Theorems of Levi and Ado-Iwasawa

Swayam Chube

December 1, 2024

Abstract

In this article, we (attempt to) present a self-contained proof of the Ado-Iwasawa theorem. The exposition closely follows [Jac79], a copy of which was kindly lent to me by Prof. Jugal Verma.

Throughout this article, k denotes a field and all Lie algebras are taken over k unless specified otherwise.

§1 Preliminaries

Most of this section is taken from [FH91].

Lemma 1.1. Let $\operatorname{char} k = 0$ and $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be a finite-dimensional representation. Then, every element of $\rho([\mathfrak{g}, \mathfrak{g}] \cap \mathfrak{s})$ is nilpotent.

Proof. Induct on the dimension of V. We reduce to the case that V is irreducible, for if W were a subrepresentation, then so is V/W. If an operator is nilpotent on W and V/W, it must be nilpotent on V.

Replacing $\mathfrak{g}$ with its image, we may suppose that ρ is injective. Therefore, we must show that $[\mathfrak{g}, \mathfrak{g}] \cap \mathfrak{s} = 0$. This is equivalent to showing that $[\mathfrak{g}, \mathfrak{g}] \cap \mathfrak{a} = 0$ for every abelian ideal $\mathfrak{a}$ of $\mathfrak{g}$.

Note that $[\mathfrak{g}, \mathfrak{a}] = 0$, for if $x \in \mathfrak{g}$, $y \in \mathfrak{a}$ and $z = [x, y] \in \mathfrak{a}$, then y and z commute, and hence, y commutes with z^n for every positive integer n. Now,

$$\operatorname{tr}([x,y]z^{n-1}) = \operatorname{tr}(xyz^{n-1} - yxz^{n-1}) = \operatorname{tr}(xz^{n-1}y - yxz^{n-1}) = 0.$$

Therefore, $\operatorname{tr}(z^n) = 0$ for every positive integer n. This shows that $z = 0$, that is, $[\mathfrak{g}, \mathfrak{a}] = 0$.

Finally, we show that $[\mathfrak{g}, \mathfrak{g}] \cap \mathfrak{a} = 0$. Indeed, if $x, y \in \mathfrak{g}$ and $[x, y] \in \mathfrak{a}$, then $[y, [x, y]] = 0$ due to the preceding paragraph. Hence, y commutes with all powers of $[x, y]$, and the same argument shows that $[x, y] = 0$. This completes the proof. ■

Lemma 1.2. If $\operatorname{char} k = 0$, then $[\mathfrak{g}, \mathfrak{s}]$ is nilpotent.

Proof. Let $\overline{\mathfrak{g}}$ and $\overline{\mathfrak{s}}$ denote the images of $\mathfrak{g}$ and $\mathfrak{s}$ under the adjoint representation. By the preceding lemma, $[\overline{\mathfrak{g}}, \overline{\mathfrak{s}}] \subseteq [\overline{\mathfrak{g}}, \overline{\mathfrak{g}}] \cap \mathfrak{s}$, and hence, consists of nilpotent elements, whence is nilpotent due to Engel's Theorem.

Since the kernel of the adjoint representation is $\mathfrak{z} = Z(\mathfrak{g})$, we see that $[\mathfrak{g}, \mathfrak{s}]/Z([\mathfrak{g}, \mathfrak{s}])$ is nilpotent whence, the conclusion follows. ■

Lemma 1.3. Let $\operatorname{char} k = 0$. If δ is a derivation of $\mathfrak{g}$, then $\delta(\mathfrak{s}) \subseteq \mathfrak{n}$.

Proof. Construct the Lie algebra $\mathfrak{g}' = \mathfrak{g} \oplus k$ with the bracket

$$[(x,a),(y,b)] = ([x,y] + a\delta(y) - b\delta(x), 0).$$

It follows that $\mathfrak{g} \oplus 0$ is an ideal in $\mathfrak{g}'$. Let $\xi = (0,1) \in \mathfrak{g}'$. It is easy to verify that $\delta = [\xi, \cdot]$ on $\mathfrak{g} \trianglelefteq \mathfrak{g}'$.

Let $\mathfrak{s}'$ denote the radical of $\mathfrak{g}'$. Obviously, $\mathfrak{s} \subseteq \mathfrak{s}'$. Then,

$$\delta(\mathfrak{s}) = [\xi, \mathfrak{s}] \subseteq [\mathfrak{g}', \mathfrak{s}'] \cap \mathfrak{g}.$$

We have seen that $[\mathfrak{g}', \mathfrak{s}']$ is a nilpotent ideal in $\mathfrak{g}'$ and hence, its intersection with $\mathfrak{g}$ is also nilpotent. This completes the proof. ∎

Lemma 1.4. Let $\operatorname{char} k = 0$ and $\mathfrak{g}_1$ an ideal of $\mathfrak{g}$. If $\mathfrak{n}_1, \mathfrak{s}_1$ denote the nilradical and solvable radical of $\mathfrak{g}_1$, then $\mathfrak{n}_1 = \mathfrak{n} \cap \mathfrak{g}_1$ and $\mathfrak{s}_1 = \mathfrak{s} \cap \mathfrak{g}_1$.

Proof. Obviously, $\mathfrak{g}_1 \cap \mathfrak{s} \subseteq \mathfrak{s}_1$. Then, $\mathfrak{s}_1 / \mathfrak{g}_1 \cap \mathfrak{s}$ is a solvable ideal in $\mathfrak{g}_1 / \mathfrak{g}_1 \cap \mathfrak{s}$. On the other hand, $\mathfrak{g}_1 / \mathfrak{g}_1 \cap \mathfrak{s} \cong (\mathfrak{g}_1 + \mathfrak{s})/\mathfrak{s}$, which is an ideal in $\mathfrak{g}/\mathfrak{s}$. The latter is semisimple whence so is the former. As a result, $\mathfrak{s}_1 = \mathfrak{g}_1 \cap \mathfrak{s}$.

Now, if $a \in \mathfrak{g}$, then $\operatorname{ad} a$ is a derivation of $\mathfrak{g}_1$. Thus, $\operatorname{ad} a(\mathfrak{n}_1) \subseteq \mathfrak{n}_1$ due to Lemma 1.3, whence $\mathfrak{n}_1$ is an ideal in $\mathfrak{g}$, consequently, $\mathfrak{n}_1 \subseteq \mathfrak{n} \cap \mathfrak{g}_1$. This completes the proof. ∎

§2 Levi's Theorem

Throughout this section, $\operatorname{char} k = 0$.

Lemma 2.1 (Whitehead's First Lemma). Let $\mathfrak{g}$ be a semisimple Lie algebra over k and M a $\mathfrak{g}$-module. Let $f : \mathfrak{g} \to M$ be a k-linear map satisfying

$$f([x,y]) = xf(y) - yf(x).$$

Proof. Let $\rho : \mathfrak{g} \to \mathfrak{gl}(M)$ be the representation and let $\mathfrak{K} = \ker \varphi$. We have a decomposition into ideals, $\mathfrak{g} = \mathfrak{K} \oplus \mathfrak{h}$ as Lie algebras. The restriction of the representation $\mathfrak{h} \to \mathfrak{gl}(M)$ is injective and hence, the trace form $(\cdot,\cdot) : \mathfrak{h} \times \mathfrak{h} \to k$ given by

$$(x,y) = \operatorname{tr}(\varphi(x)\varphi(y))$$

is a nondegenerate symmetric bilinear form. Let $u_1, \dots, u_n$ be a basis of $\mathfrak{h}$ and $u^1, \dots, u^n$ be the dual basis with respect to $(\cdot,\cdot)$.

The *Casimir operator* is given by

$$\Gamma(\cdot) = \sum_{i=1}^{n} u^i (u_i \cdot)),$$

and it is easy to check that this defines a $\mathfrak{g}$-linear map $\Gamma : M \to M$. Further, we note that $\operatorname{tr}\Gamma = \dim \mathfrak{h}$.

We now prove the statement of the lemma by induction on $\dim M$. Using the Fitting Decomposition with respect to Γ, we can write $M = M_0 \oplus M_1$ where Γ is nilpotent on M_0 and an isomorphism on M_1. It is also easy to check that both M_0 and M_1 are $\mathfrak{g}$-submodules of M.

Let $\pi_i : M \to M_i$ denote the canonical projection and $f_i = \pi_i \circ f$. If both M_0 and M_1 are proper submodules, then we are done by induction. Else, we need to examine two cases.

First, suppose $M = M_0$, that is, Γ is nilpotent on M, whence $\dim \mathfrak{h} = \operatorname{tr} \Gamma = 0$, that is, φ is a trivial representation, and hence, $f \equiv 0$. In this case, the choice of $m = 0$ works.

Now, suppose $M = M_1$, that is, Γ is invertible. Set

$$y = \sum_{i=1}^{m} u_i f(u_i) \in M.$$

A small computation gives us

$$ay = \Gamma f(a) \quad \forall\, a \in \mathfrak{g}.$$

Thus, $f(a) = a \cdot (\Gamma^{-1} y)$, thereby completing the proof. ■

Lemma 2.2 (Whitehead's Second Lemma). Let $\mathfrak{g}$ be a semisimple Lie algebra over k, M a finite-dimensional $\mathfrak{g}$-module and $g : \mathfrak{g} \times \mathfrak{g} \to M$ a bilinear map such that

(a) $g(x, x) = 0$ for all $x \in \mathfrak{g}$.

(b) For $x_1, x_2, x_3 \in \mathfrak{g}$,

$$\sum_{i=1}^{3} g(x_i, [x_{i+1}, x_{i+2}]) + x_i g(x_{i+1}, x_{i+2}) = 0.$$

Then, there is a k-linear map $\rho : \mathfrak{g} \to M$ satisfying

$$g(x_1, x_2) = x_2 \rho(x_1) - x_1 \rho(x_2) - \rho[x_1, x_2].$$

Proof. First, note that condition (a), is equivalent to stating that g is skew-symmetric. Let $\mathfrak{K}, \mathfrak{h}, u_i, u^i, \Gamma$ be as in the proof of Lemma 2.1. Set $x_3 = u_i$ in (b), multiply by u^i and sum over all i to obtain

$$\begin{aligned}
0 &= \sum_i u^i g(u_i, [x_1, x_2]) + \Gamma g(x_1, x_2) + \sum_i u^i g(x_1, [x_2, u_i]) + \sum_i u^i \left(x_1 g(x_2, u_i)\right) \\
&\quad + \sum_i u^i g(x_2, [u_i, x_1]) + \sum_i u^i \left(x_2 g(u_i, x_1)\right) \\
&= \Gamma g(x_1, x_2) + \sum_i u^i g(u_i, [x_1, x_2]) + \sum_i u^i g(x_1, [x_2, u_i]) + \sum_i [u^i, x_1] g(x_2, u_i) \\
&\quad + \sum_i x_1 \left(u^i g(x_2, u_i)\right) + \sum_i u^i g(x_2, [u_i, x_1]) + \sum_i [u^i, x_2] g(u_i, x_1) + \sum_i x_2 \left(u^i g(u_i, x_1)\right).
\end{aligned}$$

Recall that if $[u_i, x] = \sum \alpha_{ij} u_j$ and $[u^i, x] = \sum \beta_{ij} u^j$, then $\alpha_{ij} + \beta_{ji} = 0$. Using this, we get

$$\sum_i [u^i, x_1] g(x_2, u_i) = \sum_i \sum_j \beta_{ij} u^j g(x_2, u_i) = -\sum_i \sum_j \alpha_{ji} u^j g(x_2, u_i) = \sum_j u^j g(x_2, [x_1, u_j])$$
$$\sum_i [u^i, x_2] g(u_i, x_1) = \sum_i u^i g([x_2, u_i], x_1)$$

Substituting this back, we have canceled four terms to obtain,

$$0 = \Gamma g(x_1, x_2) + \sum_i u^i g(u_i, [x_1, x_2]) + \sum_i x_1 \left(u^i g(x_2, u_i) \right) + \sum_i x_2 \left(u^i g(u_i, x_1) \right).$$

If Γ is invertible, then define

$$\rho(x) = \Gamma^{-1} \sum_i u^i g(u_i, x).$$

Now, suppose Γ is nilpotent. As we saw in Lemma 2.1, the representation must be the zero representation and hence, condition (b) reduces to

$$g(x_1, [x_2, x_3]) + g(x_2, [x_3, x_1]) + g(x_3, [x_1, x_2]) = 0.$$

Let $\mathfrak{X}$ denote the k-vector space of linear maps $\mathfrak{g} \to M$. This can be given a $\mathfrak{g}$-module structure by defining, for $A \in \mathfrak{X}$, $x, y \in \mathfrak{g}$,

$$(xA)(y) = -A([x, y])$$

Note that this is just the standard $\mathfrak{g}$-module structure on $\mathrm{Hom}_k(\mathfrak{g}, M)$ where $\mathfrak{g}$ is a $\mathfrak{g}$-module through the adjoint representation.

For each $y \in \mathfrak{g}$, let $A_y \in \mathfrak{X}$ be the mapping $x \mapsto -g(x, y)$. Then, $\Phi : \mathfrak{g} \to \mathfrak{X}$ given by $y \mapsto A_y$ is k-linear. We contend that Φ satisfies the hypothesis of Lemma 2.1.

Indeed,

$$\begin{aligned} A_{[x_1, x_2]}(y) &= -g(y, [x_1, x_2]) \\ (x_2 A_{x_1})(y) &= -A_{x_1}([x_2, y]) = g([x_2, y], x_1) \\ (x_1 A_{x_2})(y) &= -A_{x_2}([x_1, y]) = g([x_1, y], x_2). \end{aligned}$$

Then,

$$\begin{aligned} \left(x_1 A_{x_2} - x_2 A_{x_1} \right)(y) &= g([x_1, y], x_2) - g([x_2, y], x_1) \\ &= -g(x_2, [x_1, y]) - g(x_1, [y, x_2]) \\ &= g(y, [x_2, x_1]) = -g(y, [x_1, x_2]) \\ &= -A_{[x_1, x_2]}(y). \end{aligned}$$

As a result, there is a $\rho \in \mathfrak{X}$ such that $A_y = y\rho$. In other words, we have a linear map $\rho : \mathfrak{g} \to M$ such that

$$-g(x, y) = A_y(x) = (y\rho)(x) = -\rho([y, x]) = \rho([x, y]).$$

And since M is a zero representation, we have our desired conclusion in the case that Γ is nilpotent.

Finally, if Γ is neither invertible nor nilpotent, we use the Fitting decomposition to write $M = M_0 \oplus M_1$ just as in the proof of Lemma 2.1 and use an induction argument to complete the proof. ■

PROPOSITION 2.3. Let $\mathfrak{g}$ be a Lie algebra over k, $\mathfrak{s}$ an abelian ideal in $\mathfrak{g}$. Set $\overline{\mathfrak{g}} = \mathfrak{g}/\mathfrak{s}$. Then, $\overline{\mathfrak{g}}$ acts on $\mathfrak{s}$ through the "adjoint", that is, $\overline{x} \cdot s = [x, s]$. Let σ be a linear section of the projection $\mathfrak{g} \twoheadrightarrow \overline{\mathfrak{g}}$. Define the skew-symmetric bilinear map $g : \overline{\mathfrak{g}} \times \overline{\mathfrak{g}} \to \mathfrak{s}$ by

$$g(\overline{x}_1, \overline{x}_2) = [\sigma\overline{x}_1, \sigma\overline{x}_2] - \sigma[\overline{x}_1, \overline{x}_2].$$

Then, $\mathfrak{s}$ has a complementary subspace which is also a subalgebra if and only if there is a linear map $\rho : \overline{\mathfrak{g}} \to \mathfrak{s}$ such that

$$g(\overline{x}_1, \overline{x}_2) = \overline{x}_2\rho(\overline{x}_1) - \overline{x}_1\rho(\overline{x}_2) - \rho[\overline{x}_1, \overline{x}_2].$$

Proof. Suppose $\tau : \overline{\mathfrak{g}} \to \mathfrak{g}$ is a linear section such that $\tau\overline{\mathfrak{g}}$ is a subalgebra of $\mathfrak{g}$. Let $\rho = \tau - \sigma$. Then,

$$\pi(\rho\overline{x}) = \pi(\sigma\overline{x}) - \pi(\tau\overline{x}) = \overline{x} - \overline{x} = 0.$$

Hence, the image of ρ is in $\mathfrak{s}$. We have

$$\begin{aligned} g(\overline{x}_1, \overline{x}_2) &= [\tau\overline{x}_1 - \rho\overline{x}_1, \tau\overline{x}_2 - \rho\overline{x}_2] + \rho[\overline{x}_1, \overline{x}_2] - \tau[\overline{x}_1, \overline{x}_2] \\ &= -[\tau\overline{x}_1, \rho\overline{x}_2] - [\rho\overline{x}_1, \tau\overline{x}_2] + [\rho\overline{x}_1, \rho\overline{x}_2] - \rho[\overline{x}_1, \overline{x}_2] \\ &= -[\tau\overline{x}_1, \rho\overline{x}_2] - [\rho\overline{x}_1, \tau\overline{x}_2] - \rho[\overline{x}_1, \overline{x}_2] \\ &= [\tau\overline{x}_2, \rho\overline{x}_1] - [\tau\overline{x}_1, \rho\overline{x}_2] - \rho[\overline{x}_1, \overline{x}_2] \\ &= \overline{x}_2\rho(\overline{x}_1) - x_1\rho(\overline{x}_2) - \rho[\overline{x}_1, \overline{x}_2]. \end{aligned}$$

This proves one direction of the proposition. The other direction follows by simply retracing the steps we did above. ■

THEOREM 2.4 (LEVI). Let $\mathfrak{g}$ be a Lie algebra over k and $\mathfrak{s}$ its solvable radical. Then, $\mathfrak{s}$ has a complementary subalgebra in $\mathfrak{g}$.

Proof. We first reduce to the case $[\mathfrak{s}, \mathfrak{s}] = 0$. Suppose $\mathfrak{t} = [\mathfrak{s}, \mathfrak{s}] \neq 0$. Let $\overline{\mathfrak{g}} = \mathfrak{g}/\mathfrak{t}$. Since $\dim \overline{\mathfrak{g}} < \dim \mathfrak{g}$, we can use an inductive argument to find a complementary subalgebra $\overline{\mathfrak{h}}$ to $\overline{\mathfrak{s}}$ in $\overline{\mathfrak{g}}$. Note that $\overline{\mathfrak{h}} = \mathfrak{h}/\mathfrak{t}$ for some subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ containing $\mathfrak{t}$. Hence, $\mathfrak{h} \cap \mathfrak{s} = \mathfrak{t}$ and $\dim \mathfrak{h} < \dim \mathfrak{g}$.

The inuction hypothesis applies to $\mathfrak{h}$ and we can isolate a subalgebra $\mathfrak{L}$ of $\mathfrak{h}$ that is complementary to $\mathfrak{t}$. It is easy to see that $\mathfrak{L}$ is the required complement of $\mathfrak{s}$ using a dimension argument.

Finally, we come to the case when $[\mathfrak{s}, \mathfrak{s}] = 0$, that is, $\mathfrak{s}$ is abelian. Set $\overline{\mathfrak{g}} = \mathfrak{g}/\mathfrak{s}$. Then, $\overline{\mathfrak{g}}$ acts on $\mathfrak{s}$ as $\overline{x} \cdot s = [x, s]$. Let $\sigma : \overline{\mathfrak{g}} \to \mathfrak{g}$ be a linear section of the projection $\mathfrak{g} \twoheadrightarrow \overline{\mathfrak{g}}$.

Consider the map $g : \overline{\mathfrak{g}} \times \overline{\mathfrak{g}} \to \mathfrak{s}$ by

$$g(\overline{x}_1, \overline{x}_2) = [\sigma\overline{x}_1, \sigma\overline{x}_2] - \sigma[\overline{x}_1, \overline{x}_2].$$

It is easy to check that this satisfies the hypothesis of Lemma 2.2. The conclusion of Lemma 2.2 along with Proposition 2.3 completes the proof of the theorem. ■

§3 THE char 0 CASE

Throughout this section, k denotes a field of characteristic 0 (it may not be algebraically closed).

LEMMA 3.1. Let $\mathfrak{g}$ be a finite-dimensional solvable Lie algebra, $\mathfrak{n}$ its nilradical, $\mathfrak{U}$ the universal enveloping algebra of $\mathfrak{g}$. Suppose $\mathfrak{X}$ is an ideal of $\mathfrak{U}$ of finite co-dimension such that every element of $\mathfrak{n}$ is nilpotent modulo $\mathfrak{X}$. Then, there exists an ideal $\mathfrak{I}$ in $\mathfrak{U}$ such that:

(a) $\mathfrak{I} \subseteq \mathfrak{X}$,

(b) $\mathfrak{I}$ is of finite co-dimension,

(c) every element of $\mathfrak{n}$ is nilpotent modulo $\mathfrak{I}$.

(d) $\delta\mathfrak{I} \subseteq \mathfrak{I}$ for every derivation δ of $\mathfrak{g}$ (extended to $\mathfrak{U}$),

Proof. Let $\mathfrak{M}$ denote the ideal in $\mathfrak{U}$ generated by $\mathfrak{X}$ and $\mathfrak{n}$. We first show that there is a positive integer k such that $\mathfrak{M}^k \subseteq \mathfrak{X}$. Consider the map $f : \mathfrak{n} \to \mathfrak{gl}(\mathfrak{U}/\mathfrak{X})$ given by $x \mapsto \ell_x$ where ℓ_x denotes left multiplication by x. Since $\mathfrak{n}$ is nilpotent, its image in $\mathfrak{gl}(\mathfrak{U}/\mathfrak{X})$ is a nilpotent Lie algebra. As a consequence of Engel's Theorem, there is a positive integer k such that the product of any k elements in the image is 0. Thus, $\ell_x = 0$ whenever x is a product of k elements in $\mathfrak{n}$.

Thus, $\mathfrak{n}^k \subseteq \mathfrak{X}$. Now (work in $\mathfrak{U}$), for any $x \in \mathfrak{n}$ and $y \in \mathfrak{g}$, $xy = [x, y] + yx$ and $[x, y] \in \mathfrak{n}$. Now consider any element in $\mathfrak{U}$ of the form $a_1 \cdots a_n$ where $n \geqslant k$ and at least k of the a_i's are from $\mathfrak{n}$. Using the commutator relations one can move all k elements of $\mathfrak{n}$ to the left of the product, and it would follow that $a_1 \cdots a_n \in \mathfrak{X}$. Thus, $\mathfrak{M}^k \subseteq \mathfrak{X}$.

Let $\mathfrak{I} = \mathfrak{M}^k$. It is easy to verify conditions (a), (b) and (c). Let δ be a derivation of $\mathfrak{g}$. Since $\mathfrak{g}$ is solvable, $\delta\mathfrak{g} \subseteq \mathfrak{n}$. Therefore, $\delta\mathfrak{U} \subseteq \mathfrak{M}$. In particular, $\delta\mathfrak{M} \subseteq \mathfrak{M}$. Which means

$$\delta\mathfrak{I} = \delta\mathfrak{M}^k \subseteq \mathfrak{M}^k = \mathfrak{I}.$$

This completes the proof. ■

LEMMA 3.2 (EXTENSION LEMMA). Let $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{h}$ as vector spaces, where $\mathfrak{s}$ is a solvable ideal and $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$. Suppose $\varphi : \mathfrak{s} \to \mathfrak{gl}(V)$ is a finite dimensional representation such that $\varphi(z)$ is nilpotent for every $z \in \mathfrak{n}$, the nilradical of $\mathfrak{s}$. Then, there is a finite-dimensional representation ψ of $\mathfrak{g}$ such that:

(a) if $\psi(x) = 0$ for some $x \in S$, then $\varphi(x) = 0$.

(b) $\psi(y)$ is nilpotent for every y of the form $z + u$ where $z \in \mathfrak{n}$ and $u \in \mathfrak{h}$ is such that $\operatorname{ad}_{\mathfrak{s}} u$ is nilpotent.

Proof. The representation induces a map $\widetilde{\varphi} : \mathfrak{U} = U(\mathfrak{s}) \to \mathfrak{gl}(V)$, whose kernel $\mathfrak{X}$ is of finite co-dimension. This puts us in the situation of Lemma 3.1. Let $\mathfrak{I} \trianglelefteq \mathfrak{U}$ denote the ideal in the conclusion of Lemma 3.1.

For $s \in \mathfrak{s}$, let $\psi(s) : \mathfrak{U} \to \mathfrak{U}$ be right multiplication by $s \in \mathfrak{U}$. For $h \in \mathfrak{h}$, let $\psi(h)$ denote the derivation on $\mathfrak{U}$ extending the derivation $s \mapsto [s, h]$ on $\mathfrak{s}$. Using the fact that $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{h}$, extend ψ to all of $\mathfrak{g}$. We shall show that ψ is a representation (may not be finite-dimensional) of $\mathfrak{g}$.

To show this, it suffices to show that $\psi([s,h]) = [\psi(s), \psi(h)]$. Note that $[s,h] \in \mathfrak{s}$ and hence, $\psi([s,h])$ is right multiplication by $[s,h] \in \mathfrak{U}$. But since $\psi(h)$ is a derivation of $\mathfrak{U}$, and $\psi(s)$ is right multiplication, it is easy to check that $[\psi(s), \psi(h)]$ is right multiplication by $\psi(h)(s) = [s,h]$. This verifies that ψ is a representation.

Since $\mathfrak{I}$ is an ideal, it is invariant under $\psi(s)$ for all $s \in \mathfrak{s}$ and since $\psi(h)$ is a derivation, $\mathfrak{I}$ must be invariant under it due to Lemma 3.1. As a result, $\mathfrak{I}$ is invariant under $\psi(g)$ for every $g \in \mathfrak{g}$, consequently, ψ induces a finite dimensional representation of $\mathfrak{g}$ on $\mathfrak{U}/\mathfrak{I}$, which, by abuse of notation, we shall denote by ψ.

Let $x \in \mathfrak{s}$ be such that $\psi(s) = 0$, that is, $\mathfrak{U}s \subseteq \mathfrak{I}$, in particular, $s \in \mathfrak{I} \subseteq \mathfrak{X} = \ker \widetilde{\varphi}$, whence $\varphi(s) = 0$.

Let $z \in \mathfrak{n}$ and $u \in \mathfrak{h}$ be such that $\operatorname{ad}_{\mathfrak{s}} u$ is nilpotent. Due to Lemma 3.1, z is nilpotent modulo $\mathfrak{I}$. Next, since $\operatorname{ad}_{\mathfrak{s}} u$ is nilpotent, $\mathfrak{s}$ generates $\mathfrak{U}$ and $\mathfrak{U}/\mathfrak{I}$ is finite-dimensional, $\psi(u)$ is nilpotent on $\mathfrak{U}/\mathfrak{I}$.

Now, $\psi(\mathfrak{s})$ is a nilpotent subalgebra of $\mathfrak{gl}(W)$. Thus, there is a basis of W with respect to which, every element of $\psi(\mathfrak{s})$ is strictly upper triangular. As a result, there exists an $n \gg 0$, such that the product of any n elements of $\psi(\mathfrak{s})$ is 0. Recall that $\psi(y) = \psi(z) + \psi(u)$. We have $\psi(u)\psi(z) = \psi(z)\psi(u) + \psi([u,z])$. Note that $\psi([u,z]) \in \psi(\mathfrak{s})$.

If m is the nilpotency class of $\psi(u)$, consider

$$\psi(y)^{mn} = (\psi(z) + \psi(u))^{mn}.$$

It is easy to see that this must be equal to 0. ■

THEOREM 3.3 (ADO'S THEOREM IN CHAR 0). Every finite-dimensional Lie algebra $\mathfrak{g}$ over k has a faithful finite-dimensional representation.

Proof. The adjoint representation has kernel $\mathfrak{z} = \mathfrak{z}(\mathfrak{g})$, the center of $\mathfrak{g}$. Thus, it suffices to find a representation that is faithful on $\mathfrak{z}$.

We first begin with a faithful representation of $\mathfrak{z}$, which is obvious to construct since $\mathfrak{z}$ is abelian. Indeed, if $\dim \mathfrak{z} = c$, then in a $c+1$-dimensional vector space, there is a nilpotent linear transformation z such that $z^c \neq 0$. Then, $\mathfrak{z}$ is isomorphic to the Lie algebra with basis $(z, z^2, \ldots, z^c)$.

We have the inclusion $\mathfrak{z} \subseteq \mathfrak{n} \subseteq \mathfrak{s}$. We can also find a filtration

$$\mathfrak{z} = \mathfrak{n}_1 \subseteq \cdots \subseteq \mathfrak{n}_k = \mathfrak{n}$$

where $\dim \mathfrak{n}_{i+1}/\mathfrak{n}_i = 1$ for all i and each $\mathfrak{n}_i$ is an ideal in $\mathfrak{n}_{i+1}$. As vector spaces, we can write $\mathfrak{n}_{i+1} = \mathfrak{n}_i \oplus k u_{i+1}$ where $k u_{i+1}$ is a subalgebra. Since each $\mathfrak{n}_{i+1}$ is a solvable ideal, Lemma 3.2 applies at each stage. This furnishes a representation of $\mathfrak{n}$ by nilpotent linear transformations that is faithful on $\mathfrak{z}$.

Now, consider another filtration

$$\mathfrak{n} = \mathfrak{s}_1 \subseteq \cdots \subseteq \mathfrak{s}_r = \mathfrak{s}.$$

where each $\mathfrak{s}_i$ is an ideal in $\mathfrak{s}_{i+1}$ and $\dim \mathfrak{s}_{i+1}/\mathfrak{s}_i = 1$. Since $\mathfrak{n}$ is the nilradical of each $\mathfrak{s}_i$, we can again use Lemma 3.2 to obtain a representation of $\mathfrak{s}$, faithful on $\mathfrak{z}$ and consisting of nilpotent linear transformations on $\mathfrak{n}$.

Finally, Theorem 2.4 decomposes $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{h}$ for some subalgebra $\mathfrak{h}$. Invoking Lemma 3.2, we have completed the proof. ■

§4 THE char $p > 0$ CASE

LEMMA 4.1. Let $\operatorname{char} k = p > 0$ and $0 \neq f(X) \in k[X]$. Then, there is a polynomial of the form

$$X^{p^m} + a_{m-1}X^{p^{m-1}} + \cdots + a_0X \in k[X]$$

that is divisible by $f(X)$. Such a polynomial is called a *p-polynomial*.

Proof. If f is a constant polynomial, then there is nothing to prove. Suppose now that f is not constant. For each $i \geqslant 0$, we can write

$$X^{p^i} = q_i(X)f(X) + r_i(X),$$

where $\deg r_i < \deg f$. Therefore, the r_i's span a vector subspace of dimension at most $\deg f$. Let $m = \deg f$. Then, $r_0, \ldots, r_m$ must be linearly dependent. The conclusion follows by just adding up the above equations with suitable weights. ■

LEMMA 4.2. Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over k with $\operatorname{char} k = p > 0$ and let $\mathfrak{U} = \mathfrak{U}(\mathfrak{g})$. Then, for every $a \in \mathfrak{g}$, there is a polynomial $m_a(X) \in k[X]$ such that $m_a(a)$ is in the center of $\mathfrak{U}$.

Proof. Note that $\operatorname{ad} a : \mathfrak{g} \to \mathfrak{g}$ is a linear transformation on a finite-dimensional k-vector space and hence, has a minimal polynomial $f(X) \in k[X]$. Using Lemma 4.1, there is a p-polynomial $p(X) \in k[X]$ such that $p(\operatorname{ad} a) = 0$. But since $(\operatorname{ad} a)^p = \operatorname{ad} a^p$, we have that $\operatorname{ad} p(a) = 0$ on $\mathfrak{g}$. This completes the proof. ■

LEMMA 4.3. Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over k with basis $\{u_i\}$ and let $\mathfrak{U} = \mathfrak{U}(\mathfrak{g})$. Let

$$\mathfrak{U}^{(k)} = k \oplus \mathfrak{g} \oplus \mathfrak{g}^2 \oplus \cdots \oplus \mathfrak{g}^k.$$

Suppose for each u_i, there is a positive integer n_i and an element z_i in the center of $\mathfrak{U}$ such that $v_i = u_i^{n_i} - z_i$ is in $\mathfrak{U}^{(n_i-1)}$.

Then, the elements of the form

$$z_{i_1}^{h_1} \ldots z_{i_r}^{h_r} u_{i_1}^{\lambda_1} u_{i_2}^{\lambda_2} \ldots u_{i_r}^{\lambda_r}$$

such that $i_1 < \cdots < i_r$, $h_j \geqslant 0$, $0 \leqslant \lambda_j < n_{i_j}$ form a basis for $\mathfrak{U}$.

Proof. We first show that the elements of the above form span $\mathfrak{U}$, for which it suffices to show that every element of the form $u_{i_1}^{k_1} \ldots u_{i_r}^{k_r}$ is a linear combination of elements of the above form. If all the k_j's are less than n_{i_j}, then there is nothing to prove. Hence, suppose that $k_j \geqslant n_{i_j}$ for some index j.

Replacing $u_{i_j}^{n_{i_j}}$ by $v_{i_j} + z_{i_j}$, we obtain

$$u_{i_1}^{k_1} \dots u_{i_r}^{k_r} = z_{i_j} u_{i_1}^{k_1} \dots u_{i_j}^{k_j - n_{i_j}} \dots u_{i_r}^{k_r} + u_{i_1}^{k_1} \dots u_{i_j}^{k_j - n_{i_j}} v_{i_j} \dots u_{i_r}^{k_r}$$

Using an induction argument, it is clear that the above sum can be written as a linear combination of elements in the desired form.

It remains to show that those elements are linearly independent. Indeed,

$$\begin{aligned} z_{i_1}^{h_1} \dots z_{i_r}^{h_r} u_{i_1}^{\lambda_1} \dots u_{i_r}^{\lambda_r} &= (u_{i_1}^{n_{i_1}} - v_{i_1})^{h_1} u_{i_1}^{\lambda_1} \dots (u_{i_r}^{n_{i_r}} - v_{i_r})^{h_r} u_{i_r}^{\lambda_r} \\ &\equiv u_{i_1}^{h_1 n_{i_1} + \lambda_1} \dots u_{i_r}^{h_r n_{i_r} + \lambda_r} \bmod \mathfrak{U}^{(k-1)}. \end{aligned}$$

where $k = \sum_{j=1}^{r} (h_j n_{i_j} + \lambda_j)$. Recall that elements of $\mathfrak{U}^{(k-1)}$ are linear combinations of standard monomials of degree at most $k-1$.

Supppose there were a linear relation between elements of the aforementioned form, with maximum "degree" k. Then, using the above congruence, we would obtain a linear combination of standard monomials elements of "degree" k. Note that every element of the aforementioned form contributes at most one standard monomial of "degree" k. Using the linear independence of standard monomials, and the fact that there is only one element of the aforementioned form contributing a certain residue class modulo $\mathfrak{U}^{(k-1)}$, we have completed the proof. ■

Theorem 4.4 (Iwasawa). Every finite-dimensional Lie algebra over a field k of characteristic $p > 0$ admits a faithful finite-dimensional representation.

Proof. Let $u_1, \dots, u_n$ be a k-basis for $\mathfrak{g}$. Using Lemma 4.2, there is a p-polynomial $m_i(X) \in k[X]$ such that $m_i(u_i)$ is in the center of $\mathfrak{U}$. Let $\deg m_i = p^{m_i}$. Then, $z_i = u_i^{p^{m_i}} + v_i$ where $v_i \in \mathfrak{U}^{p^{m_i}-1}$. Then, due to Lemma 4.3, we have an explicit generating set for $\mathfrak{U}$.

Let $\mathfrak{I}$ denote the two-sided ideal in $\mathfrak{U}$ generated by the z_i's. Consider $\mathfrak{U}/\mathfrak{I}$. This is spanned by $u_1^{\lambda_1} \dots u_n^{\lambda_n}$ with $0 \leqslant \lambda_i < p^{m_i}$. Further, it is easy to see that these are linearly independent and hence, constitute a basis of $\mathfrak{U}/\mathfrak{I}$. The canonical surjection $\mathfrak{U} \to \mathfrak{U}/\mathfrak{I}$ restricts to an isomorphism on $\mathfrak{g}$, consequently, we have obtained a faithful finite-dimensional representation of $\mathfrak{g}$. This completes the proof. ■

REFERENCES

[FH91] W. Fulton and J. Harris. *Representation Theory: A First Course*. Graduate Texts in Mathematics. Springer New York, 1991.

[Jac79] N. Jacobson. *Lie Algebras*. Dover books on advanced mathematics. Dover, 1979.