra in $\mathrm{End}_{\mathbb{K}}(A)^{[-]}$.*

PROOF: Let c, d be two derivations. It suffices to check that a linear combination $\alpha c + \beta d$ for some $\alpha, \beta \in \mathbb{K}$ and the commutator $[c,d]$ are both derivations. We leave the linear combination to a reader and check the commutator. Pick $x, y \in A$. Then $[c,d](xy) = cd(xy) - dc(xy) = c(d(x)y + xd(y)) - d(c(x)y + xc(y)) = c(d(x))y + d(x)c(y) + c(x)d(y) + xc(d(y)) - d(c(x))y - c(x)d(y) - d(x)c(y) - xd(c(y)) = c(d(x))y - d(c(x))y + xc(d(y)) - xd(c(y)) = [c,d](x)y + x[c,d](y)$. □

We denote this Lie algebra of derivations by $\mathrm{Der}(A)$. The geometric nature of this Lie algebra are vector fields under their Lie bracket. To show this in familiar surroundings, let U be a connected open subset in $\mathbb{R}^n$. Let A be the algebra of all smooth functions $U \to \mathbb{R}$. It is a commutative algebra under pointwise multiplication and addition. It will require some analysis to show that every derivation of A is a vector field (and we will avoid this) but the reverse statement is clear. Indeed, every vector field $d = \sum_i \phi_i(\mathbf{x})\partial/\partial x_i$ can be applied to functions so that $d(\Psi(\mathbf{x})) = \sum_i \phi_i(\mathbf{x})\Psi_{x_i}(\mathbf{x})$ where we use superscripts to denote partial derivatives. The product rule for d follows from the familiar product rule for derivatives. It is instructive to compute $[c,d]$ where $c = \sum_i \theta_i(\mathbf{x})\partial/\partial x_i$:

$$[c,d] = \sum_i (\sum_j (\theta_j \phi_{i x_j} - \phi_j \theta_{i x_j}))\partial/\partial x_i$$

which can be directly checked by applying to a function Ψ.

1.6 Vista: affine structures on Lie algebras

An algebra is called *Lie-admissible* if $A^{[-]}$ is a Lie algebra. It is a wide class of algebras. We saw that it includes associative algebras but not only them. Let us define $(a,b,c) = (ab)c - a(bc)$ for elements $a,b,c \in A$. This element (a,b,c) (or this triple product $A \times A \times A \to A$) is called *an associator*. It measure the failure of associativity, similarly as the commutator measure the failure of associativity. An algebra is called *left symmetric* of the associator is left symmetric, i.e., $(a,b,c) = (b,a,c)$ for all $a,b,c \in A$. It is easy to check that left symmetric algebras are Lie-admissible.

In fact, left symmetric are important in Geometry. *An affine structure* on a Lie algebra $\mathfrak{g}$ is a left symmetric multiplication on $\mathfrak{g}$ whose commutator is the usual Lie multiplication. Algebraically, affine structure represents $\mathfrak{g} = A^{[-]}$ for a left symmetric algebra A. Geometrically, it corresponds to left invariant affine connections on the Lie group. More to follow.

1.7 Exercises

Let A be a finite-dimensional algebra over complex numbers $\mathbb{C}$. Prove that if $f : A \to A$ is a derivation then $e^f = I + f + f^2/2! + \ldots = \sum_{k=0}^{\infty} f^k/k!$ is an automorphism. Prove that if $e^{\alpha f} : A \to A$ is an automorphism for each $\alpha \in \mathbb{C}$ then f is a derivation.

State and prove the first isomorphism theorem for arbitrary algebras.

Prove the analogue of Proposition 1.1 for right derivations.

Prove that $[\theta\partial/\partial x, \phi\partial/\partial y] = \theta\phi_x\partial/\partial y - \phi\theta_y\partial/\partial x$.

2 Things that fail in positive characteristic

How come so many new Lie algebras slipped into the classification theorem? The reason is that many usual results in characteristic zero suddenly fail in positive characteristic.

2.1 Complete Reducibility

Define $\mathfrak{gl}_n = \mathfrak{gl}_n(\mathbb{K}) = M_n(\mathbb{K})^{[-]}$, $\mathfrak{sl}_n$ its subalgebra of matrices with zero trace. The standard basis of $\mathfrak{sl}_2$ is $\mathbf{e} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\mathbf{f} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\mathbf{h} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The products in the standard basis are computed commuting the matrices: $\mathbf{e} * \mathbf{f} = \mathbf{h}$, $\mathbf{h} * \mathbf{f} = -2\mathbf{f}$, $\mathbf{h} * \mathbf{e} = -2\mathbf{e}$. These three products completely determine the Lie algebra structure on $\mathfrak{sl}_2$.

Proposition 2.1 *If $p \geq 3$ then $\mathfrak{sl}_2$ is a simple Lie algebra.*

PROOF: Pick a nonzero element $\mathbf{x}$ and generate an ideal $I = (\mathbf{x})$. It suffices to show that $I = \mathfrak{sl}_2$. Pick a non-zero element and multiply it by e two times. This gives you $\mathbf{e} \in I$ and now multiplying by $\mathbf{f}$, you get $I = \mathfrak{sl}_2$. □

Let us now consider the polynomial algebra $\mathbb{K}[x, y]$. We define the action of $\mathfrak{sl}_2$ on A by formulas

$$\mathbf{e}\phi(x,y) = x\frac{\partial \phi}{\partial y},\ \mathbf{h}\phi(x,y) = x\frac{\partial \phi}{\partial x} - y\frac{\partial \phi}{\partial y},\ \mathbf{f}\phi(x,y) = y\frac{\partial \phi}{\partial x}$$

and then extended by linearity to an arbitrary element.

Proposition 2.2 *Under these formulas A is a representation of $\mathfrak{sl}_2$.*

PROOF: To conclude that A is a representation we must check that $(\mathbf{a}*\mathbf{b})\phi = \mathbf{a}(\mathbf{b}\phi) - \mathbf{b}(\mathbf{a}\phi)$ for all $\mathbf{a}, \mathbf{b} \in \mathfrak{sl}_2$, $\phi \in A$. Because of linearity it is sufficient to do only for the three basic products. We do it for one of them and leave the other two to the reader: $\mathbf{h}(\mathbf{e}\phi(x,y)) - \mathbf{e}(\mathbf{h}\phi(x,y)) = \mathbf{h}(x\phi_y) - \mathbf{e}(x\phi_x - y\phi_y) = x(x\phi_y)_x - y(x\phi_y)_y - x(x\phi_x)_y + x(y\phi_y)_y = x(\phi_y + x\phi_{yx}) - xy\phi_{yy} - x^2\phi_{xy} + x(\phi_y + y\phi_{yy}) = 2x\phi_y = 2\mathbf{e}\phi$. □

It is worse pointing out that elements of $\mathfrak{sl}_2$ act by differentiations and we get injective homomorphism of Lie algebras $\mathfrak{sl}_2 \to \mathrm{Der}(A)$. We interpret these facts geometrically: A are functions on the affine space $\mathbb{K}^2$, $\mathrm{Der}(A)$ are vector fields on $\mathbb{K}^2$, and the representation is a realization of $\mathfrak{sl}_2$ as vector fields on $\mathbb{K}^2$.

Let A_n be the subspace of homogeneous polynomials of degree n, i.e., it is a span of all $x^{n-k}y^k$. As the actions of $\mathbf{e}$, $\mathbf{f}$ and $\mathbf{h}$ preserve the degree, each A_n is a subrepresentation of A. We claim that A_p is not completely reducible.

Let us recall that a representation U is *completely reducible* if for any subrepresentation $W \subseteq U$ there exists another subrepresentation $V \subseteq U$ such that $U = V \oplus W$. A module with the same property is called *semisimple*. According to Weyl's complete reducibility, a finite dimensional representation of a finite dimensional simple Lie algebra over an algebraically closed of characteristic zero is completely reducible. We can see now that it fails in characteristic $p > 2$.

Let us check the claim. Let W be the span of x^p and y^p. This clearly submodule with the trivial action $\mathbf{a}x^p = 0$ for any $\mathbf{a} \in \mathfrak{sl}_2$ because $\partial x^p/\partial x = px^{p-1} = 0$. Suppose there is a complementary submodule V and pick nonzero $\phi \in V$. We can write $\phi = \sum_{k=n}^{p} \alpha_k x^k y^{p-k}$ with $\alpha_n \neq 0$ and $0 \neq n \neq p$. Then $\mathbf{e}^{p-n}(\phi) = \alpha_n x^p$ and $x^p \in V$, contradiction.

2.2 Lie's Theorem

Let us recall some standard material from Lie algebras to make these notes self-contained. If A is a linear subspace of a Lie algebra $\mathfrak{g}$, we define *its commutant* $[A, A]$ as the span of all products $x * y$, $x, y \in A$. The name comes from thinking of the Lie multiplication as commutation. Then inductively we define the derived series: $A^{(0)} = A$, $A^{(n+1)} = [A^{(n)}, A^{(n)}]$.

Proposition 2.3 *If I is an ideal of $\mathfrak{g}$ then $I^{(n)}$ is an ideal of $\mathfrak{g}$ for each n.*

PROOF: We prove it by induction on n. The basis of induction ($n = 0$) is our assumption. For the induction step, we have to show that $[J, J]$ is an ideal whenever J is an ideal. It is clear by the product rule for L_x: $\mathbf{x}(\mathbf{ab}) = (\mathbf{xa})\mathbf{b} + \mathbf{a}(\mathbf{xb}) \in [J, J]$ if $\mathbf{x} \in \mathfrak{g}$, $\mathbf{a}, \mathbf{b} \in J$. □

We say that an ideal I is n-soluble if $I^{(n)}$. An ideal is soluble if it is n-soluble for some n. The Lie algebra $\mathfrak{g}$ is soluble if $\mathfrak{g}$ is a soluble ideal.

Proposition 2.4 *(i) If $\mathfrak{g}$ is soluble then every subalgebra of $\mathfrak{g}$ and every quotient algebra of $\mathfrak{g}$ is soluble.*

(ii) If I is an ideal of $\mathfrak{g}$ and both I and $\mathfrak{g}/I$ are soluble then $\mathfrak{g}$ is soluble.

PROOF: The first statement is obvious. For the second statement, observe that the cosets of elements of $\mathfrak{g}^{(n)}$ are in $(\mathfrak{g}/I)^{(n)}$. This, if $\mathfrak{g}/I$ is n-soluble then $\mathfrak{g}^{(n)} \subseteq I$. Now if I is m-soluble then $\mathfrak{g}^{(n+m)} = (\mathfrak{g}^{(n)})^{(m)} \subseteq I^{(m)} = 0$. □

The following proposition immediately follows.

Proposition 2.5 *A sum of two soluble ideals is soluble.*

PROOF: By the second isomorphism theorem, $I + J/J \cong I/I \cap J$ is soluble as the quotient of I. Hence $I + J$ is soluble by Proposition 2.4. □

This allows to conclude that the radical $Rad(\mathfrak{g})$ of a finite-dimensional Lie algebra, defined as the sum of all soluble ideals, is itself soluble.

Lie's theorem states that over an algebraically closed field of zero characteristic, a finite-dimensional irreducible representation of a finite dimensional soluble Lie algebra must be one-dimensional. This fails in positive characteristic.

Let us consider a two dimensional Lie algebra $\mathfrak{g}$ with basis $\mathbf{x}$, $\mathbf{y}$. The multiplication is $\mathbf{x} * \mathbf{y} = \mathbf{y}$. It is 2-soluble as $\mathfrak{g}^{(1)} = \mathbb{K}\mathbf{y}$ and $\mathfrak{g}^{(2)} = 0$. Now let us consider a vector space V with a basis e_i, $i \in \mathbb{F}$ where $\mathbb{F}$ is a prime subfield with the action of $\mathfrak{g}$ defined by $\mathbf{x}e_i = ie_i$, $\mathbf{y}e_i = e_{i+1}$ and extended by bilinearity.

Proposition 2.6 *V is an irreducible representation of $\mathfrak{g}$ of dimension p.*

PROOF: To conclude that V is a representation it suffices to follow through the following calculation $\mathbf{x}(\mathbf{y}e_i) - \mathbf{y}(\mathbf{x}e_i) = \mathbf{x}e_{i+1} - \mathbf{y}ie_i = (i+1)e_{i+1} - ie_{i+1} = e_{i+1} = \mathbf{y}e_i$.

To show irreducibility consider a nonzero subrepresentation $U \subseteq V$ and an element $0 \neq z \in U$. Write $z = \sum_{i=0}^{p-1} \alpha_i e_i$. Then $\mathbf{x}z = \sum_i i\alpha_i e_i \in U$ and $\mathbf{x}^k z = \sum_i i^k \alpha_i e_i \in U$ for each positive k. These conditions can be now written in the matrix form as

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 2 & \cdots & p-2 & p-1 \\ 0^2 & 1^2 & 2^2 & \cdots & (p-2)^2 & (p-1)^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0^{p-1} & 1^{p-1} & 2^{p-1} & \cdots & (p-2)^{p-1} & (p-1)^{p-1} \end{pmatrix} \begin{pmatrix} \alpha_0 e_0 \\ \alpha_1 e_1 \\ \vdots \\ \alpha_{p-1} e_{p-1} \end{pmatrix} \in U^p$$

Notice that the column has the coefficients in V while the matrix has the coefficients in the field $\mathbb{K}$. Hence the product apriori has the coefficients in V and the condition tells us that the coefficients are actually in U. Now the matrix is Vandermonde's matrix and, in particular, is invertible. Multiplying by its inverse gives $\begin{pmatrix} \alpha_0 e_0 \\ \alpha_1 e_1 \\ \vdots \\ \alpha_{p-1} e_{p-1} \end{pmatrix} \in U^p$. We will refer to this consideration later on as Vandermonde's trick. As all $\alpha_i e_i$ are in U and one of α_i is

nonzero, one of e_i is in U. Applying $\mathbf{y}$ $p-1$ times we get that all e_i are in U. □

2.3 Cartan's Criteria

Recall that any finite dimensional algebra A admits Killing form $K : A \times A \to \mathbb{K}$ defined as $K(\mathbf{x}, \mathbf{y}) = \mathrm{Tr}(L_{\mathbf{x}} L_{\mathbf{y}})$. Observe that it is a symmetric bilinear form. In characteristic zero, there are two Cartan's criteria. Semisimple criterion states that a Lie algebra is semisimple if and only if its Killing form is non-degenerate, i.e., of maximal possible rank. The soluble criterion states that of K vanishes on $\mathfrak{g}^{(1)}$ then $\mathfrak{g}$ is soluble. Both criteria fail in positive characteristic.

Let $\mathbb{F}$ be the finite subfield of $\mathbb{K}$ of size p^n. The Witt algebra $W(1,n)$ is a p^n-dimensional vector space with basis $\mathbf{e}_i$, $i \in \mathbb{F}$ and multiplication by $\mathbf{e}_i * \mathbf{e}_j = (i-j)\mathbf{e}_{i+j}$.

Proposition 2.7 *(i) $W(1,n)$ is a Lie algebra.*
(ii) If $p \geq 3$ then $W(1,n)$ is simple.
(iii) If $p \geq 5$ then the Killing form on $W(1,1)$ is zero.

Proof: The anticommutativity is obvious because $i - j = -(j-i)$. The Jacobi identity is verified directly $(\mathbf{e}_i * \mathbf{e}_j) * \mathbf{e}_k + (\mathbf{e}_j * \mathbf{e}_k) * \mathbf{e}_i + (\mathbf{e}_k * \mathbf{e}_i) * \mathbf{e}_j = ((i-j)(i+j-k) + (j-k)(j+k-i) + (k-i)(k+i-j))\mathbf{e}_{i+j+k} = (i^2 - j^2 - ik + jk + j^2 - k^2 - ji + ki + k^2 - i^2 - kj + ij)\mathbf{e}_{i+j+k} = 0$.

To check simplicity, let us look at the ideal I generated by a non-zero element $x = \sum_{i \in \mathbb{F}} \alpha_i \mathbf{e}_i = \sum_{i \in S} \alpha_i \mathbf{e}_i$ where S is the subset of all i such that $\alpha_i \neq 0$. It suffices to show that $I = \mathfrak{g}$.

By the ideal property $x * \mathbf{e}_0 = \sum_{i \in S} i\alpha_i \mathbf{e}_i \in I$. Applying $R_{\mathbf{e}_0}$ several more times, we get $R^k_{\mathbf{e}_0}(x) = \sum_{i \in S} i^k \alpha_i \mathbf{e}_i \in I$. Using Vandermonde trick, $\mathbf{e}_i \in I$ for all $i \in S$.

As soon as $j \neq 2i$ for some $i \in S$, it follows that $\mathbf{e}_j = (2i-j)^{-1}\mathbf{e}_i * \mathbf{e}_{j-i} \in I$. If $p > 2$, we get $I = \mathfrak{g}$ in two iterations: $\mathbf{e}_i \in I$ implies $\mathbf{e}_j \in I$ for all $j \neq 2i$, hence at least for one more $j \neq i$. Then $2i \neq 2j$ and we conclude that $\mathbf{e}_{2i} \in I$.

Let us compute $K(\mathbf{e}_i, \mathbf{e}_j)$. Since $(\mathbf{e}_i * (\mathbf{e}_j * \mathbf{e}_k)) = (j-k)(i-j-k)\mathbf{e}_{i+j+k}$, it is immediate that $K(\mathbf{e}_i, \mathbf{e}_j) = 0$ unless $i = -j$. Finally, $K(\mathbf{e}_i, \mathbf{e}_{-i}) = \sum_{k \in \mathbb{F}} (-i-k)(2i-k) = \sum_{k \in \mathbb{F}}^{p-1} (-2i^2 - ik + k^2)$. This can computed using the usual formula $\sum_{t=0}^{n} t^2 = n(n+1)(2n+1)/6$ if the characteristic is at least 5: $K(\mathbf{e}_i, \mathbf{e}_{-i}) = -2i^2 p - ip(p-1)/2 + p(p+1)(2p+1)/6 = 0$. □

Thus, $W(1,1)$ is a counterexample to both Cartan criteria. In fact, so are $W(1,n)$, which is the first example of Cartan type Lie algebra.

2.4 Vista: Semisimple Lie algebras

One usually defines *a semisimple Lie algebra* as a finite dimensional Lie algebra such that $\mathrm{Rad}(\mathfrak{g}) = 0$. In characteristic zero, such an algebra is a direct sum of simple Lie algebras. It fails in characteristic p too.

Let $A = \mathbb{K}[z]/(z^p)$ be the commutative algebra of truncated polynomials. In characteristic p this algebra admits the standard derivation $\partial(z^k) = kz^{k-1}$. One needs characteristic p for this to be well-defined: ∂ is always well-defined on $\mathbb{K}[z]$ turning $\mathbb{K}[z]$ into a representation of the one-dimensional Lie algebra. The ideal (z^p) needs to be a subrepresentation. Since $\partial(z^p) = pz^{p-1}$ it happens only in characteristic p. Notice that the product rule for ∂ on A is inherited from the product rule for ∂ on $\mathbb{K}[z]$.

Now extend ∂ to the derivation of the Lie algebra $\mathfrak{sl}_2(A)$: $\partial \begin{pmatrix} f(z) & g(z) \\ h(z) & -f(z) \end{pmatrix} = \begin{pmatrix} f'(z) & g'(z) \\ h'(z) & -f'(z) \end{pmatrix}$. Finally, we define the Lie algebra $\mathfrak{g}$ as *a semidirect product* of a one dimensional Lie algebra ans $\mathfrak{sl}_2(A)$.

Abstractly speaking, we say that a Lie algebra $\mathfrak{k}$ acts on a Lie algebra $\mathfrak{h}$ if $\mathfrak{h}$ is a representation of $\mathfrak{k}$ and for each $x \in \mathfrak{k}$ the action operator $a \mapsto xa$ is a derivation of $\mathfrak{k}$. The semidirect product is the Lie algebra $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{h}$ with the product

$$(x, a) * (y, b) = (x * y, xb - ya + a * b)$$

.

Proposition 2.8 *The semidirect product is a Lie algebra, $\mathfrak{h}$ is an ideal, and the quotient algebra $\mathfrak{g}/\mathfrak{h}$is isomorphic to $\mathfrak{k}$.*

Proof: □

Hence $\mathfrak{g} = \mathbb{K}d \oplus \mathfrak{sl}_2(A)$ is $3p+1$-dimensional Lie algebra. Let us describe its properties.

Proposition 2.9 *$\mathfrak{g}$ admits a unique minimal ideal isomorphic to $\mathfrak{sl}_2(\mathbb{K})$. The commutant $\mathfrak{g}^{(1)}$ is equal to $\mathfrak{sl}_2(A)$.*

Proof: □

The first statement implies that $\mathfrak{g}$ is semisimple. The second statement implies that $\mathfrak{g}$ is not a direct sum of simple Lie algebras.

2.5 Exercises

Prove that if the Killing of $\mathfrak{g}$ is nondegenerate then the radical of $\mathfrak{g}$ is zero.

Compute the Killing form for $W(1, 1)$ in characteristic 3 (note it is non-degenerate there).

Show that in characteristic 2 all $\mathbf{e}_i$ with $i \neq 0$ span a nontrivial ideal of $W(1, n)$.

Show that $W(1, 1)$ is solvable in characteristic 2 and that its Killing form has rank 1.

3 Free algebras

3.1 Free algebras and varieties

Let X be a set. We define a free "thingy" (X) to be a free set with a binary operation without any axioms. Informally, it consists of all non-associative monomials of elements of X. To define it formally we can use recursion:

(basis) if $a \in X$ then $(a) \in (X)$,
(step) if $a, b \in X$ then $(ab) \in (X)$.

We will routinely skip all unnecessary brackets. For instance, if $X = \{a, b\}$, then the recursion basis will give us two elements of X: a and b. Using the recursion step for the first time gives 4 new elements: aa, ab, ba, bb. Using it for the second time promises to give 36 new elements, but since 4 products are already there, it gives only 32. We will not attempt to list all of them here but we will list a few: $a(aa)$, $(aa)a$, $(aa)b$, $a(ab)$, etc.

The fact that this defines a set is standard but not-trivial: it is called *Recursion Theorem*. Notice the difference with induction. Induction is an axiom and it is used only to verify a statement. Recursion is a theorem and it is used to construct a set (or a function or a sequence). Have you heard of recursive sequences?

Now the binary operation on (X) is defined by the recursive step: $a * b = (ab)$ as in the recursion step. Let $\mathbb{K}(X)$ be the vector space formally spanned by (X). It consists of formal finite linear combinations $\sum_{t \in (X)} \alpha_t t$, finite means that $\alpha_t = 0$ except for finitely many elements t. The vector space $\mathbb{K}(X)$ is an algebra: the multiplication on (X) is extended by bilinearity. We call it *the free algebra* of X because of the following universal property.

Proposition 3.1 (Universal property of the free algebra) *For each algebra A and a function $f : X \to A$ there exists a unique algebra homomorphism $\widetilde{f} : \mathbb{K}(X) \to A$ such that $f(z) = \widetilde{f}(z)$ for each $z \in X$.*

Proof: We start by extending f to a function $\widehat{f} : (X) \to A$ preserving the multiplication:

(basis) if $a \in X$ define $\widehat{f}(a) = f(a)$,
(step) if $a, b \in X$ define $\widehat{f}(ab) = \widehat{f}(a)\widehat{f}(b)$.

This is well-defined by recursion and it preserves the multiplication because of the recursive step. Any other such extension must also satisfy the recursion basis and steps. Hence, the extension is unique.

$\widehat{f}$ is defined on the basis of $\mathbb{K}(X)$ and we extend it to $\widetilde{f} : \mathbb{K}(X) \to A$ by linearity. Uniqueness is obvious. □

We can formulate Proposition 3.1. Think of X as a subset of $\mathbb{K}(X)$. Then we have the natural restriction function $R : \mathrm{Hom}(\mathbb{K}(X), A) \to \mathrm{Fun}(X, A)$ where $\mathrm{Fun}(X, A)$ is just the set of all functions from X to A. Proposition 3.1 essentially says that R is a bijection.

The elements of $\mathbb{K}(X)$ are nonassociative polynomials. They can be evaluated on any algebra. Formally let $X = \{x_1, \dots x_n\}$, $w(x_1, \dots x_n) \in \mathbb{K}(X)$, A an algebra, $a_1, \dots a_n \in A$. Consider a function $f : X \to A$ defined by $f(x_i) = a_i$. It is extended to a homomorphism $\widetilde{f} : \mathbb{K}(X) \to A$ by Proposition 3.1. Finally, we define $w(a_1, \dots a_n) = \widetilde{f}(w)$.

We say that $w(x_1, \dots x_n)$ is *an identity* of A if $w(a_1, \dots a_n) = 0$ for all $a_1, \dots a_n \in A$. Let us write $Id_X(A)$ for the set of all identities of A in $\mathbb{K}(X)$. Now we say that an ideal I of $\mathbb{K}(X)$ is *verbal* if $w(s_1, \dots s_n) \in I$ for all $w \in I$, $s_1, \dots s_n \in \mathbb{K}(X)$

Proposition 3.2 *The set $Id_X(A)$ is a verbal ideal for any algebra A.*

Proof: Let us first check that it is a vector subspace. If $v, w \in Id_X(A)$, $\alpha, \beta \in \mathbb{K}$ and $f : X \to A$ is an arbitrary function then $\widetilde{f}(\alpha v + \beta w) = \alpha\widetilde{f}(v) + \beta\widetilde{f}(w) = 0$. Hence $\alpha v + \beta w$ is also an identity of A.

The ideal property is similar. If $w \in Id_X(A)$, $v \in \mathbb{K}(X)$ then $\widetilde{f}(vw) = \widetilde{f}(v)\widetilde{f}(w) = \widetilde{f}(v)0 = 0$. Hence vw is an identity. Similarly, wv is an identity.

The verbality is intuitively clear since of $w(a_1, \dots a_n) = 0$ on A then $w(s_1(a_1, \dots a_n), \dots s_n(a_1, \dots a_n))$ will also be zero. Formally the substitution $x_i \mapsto a_i$ corresponds to a homomorphism $\widetilde{f} : \mathbb{K}(X) \to A$ while the substitution $x_i \mapsto s_i$ corresponds to a homomorphism $\widetilde{g} : \mathbb{K}(X) \to \mathbb{K}(X)$ and $w(s_1(a_1, \dots a_n), \dots s_n(a_1, \dots a_n)) = \widetilde{f}(\widetilde{g}(w))$. Define $h = \widetilde{f} \circ g : X \to \mathbb{K}(X)$. Since $h(z) = \widetilde{f}(\widetilde{g}(z))$ for each $z \in X$, we conclude that $\widetilde{h} = \widetilde{f} \circ \widetilde{g}$ and $\widetilde{f}(\widetilde{g}(w)) = \widetilde{h}(w) = 0$. □

3.2 Varieties of algebras

A variety of algebras is a class of algebras where a certain set of identities is satisfied. We can choose enough variables so that the set of identities is a subset S of $\mathbb{K}(X)$. Let $(S)_v$ be the verbal ideal generated by S. One can formally define $(S)_v$ as the intersection of all verbal ideals containing S. It follows from Proposition 3.2 that $(S)_v$ consists of the identities in variables of X satisfied in all the algebras of the variety. We have seen the following varieties already.

Ass is given by the identity $x(yz) - (xy)z$. It consists of all associative algebras, not necessarily with identity.

Com consists of all commutative algebras in *Ass*. Its verbal ideal is generated by $x(yz) - (xy)z$ and $xy - yx$.

Lie is the variety of Lie algebras and the identities are xx $x(yz) + y(zx) + z(xy)$.

$n - Sol$ consists of all n-soluble Lie algebras. Its additional identity w_n requires 2^n variables. We define it recursively: $w_1(x_1, x_2) = x_1 x_2$. Thus, 1-soluble Lie algebras are just algebras with zero multiplication. Then $w_{n+1} = w_n(x_1, \dots x_{2^n}) * w_n(x_{2^n+1}, \dots x_{2^{n+1}})$.

Let $\mathcal{V}$ be a variety. For each set X, the variety will have a verbal ideal $I_{\mathcal{V}}$ in $\mathbb{K}(X)$ of all identities in variables X that hold in $\mathcal{V}$. We define *the free algebra in the variety* $\mathcal{V}$ as $\mathbb{K}_{\mathcal{V}} < X >= \mathbb{K}(X)/I_{\mathcal{V}}$.

Proposition 3.3 *(Universal property of the free algebra in a variety) For every algebra A in a variety V the natural (restriction) function* $\mathrm{Hom}(\mathbb{K}_{\mathcal{V}} < X >, A) \to \mathrm{Fun}(X, A)$ *is a bijection.*

PROOF: Take a function $f : X \to A$ and consider its unique extension homomorphism $\widetilde{f} : \mathbb{K}(X) \to A$. It vanishes on $I_{\mathcal{V}}$ because elements of $I_{\mathcal{V}}$ are identities of A while $\widetilde{f}(w)$ are results of substitutions. Hence, $\overline{f} : \mathbb{K}_{\mathcal{V}} < X > \to A$ where $\overline{f}(w + I_{\mathcal{V}}) = \widetilde{f}(w)$ is well-defined. This proves that the restriction is surjective.

The injectivity of the restriction is equivalent to the uniqueness of this extension, which follows from the fact that X generates $\mathbb{K}_{\mathcal{V}} < X >$. □

3.3 Vista: basis in free Lie algebra and powers of representations

Although we have defined the free Lie algebra, it is a pure existence statement. Fortunately, there are ways to put hands on the free Lie algebra, for instance, by constructing a basis. Contrast this with the free alternative algebra: this is given by the verbal ideal generated by two identities $x(xy) - (xx)y$ and $x(yy) - (xy)y$. No basis of the free alternative alternative algebra $\mathbb{K}_{Alt}(X)$ is known explicitly if X has at least 4 elements.

The most well-known basis of the free Lie algebra is Hall basis but here we construct Shirshov basis. More to follow.

3.4 Exercises

Let $\mathbb{K}(X)_n$ be the space of homogeneous polynomials of degree n. Given $|X| = m$, compute the dimension of $\mathbb{K}(X)_n$.

4 Universal enveloping algebras

4.1 Free associative algebra and tensor algebra

The free algebra $\mathbb{K}_{Ass}(X)$ has associative multiplication but no identity element. This is why it is more conventional to introduce new algebra $\mathbb{K} < X >= \mathbb{K}\mathbf{1} \oplus \mathbb{K}_{Ass}(X)$ with the obvious multiplication: $(\alpha\mathbf{1}, a) * (\beta\mathbf{1}, b) = (\alpha\beta\mathbf{1}, \alpha b + \beta a + ab)$. This algebra $\mathbb{K} < X >$ will be called *the free associative algebra*. Its basis is the free monoid (a set with associative binary and identity) product $< X >$, generated by X.

Proposition 4.1 *(The universal property of $\mathbb{K} < X >$) For every associative algebra A and every function $f : X \to A$ there exists a unique homomorphism of algebras $\widetilde{f} : \mathbb{K} < X > \to A$ such that $\widetilde{f}(x) = f(x)$ for each $x \in X$.*

Proof: The homomorphism of associative algebras takes $\mathbf{1}$ to $\mathbf{1}$ and the extension to $\widehat{f} : \mathbb{K}_{Ass}(X) \to A$ exists and is unique by Proposition 3.3). Thus, $\widetilde{f}(\alpha\mathbf{1}, a) = \alpha\mathbf{1}_A + \widehat{f}(a)$ is uniquely determined. □

It is sometimes convenient to reinterpret the free associative algebra as *tensor algebra*. Let V be a vector space. We define the tensor algebra TV as the free associative algebra $\mathbb{K} < B >$ where B is a basis of V. Notice that TV depends on B up to a canonical isomorphism. If C is another basis, the change of basis matrix $c_i = \sum_i \alpha_{i,j} b_j$ gives a function $C \to \mathbb{K} < B >$, $c_i \mapsto \sum_i \alpha_{i,j} b_j$, which can be extended to the canonical isomorphism $\mathbb{K} < C > \to \mathbb{K} < B >$.

We are paying a price here for not having defined tensor products of vector spaces. It is acceptable for a student to use tensor products instead.

Notice that the natural embedding $B \to \mathbb{K} < B >$ of sets gives a natural linear embedding $V \to TV$.

Proposition 4.2 *(The universal property of TV) For every associative algebra A the natural (restriction) function $\mathrm{Hom}(TV, A) \to \mathrm{Lin}(V, A)$ is a bijection.*

Proof: Let B be a basis of V. The basis property can be interpreted as the fact the restriction function $\mathrm{Lin}(V, A) \to \mathrm{Fun}(B, V)$ is bijective. Now everything follows from Proposition 4.1. □

4.2 Universal enveloping algebra

If the vector space $V = \mathfrak{g}$ is a Lie algebra there is a special subset $\mathrm{Hom}(\mathfrak{g}, A) \subseteq \mathrm{Lin}(\mathfrak{g}, A)$ consisting of Lie algebra homomorphisms. This motivates the definition of *a universal enveloping algebra*. The universal enveloping algebra of a Lie algebra $\mathfrak{g}$ is $U\mathfrak{g} = T\mathfrak{g}/I$ where I is generated by all

$\mathbf{ab}-\mathbf{ba}-\mathbf{a}*\mathbf{b}$ for $a, b \in \mathfrak{g}$. Notice that $\mathbf{ab}$ is the product in $T\mathfrak{g}$ while $\mathbf{a}*\mathbf{b}$ is the product in $\mathfrak{g}$. Notice also that the natural linear map $\omega = \omega_{\mathfrak{g}} : \mathfrak{g} \to U\mathfrak{g}$ defined by $\omega(\mathbf{a}) = \mathbf{a} + I$ is a Lie algebra homomorphism from $\mathfrak{g}$ to $U\mathfrak{g}^{[-]}$: $\omega(\mathbf{a})*\omega(\mathbf{b}) = (\mathbf{a}+I)(\mathbf{b}+I)-(\mathbf{b}+I)(\mathbf{a}+I) = \mathbf{ab}-\mathbf{ba}+I = \mathbf{a}*\mathbf{b}+I = \omega(\mathbf{a}*\mathbf{b})$.

Proposition 4.3 *(The universal property of $U\mathfrak{g}$) For every associative algebra A and every Lie algebra homomorphism $f : \mathfrak{g} \to A^{[-]}$ there exists a unique homomorphism of associative algebras $\varphi : U\mathfrak{g} \to A$ such that $\varphi(\omega(\mathbf{x})) = f(\mathbf{x})$ for each $\mathbf{x} \in \mathfrak{g}$.*

PROOF: It follows from Proposition 4.2 and the fact that $f(I) = 0$ is equivalent to f being Lie algebra homomorphism for a linear map f. □

Corollary 4.4 *For a vector space V and a Lie algebra $\mathfrak{g}$ there is a bijection between the set of $U\mathfrak{g}$-module structures on V and the set of $U\mathfrak{g}$-representation structures on V.*

PROOF: $U\mathfrak{g}$-module structures on V are the same as associative algebra homomorphisms $\mathrm{Hom}(U\mathfrak{g}, \mathrm{End}_{\mathbb{K}}V)$ that are in bijection with Lie algebra homomorphisms $\mathrm{Hom}(U\mathfrak{g}, \mathrm{End}_{\mathbb{K}}V^{[-]})$ that, in their turn, are $\mathfrak{g}$-representation structures on V. □

Bijections in Corollary 4.4 leave the notion of a homomorphism of representations (modules) unchanged. In fact, it can be formulated as *an equivalence of categories*, which we will discuss later on. This seems to make the notion of a representation of a Lie algebra obsolete. Why don't we just study modules over associative algebras? A point in defense of Lie algebras is that $\mathfrak{g}$ is finite-dimensional and easy to get hold of while $U\mathfrak{g}$ is usually infinite-dimensional.

The following proposition follows immediately from the Poincare-Birkhoff-Witt Theorem that will not be proved in this lectures.

Proposition 4.5 *$\omega_{\mathfrak{g}}$ is injective*

4.3 Free Lie algebra

Let $L(X)$ be the Lie subalgebra of $\mathbb{K}_{Ass}(X)^{[-]}$ generated by

Theorem 4.6 *(i) The natural map $\phi : \mathbb{K}_{Lie}(X) \to \mathbb{K}_{Ass}(X)$ gives an isomorphism of Lie algebras between $\mathbb{K}_{Lie}(X)$ and $L(X)$.*

(ii) The natural map $\psi : U\mathbb{K}_{Lie}(X) \to \mathbb{K} < X >$ is an isomorphism of associative algebras.

(iii) The following diagram is commutative.

$$\begin{array}{ccc} U\mathbb{K}_{Lie}(X) & \xrightarrow{\psi} & \mathbb{K} < X > \\ \uparrow{\scriptstyle \omega_{\mathbb{K}_{Lie}(X)}} & & \uparrow{\scriptstyle i} \\ \mathbb{K}_{Lie}(X) & \xrightarrow{\phi} & L(X) \end{array}$$

PROOF: Let us first construct both maps. Using the function $f : X \to \mathbb{K}_{Ass}(X)$ and interpreting $\mathbb{K}_{Ass}(X)$ as a Lie algebra $\mathbb{K}_{Ass}(X)^{[-]}$ gives a Lie algebra homomorphism $\phi : \mathbb{K}_{Lie}(X) \to \mathbb{K}_{Ass}(X)^{[-]}$ by the universal property of the free Lie algebra. Since $\mathbb{K}_{Lie}(X)$ is generated by X as a Lie algebra, the image of ϕ is exactly $L(X)$. Hence we have a surjective Lie algebra homomorphism $\phi : \mathbb{K}_{Lie}(X) \to L(X)$.

Now $L(X)$ is a Lie subalgebra in $\mathbb{K} < X >^{[-]}$, thus ϕ gives a Lie algebra homomorphism $\mathbb{K}_{Lie}(X) \to \mathbb{K} < X >^{[-]}$ that can be lifted to a homomorphism $\psi : U\mathbb{K}_{Lie}(X) \to \mathbb{K} < X >$ of associative algebras. Since both algebras are generated by X, the homomorphism ψ is surjective.

The commutativity of the diagram follows from the construction because $\psi(\omega(z)) = \phi(z)$ for each $z \in X$. Consequently, it should be true for any element $z \in \mathbb{K}_{Lie}(X)$ as both $\psi \circ \omega$ and ϕ are homomorphisms of Lie algebras.

The inverse of ψ is constructed from the universal property of $\mathbb{K} < X >$: let θ be the extension of function $X \to U\mathbb{K}_{Lie}(X)$ to a homomorphism $\mathbb{K} < X > \to U\mathbb{K}_{Lie}(X)$. The composition $\theta\psi$ is an identity on X, hence identity on $U\mathbb{K}_{Lie}(X)$. Similarly, the composition $\psi\theta$ is an identity on X, hence identity on $\mathbb{K} < X >$.

Finally, ω is injective by Proposition 4.5. Hence, $\psi\omega = \phi$ is injective. □

Now we get a good grasp on the free Lie algebra: it is just $L(X)$ and its universal enveloping algebra is $\mathbb{K} < X >$.

4.4 Vista: Baker-Campbell-Hausdorff formula

4.5 Exercises

State and prove the universal property of the free commutative algebra.

Prove the universal enveloping algebra of an abelian Lie algebra is isomorphic to the free commutative algebra of any basis.

5 p-th powers

We discuss various p-th powers and introduce restricted structures on Lie algebras. The field $\mathbb{K}$ has characteristic $p > 0$ throughout the lecture.

5.1 In commutative algebra

Proposition 5.1 *(Freshman's dream binomial formula) Let A be an associative algebra and $x, y \in A$ such that $xy = yx$. Then $(x+y)^p = x^p + y^p$.*

PROOF: Since x and y commute, they satisfy the binomial formula $(x+y)^p = \sum_{n=0}^{p} \begin{pmatrix} p \\ n \end{pmatrix} x^n y^{p-n}$. It remains to observe that for any n between 1 and $p-1$ the binomial coefficient $\begin{pmatrix} p \\ n \end{pmatrix} = p!/n!(p-n)!$ vanish since only the denominator is divisible by p. □

Corollary 5.2 *If T is a matrix with coefficients in $\mathbb{K}$ then $\mathrm{Tr}(T^p) = \mathrm{Tr}(T)^p$.*

PROOF: If λ_i are eigenvalues of T then λ_i^p are eigenvalues of T^p. Hence, $\mathrm{Tr}(T)^p = (\sum_i \lambda_i)^p = \sum_i \lambda_i^p = \mathrm{Tr}(T^p)$. □

Corollary 5.3 *Let A be an associative algebra and $x, y \in A$ such that $xy = yx$. Then $(x-y)^{p-1} = \sum_{n=0}^{p-1} x^n y^{p-1-n}$.*

PROOF: Let us check this identity in the free com-algebra $\mathbb{K}_{Com}(X)$ where $X = \{a, b\}$. There $(a-b)^p = a^p - b^p = (a-b)\sum_{n=0}^{p-1} a^n b^{p-1-n}$. Since $\mathbb{K}_{Com}(X)$ is a domain, we can cancel $(a-b)$ proving $(a-b)^{p-1} = \sum_{n=0}^{p-1} a^n b^{p-1-n}$. Since x, y commute the function $f : X \to A$, $f(a) = x$, $f(b) = y$ can be extended to a homomorphism $\widetilde{f}$. Hence, $(x-y)^{p-1} = \widetilde{f}((a-b)^{p-1}) = \widetilde{f}(\sum_{n=0}^{p-1} a^n b^{p-1-n}) = \sum_{n=0}^{p-1} x^n y^{p-1-n}$. □

Now look at a Lie algebra $\mathfrak{g} = \mathfrak{sl}_n$. It is a Lie subalgebra of two different associative algebras, $U(\mathfrak{g})$ and $M_n(\mathbb{K})$. Let us denote the p-th power in the former algebra by x^p and in the latter algebra by $x^{[p]}$. Observe that in $M_n(\mathbb{K})$, $\mathrm{Tr}(x^{[p]}) = \mathrm{Tr}(x)^p$ as follows from (5.1).

5.2 In associative algebra

Let us prove that

Theorem 5.4 *If $y, z \in X$ then $(z+y)^p - z^p - y^p \in \mathbb{K} < X >$ belongs to $L(X)$ and contains homogeneous components of degree at least 2.*

PROOF: We consider polynomials $\mathbb{K} < X > [T]$ in one variable T over $\mathbb{K} < X >$. One can differentiate them using the derivation $\partial : \mathbb{K} < X > [T] \to \mathbb{K} < X > [T]$ where $\partial(fT^n) = nfT^{n-1}$, $f \in \mathbb{K} < X >$. One can also

evaluate them at $\alpha \in \mathbb{K}$ using homomorphism $\mathrm{ev}_\alpha : \mathbb{K} < X > [T] \to \mathbb{K} < X >$, $\mathrm{ev}_\alpha(fT^n) = \alpha^n f$.

Before going further we observe that the associativity that operators L_s and R_s commute for any $s \in \mathbb{K} < X > [T]$. Hence, $(L_s - R_s)^{p-1} = \sum_{n=0}^{p-1} L_s^n R_s^{p-1-n}$ by Corollary 5.3.

Now we write $(zT + y)^p = z^p T^p + y^p + \sum_{n=1}^{p-1} F_n(z, y)T^n$ for some $F_n(z, y) \in \mathbb{K} < X >$. Differentiating this equality we get $\sum_{n=1}^{p-1} nF_n(z, y)T^{n-1} = \sum_{n=0}^{p-1}(zT+y)^n z(zT+y)^{p-n-1} = \sum_{n=0}^{p-1} L^n_{zT+y}(R^{p-n}_{zT+y}(z)) = (L_{zT+y} - R_{zT+y})^{p-1}(z) = [zT + y, \ldots [zT + y, z] \ldots]$. Comparing coefficients at T^{n-1} we express each $F_n(z, y)$ as a sum of commutators, hence $F_n(z, y) \in L(X)$ with homogeneous components of degree 2 and higher.

Finally, using ev_1, we get $(z + y)^p - z^p - y^p = \sum_{n=1}^{p-1} F_n(z, y) \in L(X)$. $\square$

This polynomial $\Lambda_p(z, y) = (z+y)^p - z^p - y^p$ plays a crucial role in what follows. Since it is a Lie polynomial it can be evaluated on Lie algebras.

5.3 In Lie algebra

A restricted Lie algebra is a pair $(\mathfrak{g}, \gamma)$ where $\mathfrak{g}$ is a Lie algebra and $\gamma : \mathfrak{g} \to \mathfrak{g}$ is a function (often denoted $\gamma(\mathbf{x}) = \mathbf{x}^{[p]}$ such that

(i) $\gamma(\alpha\mathbf{x}) = \alpha^p\gamma(\mathbf{x})$,
(ii) $L_{\gamma(\mathbf{x})} = L^p_{\mathbf{x}}$,
(iii) $\gamma(\mathbf{x} + \mathbf{y}) - \gamma(\mathbf{x}) - \gamma(\mathbf{y}) = \Lambda_p(\mathbf{x}, \mathbf{y})$

for all $\alpha \in \mathbb{K}$ and $\mathbf{x}, \mathbf{y} \in \mathfrak{g}$.

The following proposition gives us a tool to produce examples of restricted Lie algebras.

Proposition 5.5 *Let $\mathfrak{g}$ be a Lie subalgebra of $A^{[-]}$ where is an associative algebra. If $\mathbf{x}^p \in \mathfrak{g}$ for all $\mathbf{x} \in \mathfrak{g}$ then $\mathfrak{g}$ admits a structure of a restricted Lie algebra.*

Proof: The restricted structure is given by the associative p-th power: $\gamma(\mathbf{x}) = \mathbf{x}^p$. Axiom (i) is obvious. Axiom (iii) follows from the fact that it is the p-th power in an associative algebra: $\Lambda_p(z, y) = (z + y)^p - z^p - y^p \in \mathbb{K} < y, z >$, hence, in any associative algebra.

To prove axiom (ii), we distinguish Lie multiplication operators by adding $*$. Then $L^*_z = L_z - R_z$, i.e., the Lie multiplication is the difference of two associative multiplications for any $z \in A$. By associativity L_z and R_z commute, hence we can use Proposition 5.1: $(L^*_z)^p = (L_z - R_z)^p = L^p_z - R^p_z = L_{z^p} - R_{z^p}$. $\square$

Corollary 5.6 *If A is an algebra then* $\mathrm{Der}(A)$ *is a restricted Lie algebra.*

PROOF: Thanks to Proposition 5.5, it suffices to check that ∂^p is a derivation whenever ∂ is a derivation. Using induction on n one establishes that $\partial^n(xy) = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \partial^k(x)\partial(y)^{n-k}$. If $n = p$ all the middle terms vanish, hence ∂^p is a derivation. □

Corollary 5.7 *Classical Lie algebras $\mathfrak{sl}_n$, $\mathfrak{sp}_{2n}$ and $\mathfrak{so}_n$ are restricted.*

PROOF: It suffices to check closeness under p-th power thanks to Proposition 5.5. For $\mathfrak{sl}_n$, it follows from Corollary 5.2. Symplectic or orthogonal matrices satisfy the condition $XJ = -JX$ where J is the matrix of the form. Clearly, $X^pJ = -X^{p-1}JX = \ldots = (-1)^pJX^p = -JX^p$ □

A homomorphism between Lie algebras is called *restricted* if it commutes with γ. An ideal or a subalgebra is *restricted* if they are closed under γ. A representation V is *restricted* if $\mathbf{x}^{[p]}v = \mathbf{x}(vx(\ldots \mathbf{x}v))$ where $v \in V$ and $\mathbf{x} \in \mathfrak{g}$ appears p times. A direct sum of restricted Lie algebras is the direct sum of Lie algebras with the direct sum of restricted structures of the components as the restricted structure.

5.4 Vista: restricted Lie algebroids

5.5 Exercises

Prove by induction on n that $\partial^n(xy) = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \partial^k(x)\partial(y)^{n-k}$.

Prove that the kernel of a restricted homomorphism is a restricted ideal.

Formulate and prove the isomorphism theorem for restricted Lie algebras.

6 Uniqueness of restricted structures

We develop more efficient methods for working and constructing restricted structures.

6.1 Uniqueness of restricted structures

Recall *the centre* of a Lie algebra $\mathfrak{g}$ consists of all $\mathbf{x} \in \mathfrak{g}$ such that $\mathbf{x} * \mathbf{y} = 0$ for all $\mathbf{y} \in \mathfrak{g}$. The centre of a Lie algebra is an ideal.

A function $f : V \to W$ between vector spaces over the field $\mathbb{K}$ of positive characteristic p is *semilinear* if f is an abelian group homomorphism and $f(\alpha a) = \alpha^p a$. The following proposition addresses uniqueness.

Proposition 6.1 *If γ and δ are two distinct restricted structures on $\mathfrak{g}$ then $\delta - \gamma$ is a semilinear map $\mathfrak{g} \to Z(\mathfrak{g})$. On the opposite, if γ is a restricted structure and $\phi : \mathfrak{g} \to Z(\mathfrak{g})$ is a semilinear map then $\gamma + \phi$ is a restricted structure too.*

Proof: Let $\phi = \delta - \gamma$ where γ is a restricted structure. It is clear that $\phi(\alpha \mathbf{x}) = \alpha^p \phi(\mathbf{x})$ if and only if $\delta(\alpha \mathbf{x}) = \alpha^p \delta(\mathbf{x})$.

Then $\phi(\mathbf{x}) * \mathbf{y} = (\delta(\mathbf{x}) - \gamma(\mathbf{x})) * \mathbf{y} = L^p_{\mathbf{x}}(\mathbf{y}) - L^p_{\mathbf{x}}(\mathbf{y}) = 0$, hence $\phi(\mathbf{x}) \in Z(\mathfrak{g})$. In the opposite direction, if $\phi : \mathfrak{g} \to Z(\mathfrak{g})$ is any function then $\gamma + \phi$ satisfies axiom (ii) of the restricted structure by the same argument.

Finally, $\phi(\mathbf{x}+\mathbf{y}) - \phi(\mathbf{x}) - \phi(\mathbf{y}) = \Lambda_p(\mathbf{x}, \mathbf{y}) - \Lambda_p(\mathbf{x}, \mathbf{y}) = 0$. In the opposite direction, semilinearity of ϕ implies axioms (iii) for δ. □

We have proved that the restricted structures form an affine space over the vector space of all semilinear maps from $\mathfrak{g}$ to $Z(\mathfrak{g})$. In particular, if $Z(\mathfrak{g}) = 0$ then the restricted structure is unique if it exists. To the existence we turn our attention now.

6.2 Restricted abelian Lie algebras

Let us consider an extreme case $Z(\mathfrak{g}) = \mathfrak{g}$, i.e. the Lie algebra is abelian. Since Λ_p has no degree 1 terms, the zero map $0(\mathbf{x}) = 0$ is a restricted structure. By Proposition 6.1, any semilinear map $\gamma : \mathfrak{g} \to \mathfrak{g}$ is a restricted structure and vice versa. We consider the following abelian restricted Lie algebras: $\mathfrak{a}_0$ is a one-dimensional Lie algebra with a basis $\mathbf{x}$ and $\mathbf{x}^{[p]} = \mathbf{x}$; $\mathfrak{a}_n$ is an n-dimensional Lie algebra with a basis $\mathbf{x}_1, \dots \mathbf{x}_n$ and $\mathbf{x}_k^{[p]} = \mathbf{x}_{k+1}$, $\mathbf{x}_n^{[p]} = 0$. The following theorem is left without a proof in the course.

Theorem 6.2 *Let $\mathfrak{g}$ be a finite-dimensional abelian restricted Lie algebra over an algebraically closed field $\mathbb{K}$. Then $\mathfrak{g}$ is a direct sum of $\mathfrak{a}_n$. The multiplicity of each $\mathfrak{a}_n$ is uniquely determined by $\mathfrak{g}$.*

While uniqueness in Theorem 6.2 is relatively straightforward, the existence is similar to existence of Jordan normal forms (proofs will be either elementary and pointless or conceptual and abstract). One way you can think of this is in terms of matrices: on a basis a semilinear map γ is defined by a matrix $C = (\gamma_{i,j})$ so that on the level of coordinate columns $\gamma(\alpha_i) = (\gamma_{i,j})(\alpha_j^p)$. The change of basis Q will change C into $F(Q)CQ^{-1}$ where $F(\beta_{i,j}) = (\beta_{i,j}^p)$ is the Frobenius homomorphism $F : GL_n \to GL_n$, which is an isomorphism of groups in this case. Hence, we are just classifying orbits of this action, very much like in Jordan forms.

One interesting consequences of the theorem is that all nondegenerate matrices form a single orbit: its canonical representative is identity matrix I. The orbit map $L : GL_n \to GL_n$, $L(Q) = F(Q)IQ^{-1} = F(Q)Q^{-1}$ is surjective. This map is called Lang map and its surjectivity is called Lang's theorem.

The conceptual proof is in terms of the modules over the algebra of twisted polynomials: $A = \mathbb{K}[z]$ but z and scalars do not commute: $\alpha z = z\alpha^p$. The module structure on V comes from linear action of $\mathbb{K}$ and the action of z by the semilinear map. The algebra A is non-commutative left Euclidean domain and the theorem follows from the classification of indecomposable finite-dimensional modules over A.

6.3 PBW-Theorem and reduced enveloping algebra

After careful consideration, I have decided to include the PBW-theorem without a proof. My original plan was to spend two lectures to give a complete proof but then I decided against as a partial proof (modulo Grobner-Shirshov's basis) has featured in *Representation Theory* last year.

Theorem 6.3 *(PBW: Poincare, Birkhoff, Witt) Let X be a basis of a Lie algebra $\mathfrak{g}$ over any field $\mathbb{K}$. If we equip X with a linear order $\leq$ (we say that $\mathbf{x} < \mathbf{y}$ if $\mathbf{x} \leq \mathbf{y}$ and $\mathbf{x} \neq \mathbf{y}$) then elements $\mathbf{x}_1^{k_1}\mathbf{x}_2^{k_2}\dots\mathbf{x}_n^{k_n}$, with $k_i \in \{1, 2\dots\}$ and $\mathbf{x}_1 < \mathbf{x}_2 < \dots < \mathbf{x}_n \in X$ form a basis of $U\mathfrak{g}$.*

Now we are ready to establish the following technical proposition. Recall that the centre of an associative algebra A is a subalgebra $Z(A) = \{a \in A \mid \forall b \in A\ ab = ba\}$.

Proposition 6.4 *Let the field be of characteristic p. Let $\mathbf{x}_i$ (as i runs over linearly ordered sets) form a basis of $\mathfrak{g}$. Suppose for each i we have an element $z_i \in Z(U\mathfrak{g})$ such that $z_i - \mathbf{x}_i^p \in \mathfrak{g} + \mathbb{K}\mathbf{1} \subseteq U\mathfrak{g}$. Then the elements $z_1^{t_1}z_2^{t_2}\dots z_n^{t_n}\mathbf{x}_1^{k_1}\mathbf{x}_2^{k_2}\dots\mathbf{x}_n^{k_n}$, with $k_i \in \{0, 1, 2\dots, p-1\}$, $t_i \in \{0, 1, 2\dots,\}$, and $\mathbf{x}_1 < \mathbf{x}_2 < \dots < \mathbf{x}_n \in X$ form a basis of $U\mathfrak{g}$.*

PROOF: We refer to the PBW-basis elements as *PBW-terms* and to the new basis elements as *new terms*. To show that the new terms span $U\mathfrak{g}$ it suffices to express each PBW-term $\mathbf{x}_1^{s_1}\mathbf{x}_2^{s_2}\dots\mathbf{x}_n^{s_n}$, $s_i \geq 0$ as a linear combination of the new terms. We do it by induction on the degree $S = \sum_i s_i$. If all s_i are less than p then the PBW-term is a new term. This gives a basis of induction. For the induction step we can assume that $s_i \geq p$ for some i. Let $y_i = \mathbf{x}_i^p - z_i$. Then

$$\mathbf{x}_1^{s_1}\mathbf{x}_2^{s_2}\dots\mathbf{x}_n^{s_n} = \mathbf{x}_1^{s_1}\dots\mathbf{x}_i^{s_i-p}y_i\mathbf{x}_{i+1}^{s_{i+1}}\dots\mathbf{x}_n^{s_n} + z_i\mathbf{x}_1^{s_1}\dots\mathbf{x}_i^{s_i-p}\mathbf{x}_{i+1}^{s_{i+1}}\dots\mathbf{x}_n^{s_n}$$

The second summand is a new term and the first summand has degree $S + 1 - p < S$, i.e. it is a linear combination of PBW-terms of smaller degrees. Using induction to the terms of the first summand completes the proof.

To show the linear independence we consider U_m, the linear span of all PBW-terms of degree less or equal than m. If a new term $z_1^{t_1}z_2^{t_2}\dots z_n^{t_n}\mathbf{x}_1^{k_1}\mathbf{x}_2^{k_2}\dots\mathbf{x}_n^{k_n}$, has degree $m+1 = \sum_i(pt_i + k_i)$ then

$$z_1^{t_1}\dots z_n^{t_n}\mathbf{x}_1^{k_1}\dots\mathbf{x}_n^{k_n} = \mathbf{x}_1^{k_1}(\mathbf{x}_1^p - y_1)^{t_1}\dots\mathbf{x}_n^{k_n}(\mathbf{x}_n^p - y_n)^{t_n}$$

and, consequently,

$$z_1^{t_1}z_2^{t_2}\dots z_n^{t_n}\mathbf{x}_1^{k_1}\mathbf{x}_2^{k_2}\dots\mathbf{x}_n^{k_n} + U_m = \mathbf{x}_1^{pt_1+k_1}\dots\mathbf{x}_n^{pt_n+k_n} + U_m\ .$$

Note that this gives a bijection f between the new terms and PBW-terms. Consider a non-trivial linear relation on new terms with highest degree $m+1$. It gives a non-trivial relation on cosets of U_m. This is a relation on cosets of the corresponding PBW-terms but this is impossible: PBW-terms of degree $m+1$ are linearly independent modulo U_m by PBW-theorem. □

We can interpret this proposition in several ways. Clearly, it implies that $A = \mathbb{K}[z_1\dots z_n]$ is a central polynomial subalgebra of $U\mathfrak{g}$. Moreover, $U\mathfrak{g}$ is a free module over A with basis $\mathbf{x}_1^{k_1}\dots\mathbf{x}_n^{k_n}$, with $k_i \in \{0, 1, 2\dots, p-1\}$. In particular, if the dimension of $\mathfrak{g}$ is n then the rank of $U\mathfrak{g}$ as an A-module is p^n. Another interesting consequence is that elements z_i generate an ideal I which is spanned by all $z_1^{t_1}\dots z_n^{t_n}, \mathbf{x}_1^{k_1}\dots\mathbf{x}_n^{k_n}$ with at least one positive t_i. Hence the quotient algebra $U' = U\mathfrak{g}/I$ has a basis $\mathbf{x}_1^{k_1}\dots\mathbf{x}_n^{k_n}, +I$ with $k_i \in \{0, 1, 2\dots, p-1\}$.

The quotient algebra U' is called *the reduced enveloping algebra* and we are going to put some gloss over it slightly later.

6.4 Vista: modules over skew polynomial algebra

6.5 Exercises

Prove uniqueness part in Theorem 6.2. (Hint: kernels of semilinear maps are subspaces)

Prove Theorem 6.2 for one dimensional Lie algebras.

Using PBW-theorem, prove that the homomorphism $\omega : \mathfrak{g} \to U\mathfrak{g}$ is injective.

Using PBW-theorem, prove that the universal enveloping algebra $U\mathfrak{g}$ is an integral domain.

7 Existence of restricted structures

7.1 Existence of restricted structures

We are ready to prove the following important theorem.

Proposition 7.1 *Let $\mathfrak{g}$ be a Lie algebra with a basis $\mathbf{x}_i$. Suppose for each i there exists an element $\mathbf{y}_i \in \mathfrak{g}$ such that $L^p_{\mathbf{x}_i} = L_{\mathbf{y}_i}$. Then there exists a unique restricted structure such that $\mathbf{x}_i^{[p]} = \mathbf{y}_i$.*

Proof: If γ and δ are two such structure then $\phi = \gamma - \delta$ is a semilinear map such that $\phi(\mathbf{x}_i) = \mathbf{y}_i - \mathbf{y}_i = 0$ for all i. Thus, $\phi = 0$ and the uniqueness is established.

To establish existence, observe that $z_i = \mathbf{x}_i^p - \mathbf{y}_i \in Z(\mathfrak{g})$. The reason is that the left Lie multiplication operator is $L_{z_i} = L_{\mathbf{x}_i^p} - L_{\mathbf{y}_i} == L^p_{\mathbf{x}_i} - L_{\mathbf{y}_i} = 0$. This allows to construct the reduced enveloping algebra U' and $\mathfrak{g}$ is its Lie subalgebra. It remains to observe that the p-th powers in U' behave in the prescribed way: $(\mathbf{x}_i + I)^p = \mathbf{x}_i^p + I = \mathbf{y}_i + I$ on the basis. Off the basis, we need to observe that $\mathbf{x}^p \in \mathfrak{g}$ if $\mathbf{x} \in \mathfrak{g}$ to apply Proposition 5.5. It follows by induction on the length of a linear combination using the standard formula $(\alpha\mathbf{x} + \beta\mathbf{y})^p = \alpha^p\mathbf{x}^p + \beta^p\mathbf{y}^p + \Lambda_p(\alpha\mathbf{x}, \beta\mathbf{y})$. □

Let us describe the restricted structure on $W(1,n)$: $L^p_{\mathbf{e}_i}(\mathbf{e}_j) = -R^p_{\mathbf{e}_i}(\mathbf{e}_j) = -R^{p-1}_{\mathbf{e}_i}((j-i)\mathbf{e}_{i+j}) = -R^{p-2}_{\mathbf{e}_i}((j-i)j\mathbf{e}_{2i+j}) = \ldots = -\prod_{t=0}^{p-1}(j+ti)\mathbf{e}_j = -f(j/i)i^p\mathbf{e}_j$. The polynomial $f(z) = \prod_{t=0}^{p-1}(z+t)$ has p distinct roots, all elements of the prime subfield. Elements of the prime subfield satisfy $z^p - z = 0$. Comparing the top degree coefficients, $f(z) = z^p - z$ and $L^p_{\mathbf{e}_i}(\mathbf{e}_j) = -(j^p - ji^{p-1})\mathbf{e}_j$. If $n = 1$ then i and j lie in the prime subfield. If $i \neq 0$ then $i^{p-1} = 1$ and $j^p - ji^{p-1} = j^p - j = 0$ and $\mathbf{e}_i^{[p]} = 0$. If $i = 0$ then $j^p - ji^{p-1} = j^p = j$ and $\mathbf{e}_0^{[p]} = \mathbf{e}_0$.

Now if $n \geq 2$ then consider $i = 0$ and $j \neq 0$. As $j^p - ji^{p-1} = j^p$ it forces $\mathbf{e}_0^{[p]} = j^{p-1}\mathbf{e}_0$. It depends on j and is not well-defined. Thus, $W(1,n)$ admits no restricted structure in this case.

7.2 Glossing reduced enveloping algebra up

Let $(\mathfrak{g}, \gamma)$ be a restricted Lie algebra. It follows that $\mathbf{x} \mapsto \mathbf{x}^p - \mathbf{x}^{[p]}$ is a semilinear map $\mathfrak{g} \to Z(U\mathfrak{g})$. Its image generates a polynomial subalgebra of the centre of $U\mathfrak{g}$ which we call *the p-centre* from now one and denote $Z_p(U\mathfrak{g})$.

Pick a basis $\mathbf{x}_i$ of $\mathfrak{g}$. Now for each $\chi \in \mathfrak{g}^*$ we define $z_i = \mathbf{x}_i^p - \mathbf{x}_i^{[p]} - \chi(\mathbf{x}_i)^p\mathbf{1}$. Finally, we define reduced enveloping algebra $U_\chi\mathfrak{g}$ the algebra U' for this particular choice of basis. Clearly, it is just the quotient of $U\mathfrak{g}$ by the ideal generated by $\mathbf{x}^p - \gamma(\mathbf{x}) - \chi(\mathbf{x})^p\mathbf{1}$ for all $\mathbf{x} \in \mathfrak{g}$.

Proposition 7.2 *(Universal property of reduced enveloping algebra) For every associative algebra A and every Lie algebra homomorphism $f : \mathfrak{g} \to A^{[-]}$ such that $f(\mathbf{x})^p - f(\gamma(\mathbf{x})) = \chi(\mathbf{x})^p \mathbf{1}$ for all $\mathbf{x} \in \mathfrak{g}$ there exists a unique homomorphism of associative algebra $\widetilde{f} : U_\chi \mathfrak{g} \to A$ such that $f(\mathbf{x}) = \widetilde{f}(\mathbf{x})$ for all $\mathbf{x} \in \mathfrak{g}$.*

We say that a representation V of $\mathfrak{g}$ admits a p-character $\chi \in \mathfrak{g}^*$ if $\mathbf{x}^p(v) - \mathbf{x}^{[p]}(v) = \chi(x)^p v$ for all $v \in V$.

Corollary 7.3 *For a vector space V there is a natural bijection between structures of a representation of $\mathfrak{g}$ with a p-character χ and structures of a $U\chi\mathfrak{g}$-module.*

One particular important p-character is zero. Representations with zero p-character are called *restricted* while the reduced enveloping algebra $U_0\mathfrak{g}$ is called *the restricted enveloping algebra*.

Example. Clearly, $U\mathfrak{a}_0 \cong U\mathfrak{a}_1 \cong \mathbb{K}[z]$, making their representations identical. However, $U_\chi\mathfrak{a}_0$ and $U_\chi\mathfrak{a}_1$ are drastically different. $U_\chi\mathfrak{a}_0 \cong \mathbb{K}[z]/(z^p - z - \chi(z)^p\mathbf{1})$ and the polynomial $z^p - z - \chi(z)^p\mathbf{1}$ has p distinct roots because $(z^p - z - \chi(z)^p\mathbf{1})' = -1$. Hence $U_\chi\mathfrak{a}_0 \cong \mathbb{K}^p$ is a semisimple algebra. Consequently, representations of $U_\chi\mathfrak{a}_0$ with any p-character are completely reducible.

On the other hand, $U_\chi\mathfrak{a}_1 \cong \mathbb{K}[z]/(z^p - \chi(z)^p\mathbf{1})$ and the polynomial $z^p - \chi(z)^p\mathbf{1} = (z - \chi(z)\mathbf{1})^p$ has one multiple root. Hence $U_\chi\mathfrak{a}_1 \cong \mathbb{K}[z]/(z^p)$ is a local algebra. Consequently, there is a single irreducible representation of $U_\chi\mathfrak{a}_1$ with any given p-character.

7.3 exercises

Prove Proposition 7.2 and Corollary 7.2.

Choose a basis of $\mathfrak{sl}_n$ and describe the restricted structure on the basis.

8 Schemes

8.1 Schemes, points and functions

A scheme $\mathcal{X}$ is a commutative algebra A. To be precise we are talking about proaffine schemes. To be even more precise, "the category of schemes is the opposite category to the category of commutative algebras". This means that if a scheme $\mathcal{X}$ is an algebra A and $\mathcal{Y}$ is an algebra B then morphisms from $\mathcal{X}$ to $\mathcal{Y}$ are algebra homomorphisms from B to A. To emphasize this distinction between schemes and algebras we say that $\mathcal{X}$ *is the spectrum of* A and write $\mathcal{X} = \text{Spec } A$. We are going to study geometry of schemes.

We will regard algebra A as functions on the scheme $\mathcal{X} = \text{Spec } A$. Functions can be evaluated at points and the scheme has various notions of a point. We will just use only one: a point is an algebra homomorphism $A \to R$ to another commutative algebra R. If R is fixed we call them R-points and denote them $\mathcal{X}(R)$. Notice that a morphism of schemes $\phi : \mathcal{X} \to \mathcal{Y}$ gives rise to a function on points $\phi(R) : \mathcal{X}(R) \to \mathcal{Y}(R)$ via composition $\phi(R)(a) = a \circ \phi$.

We have to learn how to compute the value of a function $F \in A$ at a point $a \in \mathcal{X}(R)$. Well, it is just $F(a) = a(F)$ as $a : A \to R$ is a homomorphism and F is an element of A.

As an example, let us consider $A = \mathbb{K}[X, Y]$. We can regard the corresponding scheme as "an affine plane". What are its R-points? A homomorphism a is given by any two elements $a(X), a(Y) \in R$. Hence, $\mathcal{X}(R) = R^2$.

Let us consider "a circle" $\mathcal{X} = \text{Spec } \mathbb{K}[X, Y]/(X^2 + Y^2 - 1)$. Indeed, what are the R-points? To define a homomorphism $a(X), a(Y) \in R$ must satisfy $a(X)^2 + a(Y)^2 = 1$. Hence, $\mathcal{X}(R) = \{(x, y) \in R^2 \mid x^2 + y^2 = 1\}$.

8.2 Product of schemes

A product of schemes $\mathcal{X} = \text{Spec } A$ and $\mathcal{Y} = \text{Spec } B$ is the spectrum of the tensor product of algebras A and B, i.e., $\mathcal{X} \times \mathcal{Y} = \text{Spec } A \otimes B$. The tensor product of algebras is the standard tensor product of vectors spaces with the product defined by $a \otimes b \cdot a' \otimes b' = aa' \otimes bb'$. Observe that $\mathcal{X} \times \mathcal{Y}(R) = \mathcal{X}(R) \times \mathcal{Y}(R)$ for each commutative algebra R.

8.3 Algebraic varieties and local schemes

The circle and the affine plane are very special schemes. Their algebras are finitely generated domains (with an exception of the circle in characteristic 2, which is no longer a domain). If A is a finitely generated domain, the scheme is called *an affine algebraic variety*.

We are more interested in *local schemes*, i.e., spectra of local rings. Recall

that a commutative ring A is *local* if it accepts an ideal I such that every element $a \in A \setminus I$ is invertible. One particular scheme of interest is the local affine line $\mathbb{A}^{1,n}$. Let us emphasize that the characteristic of $\mathbb{K}$ is p. The algebra A has a basis $X^{(k)}$, $0 \leq k \leq p^n - 1$ and the product

$$X^{(k)}X^{(m)} = \left(\begin{array}{c} m+k \\ k \end{array} \right) X^{(m+k)}.$$

We think that $X^{(k)} = 0$, if $k \geq p^n$.

As a scheme, $\mathbb{A}^{1,n} = (\mathbb{A}^{1,1})^n$. All we need is to construct an algebra isomorphism between $\mathbb{K}[Y_1, \dots Y_n]/(Y_i^p)$ and A. It is given by $\phi(Y_i) = X^{(p^i)}$. Hence points $\mathbb{A}^{1,n}(R)$ are just collections $(r_1, \dots r_n) \in R^n$ such that $r_i^p = 0$ for all i. However, we want to distinguish $\mathbb{A}^{1,n}$ and $(\mathbb{A}^{1,1})^n$ by equipping them with different *PD-structure*.

8.4 PD-schemes

Let R be a commutative ring, I it ideal. A PD-structure on I is a sequence of functions $\gamma_n : I \to A$ such that

[i] $\gamma_0(x) = \mathbf{1}$ for all $x \in I$,
[ii] $\gamma_1(x) = x$ for all $x \in I$,
[iii] $\gamma_n(x) \in I$ for all $x \in I$,
[iv] $\gamma_n(ax) = a^n\gamma_n(x)$ for all $x \in I$, $a \in A$,
[v] $\gamma_n(x+y) = \sum_{i=0}^n \gamma_i(x)\gamma_{n-i}(y)$ for all $x, y \in I$,
[vi] $\gamma_n(x)\gamma_m(x) = \left(\begin{array}{c} n+m \\ n \end{array} \right) \gamma_{n+m}(x)$ for all $x, y \in I$,
[vii] $\gamma_n(\gamma_m(x)) = A_{n,m}\gamma_{nm}(x)$ where $A_{n,m} = (nm)!/(m!)^n n! \in \mathbb{K}$ for all $x \in I$,

The number $A_{n,m}$ needs to be integer for the scalar $A_{n,m} \in \mathbb{K}$ to make sense. It follows from the formula $A_{n,m} = \prod_{j=1}^{n-1} \left(\begin{array}{c} jm+m-1 \\ jm \end{array} \right)$.

A PD-structure on a scheme $\mathcal{X} = \operatorname{Spec} A$ is an ideal I of A and a PD-structure on I. Let us describe some basic properties of it. We think that $x^0 = \mathbf{1}$ for any $x \in A$ including zero.

Proposition 8.1 *[i]* $\gamma_n(0_A) = 0_A$ *if* $n > 0$.
[ii] $n!\gamma_n(x) = x^n$ *for all* $x \in I$ *and* $n \geq 0$.

Proof: Statement [i] follows from axiom [iv]. Statement [ii] follows from axioms [i], [ii] and [vi] by induction. See lecture notes for details. □

Statement [ii] has profound consequences in all characteristics. In characteristic zero it implies that each ideal has a canonical DP-structure $\gamma_n(x) =$

$x^n/n!$. Observe how the axioms and the intuition agrees with this structure. In characteristic p it implies that $x^p = p!\gamma_p(x) = 0$ for each $x \in I$. Thus, it is a necessary condition for an ideal I to admit a p-structure.

8.5 Local affine n-space

Let $\phi : \{1, \dots n\} \to \mathbb{Z}_{\geq 1}$ be a function. We introduce the local affine space $\mathbb{A}^{n,\phi}$ including its PD-structure. It is the spectrum of an algebra A_ϕ whose vector space basis consists of commutative monomials $X^{(a)} = X_1^{(a_1)} \dots X_n^{(a_n)}$ which we will write in multi-index notation. The multi-index entries vary in the region determined by ϕ: $0 \leq a_i < p^{\phi(i)}$ and we will think that $X^{(a)} = 0$ if one of entries falls outside this region.

The multiplication is defined similarly to the space $\mathbb{A}^{1,n}$ above:

$$X_i^{(k)} X_i^{(m)} \;=\; \left(\begin{array}{c} m+k \\ k \end{array} \right) X_i^{(m+k)}$$

while the different variables are multiplied by concatenation (don't forget commutativity). The element $X^{(0,0,\dots 0)}$ is the identity of A_ϕ. If $n = 1$, we just write A_n for A_ϕ. In the general case, A_ϕ is isomorphic to the tensor product $A_{\phi(1)} \otimes \dots \otimes A_{\phi(n)}$. Hence, on the level of schemes $\mathbb{A}^{n,\phi} \cong \prod_{i=1}^n \mathbb{A}^{1,\phi(i)}$.

Finally, we describe the PD-structure. The ideal I is the unique maximal ideal. It is generated by all non-identity monomials $X^{(a)}$. Finally, $\gamma_n(X_i^{(1)}) = X_i^{(n)}$ determines the PD-structure. Indeed,

$$\gamma_n(X_i^{(m)}) = \gamma_n(\gamma_m(X_i^{(1)})) = A_{n,m} X_i^{(nm)}$$

from axiom [vii]. Axiom [iv] allows us to extend this to multiples of monomials $\gamma_n(\lambda X^{(a)}) = \lambda^n (n!)^s X^{(na)}$ where $n(a_i) = (na_i)$ and $s+1$ is the number of nonzero elements among a_i. Finally, axiom [v] extends γ_n to any element of I.

One should ask why this is well-defined. Rephrasing this question, we can wonder why the repeated use of the axioms on a element $x \in I$ will always produce the same result for $\gamma_n(x)$. This will not be addressed in the lecture notes (maybe in the next vista section).

8.6 Vista: divided powers symmetric algebra of a vector space

8.7 Exercises

Prove that $A_{n,m} = \prod_{j=1}^{n-1} \left(\begin{array}{c} jm+m-1 \\ jm \end{array} \right)$.

9 Differential geometry of schemes

9.1 Tangent bundle and vector fields on a scheme

For a scheme $\mathcal{X} = \operatorname{Spec} A$ we discuss its tangent bundle $T\mathcal{X}$. It is a scheme but it is easier to describe its points than its functions.

As far as points are concerned $T\mathcal{X}(R) = \mathcal{X}(R[z]/(z^2))$. A homomorphism $\phi : A \to R[z]/(z^2)$ can be written as $\phi(a) = x(a)+\tau(a)z$ using a pair of linear maps $x, \tau : A \to R$. The homomorphism condition $\phi(ab) = \phi(a)\phi(b)$ gets rewritten as $x(ab) + \tau(ab)z = (x(a) + \tau(a)z)(x(b) + \tau(b)z)$ or as a pair of conditions

$$x(ab) = x(a)x(b),\ \tau(ab) = x(a)\tau(b) + x(b)\tau(a).$$

The former condition means $x \in \mathcal{X}(R)$, i.e., it is a point where the tangent vector is attached. The latter condition is a relative (to x) derivation condition. All such elements belong to a vector space $\operatorname{Der}_x(A, R)$ which we can think of as the tangent space $T_x\mathcal{X}$.

To see that the tangent bundle is a scheme we have to understand differentials. At this point we judge fudge them up. Associated to an algebra A we consider a new commutative algebra $\widetilde{A}$ generated by elements a and da for each $a \in A$. We are going to put three kinds of relations on $\widetilde{A}$. The first kind just says that $A \to \widetilde{A}$ defined by $a \mapsto a$ is a homomorphism of algebras. The second kind says that $A \to \widetilde{A}$ defined by $a \mapsto da$ is a linear map. Finally, we add relations $d(ab) = adb + bda$ for all $a, b \in A$.

Proposition 9.1 *If $\mathcal{X} = \operatorname{Spec} A$ then we can define $T\mathcal{X}$ as $\operatorname{Spec} \widetilde{A}$.*

Proof: We need to come up with a "natural" bijection between $\operatorname{Hom}(A, R[z]/(z^2))$ and $\operatorname{Hom}(\widetilde{A}, R)$. Naturality means that the bijection agrees with homomorphisms $R \to$ in a sense that the following diagram commutes:

$$\begin{array}{ccc} \operatorname{Hom}(A, R[z]/(z^2)) & \longrightarrow & \operatorname{Hom}(\widetilde{A}, R) \\ \downarrow & & \downarrow \\ \operatorname{Hom}(A, S[z]/(z^2)) & \longrightarrow & \operatorname{Hom}(\widetilde{A}, S) \end{array}$$

We describe the bijections and leave necessary details (well-definedness, inverse bijections, naturality) to the student. An element $x+\tau z \in \operatorname{Hom}(A, R[z]/(z^2))$ defines $\phi \in \operatorname{Hom}(A, \widetilde{R})$ by $\phi(a) = x(a)$ and $\phi(da) = \tau(a)$. In the opposite direction $\phi \in \operatorname{Hom}(A, \widetilde{R})$ defines $q \in \operatorname{Hom}(A, R[z]/(z^2))$ by $q(a) = \phi(a) + \phi(da)z$. □

Finally derivations $\partial \in \mathrm{Der}(A)$ can be thought of as global vector fields because they define give sections of tangent sheaf. We leave a proof of the following proposition as an exercise.

Proposition 9.2 *If $x \in \mathcal{X}(R)$, $\partial \in \mathrm{Der}(A)$ then $x \circ \partial \in \mathrm{Der}_x(A, R)$.*

9.2 PD-derivations

We already saw that derivations form a restricted Lie algebra. Now we say that ∂ is a PD-derivation if $\partial(\gamma_n(x)) = \gamma_{n-1}(x)\partial(x)$ for all $x \in I$. This definition is motivated by the following calculation using the chain rule or repeated product rule: $\partial(f^n/n!) = \partial(f)f^{n-1}/(n-1)!$. It also show that in characteristic zero every derivation is a PD-derivation.

It is no longer true in characteristic p even if the PD-structure is trivial. Say $A = \mathbb{K}[z]/(z^p)$. The PD-structure is $\gamma_k(f) = f^k/k!$ for $k < p$ and $\gamma_k(f) = 0$ for $k \geq p$. Then $\partial = \partial/\partial z$ is not a PD-derivation as it marginally fails the definition: $\partial(\gamma_p(x)) = 0 \neq \gamma_{p-1}(x)\partial(x)$. Let $\mathrm{PD} - \mathrm{Der}(A, I, \gamma)$ be the set of all PD-derivations.

Proposition 9.3 $\mathrm{PD} - \mathrm{Der}(A, I, \gamma)$ *is a Lie algebra.*

Proof: For the Lie algebra $(\partial * \delta)(\gamma_n(x)) = \partial(\delta(\gamma_n(x))) - \delta(\partial(\gamma_n(x))) = \partial(\gamma_{n-1}(x)\delta(x)) - \delta(\gamma_{n-1}(x)\partial(x)) = \gamma_{n-1}(x)\partial(\delta(x)) + \gamma_{n-2}(x)\partial(x)\delta(x) - \gamma_{n-1}(x)\delta(\partial(x)) - \gamma_{n-2}(x)\partial(x)\delta(x) = \gamma_{n-1}(x)(\partial * \delta)(x)$. □

Notice that $\mathrm{PD} - \mathrm{Der}(A)$ is not restricted, in general. One can show that $\partial^p(\gamma_n(x)) = \gamma_{n-1}(x)\partial^p(x) + \gamma_{n-p}(x)\partial(x)^p$ The best one can conclude from this that is that PD-derivations preserving I, i.e $\partial(I) \subseteq I$ form a restricted Lie algebra.

9.3 Exercises

Prove that if A is finitely generated then $\widetilde{A}$ is finitely generated.

Prove Proposition 9.2.

Compute $\mathrm{PD} - \mathrm{Der}(\mathbb{K}[z]/(z^p), (z), \gamma)$.

10 Generalised Witt algebra

10.1 Definition

We define a derivation ∂_i of A_ϕ by $\partial_i(X_i^{(k)}) = X_i^{(k-1)}$. On a general monomial $\partial_i(X^{(a)}) = (X^{(a-\epsilon_i)}$ where ϵ_i is the multi-index with the only nonzero entry 1 in position i. *A special derivation* is a derivation of A_ϕ of the form $\sum_{i=1}^n f_i\partial_i$ for some $f_i \in A_\phi$. We define the generalised Witt algebra as $W(n,\phi)$ as the Lie algebra of special derivations of A_ϕ.

We start by stating some basic properties.

Proposition 10.1 *(i) $W(n,\phi)$ is a free A_ϕ-module with a basis ∂_i, $i = 1,\dots n$.*
(ii) $W(n,\phi)$ is a Lie subalgebra of $\mathrm{Der}(A_\phi)$.
(iii) $W(n,\phi)$ is a restricted Lie algebra if and only if $\phi(i) = 1$ for all i.

Proof: (i) By definition $\sum_{i=1}^n f_i\partial_i(X_i) = f_i$. Hence $\sum_{i=1}^n f_i\partial_i = 0$ if and only if all f_i are zero.

(ii) It follows from the standard commutations formula $f\partial_i * g\partial_j = f\partial_i(g)\partial_j - g\partial_j(f)\partial_i$.

(iii) If all $\phi(i) = 0$ then $W(n,\phi) = \mathrm{Der}(A_\phi)$ is restricted. In the opposite direction, suppose $\phi(i) \geq 2$ for some i. Observe that $L_{\partial_i}(F\partial_j) = \partial_i(F)\partial_j$. Suppose $W(n,\phi)$ is restricted. Then $L_{\partial_i}^p = L_{\mathbf{x}}$ for $\mathbf{x} = \partial_i^{[p]} = \sum_j f_j\partial_j$. Hence, $L_{\partial_i}^p(X_i^{(p)}\partial_i) = \partial_i$ while, on the other hand, $L_{\mathbf{x}}(X_i^{(p)}\partial_i) = (\sum_j f_j\partial_j) * X_i^{(p)}\partial_i = f_iX_i^{(p-1)}\partial_i - \sum_j X_i^{(p)}\partial_i(f_j)\partial_j$. The resulting equation

$$\partial_i = f_iX_i^{(p-1)}\partial_i - \sum_j X_i^{(p)}\partial_i(f_j)\partial_j$$

contains a contradiction as the degrees of the monomials in the right hand side are at least $p-1 \geq 1$ while it is zero in the left hand side. □

It follows that the dimension of $W(n,\phi)$ is $n \cdot \dim(A) = np^{\sum\phi(t)}$. To understand the Lie multiplication we write the standard formula

$$X^{(n)}\frac{\partial}{\partial X} * X^{(m)}\frac{\partial}{\partial X} = (X^{(n)}X^{(m-1)} - X^{(n-1)}X^{(m)})\frac{\partial}{\partial X} =$$

$$(\left(\begin{array}{c} n+m-1 \\ n \end{array}\right) - \left(\begin{array}{c} n+m-1 \\ n-1 \end{array}\right))\frac{\partial}{\partial X}$$

Let us clear the connection between special and PD-derivations. The special derivation ∂_i is not a PD-derivation as $\partial_i(\gamma_{p^{\phi(i)}}(X_i)) = 0 \neq \gamma_{p^{\phi(i)}-1}(X_i)\partial_i(X_i)$.

Proposition 10.2 *Every PD-derivation is special.*

PROOF: Every element $\delta \in \mathrm{PD} - \mathrm{Der}(\mathbb{A}^{1,n})$ is determined by n elements $\delta(X_i)$. Indeed, $\delta(X^{(a)}) = \sum_i X^{(a-\epsilon_i)}\delta(X_i)$. Hence $\delta = \sum_i \delta(X_i)\partial_i$ is special. □

10.2 Gradings

A graded algebra is an algebra A together with a direct sum decomposition $A = \oplus_{n\in\mathbb{Z}} A_n$ such that $A_n * A_m \subseteq A_{n+m}$. In a graded algebra we defiance subspaces $A_{\leq n} = \oplus_{k\leq n} A_k$ and $A_{\geq n} = \oplus_{k\geq n} A_k$. Let us observe some obvious facts. A_0 is a subalgebra. If $n \geq 0$ then $A_{\geq n}$ is a subalgebra and an ideal of $A_{\geq 0}$.

A graded Lie algebra is a Lie algebra and a graded algebra. Observe that in a graded Lie $\mathfrak{g}_i$ is a representation of $\mathfrak{g}_0$.

The algebra A_ϕ is a graded commutative algebra. We define the degree of $X^{(a)}$ as $|a| = \sum_i |a_i|$. Now we extend this grading to $W(n,\phi)$ by defining the degree of ∂_i to be -1. Let $|\phi| = \sum_t (|\phi(t)| - 1)$.

Proposition 10.3 *(i)* $W(n,\phi) = \oplus_{k=-1}^{|\phi|-1} W(n,\phi)$ *is a graded Lie algebra.*
(ii) $W(n,\phi)_0 \cong \mathfrak{gl}_n$.
(iii) $W(n,\phi)_{-1}$ *is the standard representation of* $\mathfrak{gl}_n$. *In particular, it is irreducible.*
(iv) $W(n,\phi)_k = W(n,\phi)_{-1} * W(n,\phi)_{k+1}$ *for every* $k \neq |\phi| - 1$.
(v) $W(n,\phi)_{|\phi|-1} = W(n,\phi)_0 * W(n,\phi)_{|\phi|-1}$ *unless* $p = 2$ *and* $n = 1$

PROOF: (i) follows from the standard Lie bracket formula..

(ii) The isomorphism is given by $X_i\partial_j \mapsto E_{i,j}$.

(iii) $\mathfrak{gl}_n$ has two standard representations coming from the actions on rows or columns. For the column representation $A \cdot v = Av$ where A is a matrix, v is a column. For the row representation $A \cdot v = -A^T v$ where A is a matrix, v is a column. It follows from the standard representation formula that $W(n,\phi)_{-1}$ is the standard row-representation of $\mathfrak{gl}_n$.

(iv) Since $\partial_i * X^{(a)}\partial_j = X^{(a-\epsilon_i)}\partial_j$, the statement is obvious as you can increase one of the indices.

(v) In the top degree $|\phi|-1$ we consider the multi-index $a = (\phi(1)-, \ldots \phi(n)-1)$. The elements $X^{(a)}\partial_i$ span the top degree space and $X_i\partial_i * X^{(a)}\partial_j = X_i X^{(a-\epsilon_i)}\partial_j - \delta_{i,j}X^{(a)}\partial_i = (p^{\phi(i)} - 1)X^{(a)}\partial_j - \delta_{i,j}X^{(a)}\partial_i$. It is now obvious if $p > 2$ and we leave the case of $p = 2$ as an exercise. □

10.3 Simplicity

Theorem 10.4 *If* $p > 2$ *or* $n > 1$ *then* $W(n,\phi)$ *is a simple Lie algebra.*

PROOF: Pick a non-zero ideal $I \trianglelefteq W(n,\phi)$ and a non-zero element $\mathbf{x} \in I$. Multiplying by various ∂_i, elements of degree -1, we get a nonzero element

$\mathbf{y} \in I \cap \mathfrak{g}_{-1}$.

Since $W(n,\phi)_{-1}$ is an irreducible $W(n,\phi)_0$-representation, we, multiplying by elements of degree 0, conclude that $\mathfrak{g}_{-1} \subseteq I$.

Using part [iv] of proposition 10.3, we get $\mathfrak{g}_k \subseteq I$ for each $k < |\phi| - 1$. Finally, $\mathfrak{g}_{|\phi|-1|} = \mathfrak{g}_0 * \mathfrak{g}_{|\phi|-1|} \subseteq I$ by part [v] of proposition 10.3. □

10.4 Exercises

Finish the proof of part (v) of Proposition 10.3 in characteristic 2.

Demonstrate a non-trivial ideal of $W(1,\phi)$ in characteristic 2.

Let $p > 2$. Describe $W(n,\phi)_1$ as a representation of $W(n,\phi)_0$. Is it irreducible?

11 Filtrations

11.1 Consequences of two descriptions

We intend to establish an isomorphism $W(1,\phi) * W(1,\phi(1))$ between the generalised Witt algebra and the Witt algebra. This isomorphism is non-trivial. Here we discuss four consequences of this isomorphism.

First, $W(1,\phi)$ is defined over the prime field $\mathbb{F}(p)$ while $W(1,k)$ is defined over the field $\mathbb{F}(p^k)$ of cardinality p^k. The field of definition is the field where the multiplication coefficients $\mu_{i,j}^k$ belong. The multiplication coefficients appear when you write the product on a basis: $\mathbf{e}_i * \mathbf{e}_j = \sum_k \mu_{i,j}^k \mathbf{e}_k$.

Second, $W(1,\phi)$ is graded while there is no obvious grading on $W(1,k)$. To be more precise, the natural grading on $W(1,k)$ ($\mathbf{e}_\alpha \in W(1,k)_\alpha$) is a grading by the additive group of the field $\mathbb{F}(p^k)$, not by $\mathbb{Z}$.

Third, in characteristic zero there is an analogue of both Lie algebras and the proof of isomorphism is nearly obvious. One sets it up by $\phi(\mathbf{e}_i) = -X^{i+1}\partial$. While this map works for some elements in characteristic p it is not useful, in general. The product $\mathbf{e}_i * \mathbf{e}_j$ is never zero unless $i = j$ while $X^{(a)}\partial * X^{(b)}\partial = 0$ if $a + b > p^{\phi(1)}$.

Finally, these two realisations will lead to two completely different Cartan decompositions. Recall that *a Cartan subalgebra* is a soluble subalgebra which coincides with its normaliser. *The normaliser* of a subalgebra $\mathfrak{l} \leq \mathfrak{g}$ consists of all $\mathbf{x} \in \mathfrak{g}$ such that $\mathbf{x} * \mathfrak{l} \subseteq \mathfrak{l}$. A Cartan subalgebra $\mathfrak{l}$ leads to Cartan decomposition, which is essentially considering $\mathfrak{g}$ as a representation of $\mathfrak{l}$.

In a simple Lie algebra in characteristic zero, a Cartan subalgebra is abelian and unique up to an automorphism. It is no longer the case in characteristic p. For the Witt algebra realisation $W(1,k)$ we see one-dimensional Cartan subalgebra $\mathbb{K}\mathbf{e}_0$. From the generalised Witt algebra realisation $W(1,\phi)$ we see another Cartan subalgebra $\oplus_{p|n} W(1,\phi)_n$. Notice that these coincide for $W(1,1)$.

11.2 Filtrations

Gradings on an algebra are very helpful because of the way they structure multiplication. However, they may be difficult to find. For instance, $W(1,k)$ has no obvious grading as far as we can see. The second best thing after a grading is a filtration.

We fix $\varepsilon \in \{1,-1\}$. *A filtration* on an algebra A is a collection of vector subspaces F_nA, $n \in \mathbb{Z}$. It has to satisfy two properties: $F_nA * F_mA \subseteq F_{n+m}A$ and $F_nA \subseteq F_{n+\varepsilon}A$ for all $n, m \in \mathbb{Z}$. The filtration is *ascending* if $\varepsilon = 1$. It is *descending* if $\varepsilon = -1$.

Every graded algebra has two associated filtrations: ascending $F_nA = \oplus_{k\le n}A_k$ and descending $F_nA = \oplus_{k\ge n}A_k$. In the opposite direction, from a filtered algebra A we can construct *an associated graded algebra* $\mathrm{gr}A = \oplus_n A_n/A_{n-\varepsilon}$ with multiplication defined by

$$(a + A_{n-\varepsilon})(b + A_{m-\varepsilon}) = ab + A_{n+m-\varepsilon}.$$

Ascending filtrations are more common. Given generators x_i of an algebra A, we define $F_{-1}A = 0$ and F_0A as either 0 or $\mathbb{K}\mathbf{1}$, the latter in case of associative or commutative algebras. For a positive n we define F_nA as the linear span of all products (any order of brackets) of k generators, for all $k \le n$. This filtration is particularly useful for the universal enveloping algebra $U\mathfrak{g}$. Its associated graded algebra is *the symmetric algebra* $S\mathfrak{g}$ which can be defined as the universal enveloping algebra of $\mathfrak{g}$ with zero multiplication. This fact follows from the PBW-theorem and we leave it as exercise.

Let us explain a method of obtaining a descending filtration on a Lie algebra. Let $\mathfrak{g}$ be a Lie algebra, $\mathfrak{l}$ its subalgebra. We define vector subspaces $F_n\mathfrak{g}$ recursively:

$$F_{-1}\mathfrak{g} = \mathfrak{g},\ F_0\mathfrak{g} = \mathfrak{l},\ F_{n+1}\mathfrak{g} = \{\mathbf{x} \in F_n\mathfrak{g} \mid \mathbf{x} * \mathfrak{g} \subseteq F_n\mathfrak{g}\}.$$

For example, if $\mathfrak{l}$ is an ideal then all positive $F_n\mathfrak{g}$ are equal to $\mathfrak{l}$.

Proposition 11.1 *Subspaces $F_n\mathfrak{g}$ form a descending filtration and $\cap F_n\mathfrak{g}$ is an ideal of $\mathfrak{g}$.*

Proof: The descending property is clear. The multiplicative property of the filtration is observe by induction. As an induction basis, $F_{-1}\mathfrak{g} * F_n\mathfrak{g} \subseteq F_{n-1}\mathfrak{g}$ be the definition of $F_n\mathfrak{g}$ and $F_0\mathfrak{g} * F_0\mathfrak{g} \subseteq F_0\mathfrak{g}$ because $F_0\mathfrak{g} = \mathfrak{l}$ is a subalgebra. Now we assume that we have proved $F_i\mathfrak{g} * F_j\mathfrak{g} \subseteq F_{i+j}\mathfrak{g}$ for $i + j \le k$ and consider the case of $i + j = k$. Using Jacobi's identity, $(F_i\mathfrak{g} * F_j\mathfrak{g}) * \mathfrak{g} = (F_i\mathfrak{g} * \mathfrak{g}) * F_j\mathfrak{g} + F_i\mathfrak{g} * (F_j\mathfrak{g} * \mathfrak{g}) = F_{i-1}\mathfrak{g} * F_j\mathfrak{g} + F_i\mathfrak{g} * F_{j-1}\mathfrak{g} \subseteq F_{i+j-1}\mathfrak{g}$. This implies that $F_i\mathfrak{g} * F_j\mathfrak{g} \subseteq F_{i+j}\mathfrak{g}$.

Finally, $\mathfrak{g} * \cap_j F_j\mathfrak{g} \subseteq \cap_j F_{j-1}\mathfrak{g} \subseteq \cap_j F_j\mathfrak{g}$. □

11.3 Filtration on Witt algebra

To conclude we exhibit a useful subalgebra of $W(1,k)$ to construct a filtration on.

Proposition 11.2 $\mathfrak{l} = \{\sum_i \alpha_i \mathbf{e}_i \in W(1,k) \mid \sum_i \alpha_i = 0\}$ *is a Lie a subalgebra of $W(1,k)$.*

Proof: Let $\sum_i \alpha_i = 0 = \sum_i \beta_i$. Then $(\sum_i \alpha_i \mathbf{e}_i) * (\sum_i \beta_i \mathbf{e}_i) = \sum_{i,j} \alpha_i\beta_j(i - j)\mathbf{e}_{i+j}$ belongs to $\mathfrak{l}$ because $\sum_{i,j} \alpha_i\beta_j(i-j) = \sum_i \alpha_i i \sum_j \beta_j - \sum_j \beta_j j \sum_i \alpha_i = 0$. □

11.4 Exercises

Prove that the normaliser of a subalgebra (in a Lie algebra) is a subalgebra.

Prove that the normaliser of a subalgebra $\mathfrak{a}$ (in a Lie algebra) is the unique maximal subalgebra that contains $\mathfrak{a}$ as an ideal.

Prove that $\mathbb{K}\mathbf{e}_0$ and $\oplus_{p|n} W(1,\phi)_n$ are both Cartan subalgebras.

What is the dimension of $\oplus_{p|n} W(1,\phi)_n$? When is it non-abelian?

Let $\mathbf{e}_i$ be a basis of a Lie algebra $\mathfrak{g}$. Prove that $\mathrm{gr}(U\mathfrak{g})$ is isomorphic to the (commutative) polynomial algebra $\mathbb{K}[\mathbf{e}_i]$ in variables $\mathbf{e}_i$.

Let $\mathfrak{g} = \oplus_k \mathfrak{g}_k$ be a graded Lie algebra. We consider the standard filtration $F_n U$ given by $\mathfrak{g}$ as generators of $U\mathfrak{g}$. Choosing a basis of homogeneous elements of $\mathfrak{g}$ and using PBW, we can see that $U\mathfrak{g}$ is graded. We denote U_n its n-th graded piece. Let $F'_n U$ be the span of all $F_i U \cap U_j$ for all $2i + j \leq n$. Prove that this is an ascending filtration[1]. Prove that if $\mathbf{e}_i$ is a homogeneous basis of $\mathfrak{g}$ then $\mathrm{gr}(U\mathfrak{g})$ is isomorphic to the (commutative) polynomial algebra $\mathbb{K}[\mathbf{e}_i]$ in variables $\mathbf{e}_i$.

[1] called Kazhdan filtration

12 Witt algebras are generalised Witt algebra

12.1 Graded algebras of certain filtered Lie algebras

Theorem 12.1 *Let $\mathfrak{g}$ be a simple Lie algebra of dimension p^k with a subalgebra of codimension 1. Using filtration of Proposition 11.1, the associated grade algebra $\mathrm{gr}(\mathfrak{g})$ is isomorphic to $W(1,\phi)$ where $\phi(1)=k$.*

Proof: We start with two general observations. First, $\cap_n F_n\mathfrak{g}=0$ since $\mathfrak{g}$ is simple.

Second, the codimension of $F_{n+1}\mathfrak{g}$ in $F_n\mathfrak{g}$ is 1 unless both spaces are zero. If the codimension is zero then $F_n\mathfrak{g}=F_{n+1}\mathfrak{g}=F_{n+2}\mathfrak{g}=\dots$ and $F_n\mathfrak{g}=\cap_k F_k\mathfrak{g}$ is an ideal. Hence, $F_n\mathfrak{g}=F_{n+1}\mathfrak{g}=0$. To prove that the codimension is always less than 2, suppose the contrary. Pick the smallest n when it is at least 2. For each $k=-1,0,\dots n-1$ choose $\mathbf{a}_k\in F_k\mathfrak{g}$ so that $\overline{\mathbf{a}}_k=\mathbf{a}_k+F_{k+1}\mathfrak{g}$ forms a basis of $F_k\mathfrak{g}/F_{k+1}\mathfrak{g}$. When we reach n we choose at least two elements $\mathbf{b}_1,\mathbf{b}_2,\dots\in F_n\mathfrak{g}$ so that $\overline{\mathbf{b}}_j=\mathbf{b}_j+F_{n+1}\mathfrak{g}$ forms a basis of $F_n\mathfrak{g}/F_{n+1}\mathfrak{g}$. In the graded algebra $\overline{\mathbf{a}}_{-1}*\overline{\mathbf{b}}_j=\lambda_j\overline{\mathbf{a}}_{n-1}$, which is equivalent to $\mathbf{a}_{-1}*\mathbf{b}_j\in\lambda_j\mathbf{a}_{n-1}+F_n\mathfrak{g}$ in $\mathfrak{g}$ itself. Notice that $\lambda_j\neq 0$ because $\lambda_j=0$ would imply $\mathbf{b}_j\in F_{n+1}\mathfrak{g}$ and $\overline{\mathbf{b}}_j=0$ contradicting the basis property. Finally, $\overline{\mathbf{a}}_{-1}*(\lambda_i\overline{\mathbf{b}}_j-\lambda_j\overline{\mathbf{b}}_i)=0$ implying as just above that $\lambda_i\mathbf{b}_j-\lambda_j\mathbf{b}_i\in F_{n+1}\mathfrak{g}$, contradiction.

Since the codimension is always 1 unless things degenerate into zero, we can choose choose $\mathbf{a}_{-1}\in\mathfrak{g}$ so that $\overline{\mathbf{a}}_{-1}=\mathbf{a}_{-1}+F_0\mathfrak{g}$ forms a basis of $F_{-1}\mathfrak{g}/F_0\mathfrak{g}$. Also for the top degree $N=|\phi|-1$ we choose nonzero $\mathbf{a}_N\in F_n\mathfrak{g}$. With this choices, we define all the elements in the middle recursively: $\mathbf{a}_n=\mathbf{a}_{-1}*\mathbf{a}_{n+1}$. Notice that $\overline{\mathbf{a}}_n\neq 0$ because if $\mathbf{a}_n\in F_{n+1}\mathfrak{g}$ then $F_{n+1}\mathfrak{g}$ is an ideal that contradicts simplicity of $\mathfrak{g}$.

When we reach the bottom degree the element is already predefined there. Nevertheless, we can conclude that $\lambda\mathbf{a}_{-1}+\mathbf{x}_0=\mathbf{a}_{-1}*\mathbf{a}_0$ for some $\mathbf{x}_0\in F_0\mathfrak{g}$. Without loss of generality $\lambda=1$ because we can replace $\mathbf{a}_N$ by $\lambda^{-1}\mathbf{a}_N$. In the associated graded algebra, $\overline{\mathbf{a}}_i*\overline{\mathbf{a}}_j=\alpha_{i,j}\overline{\mathbf{a}}_{i+j}$ and we can compute the coefficients $\alpha_{i,j}$ recursively:

$$\alpha_{-1,j}=1=-\alpha_{j,-1},\ \alpha_{i,j}=\alpha_{i-1,j}+\alpha_{i,j-1}.$$

The second formula follows from $\alpha_{i,j}\overline{\mathbf{a}}_{i+j-1}=\overline{\mathbf{a}}_{-1}*\alpha_{i,j}\overline{\mathbf{a}}_{i+j}=(\overline{\mathbf{a}}_{-1}*\overline{\mathbf{a}}_i)*\overline{\mathbf{a}}_j+\overline{\mathbf{a}}_i*(\overline{\mathbf{a}}_{-1}*\overline{\mathbf{a}}_j)=\overline{\mathbf{a}}_{i-1}*\overline{\mathbf{a}}_j+\overline{\mathbf{a}}_i*\overline{\mathbf{a}}_{j-1}$. By induction, it follows that

$$\alpha_{i,j}=\left(\begin{array}{c}i+j+1\\ i+1\end{array}\right)-\left(\begin{array}{c}i+j+1\\ i\end{array}\right)$$

and $\overline{\mathbf{a}}_k \mapsto X^{(k+1)}\partial$ is an isomorphism since $X^{(n)}\partial * X^{(m)}\partial = (X^{(n)}X^{(m-1)} - X^{(n-1)}X^{(m)})\partial = (\begin{pmatrix} n+m-1 \\ n \end{pmatrix} - \begin{pmatrix} n+m-1 \\ n-1 \end{pmatrix})X^{(n+m-1)}\partial$. □

We have used the dimension assumption only at the end. In fact, it is not required. One can use the properties of binomial coefficients to fiddle the argument at the end to show a stronger statement that any finite dimensional simple Lie algebra with subalgebra of codimension 1 and the associated filtration has $\mathrm{gr}(\mathfrak{g})$ isomorphic to $W(1,\phi)$ for some ϕ.

A more interesting question is whether we can change $\mathbf{a}_{-1}$ to force $\mathbf{b}_0 = 0$. This would lead to an even stronger statement that $\mathfrak{g} \cong W(1,\phi)$. While the answer to this question is positive we are in position to tackle it here. It involves subtleties of the deformation theory[2] of $W(1,\phi)$. In characteristic zero, a simple Lie algebra is rigid, i.e., all its deformations are isomorphic to itself. $W(1,\phi)$ is no longer rigid but its non-trivial deformations are no longer simple.

12.2 Filtration properties of the Witt algebra

We are ready to describe the filtration on $\mathfrak{g} = W(1,k)$ described in Proposition 11.1,

Proposition 12.2 *If $n \geq 0$ then $F_n\mathfrak{g} = \{\sum_i \alpha_i \mathbf{e}_i \in W(1,k) \mid \forall k \in \{0,\ldots,n\} \ \sum_i \alpha_i i^k = 0\}$.*

Proof: We go by induction on n. The basis of the induction is the definition of ł.

Suppose we have proved it for $n-1$. Consider an element $\mathbf{x} = \sum_i \alpha_i \mathbf{e}_i \in F_{n-1}\mathfrak{g}$. By induction assumption, $\sum_i \alpha_i i^k = 0$ for $k < n$. Now $\mathbf{x} * \mathbf{e}_t = \sum_i \alpha_i (i-t)\mathbf{e}_{i+t}$. Clearly, $\mathbf{x} \in F_n\mathfrak{g}$ if and only if $\mathbf{x} * \mathbf{e}_t \in F_{n-1}\mathfrak{g}$ for all t if and only if $\sum_i \alpha_i (i-t)(i+t)^k = 0$ for all $k < n$ and t. Now observe that $\sum_i \alpha_i (i-t)(i+t)^{n-1} = \sum_i \alpha_i i^n$ while $\sum_i \alpha_i (i-t)(i+t)^k = 0$ for $k \leq n-2$ by induction assumption. □

12.3 Main theorem

Let $\mathbb{F}(p^k)$ be the field of p^k elements.

Lemma 12.3 *If $0 < m < p^k - 1$ then $\sum_{\alpha \in \mathbb{F}(p^k)} \alpha^m = 0$. If $m = p^k - 1$ then $\sum_{\alpha \in \mathbb{F}(p^k)} \alpha^m = -1$.*

Proof: Let d be the greatest common divisor of m and $p^k - 1$. Write $m = dm'$. Since the multiplicative group of $\mathbb{F}(p^k)$ is the cyclic group[3] of order

[2] never mind, it is not examinable

[3] In general, any finite subgroup A of the multiplicative group of any field is finite as you have learnt in Algebra-II. This follows from the unique factorisation property of the

p^k-1, $a \mapsto a^{m'}$ is a permutation of the field and $\sum_{\alpha\in\mathbb{F}(p^k)} \alpha^m = \sum_{\alpha\in\mathbb{F}(p^k)} \alpha^d$.

Now let $p^k - 1 = dq$. The map $a \mapsto a^d$ is an endomorphism of the multiplicative group whose image consists of all the elements with orders dividing q. Calling this image A we get $\sum_{\alpha\in\mathbb{F}(p^k)} \alpha^d = d\sum_{\alpha\in A} \alpha$.

Observe that A is a cyclic group of order q. If $m = p^k - 1$ then $q = 1$, $d = p^k - 1$ and we get the second statement. If $0 < m < p^k - 1$ then the q elements of A are the roots of $z^q - 1$. Hence, $z^q - 1 = \prod_{\alpha\in A}(z - \alpha)$ and, consequently, $\sum_{\alpha\in A} \alpha = 0$ as the coefficients at z^{q-1} is zero. □

Theorem 12.4 *Let $n = 1$ and $\phi(1) = k$. Then $W(1, \phi) \cong W(1, k)$.*

PROOF: (partial, $k = 1$ only) Lemma 12.3 and Proposition 12.2 give us a non-zero element in the top of the filtration: $\mathbf{a}_{p^k-2} = \sum_i \mathbf{e}_i$. It remains to choose $\mathbf{a}_{-1}$ and I can do this painlessly only if $k = 1$. Let $\mathbf{a}_{-1} = -\mathbf{e}_1$. Observe that by induction

$$\mathbf{a}_{p^k-2-t} = \mathbf{a}_{-1} * \mathbf{a}_{p^k-1-t} = \sum_i (-1)^t(1 - i)(0 - i)(-1 - i)\dots(2 - t - i)\mathbf{e}_{i+t}$$

for non-negative grades. If $k = 1$ each consecutive element has one less term as zeros will appear in the product which will give $\mathbf{a}_{-1} * \mathbf{a}_0 = (-1)^{p-1}(p - 1)!\mathbf{e}_1 = \mathbf{a}_{-1}$ because $(p - 1)! = -1$ by Wilson's theorem[4] □

12.4 Exercises

Prove that $\prod_{\alpha\in\mathbb{F}(p^k)} \alpha = -1$.

polynomials as every $z - \alpha$, $\alpha \in A$ divides $z^m - 1$ where m is the exponent of A. Thus, the exponent A must be equal to the order of A that characterises cyclic groups.

[4]Observe that the product of all elements in an abelian group is equal to the product of elements of order 2 as the rest of the elements can be paired up with their inverses. Now the multiplicative group of $\mathbb{F}(p)$ is cyclic and has only one element -1 of order 2.

13 Differentials on a scheme

We already know how to do vector fields on a scheme and we are about to learn how to do differentials.

13.1 Calculus

We would like to consider a module M over a commutative algebra A as a geometric object over the scheme Spec (A). The correct geometric notion is the one of *quasicoherent sheaf* but we would like it have more structure. We define *a calculus* on a scheme Spec (A) as a pair $(M, \mathbf{d}_M)$ where M is an A-module M and $\mathbf{d}_M : A \to M$ is a linear map such that $\mathbf{d}_M(ab) = a\mathbf{d}_M b + b\mathbf{d}_M a$.

As a primary example, let us consider *the universal calculus*. As an A-module, $\mathcal{C}(A)$ is generated by symbols $\mathbf{d}a$ for all $a \in A$. There are two types of relations:

$$\mathbf{d}(\alpha a+\beta b) = \alpha\mathbf{d}a+\beta\mathbf{d}b \text{ and } \mathbf{d}(ab) = a\mathbf{d}(b)+b\mathbf{d}(a) \text{ for all } a, b \in A, \alpha, \beta \in \mathbb{K}.$$

The first type of relations makes $\mathbf{d}$ linear and the second type enforces the product rule. Since these relations hold in any calculus, we can immediately observe the universal property of the universal calculus. For any other calculus $(M, \mathbf{d}_M)$ there exists a unique homomorphism $\phi : \mathcal{C}(A) \to M$ of A-modules such that $\phi(\mathbf{d}a) = \mathbf{d}_M(a)$ for each $a \in A$. This property justifies writing $\mathbf{d}a$ rather than $\mathbf{d}_{\mathcal{C}(A)}a$ while working with universal calculus.

For example:, consider $A = \mathbb{K}[z]/[z^2]$. If $p \neq 2$, $z\mathbf{d}z = \mathbf{d}(z^2)/2 = 0$ and $\mathcal{C}(A)$ is one-dimensional vector space with a basis $\mathbf{d}z$. If $p = 2$, $z\mathbf{d}z \neq 0$ as it does not formally follows from the relations and the universal calculus is a two-dimensional vector space, a free A-module with a basis $\mathbf{d}z$. It is significant as the freeness of the universal calculus is a sign of smoothness. We will not discuss it here but Spec A, indeed, becomes very special in characteristic 2 as this becomes *a group scheme*.

We will now give a less formal view of the universal calculus. The multiplication $\mu : A \times A \to A$ is a bilinear map and as such it uniquely defines a linear map from the tensor product $\mu : A \otimes A \to A$, which we can denote by the same letter. Notice that $A \otimes A$ is a commutative algebra (under $a \otimes b \cdot a\prime \otimes b\prime = aa' \otimes bb'$) and μ is a an algebra homomorphism. Hence, its kernel I is an ideal. It has two distinct A-modules structures given by multiplication in the left and right factors: $a \star (b \otimes c) = ab \otimes c$ and $a * (b \otimes c) = b \otimes ac$.

We define $M = I/I^2$ with one of these structures and $\mathbf{d}_M : A \to I/I^2$ by $\mathbf{d}_M(f) = 1 \otimes f - f \otimes 1 + I^2$.

Proposition 13.1 *Both A-module structures on I/I^2 are the same. The map $\mathbf{d}_M$ defines a calculus structure on M, isomorphic to the universal calculus $\mathcal{C}(A)$.*

PROOF: Let us check the first statement: $a * x - a \star x = (1 \otimes a - a \otimes 1)x$ belongs to I^2 if $x \in I$. Hence $a * (x + I^2) = a \star (x + I^2)$ if $x \in I$.

Now we define linear maps $\phi : M \to \mathcal{C}(A)$, $\phi(\sum_i a_i \otimes b_i + I^2) = \sum_i a_i \mathbf{d} b_i$ and $\psi : \mathcal{C}(A) \to M$, $\psi(\sum_i a_i \mathbf{d} b_i) = \sum_i (a_i \otimes b_i - a_i b_i \otimes \mathbf{1}) + I^2$. The first task is to establish that these are well-defined.

To show that ϕ is well-defined we need to prove that $\phi(x) = 0$ for each $x \in I^2$. Such x is a linear combination of $(\sum_i a_i \otimes b_i)(\sum_j c_j \otimes d_j)$ with $\sum_i a_i b_i = \sum_j c_j d_j = 0$. Hence $\phi(x)$ is a linear combination of $\sum_{i,j} a_i c_j \mathbf{d}(b_i d_j) = \sum_{i,j} a_i b_i c_j \mathbf{d}(d_j) + \sum_{i,j} a_i c_j d_j \mathbf{d}(b_i) = 0$.

To show that ψ is well-defined it is necessary and sufficient to check the axiom of calculus on M. Indeed, ψ defines a map on the free module with generators $\mathbf{d}a$. Well-definedness is equivalent to vanishing on the submodule of relations. The first relation is just linearity and it is obvious. The second relation is equivalent to the product rule for $\mathbf{d}_M$ and needs verification: $\mathbf{d}_M(ab) = 1 \otimes ab - ab \otimes 1 + I^2 = a \cdot (1 \otimes b - b \otimes 1) + b * (1 \otimes a - a \otimes 1) + I^2 = a\mathbf{d}_M(b) + b\mathbf{d}_M(a)$.

Thus, we know that M is a calculus and it remains to establish that ϕ and ψ are inverse bijections: $\psi(\phi(\sum_i a_i \otimes b_i + I^2)) = \psi(\sum_i a_i \mathbf{d} b_i) = \sum_i (a_i \otimes b_i - a_i b_i \otimes \mathbf{1}) + I^2 = \sum_i a_i \otimes b_i + I^2$ since $\sum_i a_i b_i = 0$. In the opposite direction, $\phi(\psi(\sum_i a_i \mathbf{d} b_i)) = \phi(\sum_i (a_i \otimes b_i - a_i b_i \otimes \mathbf{1}) + I^2) = \sum_i (a_i \mathbf{d}_M(b_i) - a_i b_i \mathbf{d}_M(\mathbf{1})) = \sum_i (a_i \mathbf{d}_M(b_i)$ since $\mathbf{d}_M(\mathbf{1}) = 0$. □

Again in the example of $A = \mathbb{K}[z]/[z^2]$, I is two dimensional with a basis $1 \otimes z - z \otimes 1$ and $z \otimes z$. If $p \neq 2$ then I^2 contain $z \otimes z = -(1 \otimes z - z \otimes 1)^2/2$ and I/I^2 is one dimensional with basis $1 \otimes z - z \otimes 1 + I^2 = \mathbf{d}_M(z)$. On the other hand, if $p = 2$ then $I^2 = 0$ and $M = I$ is two-dimensional.

In analysis you may have got used to the fact that differentials are linear functionals on tangent spaces. The same is true here. Each $\omega = g\mathbf{d}f \in \mathcal{C}(A)$ defines a linear map $\omega_x = g(x) d_x f : T_x\mathcal{X} \to R$ where x is a point of Spec (A) over R. As a tangent vector $\tau \in T_x\mathcal{X}$ is a derivation $\tau : A \to R$, we can define $\omega_x(\tau) = g(x)\tau(f)$. We leave it to the reader to check that this is well-defined.

13.2 Differential calculus

We would like to see how the universal calculus behaves with respect to derivations. We consider the Lie algebra $\mathfrak{g} = \mathrm{Der}(A)$ and its natural representation on A. It is instructive to work with the second realization of the universal calculus in the next proposition.

Proposition 13.2 *The universal calculus $\mathcal{C}(A)$ is a representation of* $\mathrm{Der}(A)$. *The differential $\mathbf{d} : A \to \mathcal{C}(A)$ is a homomorphism of representations. The product rule $\partial(a\omega) = \partial(a)\omega + a\partial(\omega)$ holds for all $\partial \in \mathrm{Der}(A)$, $a \in A$, $\omega \in \mathcal{C}(A)$.*

Proof: A tensor product of representations is a representation. This defines a representation structure on $A \otimes A$ via $\partial(a \otimes b) = \partial(a) \otimes b + a \otimes \partial(b)$. To see that $\mathcal{C}(A)$ is a representation it suffices to establish that both I and I^2 are subrepresentations. If $x = \sum_i a_i \otimes b_i \in I$ then $\partial(x) = \sum_i (\partial(a_i) \otimes b_i + a_i \otimes \partial(b_i))$. Observe that $\partial(x) \in I$ because $\mu(\partial(x)) = \sum_i (\partial(a_i)b_i + a_i\partial(b_i)) = \partial(\sum_i a_i b_i) = 0$. Finally, because of the product rule $\partial(I^2) \subseteq I\partial(I) \subseteq I^2$.

Since $\partial(\mathbf{1}) = 0$, the second statement is straightforward: $\partial(\mathbf{d}a) = \partial(\mathbf{1} \otimes a - a \otimes \mathbf{1} + I^2) = \mathbf{1} \otimes \partial(a) - \partial(a) \otimes \mathbf{1} + I^2 = \mathbf{d}(\partial a)$.

Finally, $\partial(a \cdot (\sum_i b_i \otimes c_i + I^2)) = \partial(\sum_i ab_i \otimes c_i + I^2) = \sum_i (\partial(a)b_i \otimes c_i + a\partial(b_i) \otimes c_i + ab_i \otimes \partial(c_i)) + I^2 = \partial(a) \cdot (\sum_i b_i \otimes c_i + I^2) + a \cdot \partial(\sum_i b_i \otimes c_i + I^2)$. □

Such situation should be really called *a differential calculus*, i.e., a differential calculus is a triple $(M, \mathbf{d}, \mathfrak{g})$ where $(M, \mathbf{d})$ is a calculus, $\mathfrak{g}$ is a Lie subalgebra of $\mathrm{Der}(A)$ and the statements of Proposition 13.2 hold. While we use this terminology, it is definitely non-standard. Thus, we will not examine the usage of this terminology.

13.3 PD-calculus

This short section is of little relevance because the special derivations are not PD-derivations. They come quite close, so this section comes quite close to defining the necessary differential calculus. Hence, we think it is instructive to spell out the necessary structures.

A calculus $(M, \mathbf{d}_M)$ on a PD-scheme Spec (A, I, γ_n) is called *a PD-calculus* if $\mathbf{d}_M(\gamma_n(x)) = \gamma_{n-1}(x)\mathbf{d}_M x$ for all $x \in I$ and n.

One can turn a calculus $(M, \mathbf{d}_M)$ into a PD-calculus by imposing these relation, i.e. let N be the A-submodule of M generated by all $\mathbf{d}_M(\gamma_n(x)) - \gamma_{n-1}(x)\mathbf{d}_M x$ for all $x \in I$ and n. We the new calculus $\widetilde{M} = M/N$ with $\mathbf{d}_{\widetilde{M}}(x) = \mathbf{d}_M(x) + N$. Clearly, it is a PD-calculus.

The universal PD-calculus $\widetilde{\mathcal{C}}(A)$ is the quotient of $\mathcal{C}(A)$. It satisfies the universal property among all PD-calculi.

As an example, consider $\widetilde{\mathcal{C}}(A)$ for $A = \mathbb{K}[z]/[z^2]$ in characteristic 2. The PD-condition forces $0 = \mathbf{d}(\gamma_2(z)) = z\mathbf{d}(z)$ making $\widetilde{\mathcal{C}}(A)$ one-dimensional vector space with a basis $\mathbf{d}(z)$, similarly to the universal calculus in odd characteristic.

We leave the following proposition as an exercise and we will not use it

later.

Proposition 13.3 *If A is an algebra with a PD-structure then $(\widetilde{\mathcal{C}}(A), \mathbf{d}, \mathrm{PD}-\mathrm{Der}(A)$ is a differential calculus.*

13.4 Exercises

Prove that in a calculus $\mathbf{d}_M(\alpha\mathbf{1}) = 0$ for any $\alpha \in \mathbb{K}$.

Prove that, given a calculus on an algebra A, the set of all $x \in A$ such that $\mathbf{d}_M(x) = 0$ form a subalgebra (constants of the calculus) of A_0. Prove that $\mathbf{d}_M$ is a homomorphism of A_0-modules.

Consider $A = \mathbb{K}[X]$ and a finite-dimensional A-module M. Show that for each $m \in M$ the assignment $d_M(X) = m$ can be uniquely extended to a calculus. Prove that constants depend only on the generalised minimal polynomial $\mu_{X,m}(Z)$ of X (as it acts on M) and describe the constants explicitly.

Prove that if A is a finitely generated algebra then $\mathcal{C}(A)$ is finitely generated A-module.

Prove Proposition 13.3.

14 Lie algebras of Cartan type

We define what it means for a Lie algebra to be of Cartan type and state their classification.

14.1 Differential forms

Given a commutative algebra A and an A-module M, we construct its external powers $\wedge_A^n M$ as an A-module in two steps. As a first step, the tensor power $T_A^n M$ is the quotient of the tensor power vector space $T_{\mathbb{K}}^n M = M \otimes M \otimes \dots M$ by the vector subspace V spanned by tensors $x_1 \otimes \dots x_{k-1} \otimes (ax_k \otimes x_{k+1} - x_k \otimes ax_{k+1}) \otimes x_{k+2} \otimes \dots x_n$ for all $a \in A$, $x_i \in M$. Clearly, $T_A^n M$ has a canonical A-module structure as the A-action on each factor produces the same result. At the second step $\wedge_A^n M$ is the quotient of $T_A^n M$ by the A-submodule, generated by all $u \otimes x \otimes v \otimes x \otimes w + V$ where $x \in M$, u, v and w are elements of various tensor products. Notice that if the characteristics is not 2, the latter submodule is generated by all $x_1 \otimes \dots x_{k-1} \otimes (x_k \otimes x_{k+1} + x_k \otimes x_{k+1}) \otimes x_{k+2} \otimes \dots x_n + V$.

We denote $x_1 \wedge \dots \wedge x_n = x_1 \otimes \dots \otimes x_n + W$ where W is the kernel of the natural linear map $T_{\mathbb{K}}^n M \to \wedge_A^n M$.

In the case of calculus $(M, \mathbf{d}_M)$ the elements of $\wedge_A^n M$ should be referred as n-forms. You may have seen them in differential geometry and analysis.

Proposition 14.1 *If $(M, \mathbf{d}_M, \mathfrak{g})$ is a differential calculus then each $\wedge_A^n M$ is an $\mathfrak{g}$-module.*

Proof: By routine check that $\partial\omega \in W$ when $\omega \in W$. Consult your lecture notes. □

14.2 Special differential calculus

We consider the PD-algebra A_ϕ where $\phi : \{1, 2 \dots n\} \to \mathbb{Z}_{\geq 1}$. It is a representation of the Witt algebra $\mathfrak{g} = W(n, \phi)$. We construct *a special differential calculus* to go along with it. As a module $M = \oplus_{j=1}^n A_\phi \mathbf{d}X_j$ is a free A_ϕ-module with a basis $\mathbf{d}X_j$. The differential is given by the usual formula $\mathbf{d}_M(f) = \sum_j \partial_j(f)\mathbf{d}X_j$ using the basis of the special derivations. Finally, the action of $W(n, \phi)$ is given by the standard formula: $\partial(f\mathbf{d}X_j) = \partial(f)\mathbf{d}X_j + f\mathbf{d}_M(\partial(X_j))$.

Proposition 14.2 *With the maps defined above, $(M, \mathbf{d}_M, W(n, \phi))$ is a differential calculus.*

Proof: This routine check is left as an exercise. The following formula is useful: $g\partial_i(f\mathbf{d}X_j) = g\partial_i(f)\mathbf{d}X_j + \delta_{i,j} \sum_k f\partial_k(g)\mathbf{d}X_k$. □

14.3 Contact, symplectic and volume forms and certain graded Lie algebras

In differential geometry, various forms play various important roles and usually have names as certain "structures" on manifolds. In particular, a pointwise non-vanishing n-form ω on an n-dimensional manifold $\mathcal{X}$ is *a volume form*. Indeed, it locally records the volume and allows one to integrate functions by $\int_{\mathcal{X}} f(X) = \int_{\mathcal{X}} f\omega$. Here we are more in special n-forms on A_ϕ and by analogy with the the differential geometry we call

$$\omega_S = \mathbf{d}X_1 \wedge \mathbf{d}X_k \ldots \wedge \mathbf{d}X_n \in \wedge^n_{A_\phi} M$$

the volume form. It may be worse pointing out that in differential geometry every volume form looks like this in a certain choice of local coordinates. It is an easy (but non-examinable) exercise.

A pointwise non-vanishing 1-form ω on an n-dimensional manifold $\mathcal{X}$ is *a contact form* if it satisfies a certain "integrability condition", which amounts to the vector fields in the kernel of this form comprising a Lie subalgebra inside all vector fields. You can observe this form and appreciate its name by riding an bicycle (non-examinable too). Observe that while the rotation of the front wheel is unrestricted, its velocity lies the direction of the wheel at any given moment. This says that the velocity (tangent vector) lies in the kernel of the contact structure. Contact structures play significant role in control theory and thermodynamics but I doubt that this will be discussed in undergraduate courses on these topics. Contact structures exist only on odd dimensional spaces, so we define

$$\omega_K = \mathbf{d}X_n + \sum_{j=1}^{t} (X_j \mathbf{d}X_{j+t} - X_{j+t}\mathbf{d}X_j) \in M$$

where $n = 2t + 1$. Again in differential geometry every contact form looks like this in a certain choice of local coordinates. It is a non-trivial result called Darboux's Theorem.

Finally, a non-degenerate closed 2-form ω on an n-dimensional manifold $\mathcal{X}$ is *a symplectic form*. They are very similar to contact forms. Closeness plays role of "the integrability condition". Non-degeneracy (the local skew-symmetric matrix has rank n) replaces non-vanishing. Symplectic forms first appear in Hamiltonian approach to classical mechanics but became ubiquitous throughout modern mathematics. Symplectic structures exist only on even dimensional spaces, so we define

$$\omega_H = \sum_{j=1}^{t} \mathbf{d}X_j \wedge \mathbf{d}X_{j+t} \in \wedge^2_{A_\phi} M$$

where $n = 2t$. Again in differential geometry every symplectic form looks like this in a certain choice of local coordinates, which is again called Darboux's Theorem.

Using these forms we define a series of new Lie algebras, which are of Cartan type, although we have not defined what it means. Cartan has studied these Lie algebras in differential geometry where they remain simple but become infinite-dimensional:

$$S(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_S) = 0\},$$

$$H(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_H) = 0\},$$

$$K(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_K) \in A_\phi \omega_K\},$$

$$CS(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_S) \in \mathbb{K}\omega_S\},$$

$$CH(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_H) \in \mathbb{K}\omega_H\}.$$

While it is easy to observe that all five are Lie subalgebras of the Witt algebra, the following theorem is more involved. While we have all the necessary tools to prove it, we do not have time, so it is given without a proof.

Theorem 14.3 *Algebras $S(n,\phi)$, $H(n,\phi)$, $K(n,\phi)$, $CS(n,\phi)$, $CH(n,\phi)$ are graded Lie algebras. Of $p \geq 3$ then Lie algebras $S(n,\phi)$, $H(n,\phi)$, $K(n,\phi)$ are simple.*

Maybe, it is worse pointing out that the grading on $K(n,\phi)$ is slightly unusual. The remaining 4 algebras inherit their grading for $W(n,\phi)$ but in $K(n,\phi)$ we need to assign degree 2 to X_n and -2 to ∂_n. See also the exercises below.

The Lie algebra $S(n,\phi)$ is called *the special Lie algebra*, $H(n,\phi)$ *the hamiltonian Lie algebra* and $K(n,\phi)$ *the contact Lie algebra*.

14.4 Lie algebras of Cartan type

We have constructed several Lie algebra of Cartan type but there are more. The following definition is rather technical but it has been adopted throughout the classification. A finite-dimensional simple Lie algebra $\mathfrak{g}$ is *a Lie algebra of Cartan type* if it admits a descending filtration $F_n\mathfrak{g}$ such that the associated graded Lie algebra $\mathrm{gr}(\mathfrak{g})$ is a transitive graded Lie subalgebra of one of the algebras $W(n,\phi)$, $S(n,\phi)$, $H(n,\phi)$, $K(n,\phi)$, $CS(n,\phi)$, $CH(n,\phi)$. transitivity can be formulated as for each $\mathbf{x} \in \mathrm{gr}(\mathfrak{g})_k$ with $k \geq 0$ the condition $\mathbf{x} * \mathrm{gr}(\mathfrak{g})_{-1} = 0$ implies $\mathbf{x} = 0$.

The new algebras that appear are no longer graded. They appear because there are more volume and symplectic forms on A_ϕ. Amazingly, Darboux's Theorem holds for contact forms but fails for symplectic. We consider forms

$$\omega_S^1 = e^{X_1}\omega_S = (\sum_k X_1^{(k)})\mathbf{d}X_1 \wedge \mathbf{d}X_k \ldots \wedge \mathbf{d}X_n \in \wedge^n_{A_\phi} M,$$

$$\omega_S^1 = (1 - X^{(1,1,\ldots 1)})\omega_S = (1 - \prod_k X_k)\mathbf{d}X_1 \wedge \mathbf{d}X_k \ldots \wedge \mathbf{d}X_n \in \wedge^n_{A_\phi} M,$$

$$\omega_H^1 = \mathbf{d}_{\wedge^2 M}(e^{X_1}\sum_{j=1}^{t} X_j \mathbf{d}X_{j+t}) = e^{X_1}\omega_H + \ldots \in \wedge^2_{A_\phi} M,$$

$$\omega_H^2 = \omega_H + \sum_{i,j} \alpha_{i,j} X_i X_j \mathbf{d}X_i \wedge \mathbf{d}X_j + \ldots \in \wedge^2_{A_\phi} M.$$

In the definition of ω_H^1 we use $\mathbf{d}_{\wedge^2 M}(f\mathbf{d}X_i) = \mathbf{d}_M(f) \wedge \mathbf{d}X_i = \sum_j \partial_j(f)\mathbf{d}X_j \wedge \mathbf{d}X_i$. In the definition of ω_H^2 we use a nonsingular skew-symmetric matrix. It is know which matrices define equivalent forms but the relation is too cumbersome to attempt to state it here. The forms give rise to new special and hamiltonian Lie algebras

$$S^i(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_S^i) = 0\},$$

$$H^i(n,\phi) = \{\partial \in W(n,\phi) \mid \partial(\omega_H^i) = 0\},$$

The following theorem is the classification of Lie algebras of Cartan type. The proof is too long even to contemplate to explain it here.

Theorem 14.4 *Let $\mathfrak{g}$ be a finite-dimensional simple Lie algebra of Cartan type over an algebraically closed field of characteristic $p \geq 5$. Then $\mathfrak{g}$ is isomorphic to one of the Lie algebras $W(n,\phi)$, $S(n,\phi)$, $H(n,\phi)$, $K(n,\phi)$, $S^i(n,\phi)$, $H^i(n,\phi)$ where $i \in \{1,2\}$.*

14.5 Exercises

Prove Proposition 14.2.

Prove that $S(n,\phi)$ is an ideal of $CS(n,\phi)$.

Prove that $H(n,\phi)$ is an ideal of $CH(n,\phi)$.

We define *divergence* $\mathrm{Div} : W(n,\phi) \to A_\phi$ as a linear map defined by the formula $\mathrm{Div}(\sum_j f_j\partial_j) = \sum_j \partial_j(f_j)$. Prove that $S(n,\phi)$ consists of vector fields with zero divergence.

15 Root systems

We recall some important information about semisimple Lie algebras that you should have covered in Lie Algebras. So we just state the results without proofs.

15.1 Roots

A finite-dimensional semisimple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$ admits a Cartan subalgebra $\mathfrak{h}$ which is abelian. This leads to the Cartan decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha \text{ where } \mathfrak{g}_\alpha = \{\mathbf{x} \in \mathfrak{g} \mid \forall \mathbf{h} \in \mathfrak{h} \mathbf{h} * \mathbf{x} = \alpha(\mathbf{h})\mathbf{x}\} \ .$$

Elements of R are called roots and R is a subset of $\mathfrak{h}^*$. The subspaces $\mathfrak{g}_\alpha$ are called root subspaces and all of them are one dimensional. They satisfy $\mathfrak{g}_\alpha * \mathfrak{g}_\beta \subseteq \mathfrak{g}_{\alpha+\beta}$ with equality if $\alpha + \beta$ is a root, so the Cartan decomposition is a grading by the free abelian group Λ generated by all $\alpha \in R$ inside the group $\mathfrak{h}^*$. The group Λ is called *the root lattice* but its elements are not called roots!! You may call them weights, although there may be more weights than elements of the root lattice. There is some rationale in calling zero a root and $\mathfrak{g}_0 = \mathfrak{h}$ a zero root subspace but there are also good reasons not to do it. So we won't.

Now R is a root system and have all the structures discusses in Lie algebras. One particularly useful feature is an ability to choose a basis α_1, α_2, $\ldots \alpha_n$, elements of each are called *simple roots*. A basis of the root system must be a basis of the vector space $\mathfrak{h}^*$ but needs to satisfy a further property: each root must be a linear combination of simple roots with either integral non-negative or integral non-positive coefficients.

The choice of such a basis is far from unique but they are all isomorphic, in a sense that one can move one basis into another basis by an element of the Weyl group, which will be discussed in the next subsection.

15.2 Coroots

The crucial bit of structure is the Killing form on $\mathfrak{g}$. It is a non-degenerate symmetric bilinear form on $\mathfrak{g}$ by Cartan criterion. Taking into account that $K(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$ unless $\alpha + \beta = 0$. This forces the restriction of the Killing form to $\mathfrak{h}$ being a non-degenerate symmetric bilinear form as well. This form provides a canonical linear isomorphism $\mathfrak{h} \to \mathfrak{h}^*$ via $\mathbf{x} \mapsto K(\mathbf{x}, \quad)$. We find this isomorphism particularly useful in the opposite direction, so we write $\alpha^* \in \mathfrak{h}$ for the image of an element $\alpha \in \mathfrak{h}$. One useful thing this isomorphism does is transferring the Killing form from $\mathfrak{h}$ to $\mathfrak{h}^*$. We denote

the transferred form by $\alpha \bullet \beta$. Observe that $\alpha \bullet \beta = K(\alpha^*, \beta^*)$ by the definition of the transferred form.

As you know from Algebra-I, bilinear forms are rather dull on complex vector spaces. The useful trick is to turn to real vector spaces, namely let $\mathfrak{h}^*_{\mathbb{R}}$ be the real subspace of $\mathfrak{h}$ spanned by roots. From the properties of the root system it is clear that simple roots form a basis of $\mathfrak{h}^*_{\mathbb{R}}$. It is a slightly more subtle observation that the form restricted to $\mathfrak{h}^*_{\mathbb{R}}$ is positive definite. Thus, $\mathfrak{h}^*_{\mathbb{R}}$ is naturally a Euclidean space and we can usual Euclidean things there such as talking about lengths, angles, etc. In particular, $||\alpha|| = \sqrt{\alpha \bullet \alpha}$ for each coroot α.

Now we are ready to define the coroots. For a root $\alpha \in R$, we define its coroot as

$$\alpha^\vee = 2\alpha^*/||\alpha||^2 \in \mathfrak{h} \ .$$

Thus, a coroot is an element of the Lie algebra $\mathfrak{g}$! One can play the root games with the coroots. Coroots form a root system $R^\vee$. Coroots $\alpha_i^\vee$ of simple roots form a basis the (co)root system $R^\vee$ and fully deserve the name of simple coroots. If R is simple then $R^\vee$ is usually of the same type with an exceptions of types B_n and C_n, $n \geq 3$. These two are swapped, i.e., the root system of type B_n has the coroot system of type C_n and vice versa.

One useful thing a coroot does is it defines a reflection $S_\alpha(\mathbf{x}) = \mathbf{x} - \alpha^\vee(\mathbf{x})\alpha$. We can equally write $\alpha^\vee(\mathbf{x})$ or $\mathbf{x}(\alpha^\vee)$ as we are ambivalent which of the vector spaces $\mathfrak{h}$, $\mathfrak{h}^*$ consist of "elements" and which one consists of "functionals on elements". I hope you do not need reminding that the canonical map $V \to (V^*)^*$ is an isomorphism for finite-dimensional vector spaces. One can define reflections S_α as either complex linear transformations of $\mathfrak{h}$ or real linear transformations of $\mathfrak{h}_{\mathbb{R}}$ or lattice automorphisms of $\mathfrak{h}$, depending on particular aims. The group W generated by them is the same in each case. It is called the Weyl group. For instance, to see that W is finite it is instructive to look at $\mathfrak{h}_{\mathbb{R}}$. One observes that W is a discrete subgroup of the orthogonal group, and as the orthogonal group is compact, W must be finite.

Another useful thing derived from coroots is Cartan matrix

$$(C_{i,j}) = \alpha_j^\vee(\alpha_i) \ .$$

It is a matrix with integral coefficients with diagonal elements $C_{i,i}$ equal to 2. Off-diagonal elements are either 0, -1, -2 or -3 depending on the angle between α_i and α_j as well as their lengths. One interpretation of the Cartan matrix is that its columns are coordinate expressions of simple roots in the basis of fundamental weights. Recall that a fundamental weight

$\omega_i \in \mathfrak{h}^*$ is an element of the dual basis to the basis of simple coroots, that is, $\omega_i(\alpha_j^\vee) = \delta_{i,j}$.

15.3 Cartan automorphism

There exists a unique Lie algebra automorphism $\kappa : \mathfrak{g} \to \mathfrak{g}$ satisfying the following properties:

(i) $\kappa^2 = I_{\mathfrak{g}}$,
(ii) $\kappa_{\mathfrak{h}} = -I_{\mathfrak{h}}$,
(iii) $\kappa(\mathfrak{g}_\alpha) = \mathfrak{g}_{-\alpha}$.

The easiest way to see this is via Serre's theorem. The latter defines $\mathfrak{g}$ via generators $\mathbf{h}_i, \mathbf{e}_i, \mathbf{f}_i$ and Serre's relations. One can κ on generators by $\kappa(\mathbf{h}_i) = -\mathbf{h}_i$, $\kappa(\mathbf{e}_i) = -\mathbf{f}_i$, $\kappa(\mathbf{f}_i) = -\mathbf{e}_i$. This defines an automorphism of the free Lie algebra with the same generators. It remains to check that the ideal generated by relations is stable under κ. We leave details as an exercise.

15.4 Series of roots

You have seen in Lie Algebras that, given a root α, the intersection $\mathbb{C}\alpha \cap R$ is equal to $\{\alpha, -\alpha\}$. This property ensures that the root system is reduced.

We need a slightly more subtle property which was probably covered but we will sketch a proof to improve self-consistency of these notes. Given two roots α, β the intersection $\beta + \mathbb{Z}\alpha \cap R$ is called *the α-series via β*.

Proposition 15.1 *Let $\alpha, \beta \in R$ such that $\alpha \neq \pm\beta$. The following statements hold.*

(i) $\beta + \mathbb{Z}\alpha \cap R = \{\beta - r\alpha, \beta - (r-1)\alpha, \ldots, \beta + q\alpha\}$ *for some* $r, q \in \{0, 1, 2, 3\}$.
(ii) $r - q = \alpha^\vee(\beta)$.
(iii) If $\alpha + \beta \in R$ *then* $r + 1 = q\frac{||\alpha+\beta||^2}{||\beta||^2}$.

Proof: Everything happens inside the span of α and β. This span's intersection with R is a root system of rank 2. It suffices to go over all pairs of roots in the rank 2 systems $A_1 \times A_1$, A_2, B_2, G_2. Actually, one does not have to go over all pairs but over each possible angle between roots. The possible angles are $\pi/2$, $\pi/3$, $2\pi/3$, $\pi/4$, $3\pi/4$, $\pi/6$, $5\pi/6$ and going through all the cases is not long.

Refer to in-class lecture notes where I went through 3 of the angles. □

15.5 Lie algebras of classical type

Let $\mathbb{K}$ be a field of characteristic $p \geq 5$. A simple finite-dimensional Lie algebra $\mathfrak{g}$ over $\mathbb{K}$ is *a Lie algebra of classical type* if it satisfies the following 4 conditions:

(i) there exists an abelian Cartan subalgebra $\mathfrak{h}$,
(ii) there exists a Cartan decomposition $\mathfrak{g} = \mathfrak{h} \oplus \oplus_{\alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha$ where $\mathfrak{g}_\alpha = \{\mathbf{x} \in \mathfrak{g} \mid \forall \mathbf{h} \in \mathfrak{h} \mathbf{h} * \mathbf{x} = \alpha(\mathbf{h})\mathbf{x}\}$ with respect to $\mathfrak{h}$,
(iii) if $\mathfrak{g}_\alpha \neq 0$ then $\mathfrak{g}_\alpha * \mathfrak{g}_{-\alpha}$ is one-dimensional,
(iv) if $\alpha \neq 0 \neq \beta$ and $\mathfrak{g}_\alpha \neq 0 \neq \mathfrak{g}_\beta$ then there exists k in the prime subfield of $\mathbb{K}$ such that $\mathfrak{g}_{\alpha+k\beta} = 0$.

Over an algebraically close field, such Lie algebras follow Cartan-Killing classification. We do not intend to prove this but we would like to construct these Lie algebras.

15.6 Exercises

Prove that the angle between two simple roots is obtuse, i.e. greater or equal to $\pi/2$.

Verify that the columns of Cartan matrix are coordinate expressions of simple roots in the basis of fundamental weights.

Verify that κ is well-defined by writing images of Serre's relations under κ.

Argue why κ is unique.

Complete the proof of Proposition 15.1 by going through all possible angles.

16 Chevalley theorem

16.1 Representations of $\mathfrak{sl}_2$

In proposition 2.2, we constructed $n+1$ dimensional representation A_n of Lie algebra $\mathfrak{sl}_2(\mathbb{K})$ over any field. Over the field of complex numbers these are the only non-isomorphic representations of $\mathfrak{sl}_2(\mathbb{C})$. Furthermore, by Weyl's Complete Reducibility Theorem, every finite-dimensional representation of $\mathfrak{sl}_2(\mathbb{C})$ is completely reducible. This means that every finite-dimensional representation of $\mathfrak{sl}_2(\mathbb{C})$ is isomorphic to a direct sum of representations A_n. This has also been done in Lie Algebras and we will use this fact soon.

16.2 Chevalley basis

We would like to pick a very special basis of a simple finite-dimensional Lie algebra $\mathfrak{g}$ of $\mathbb{C}$. In the Cartan we use simple coroots $\alpha_i^\vee$. In each root space we choose a non-zero $\mathbf{e}_\alpha \in \mathfrak{g}_\alpha$.

Let us see what we can say about the products in this basis. By the definition of a root space $\alpha_i^\vee * \mathbf{e}_\beta = \alpha_i^\vee(\beta)\mathbf{e}_\beta$. Since the Cartan subalgebra is abelian, $\alpha_i^\vee * \alpha_j^\vee = 0$. It remains to see what happens with root vectors. First, $\mathbf{e}_\alpha * \mathbf{e}_{-\alpha} \in \mathfrak{h}$ but it is not immediately obvious what this element is. Second, if $\alpha \neq -\beta$ but $\alpha+\beta$ is not a root then $\mathbf{e}_\alpha * \mathbf{e}_\beta = 0$. Finally, if $\alpha+\beta$ is a root then $\mathbf{e}_\alpha * \mathbf{e}_\beta = c_{\alpha,\beta}\mathbf{e}_{\alpha+\beta}$ but the values of the constants $c_{\alpha,\beta} \in \mathbb{C}$ are not immediately clear.

The point of the following fact (Chevalley Theorem) is that one can do much better job determining the remaining products.

Theorem 16.1 *It is possible to choose $\mathbf{e}_\alpha \in \mathfrak{g}_\alpha$ so that the following two properties hold:*

(i) $\mathbf{e}_\alpha * \mathbf{e}_{-\alpha} = \alpha^\vee$ *for each root* α,

(ii) $c_{\alpha,\beta} = \pm(r+1)$ *for each pair of roots such that* $\alpha+\beta \in R$ *where* $\beta + \mathbb{Z}\alpha \cap R = \{\beta - r\alpha, \beta-(r-1)\alpha, \ldots, \beta+q\alpha\}$.

Proof: Let us choose $\widetilde{\mathbf{e}}_\alpha \in \mathfrak{g}_\alpha$ for each positive root α. For the negative roots we define $\widetilde{\mathbf{e}}_\alpha = -\kappa(\widetilde{\mathbf{e}}_{-\alpha})$ using Cartan's automorphism κ. We will readjust this basis once during the course of the proof to arrive at a basis with desired properties.

Let us first compute $\widetilde{\mathbf{e}}_\alpha * \widetilde{\mathbf{e}}_{-\alpha} \in \mathfrak{h}$. For arbitrary $\mathbf{x} \in \mathfrak{h}$, we compute Killing form $K(\mathbf{x}, \widetilde{\mathbf{e}}_\alpha * \widetilde{\mathbf{e}}_{-\alpha}) = K(\mathbf{x} * \widetilde{\mathbf{e}}_\alpha, \widetilde{\mathbf{e}}_{-\alpha}) = \alpha(\mathbf{x})K(\widetilde{\mathbf{e}}_\alpha, \widetilde{\mathbf{e}}_{-\alpha}) =$. On the other hand, $K(\mathbf{x}, \alpha^\vee) = 2K(\mathbf{x}, \alpha^*)/||\alpha||^2 = 2\alpha(\mathbf{x})/||\alpha||^2$. Since the form is non-degenerate, we conclude that

$$\widetilde{\mathbf{e}}_\alpha * \widetilde{\mathbf{e}}_{-\alpha} = \frac{1}{2}||\alpha||^2 K(\widetilde{\mathbf{e}}_\alpha, \widetilde{\mathbf{e}}_{-\alpha})\alpha^\vee \ .$$

Notice that $K(\widetilde{\mathbf{e}}_\alpha, \widetilde{\mathbf{e}}_{-\alpha}) \neq 0$ because the Killing form is non-degenerate and $K(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$ unless $\alpha + \beta = 0$.

Now we define

$$\mathbf{e}_\alpha = \frac{\sqrt{2}}{||\alpha||\sqrt{K(\widetilde{\mathbf{e}}_\alpha, \widetilde{\mathbf{e}}_{-\alpha})}}\widetilde{\mathbf{e}}_\alpha$$

for all the roots and these elements satisfy property (i). It suffices to verify property (ii).

Let us consider constants $c_{\alpha,\beta}$ in this basis. As the basis still satisfies $\kappa(\mathbf{e}_\alpha) = -\mathbf{e}_{-\alpha}$, applying κ to $\mathbf{e}_\alpha * \mathbf{e}_\beta = c_{\alpha,\beta}\mathbf{e}_{\alpha+\beta}$ gives $\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta} = -c_{\alpha,\beta}\mathbf{e}_{-\alpha-\beta}$. This implies that $c_{-\alpha,-\beta} = -c_{\alpha,\beta}$. Now we compute the product $(\mathbf{e}_\alpha * \mathbf{e}_\beta) * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta}) = c_{\alpha,\beta}c_{-\alpha,-\beta}\mathbf{e}_{\alpha+\beta} * \mathbf{e}_{-\alpha-\beta} = -c^2_{\alpha,\beta}(\alpha+\beta)^\vee = -c^2_{\alpha,\beta}/||\alpha+\beta||^2(\alpha^* + \beta^*)$.

Let us recompute this product using Jacobi's identity first: $(\mathbf{e}_\alpha * \mathbf{e}_\beta) * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta}) = \mathbf{e}_\alpha * (\mathbf{e}_\beta * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta})) + (\mathbf{e}_\alpha * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta})) * \mathbf{e}_\beta = -\mathbf{e}_\alpha * (\mathbf{e}_\beta * (\mathbf{e}_{-\beta} * \mathbf{e}_{-\alpha})) - \mathbf{e}_\beta * (\mathbf{e}_\alpha * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta}))$. These two products can be computed using representations of $\mathfrak{sl}_2$. The elements $\mathbf{e}_\alpha$, $\mathbf{e}_{-\alpha}$ and $\alpha^\vee$ span an $\mathfrak{sl}_2$-subalgebra in $\mathfrak{g}$. We consider $\mathfrak{g}$ as a representation of this $\mathfrak{sl}_2$. Subspaces $\mathfrak{g}_\gamma$, as γ runs through the α-series via $-\beta$, span an irreducible subrepresentation of dimension $r + q + 1$ forcing it to be isomorphic to A_{r+q}. Since $L^{r+1}_{\mathbf{e}_\alpha}(\mathbf{e}_{-\beta}) = L^{r+1}_{\mathbf{e}_{-\alpha}}(\mathbf{e}_{-\beta}) = 0$, an isomorphism must send $\mathbf{e}_{-\beta}$ into a multiple of $x^q y^r$. It follows that $\mathbf{e}_\alpha * (\mathbf{e}_{-\alpha} * \mathbf{e}_{-\beta}) = q(r+1)\mathbf{e}_{-beta}$ and the whole product is equal to $-q'(r'+1)\alpha^* - q(r+1)\beta^\vee$. It follows that

$$\frac{c^2_{\alpha,\beta}}{||\alpha+\beta||^2}\beta^* = q(r+1)\beta^\vee = \frac{q(r+1)}{||\beta||^2}\beta^*$$

and, finally, by part (iii) of Proposition 15.1

$$c^2_{\alpha,\beta} = q(r+1)\frac{||\alpha+\beta||^2}{||\beta||^2} = (r+1)^2 \ .$$

□

Any basis satisfying conditions of Theorem 16.1 will be called *Chevalley basis*. This basis depends on a choice of Cartan subalgebra. Besides, we have not addressed the issue of the signs. This means that the basis is not unique even if the choice of Cartan subalgebra is fixed.

16.3 G_2

As an example, we would like to write a part (positive Borel subalgebra) of multiplication table in Chevalley basis for Lie algebra of type G_2. The Cartan matrix is $\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$. The 12 roots are vertices of David's start.

Let $\alpha = \alpha_1$ be the long simple root, $\beta = \alpha_2$ the short simple root. Simple coroots are

$$\alpha^\vee = \frac{2}{3}\alpha^*,\ \beta^\vee = 2\beta^*\ .$$

Now we can fill the multiplication table (up to signs) of the positive Borel subalgebra of Lie algebra of type G_2:

	$\mathbf{e}_\alpha$	$\mathbf{e}_\beta$	$\mathbf{e}_{\alpha+\beta}$	$\mathbf{e}_{\alpha+2\beta}$	$\mathbf{e}_{\alpha+3\beta}$	$\mathbf{e}_{2\alpha+3\beta}$
$\alpha^\vee$	$2\mathbf{e}_\alpha$	$-\mathbf{e}_\beta$	$\mathbf{e}_{\alpha+\beta}$	0	$-\mathbf{e}_{\alpha+3\beta}$	$\mathbf{e}_{2\alpha+3\beta}$
$\beta^\vee$	$-3\mathbf{e}_\alpha$	$2\mathbf{e}_\beta$	$-\mathbf{e}_{\alpha+\beta}$	$\mathbf{e}_{\alpha+2\beta}$	$3\mathbf{e}_{\alpha+3\beta}$	0
$\mathbf{e}_\alpha$	0	$\pm\mathbf{e}_{\alpha+\beta}$	0	0	$\pm\mathbf{e}_{\alpha+3\beta}$	0
$\mathbf{e}_\beta$	$\pm\mathbf{e}_{\alpha+\beta}$	0	$\pm 2\mathbf{e}_{\alpha+2\beta}$	$\pm 3\mathbf{e}_{\alpha+3\beta}$	0	0
$\mathbf{e}_{\alpha+\beta}$	0	$\pm 2\mathbf{e}_{\alpha+2\beta}$	0	$\pm 3\mathbf{e}_{2\alpha+3\beta}$	0	0
$\mathbf{e}_{\alpha+2\beta}$	0	$\pm 3\mathbf{e}_{\alpha+3\beta}$	$\pm 3\mathbf{e}_{2\alpha+3\beta}$	0	0	0
$\mathbf{e}_{\alpha+3\beta}$	$\pm\mathbf{e}_{2\alpha+3\beta}$	0	0	0	0	0
$\mathbf{e}_{2\alpha+3\beta}$	0	0	0	0	0	0

To fill the rest of the table one needs the remaining coroots:

$$(\alpha+\beta)^\vee = 2(\alpha^*+\beta^*) = 3\alpha^\vee + \beta^\vee,\ (\alpha+2\beta)^\vee = 2(\alpha^*+2\beta^*) = 3\alpha^\vee + 2\beta^\vee,$$

$$(\alpha+3\beta)^\vee = \frac{2}{3}(\alpha^*+3\beta^*) = \alpha^\vee+\beta^\vee,\ (2\alpha+3\beta)^\vee = \frac{2}{3}(2\alpha^*+3\beta^*) = 2\alpha^\vee+\beta^\vee\ .$$

16.4 Exercises

In a Lie algebra of type A_2 with a fixed choice of Cartan subalgebra describe all possible Chevalley bases.

Fill the rest of the table for G_2.

Fill the full multiplication (up to signs) in type B_2.

17 Chevalley reduction

17.1 Reduced Lie algebra

Let $\mathfrak{g}_{\mathbb{C}}$ be a simple finite-dimensional Lie algebra over $\mathbb{C}$. The abelian subgroup of $\mathfrak{g}_{\mathbb{C}}$ generated by the Chevalley basis is *a Lie ring*. By Theorem 16.1, it is closed under the products and the only axioms of a Lie algebra it fails are the ones related to vectors space structure. We call this ring $\mathfrak{g}_{\mathbb{Z}}$. As an abelian group it is free with the Chevalley basis as a basis.

Using this ring we define the Lie algebra $\mathfrak{g}_{\mathbb{K}} = \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}$ over any field $\mathbb{K}$. As a vector space, it has the Chevalley basis as a basis. It has the same multiplication as the one in Chevalley basis but the coefficients are considered in $\mathbb{K}$.

We call $\mathfrak{g}_{\mathbb{K}}$ *the Chevalley reduction* of $\mathfrak{g}_{\mathbb{C}}$, which is a sensible name over the fields of positive characteristic. In zero characteristic a better name may be *the split form of* $\mathfrak{g}_{\mathbb{C}}$.

In the rest of the lecture we consider some examples but now we would like to describe the restricted structure on $\mathfrak{g}$.

Proposition 17.1 *Let $p \geq 5$. Then a restricted structure on $\mathfrak{g}_{\mathbb{K}}$ is determined by ${\mathbf{e}_\alpha}^{[p]} = 0$ and $\alpha_i^{[p]} = \alpha_i$.*

Proof: The operator L_α^p sends L_β to $L_{\beta+p\alpha}$. By Proposition 15.1, $\beta + 4\alpha$ is not a root. Hence, $L_{\beta+p\alpha} = 0$ and $L_\alpha^p = 0 = L_0$. On the other hand, $L_{\alpha^\vee}$ sends an element $\mathbf{x}$ of Chevalley basis into $n\mathbf{x}$ where n is an integer modulo p, i.e. an element of the prime subfield. Hence, it satisfies $n^p = n$ and $L_{\alpha^\vee}^p = L_{\alpha^\vee}$. We are done by Proposition 7.1. □

To describe all restricted structures we need to know the centre of $\mathfrak{g}_{\mathbb{K}}$, which we will compute in the next lecture.

17.2 $\mathfrak{sl}_2$ in characteristic 2

The Chevalley basis is the standard basis $\mathbf{e}$, $\mathbf{f}$, $\mathbf{h}$ with the products $\mathbf{e}*\mathbf{f} = \mathbf{h}$, $\mathbf{h}*\mathbf{f} = -2\mathbf{f}$, $\mathbf{h}*\mathbf{e} = 2\mathbf{e}$. The resulting Lie algebra $\mathfrak{g}_{\mathbb{K}}$ is isomorphic to $\mathfrak{sl}_2(\mathbb{K})$. It is simple unless the characteristic is 2. In characteristic 2, it is a nilpotent Lie algebra: $\mathfrak{g}^{(1)} = \mathbb{K}\mathbf{h} = Z(\mathfrak{g})$.

There is a second integral form on $\mathfrak{g}_{\mathbb{C}}$. One takes $\mathbf{r} = \mathbf{h}/2$ instead of $\mathbf{h}$. In this basis the products are $\mathbf{e} * \mathbf{f} = 2\mathbf{r}$, $\mathbf{r} * \mathbf{f} = -\mathbf{f}$, $\mathbf{r} * \mathbf{e} = \mathbf{e}$. The resulting Lie algebra $\widetilde{\mathfrak{g}}_{\mathbb{K}}$ is isomorphic to $\mathfrak{g}_{\mathbb{K}}$ if the characteristic is not two. In characteristic 2, it is a 2-soluble non-nilpotent Lie algebra: $\widetilde{\mathfrak{g}}^{(1)} = \mathbb{K}\mathbf{e} + \mathbb{K}\mathbf{f}$ and $\widetilde{\mathfrak{g}}^{(2)} = 0$ but there are non-zero products of arbitrary long length: $\mathbf{r} * (\mathbf{r} \dots (\mathbf{r} * \mathbf{e})) = \mathbf{e}$. One can think of $\widetilde{\mathfrak{g}}_{\mathbb{K}}$ as the projective special linear algebra $\mathfrak{psl}_2(\mathbb{K})$.

17.3 $\mathfrak{sl}_n$ in characteristic p

The standard choice of Cartan subalgebra is diagonal matrices $\mathfrak{h}$. The root spaces are spanned by elementary matrices $\mathbf{e}_{i,j}$ with $i \neq j$. If $\mathbf{h} \in \mathfrak{h}$ with entries h_i on the diagonal then $\mathbf{h} * \mathbf{e}_{i,j} = (h_i - h_j)\mathbf{e}_{i,j}$, so the corresponding root $\alpha_{i,j} \in \mathfrak{h}^*$ is defined by $\alpha_{i,j}(\mathbf{h}) = h_i - h_j$. The standard choice of simple roots is $\alpha_i = \alpha_{i,i+1}$, $i = 1, \dots n-1$. These root vectors give Chevalley basis and the corresponding simple coroots are $\alpha_i^\vee = \mathbf{e}_{i,i} - \mathbf{e}_{i+1,i+1}$.

If p does not divide $n+1$, the reduced Lie algebra $\mathfrak{g}_{\mathbb{K}}$ is simple. If p does divide $n+1$, the reduced Lie algebra $\mathfrak{g}_{\mathbb{K}}$ admits a central element $\sum_i i\alpha_i^\vee$. If $n > 2$ the quotient by the centre is simple and should be denoted $\mathfrak{psl}_n(\mathbb{K})$.

17.4 G_2 in characteristic 2

All Lie algebras experience some collapse of the root structure in characteristic 2. For each root $\alpha \in R$ we consider $\overline{\alpha} \in \mathfrak{h}^*_{\mathbb{K}}$. These functionals determine Cartan decomposition of $\mathfrak{g}_{\mathbb{K}}$. Since $\overline{\alpha} = \overline{-\alpha}$, the root spaces are at least 2-dimensional in characteristic 2.

For G_2, there is a further collapse: $\overline{\alpha} = \overline{-\alpha} = \overline{\alpha + 2\beta} = \overline{-\alpha - 2\beta}$, $\overline{\alpha + \beta} = \overline{-\alpha - \beta} = \overline{\alpha + 3\beta} = \overline{-\alpha - 3\beta}$ and $\overline{\beta} = \overline{-\beta} = \overline{2\alpha + 3\beta} = \overline{-2\alpha - 3\beta}$. Thus, there are three 4-dimensional root spaces. Amazingly enough, the Lie algebra $\mathfrak{g}_{\mathbb{K}}$ of type G_2 is still simple in characteristic 2.

17.5 G_2 in characteristic 3

There is a mild collapse of the root structure: $\overline{\alpha} = \overline{\alpha + 3\beta} = \overline{-2\alpha - 3\beta}$ and $\overline{-\alpha} = \overline{-\alpha - 3\beta} = \overline{2\alpha + 3\beta}$. So long root vectors join together to form two 3-dimensional root spaces. Short roots stay distinct, so short root vectors give six more 1-dimensional root spaces.

A similar accident happens with long coroots (coroots as short roots). As a result the short root vectors generate a 7-dimensional ideal in $\mathfrak{g}_{\mathbb{K}}$. Check details yourself...

17.6 Exercises

Describe the Cartan decomposition of the Lie algebra of type B_2 in characteristic 2. Is the Lie algebra simple?

Describe the dimensions of root spaces of $\mathfrak{psl}_3(\mathbb{K})$ in characteristic 3 and of $\mathfrak{psl}_4(\mathbb{K})$ in characteristic 2.

Consider $\mathfrak{g}_{\mathbb{K}}$ of type G_2 in characteristic 3. Prove that its 7-dimensional ideal I is isomorphic to $\mathfrak{psl}_3(\mathbb{K})$ as Lie algebras. Prove that the quotient algebra $\mathfrak{g}_{\mathbb{K}}/I$ is isomorphic to $\mathfrak{psl}_3(\mathbb{K})$ as Lie algebras.

18 Simplicity of Chevalley reduction

We prove simplicity of the reduced algebras $\mathfrak{g}_{\mathbb{K}}$. Throughout the lecture $\mathfrak{g}_{\mathbb{K}}$ is the reduction of a simple finite-dimensional Lie algebra $\mathfrak{g}_{\mathbb{C}}$ to the field $\mathbb{K}$ of characteristic $p > 0$.

18.1 Centres of reduced algebras

First, we would like to compute the centre of $\mathfrak{g}_{\mathbb{K}}$. The centre is an ideal, thus, the presence of non-zero centre is incompatible with simplicity. Besides, the centre makes the restricted structures non-unique.

Proposition 18.1 *The dimension of the centre of $\mathfrak{g}_{\mathbb{K}}$ is equal to either 2 (if $p = 2$ and $\mathfrak{g}$ is of type D_{2n}), or 1 (if $p = 3$ and $\mathfrak{g}$ is of type E_6, or $p = 2$ and $\mathfrak{g}$ is of type B_n or C_n or D_{2n+1} or E_6, or $p|(n+1)$ and $\mathfrak{g}$ is of type A_n) or 0 other wise.*

Proof: This is done in several steps and you should look in your lecture notes for further details of each step.

(Step 1) We observe that any central element $\mathbf{x} \in Z(\mathfrak{g}_{\mathbb{K}})$ must lie in the Cartan. Otherwise, $\mathbf{x} = a\mathbf{e}_\alpha + \ldots$ where $a \neq 0$ and the dots denote some linear combination of the remaining elements of the Chevalley basis. From "Lie Algebras", it is possible to choose a basis of the root system so that α is one of simple roots. Let β be another simple root connected to α by an edge. Notice that such β does not exist if $\mathfrak{g}$ is of type A_1 but one can use $\beta = -\alpha$ in this case.

As there is an edge $\alpha + \beta$ is a root and $\beta - \alpha$ is not a root as both are simple. Hence, $\mathbf{x} * \mathbf{e}_\beta = \pm a\mathbf{e}_{\alpha+\beta} + \ldots$, contradicting centrality of $\mathbf{x}$. In case of A_1 one gets $\mathbf{x} * \mathbf{e}_{-\alpha} = \pm a\alpha^\vee + \ldots$, arriving at the same conclusion.

(Step 2) Hence we are confined to considering linear combinations of simple coroots $\mathbf{x} = \sum_i a_i \alpha_i^\vee$. Such $\mathbf{x}$ commutes with coroots. For root vectors $\mathbf{x} * \mathbf{e}_\beta = \beta(\mathbf{x})\mathbf{e}_\beta$, so $\mathbf{x}$ is central if and only if $\alpha_i(\mathbf{x}) = \sum_j \alpha_i(\alpha_j^\vee)a_j = 0$ for each simple root α_i. This says that the matrix product $(C_{i,j})(a_j) = 0$, so the dimension of the centre is equal to the corank (nullity) of the Cartan matrix (considered as the matrix of $\mathbb{K}$).

(Step 3) To get an idea of coranks it would useful to compute determinants of Cartan matrices (over $\mathbb{Z}$). Let $x_n = \det(X_n)$ be the determinant of the Cartan matrix of type X_n, By abuse of notation X_n is a type and the Cartan matrix and the Dynkin diagram!

We derive a formula for computing determinants explicitly. Let Γ be a Dynkin diagram. Pick a vertex that is connected to a single other

vertex and the arrow is single. Let Γ_1 be the Dynkin diagram obtained by removing the former vertex, Γ_1 the Dynkin diagram obtained by removing both vertices. Expanding first the row, then the column of Dynkin diagram gives the recursive formula:

$$\det(\Gamma) = 2\det(\Gamma_1) - \det(\Gamma_2)\,.$$

(Step 4) Before we do the recursions, we precompute for ranks 1 and 2: $a_1 = 2$, $a_2 = 2\cdot 2-(-1)\cdot(-1) = 3$, $b_2 = 2\cdot 2-(-1)\cdot(-2) = 2$, $g_2 = 2\cdot 2-(-1)\cdot(-3) = 1$. In type A_n we remove the side vertex to derive that $a_n = 2a_{n-1} - a_{n-2} = 2n-(n-1) = n+1$. In type B_n we also remove the side vertex to derive that $b_3 = 2b_2 - a_1 = 2\cdot 2-2 = 2$ and $b_n = 2b_{n-1} - b_{n-2} = 2\cdot 2-2 = 2$. Cartan matrices in types B_n and C_n are related by transposition, so $c_n = b_n$. In type D_n we remove one the two (or three in type D_4) end vertices connected to the only trivalent vertex to derive that $d_n = 2a_{n-1}-a_1\cdot a_{n-3} = 2n-2(n-2) = 4$. In type E_n we remove the end vertex connected to the only trivalent vertex to derive that $e_n = 2a_{n-1}-a_2\cdot a_{n-4} = 2n-3(n-3) = 9-n$. In particular, $e_8 = 1$, $e_7 = 2$, $e_6 = 3$. Finally, $f_4 = 2b_3-a_2 = 2\cdot 2-3 = 1$.

If $x_n = 1$ this means that the corank is always zero and the Lie algebra of type X_n has no centre in any characteristic. If $x_n = p$, a prime number then the corank is zero except characteristic p where it is 1. The Lie algebra of type X_n has one dimensional centre in characteristic p and no centre, otherwise. It remains to sort composite number $a_n = n+1$ and $d_n = 4$.

(Step 5) In type A_n we observe that the elementary transformations over $\mathbb{Z}$ are also elementary transformations in any characteristic p. Thus, we can use reduction of Smith's normal over $\mathbb{Z}$ to determine the rank in characteristic p. Using the following chain of transformations recursively

$$\begin{pmatrix} \vdots & -1 & 0 & \vdots \\ \dots & 2 & -1 & 0 \\ \dots & -1 & 2 & 1-k \\ \dots & 0 & -1 & k \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots & -1 & 0 & \vdots \\ \dots & 2 & -1 & -k \\ \dots & -1 & 2 & k+1 \\ \dots & 0 & -1 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots & -1 & 0 & \vdots \\ \dots & 2 & -k & 0 \\ \dots & -1 & k+1 & 0 \\ \dots & 0 & 0 & 1 \end{pmatrix}$$

leads as to conclude that the Smith's normal of Cartan matrix of type A_n has $n+1$ and n ones on the diagonal. Hence, the centre will be one-dimensional whenever p divides $n+1$.

(Step 6) In type D_n we have to understand what happens in characteristic 2 as the Smith's normal form could have either $(4,1,\dots)$ or $(2,2,1,\dots)$

on the diagonal. Consider the Cartan matrix $(\overline{C_{j,i}})$ reduced to characteristic 2 with the last two columns corresponding to the two vertices connected to the trivalent vertex. This makes the last two rows and the last two columns equal. Hence, the rank of $(\overline{C_{j,i}})$ is the same as the rank of its $(n-1)\times(n-1)$-minor obtained deleting n-th row and column. The minor is Cartan's matrix of type A_{n-1} which, by step 5, has rank $n-2$ if n is even and $n-1$ if n is odd.

□

18.2 Root structure collapse

Proposition 18.2 *Let $p \geq 5$ and $(n+1)$ not divisible by p if $\mathfrak{g}$ is of type A_n. For any root $\alpha \neq \beta \in R$ the root space $\mathfrak{g}_{\overline{\alpha}} \subseteq \mathfrak{g}_{\mathbb{K}}$ is one dimensional.*

PROOF: It suffices to show that for any two distinct root $\alpha \neq \beta \in R$ their restrictions $\overline{\alpha}$, $\overline{\beta} \in \mathfrak{h}^*$ are distinct. Because of the restriction on p, $\mathfrak{g}$ has no centre and simple roots form a basis of the dual space $\mathfrak{h}^*$. Because of this, the proposition becomes a "local" question, i.e., a question about the rank 2 root system $(\mathbb{Z}\alpha+\mathbb{Z}\beta)\cap R$. If Λ is the root lattice, we would like to know whether it is possible that $\alpha-\beta \in p\Lambda$. Going over all roots in the rank 2 systems $A_1\times A_1$, A_2, B_2, G_2 shows that it is impossible. □

Notice that the columns of Cartan matrix are coordinates of simple roots in the basis of fundamental weights. It follows that the cokernel of Cartan's matrix, which we essentially computed, is the quotient Φ/Λ of the weight lattice by the root lattice. This group has further significance: it is isomorphic to the centre of the corresponding simply-connected group G_{sc} and the fundamental group of the corresponding adjoint group G_{ad}.

18.3 Simplicity

Theorem 18.3 *Let $p \geq 5$ and $(n+1)$ not divisible by p if $\mathfrak{g}$ is of type A_n. Then the reduced Lie algebra $\mathfrak{g}_{\mathbb{K}}$ is simple.*

PROOF: By Proposition 18.1, the centre of $\mathfrak{g}_{\mathbb{K}}$ is zero. By Proposition 18.2, all root spaces $\mathfrak{g}_\alpha$ in the Cartan decomposition of $\mathfrak{g}_{\mathbb{K}}$ are one-dimensional.

We consider a nonzero ideal $I \trianglelefteq \mathfrak{g}_{\mathbb{K}}$. Let $I_\alpha = I \cap \mathfrak{g}_\alpha$. First, we observe that $I = \oplus_\alpha I_\alpha$. Pick arbitrary $\mathbf{x} = \sum_\alpha \mathbf{x}_\alpha \in I$ where $\mathbf{x}_\alpha \in \mathfrak{g}_\alpha$. It suffices to prove that all $\mathbf{x}_\alpha \in I$. We use Vandermonde trick. Pick $\mathbf{h}_i \in \mathfrak{h}$ so that $\alpha_j(\mathbf{h}_i) = \delta_{j,i}$. In characteristic zero, these are fundamental weights but we have to argue why these exist in characteristic p: conditions on p ensure that simple roots $\overline{\alpha_i} \in \mathfrak{h}^*$ form a basis, hence $\mathbf{h}_i$ is just the dual basis. Now $\mathbf{h}_i * \mathbf{x} = \sum_\alpha \alpha(\mathbf{h}_i)\mathbf{x}_\alpha \in I$. Repeating this k times,

$$L^k_{\mathbf{h}_i}(\mathbf{x}) = \sum_\alpha \alpha(\mathbf{h}_i)^k \mathbf{x}_\alpha \in I\,.$$

By Vandermonde trick,

$$\sum_{\alpha,\, \mathbf{h}_i(\alpha)=m} \mathbf{x}_\alpha \in I$$

for all m. Repeating this for all i we conclude that all $\mathbf{x}_\alpha$ are in I and $I = \oplus_\alpha I_\alpha$.

If $I_0 \neq 0$, pick $\mathbf{h} \in I_0$. Since the centre is zero, there exists a root α such that $\overline{\alpha}(\mathbf{h}) \neq 0 \in \mathbb{K}$. Hence, $\mathbf{e}_\alpha = \overline{\alpha}(\mathbf{h})^{-1}\mathbf{h} * \mathbf{e}_\alpha \in I$ and $I_\alpha \neq 0$. Even if $I_0 = 0$, there exist α with $I_\alpha \neq 0$ since $I \neq 0$. By proposition 15.1, whenever $\alpha+\beta$ is a root and $\mathbf{e}_\alpha * \mathbf{e}_\beta = c_{\alpha,\beta}\mathbf{e}_{\alpha+\beta} \in \mathfrak{g}_\mathbb{C}$, the coefficient satisfies $1 \leq |c_{\alpha,\beta}| \leq 4 < p$, so it is non-zero in $\mathbb{K}$. As the root system is irreducible, we conclude that all $\mathbf{e}_\alpha$ are in I. Finally, all $\alpha^\vee = \mathbf{e}_\alpha * \mathbf{e}_{-\alpha}$ are in I too and $I = \mathfrak{g}_\mathbb{K}$. □

18.4 Exercises

Write the Cartan matrix of type A_n in characteristic 2 and prove directly what its rank is.

Write a non-zero central element of $\mathfrak{g}_\mathbb{K}$ explicitly when $\mathfrak{g}_\mathbb{K}$ is of type F_4 and the characteristic of $\mathbb{K}$ is 2.

Write a non-zero central element of $\mathfrak{g}_\mathbb{K}$ explicitly when $\mathfrak{g}_\mathbb{K}$ is of type E_6 and the characteristic of $\mathbb{K}$ is 3.

19 Chevalley groups

We associate a group, called Chevalley group, to the reduced Lie algebra $\mathfrak{g}_{\mathbb{K}}$. If the field $\mathbb{K}$ is finite, this is a finite simple group.

19.1 Exponentials

Let $\mathfrak{g}_{\mathbb{C}}$ be a simple finite-dimensional Lie algebra, $\mathfrak{g}_{\mathbb{Z}}$ its Lie subring spanned over $\mathbb{Z}$ by Chevalley basis. We would like to extend scalars to the polynomial ring $\mathbb{Z}[t]$ by considering $\mathfrak{g}_{\mathbb{Z}[t]} = \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[t]$. In an elementary language, $\mathfrak{g}_{\mathbb{Z}[t]}$ is a free abelian group with basis $t^n\mathbf{x}$, $n \in \mathbb{Z}_{\geq 0}$, $\mathbf{x}$ an element of Chevalley basis. The product is $\mathbb{Z}$-bilinear and defined on the basis by $t^n\mathbf{x} * t^m\mathbf{x} = t^{n+m}(\mathbf{x} * \mathbf{y})$.

In fact, the product $\mathfrak{g}_{\mathbb{Z}[t]}$ is $\mathbb{Z}[t]$-bilinear turning $\mathfrak{g}_{\mathbb{Z}[t]}$ into a Lie algebra over the ring $\mathbb{Z}[t]$. We would like to define exponential

$$X_\alpha(t) = e^{t\mathbf{e}_\alpha} = \sum_n^\infty \frac{t^n}{n!} L^n_{\mathbf{e}_\alpha}$$

to be a $\mathbb{Z}[t]$-linear map from $\mathfrak{g}_{\mathbb{Z}[t]}$ to itself. The most urgent question why is it well-defined?

Proposition 19.1 *For each root $X_\alpha(t)$ a well-defined $\mathbb{Z}[t]$-linear Lie algebra automorphism of $\mathfrak{g}_{\mathbb{Z}[t]}$.*

Proof: To see that $X_\alpha(t)$ is well-defined, we will derive explicit formulas for its action on Chevalley basis. First of all, since 2α is not a root

$$X_\alpha(t)(\mathbf{e}_\alpha) = \mathbf{e}_\alpha,\ X_\alpha(t)(\beta^\vee) = \beta^\vee - \beta^\vee(\alpha)t\mathbf{e}_\alpha,\ X_\alpha(t)(\mathbf{e}_{-\alpha}) = \mathbf{e}_{-\alpha} + t\alpha^\vee - t^2\mathbf{e}_\alpha\,.$$

If $\beta \neq \pm\alpha$ is another root then we need the α-series via β: $\beta + \mathbb{Z}\alpha \cap R = \{\beta - r\alpha, \beta - (r-1)\alpha, \ldots, \beta + q\alpha\}$. Since $\beta + 4\alpha$ is not a root,

$$X_\alpha(t)(\mathbf{e}_\beta) = \mathbf{e}_\beta \pm (r+1)t\mathbf{e}_{\alpha+\beta} \pm \frac{(r+1)(r+2)}{2}t^2\mathbf{e}_{2\alpha+\beta} \pm \frac{(r+1)(r+2)(r+3)}{6}t^3\mathbf{e}_{3\alpha+\beta}\,.$$

Clearly, $X_\alpha(t)$ is a $\mathbb{Z}[t]$-linear map and its inverse is $X_\alpha(t)$. It is an automorphism because $L_{\mathbf{e}_\alpha}$ is a derivation, similarly to exercises to Lecture 1. □

19.2 Specialized exponentials and Chevalley groups

Now consider the reduced algebra $\mathfrak{g}_{\mathbb{K}}$. For each root α and each $s \in \mathbb{K}$ we get a Lie algebra automorphism $X_\alpha(s)$ of $\mathfrak{g}_{\mathbb{K}}$ by specialising $X_\alpha(t)$. In a high-tech language, we choose a ring homomorphism $\mathbb{Z}[t] \to \mathbb{K}$ by sending t to s and define $X_\alpha(s) = X_\alpha(t) \otimes I$, an automorphism of $\mathfrak{g}_{\mathbb{Z}[t]} \otimes_{\mathbb{Z}[t]} \mathbb{K} =$

$(\mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[t]) \otimes_{\mathbb{Z}[t]} \mathbb{K} \cong \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}[t] \otimes_{\mathbb{Z}[t]} \mathbb{K}) \cong \mathfrak{g}_{\mathbb{K}}$, with the two natural isomorphisms. In an elementary language, we define $X_\alpha(s)$ by formulas in Proposition 19.1 with substituting s for t.

The Chevalley group $G(\mathfrak{g}, \mathbb{K})$ is defined to be the subgroup of $\mathrm{GL}(\mathfrak{g}_{\mathbb{K}})$ generated by all $X_\alpha(s)$ for all roots α and $s \in \mathbb{K}$. It is unfortunate that we had to make several choice to arrive at this group. How justifiable is the notation $G(\mathfrak{g}, \mathbb{K})$? Don't we have to add all the choices we have made to the list of arguments?

Proposition 19.2 *A different set of choices leads to isomorphic reduced algebra* $\mathfrak{g}_{\mathbb{K}}$ *and Chevalley group* $G(\mathfrak{g}, \mathbb{K})$.

Proof: We have made three choices in the process of construction:

(i) Cartan subalgebra $\mathfrak{h}$,
(ii) simple roots $\alpha_1, \dots \alpha_n$,
(iii) root vectors $\mathbf{e}_\alpha$ in the Chevalley basis.

Choice (i) is up to conjugation. Any two Cartan subalgebras $\mathfrak{h}$, $\mathfrak{h}'$ of $\mathfrak{g}_{\mathbb{C}}$ can be moved one to another by non-unique element of the adjoint group (from Lie algebras). Two different choices (ii) (of simple roots) are related by a canonical element of the Weyl group. Choice (iii) of root vectors is just up to sign (one can replace some $\mathbf{e}_\alpha$ with $-\mathbf{e}_\alpha$) as we saw in the proof of Theorem 16.1.

In fact choices (ii) and (iii) do not change the Lie ring $\mathfrak{g}_{\mathbb{Z}}$ but may change $X_\alpha(s)$ into $X_\alpha(-s)$ but both elements are among generators of the Chevalley group anyway. Hence, the Lie algebra $\mathfrak{g}_{\mathbb{K}}$ and the Chevalley group $G(\mathfrak{g}, \mathbb{K})$ are the same if one makes different choices (ii) and (iii).

Different choice in (i) will lead to isomorphic $\mathfrak{g}_{\mathbb{K}}$ and $G(\mathfrak{g}, \mathbb{K})$ but there is no canonical isomorphism. □

19.3 Exercises

Prove that $X_\alpha(s)X_\alpha(s') = X_\alpha(s + s')$.

20 Abstract Chevalley groups

20.1 Definition

Let $(\mathfrak{g}, \gamma)$ be a restricted Lie algebra over a field $\mathbb{K}$ of characteristic p, V its restricted representation. For all purposes, it is sufficient to consider finite-dimensional V only.

The restricted representation gives a homomorphism of restricted Lie algebras $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$. This means that $\rho(\gamma(\mathbf{x})) = \rho(\mathbf{x})^p$, i.e, $\mathfrak{gl}(V)$ carries its canonical restricted structure.

Let $N(\mathfrak{g})$ be the set of all $\mathbf{x} \in \mathfrak{g}$ such that $\gamma(\mathbf{x}) = 0$. We call this set the p-nilpotent cone of $\mathfrak{g}$. For each $\mathbf{x} \in N(\mathfrak{g})$ we can define an exponential

$$e^{\rho(\mathbf{x})} = \sum_{k=0}^{p-1} \frac{1}{k!} \rho(\mathbf{x})^k \in \mathfrak{gl}(V) \ .$$

Moreover, $e^{\rho(\mathbf{x})} \in \mathrm{GL}(V)$ because $(e^{\rho(\mathbf{x})})^{-1} = e^{\rho(-\mathbf{x})}$. We define *an abstract Chevalley group* $G(\mathfrak{g}, V)$ as the subgroup of $\mathrm{GL}(V)$ generated by all exponentials $e^{\rho(\mathbf{x})}$ for all $\mathbf{x} \in N(\mathfrak{g})$. If one consider adjoint representation then, barring accidents in small characteristic, say $p \geq 5$, one arrives at the usual Chevalley group. Only one inclusion is obvious but we will not prove the opposite inclusion here.

Proposition 20.1 *If ρ is a restricted representation of a restricted Lie algebra $\mathfrak{g}$ then*

$$\rho(e^{L_{\mathbf{x}}}(\mathbf{y})) = e^{\rho(\mathbf{x})} \rho(\mathbf{y}) e^{-\rho(\mathbf{x})}$$

for all $\mathbf{x} \in N(\mathfrak{g})$, $\mathbf{y} \in \mathfrak{g}$.

Proof: First, observe by induction that for each $k = 1, 2, \ldots p-1$

$$\rho(\frac{1}{k!} L_{\mathbf{x}}^k(\mathbf{y})) = \sum_{j=0}^{k} \frac{(-1)^j}{(k-j)!j!} \rho(\mathbf{x})^{k-j} \rho(\mathbf{y}) \rho(\mathbf{x})^j \ .$$

For $k = 1$ it is just the definition of a representation: $\rho(L_{\mathbf{x}}(\mathbf{y})) = \rho(\mathbf{x} * \mathbf{y}) = \rho(\mathbf{x})\rho(\mathbf{y}) - \rho(\mathbf{y})\rho(\mathbf{x})$. Going from k to $k+1$, $\rho(\frac{1}{(k+1)!} L_{\mathbf{x}}^{k+1}(\mathbf{y})) = \frac{1}{k+1}(\rho(\mathbf{x})\rho(\frac{1}{k!} L_{\mathbf{x}}^k(\mathbf{y})) - \rho(\frac{1}{k!} L_{\mathbf{x}}^k(\mathbf{y})\rho(\mathbf{x})) = \sum_{j=0}^{k} \frac{(-1)^j}{k+1}(\frac{1}{(k-j)!j!} \rho(\mathbf{x})^{k-j+1} \rho(\mathbf{y}) \rho(\mathbf{x})^j - \frac{1}{(k-j)!j!} \rho(\mathbf{x})^{k-j} \rho(\mathbf{y}) \rho(\mathbf{x})^{j+1} = \sum_{i=0}^{k+1} \frac{(-1)^i}{(k+1)(k-i)!(i-1)!}(\frac{1}{i} + \frac{1}{k+1-i}) \rho(\mathbf{x})^{k+1-i} \rho(\mathbf{y}) \rho(\mathbf{x})^i = \sum_{i=0}^{k+1} \frac{(-1)^i}{(k+1-i)!i!} \rho(\mathbf{x})^{k+1-i} \rho(\mathbf{y}) \rho(\mathbf{x})^i$.

Finally, $\rho(e^{L_{\mathbf{x}}(\mathbf{y})}) = \sum_{k=0}^{p-1} \rho(\frac{1}{k!} L_{\mathbf{x}}^k(\mathbf{y})) = \sum_{i,j=0}^{p-1} \frac{(-1)^j}{i!j!} \rho(\mathbf{x})^i \rho(\mathbf{y}) \rho(\mathbf{x})^j = e^{\rho(\mathbf{x})} \rho(\mathbf{y}) e^{-\rho(\mathbf{x})}$. □

20.2 Examples

Let us consider $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{K})$ and its natural representation $\rho : \mathfrak{g} \to \mathfrak{gl}_2(\mathbb{K})$. For each $\mathbf{x} \in N(\mathfrak{sl}_2)$ we have $\mathbf{x}^2 = 0$ in $\mathfrak{gl}_2$ which implies that

$$e^{\rho(\mathbf{x})} = I + \mathbf{x} \text{ , in particular } e^{t\mathbf{e}} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \ e^{t\mathbf{f}} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Since these matrices generate $\mathrm{SL}_2(\mathbb{K})$ (see the exercise), we can use Proposition 20.1 to derive a surjective homomorphism $\phi : \mathrm{SL}_2(\mathbb{K}) \to G(\mathfrak{g}, \mathbb{K})$. Indeed, we define $\phi(e^{\rho(\mathbf{x})}) = e^{L_{\mathbf{x}}}$ on generators. Whenever, there is a relation in $\mathrm{SL}_2(\mathbb{K})$, say

$$e^{\rho(\mathbf{x}_1)} e^{\rho(\mathbf{x}_2)}) \dots e^{\rho(\mathbf{x}_n)} = I \ ,$$

using Proposition 20.1, we conclude that

$$\rho(e^{L_{\mathbf{x}_1}} e^{L_{\mathbf{x}}} \dots e^{L_{\mathbf{x}_n}}(\mathbf{y})) = \rho(\mathbf{y})$$

for all $\mathbf{y}$. Since ρ is injective it follows that that

$$e^{L_{\mathbf{x}_1}} e^{L_{\mathbf{x}}} \dots e^{L_{\mathbf{x}_n}} = I$$

and the homomorphism ρ is well-defined. It remains to figure out the kernel of ϕ. Again using Proposition 20.1, $\phi(A)(\mathbf{y}) = A\mathbf{y}A^{-1}$ and the kernel consists of scalar matrices. It follows that $G(\mathfrak{g}, \mathbb{K})$ is isomorphic to $\mathrm{P}SL_2(\mathbb{K})$.

I believe Witt was originally interested in finding new finite simple groups using other simple Lie algebras. It was a disappointment. For instance, $G(W(1,1), W(1,1))$ is soluble.

20.3 Exercises

Prove that matrices $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ for all $t \in \mathbb{K}$ generate $\mathrm{SL}_2(\mathbb{K})$.

21 Engel Lie algebras

21.1 Engel Theorem

Let us consider the following two elements of the free Lie algebra:

$$\mathcal{N}_2(x,y) = \mathcal{E}_1(x,y) = x * y \ ,$$

$$\mathcal{N}_{n+1}(x_1, \dots x_n, y) = x_1 * \mathcal{N}_n(x_2, \dots x_n, y) = L_{x_1} L_{x_2} \dots L_{x_n}(y) \ ,$$

$$\mathcal{E}_n(x,y) = x * \mathcal{E}_{n-1}(x,y) = L_x^n(y)$$

A Lie algebra is called *n-Engel* if it satisfies $\mathcal{E}_n$. It is called *Engel* if it is n-Engel for some n. A Lie algebra is called *n-nilpotent* if it satisfies $\mathcal{N}_n$. It is *nilpotent* if it is n-nilpotent for some n.

Theorem 21.1 *A finitely generated Engel Lie algebra is nilpotent.*

For finite-dimensional Lie algebras it is classical Engel's theorem. It is usually formulated for *ad*-nilpotent Lie algebra, i.e. such Lie algebras where each $L_{\mathbf{x}}$ is nilpotent. But clearly then $L_{\mathbf{x}}^n = 0$ where n is the dimension of the Lie algebra, i.e., it satisfies $\mathcal{E}_n$.

Let us observe what happens for small n. Since $\mathcal{N}_2(x,y) = \mathcal{E}_1(x,y) = x * y$, 1-Engel Lie algebras are the same as 2-nilpotent ones.

Let us look at the free 2-Engel algebra $\mathfrak{g} = L(X)/(\mathcal{N}_2)_w$. For every $\mathbf{x}, \mathbf{y} \in \mathfrak{g}$, we can see that $0 = L^2_{\mathbf{x}+\mathbf{y}} - L^2_{\mathbf{x}} - L^2_{\mathbf{y}} = L_{\mathbf{x}} L_{\mathbf{y}} + L_{\mathbf{y}} L_{\mathbf{x}}$. On the other hand, $(L_{\mathbf{x}} L_{\mathbf{y}} - 2L_{\mathbf{y}} L_{\mathbf{x}})(\mathbf{z}) = \mathbf{x} * (\mathbf{y} * \mathbf{z}) - 2\mathbf{y} * (\mathbf{x} * \mathbf{z}) = (\mathbf{x} * \mathbf{y}) * \mathbf{z} - \mathbf{y} * (\mathbf{x} * \mathbf{z}) = (L_{\mathbf{z}} L_{\mathbf{y}} + L_{\mathbf{y}} L_{\mathbf{z}})(\mathbf{x}) = 0$. We conclude that $3L_{\mathbf{y}} L_{\mathbf{x}} =$ and $\mathfrak{g}$ is 3-nilpotent unless $p = 3$. If $p = 3$ then further analysis along the same line reveals that $\mathfrak{g}$ (and consequently any 2-Engel Lie algebra) is 4-nilpotent.

So far we have never used the fact that the Lie algebra is finitely generated. It starts playing a role in 3-Engel algebras. Let $\mathfrak{g} = L(X)/(\mathcal{N}_3)_w$ be the free 3-Engel algebra. If $p \neq 5$ then it is 7-nilpotent. However, if $p = 5$ then it is $(2|X|+1)$-nilpotent and finite generation is crucial: if X is infinite, $\mathfrak{g}$ is no longer nilpotent. nevertheless, it is known that in characteristic zero, any Engel Lie algebra is nilpotent.

21.2 Linearized Engel identity

The identity $\mathcal{E}_n(\mathbf{x}, \mathbf{y})$ has degree n in x. In particular, it is not linear if $n > 1$. However, one can polarise it to derive a linear identity. Consider the following polynomial in the free Lie algebra:

$$\mathcal{LE}_n(\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_n, \mathbf{y}) = \sum_{\sigma \in S_n} \mathcal{N}_n(\mathbf{x}_{\sigma(1)}, \dots \mathbf{x}_{\sigma(n)}, \mathbf{y})$$

The identity $\mathcal{LE}_n$ is called linearised n-Engel identity.

Proposition 21.2 *An n-Engel Lie algebra $\mathfrak{g}$ satisfies $\mathcal{LE}_n$. In the opposite direction, if $\mathfrak{g}$ is a Lie algebra satisfying $\mathcal{LE}_n$ and the ground field has either characteristic 0 or $p > n$ then $\mathfrak{g}$ is n-Engel.*

PROOF: The second statement is obvious: $\mathcal{LE}_n(\mathbf{x}, \mathbf{x}, \dots \mathbf{x}, \mathbf{y}) = n!\mathcal{E}_n(\mathbf{x}, \mathbf{y})$ and the condition on characteristic allows us to divide by $n!$ in the field $\mathbb{K}$.

For the first statement, rewrite $\mathcal{E}_n(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + a_n\mathbf{x}_n, \mathbf{y}) = Q_0 + a_1Q_1 + a_1a_2Q_2 + \ldots + a_1a_2 \ldots a_n\mathbb{Q}_n$ in the free Lie algebra $\mathbb{K}[a_1, \dots a_n](\mathbf{x}_1, \dots \mathbf{x}_n)$ over the polynomial ring $\mathbb{K}[a_1, \dots a_n]$. The Lie polynomial $a_1a_2 \dots a_s\mathbb{Q}_s$ is a combination of all the terms divisible by a_1, a_2 $\dots a_s$ but not by a_{s+1}. Plugging concrete values from $\mathbb{K}$ for all a_s gives us an identity of an n-Engel Lie algebra over $\mathbb{K}$. Plug $a_1 = 0$. Hence, Q_0 is an identity. Now plug $a_1 = 1$ and $a_2 = 0$. Hence, both $Q_0 + Q_1$ and Q_1 are identities. Repeating this argument n times, we derive that all Q_i are identities of an n-Engel Lie algebra.

Notice that Q_i may still depend on a_j, $j > i$. These identities Q_i are (partial) linearisations (or polarisations) of $\mathcal{E}_n$. Observe, that $Q_n = \mathcal{LE}_n$, which is called *the full linearisation.* □

21.3 Properties of group commutators

A commutator of two elements in a group is $[x, y] = x^{-1}y^{-1}xy$. We denote $x^y = y^{-1}xy$ and $x^{-y} = y^{-1}x^{-1}y$. We will write x^* and x^{-*} for x^y and x^{-y} if we are to lazy to specify y. If H and F are subgroups then $[H, F]$ is the subgroup generated by all commutators.

Using commutators a group starts looking a bit like Lie algebra. Identities in the next proposition look like anti-commutativity, distributivity and Jacobi identity.

Proposition 21.3 *The following commutator identities hold in any group:*

(i) $[x, y]^{-1} = [y, x]$,
(ii) $[x, yz] = [x, z][x, y]^z$,
(iii) $[[x, y]z^x][[z, x]y^z][[y, z]x^y] = 1$,
(iv) $[[x, y^{-1}]z]^y[[y, z^{-1}]x]^z[[z, x^{-1}]y]^x = 1$.

PROOF: We check only identity (iii) (call The Hall identity). We keep brackets around what is left of the commutators: $[[x, y]z^x][[z, x]y^z][[y, z]x^y] =$
$[y, x]z^{-x}[x, y]z^x[x, z]y^{-z}[z, x]y^z[z, y]x^{-y}[y, z]x^y =$
$(y^{-1}x^{-1}y)z^{-1}(y^{-1}xy)x^{-1}z(z^{-1}x)y^{-1}(x^{-1}zx)z^{-1}y(y^{-1}z)x^{-1}(z^{-1}yz)y^{-1}xy =$
$(y^{-1}x^{-1}y)z^{-1}(y^{-1}xy)y^{-1}(x^{-1}zx)x^{-1}(z^{-1}yz)y^{-1}xy =$
$(y^{-1}x^{-1}y)z^{-1}(y^{-1}x)(x^{-1})(yz)y^{-1}xy = (y^{-1}x^{-1}y)y^{-1}xy = 1.$ □

21.4 Exercises

Prove all the identities in Proposition 21.3.

Linearise the elasticity identity $(xy)x = x(yx)$ in the free algebra. Show that if the characteristic is not two, the elastic algebras are the same as linearised elastic algebras.

22 Lie algebra associated to a group

22.1 Lie algebra associated to a strongly central series in a group

Let G be a group, $G = G_1 \trianglerighteq G_2 \trianglerighteq \dots G_n \dots$ a descending chain of normal subgroups, i.e., each G_n is normal in G. It is called *a central series* if G_{n-1}/G_n is in the centre of G/G_n for each n. It is called *a strongly central series* if $[G_n, G_m] \subseteq G_{n+m}$ for all n and m. Observe that each strongly central series is central since the centrality is equivalent to $[G_n, G] \subseteq G_{n+1}$ for all n. The opposite is false: not every central series is strongly central. My lack of group theory background doesn't let me give you an example of the top of my head but, in general, there is no reason for the upper central series of a nilpotent group to be strongly central. On the other hand, lower central series of G is strongly central. We discuss a slight generalisation of this in the next section.

To each central series we can associate a (graded) Lie ring. As an abelian group, $L(G, G_n) = \oplus_{n=1}^{\infty} G_{n-1}/G_n$. The Lie product on this group is defined using group commutator $[x, y] = x^{-1}y^{-1}xy$ via

$$xG_{n+1} * yG_{m+1} = [x, y]G_{n+m+1} \ , x \in G_n \ , y \in G_m \ .$$

Theorem 22.1 *If G_n is a strongly central series then $L(G, G_n)$ is a Lie ring. If there exists a prime p such that each G_{n-1}/G_n is an elementary abelian p-group then $L(G, G_n)$ is a Lie algebra over the field of p elements.*

Proof: Since each G_n/G_{n+1} is an abelian group then their direct sum $L(G, G_n)$ is also an abelian group.

Let us see that the product is well-defined. If $x \in G_n$, $y \in G_m$ then their commutator $[x, y]$ belongs to G_{n+m}. The product needs to be independent of the representatives of the cosets. Pick $z \in G_{m+1}$, so that $yG_{m+1} = yzG_{m+1}$. Then $[x, yz]G_{n+m+1} = [x, z][x, y]^z G_{n+m+1} = [x, y]^z G_{n+m+1}$ since $[x, z] \in G_{n+m+1}$ and G_{n+m+1} is normal. Finally, $[x, y]^z G_{n+m+1} = [x, y]G_{n+m+1}$ because $[x, y]G_{n+m+1}$ is in the centre of G/G_{n+m+1}, hence commutes with zG_{n+m+1}.

Let us see that the product is bilinear. Pick $x \in G_n$, $y \in G_m$, $z \in G_k$. If $m \neq k$ then $xG_{n+1} * (yG_{m+1} - zG_{k+1}) = (xG_{n+1} * yG_{m+1}) - (xG_{n+1} * zG_{k+1})$ by definition of the product. If $m = k$ then the left hand side is $[x, yz^{-1}]G_{n+m+1} = [x, z^{-1}][x, y]^{z^{-1}} G_{n+m+1} = [x, y]G_{n+m+1}[x, z^{-1}]G_{n+m+1}$ equal to the right hand side. Here again, we used the fact that $[x, y]G_{n+m+1}$ is central in G/G_{n+m+1}. Similarly, $(xG_{n+1} - yG_{m+1}) * zG_{k+1} = (xG_{n+1} * zG_{k+1}) - (yG_{m+1} * zG_{k+1})$.

Let us see observe anticommutativity. A general element $\mathbf{e}$ is a Z-linear combinations of various cosets xG_n. For the cosets $xG_{n+1} * xG_{n+1} = [x,x]G_{2n+1} = 0$ and $xG_{n+1} * yG_{m+1} = [x,y]G_{n+m+1} = [y,x]^{-1}G_{n+m+1} = yG_{m+1} * xG_{n+1}$. It follows that $\mathbf{e} * \mathbf{e} = 0$.

Finally, the Jacobi identity can be checked on homogeneous elements (cosets). From the Hall identity, $[[x,y^{-1}]z]^y G_{n+m+k+2} + [[y,z^{-1}]x]^z G_{n+m+k+2} + [[z,x^{-1}]y]^x G_{n+m+k+2} = 0$. Using the centrality trick, $[[x,y^{-1}]z]^y G_{n+m+k+2} = [[x,y^{-1}]z]G_{n+m+k+2} = -[[x,y]z]G_{n+m+k+2}$. □

22.2 Lower central m-series

Let $m \in \mathbb{Z}_{\geq 0}$. We define G_n recursively. The definition depends on m, which is not reflected in the notation but we find alternatives such as $G_{n,m}$ or $G_n(m)$ too cumbersome. We set $G_1 = G$. Recursively, G_{n+1} is the subgroup of G generated by all $[x,y]$ and y^m for all $x \in G$, $y \in G_n$.

Proposition 22.2 *For each m, the series G_n is strongly normal.*

PROOF: First observe inductively that G_n is normal. Clearly, $G = G_1$ is normal. Let G_n be normal. Since $[x,y]^z = [x^z, y^z]$ and $(y^m)^z = (y^z)^m$ for all $x, z \in G$, $y \in G_n$, the next subgroup G_{n+1} is normal too.

Now we prove that $[G_n, G_k] \subseteq G_{n+k}$ by induction on minimum of n and k. By the definition of G_{n+1} it contains $[G_n, G]$. Now we assume that $n \geq k$ and that we have proved $[G_n, G_{k-1}] \subseteq G_{n+k-1}$. Now G_k is generated by two types of elements and it is sufficient to check that $[x,[y,z]]$ and $[x,y^m]$ belong to G_{n+k} for all $x \in G_n$, $y \in G_{k-1}$, $z \in G$.

For the first element, $[x,[y,z]] = [[x^*,y]z^*][[z,x^*]y^*]$, thanks to part (iii) of Proposition 21.3. Since all the subgroup are normal, $x^* \in G_n$, $y^* \in G_{k-1}$. Then $[[x^*,y]z^*] \in [G_{n+k-1}, G_1] \subseteq G_{n+k}$ and $[[z,x^*]y^*] \in [G_{n+1}, G_{k-1}] \subseteq G_{n+k}$ by the induction assumptions.

For the second element, $[x,y^m] = [x,y][x,y]^* \dots [x,y]^*$ with m commutators on the right, thanks to part (ii) of Proposition 21.3. Since $[x,y] \in G_{n+k-1}$ and G_{n+k-1}/G_{n+k} is central in G/G_{n+k} we conclude that on the level of cosets $[x,y]^* G_{n+k} = [x,y]G_{n+k}$. Hence, $[x,y^m]G_{n+k} = ([x,y]G_{n+k})^m = [x,y]^m G_{n+k} = G_{n+k}$ since G_{n+k} contains m-th powers. Hence $[x,y^m] \in G_{n+k}$. □

We write $L_m(G) = L(G, G_n)$ where G_n is the lower central m-series. Some values of m are more useful then the others. $L_1(G)$ is always zero and quite useless. $L_0(G)$ is the Lie ring of the group G but may not be a Lie algebra. $L_p(G)$ is a Lie algebra over the field of p elements and is particularly useful.

Let us consider three concrete examples. As the first example, $G = D_{2n} =< a, b | a^n = b^2 = 1\ , a^b = a^{-1} >$ is the dihedral group of order $2n$ where $n = 2^s m$ for odd m. Working out the central 0-series, the commutator subgroup is $G_2 =< a^2 >$, and, in general, $G_t =< a^{2^{t-1}} >$. Hence, starting from $s+1$, $G_{s+1} = G_{s+2} = \ldots =< a^m >$. The elements $\mathbf{b} = bG_2$, $\mathbf{a}_i = a^{2^{i-1}} G_{i+1}$, $1 \leq i \leq s$ form a basis $L_0(D_{2n})$ over the field of two elements. It follows that $L_0(D_{2n}) = L_2(D_{2n})$. The products of the basis elements are $\mathbf{b} * \mathbf{a}_i = \mathbf{a}_{i+1}$ and $\mathbf{b} * \mathbf{a}_s = \mathbf{a}_i * \mathbf{a}_j = 0$.

As the second example, we consider one of two non-abelian groups of order p^3, p is prime, the extraspecial group $C_p^2 \leftthreetimes C_p$. The normal subgroup is a vector space over $\mathbb{F}_p$. The generator of the second group acts via matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ that has order p in characteristic p. In generators and relations, $G =< x, y, z | x^p = y^p = z^p = 1, y^z = yx, xy = yx, x^z = x >$ Its 0-series is $G_2 =< x >$ and $G_3 = \{1\}$. The elements $\mathbf{y} = yG_2$, $\mathbf{z} = zG_2$ and $\mathbf{x} = xG_3$ form a basis of $L_0(G) = L_p(G)$ over $\mathbb{F}_p$. The Lie structure is given by $\mathbf{y} * \mathbf{z} = \mathbf{x}$, $\mathbf{x} * \mathbf{z} = \mathbf{x} * \mathbf{y} = 0$. Thus, $L_0(G)$ is the Heisenberg Lie algebra over $\mathbb{F}_p$.

As the final example, we consider the modular group $G = C_{p^2} \leftthreetimes C_p$. In generators and relations, $G =< y, z | y^{p^2} = z^p = 1, y^z = y^{p+1} >$. Notice that $(p+1)^p \equiv 1 \text{ modulo } p^2$. Again $G_2 =< y^p >$, $G_3 = \{1\}$ and $\mathbf{y} = yG_2$, $\mathbf{z} = zG_2$ and $\mathbf{x} = y^p G_3$ form a basis of $L_0(G) = L_p(G)$ over $\mathbb{F}_p$. The Lie structure is the same as for the extraspecial group: $\mathbf{y} * \mathbf{z} = \mathbf{x}$, $\mathbf{x} * \mathbf{z} = \mathbf{x} * \mathbf{y} = 0$.

22.3 Exercises

Prove that each strongly central series is central.

Prove that the intersection of finitely many subgroups of finite index has finite index too.

Use this to prove that a subgroup of finite index contains a normal subgroup of finite index.

Prove that every finite p-group is nilpotent.