Restricted Lie Algebras

Jared Warner
1. Definitions and Examples

**Definition 1.1.** Let $k$ be a field of characteristic $p$. A **restricted Lie algebra** $(\mathfrak{g}, (\cdot)^{[p]})$ is a Lie algebra $\mathfrak{g}$ over $k$ and a map $(\cdot)^{[p]} : \mathfrak{g} \to \mathfrak{g}$ called the **p-operation** such that for all $a \in k$ and for all $x, y \in \mathfrak{g}$ we have:

- $(ax)^{[p]} = a^{p}x^{[p]}$
- $\text{ad}_{x^{[p]}} = \text{ad}_{x}^{p}$ and
- $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_{i}(x, y) \frac{x^{i-1}}{i}$ where $s_{i}(x, y)$ is the coefficient of $t^{i-1}$ in the expression $\text{ad}_{tx+y}(x)$

Recall that for any $x \in \mathfrak{g}$ $\text{ad}_{x} : \mathfrak{g} \to \mathfrak{g}$ is the linear map defined by $\text{ad}_{x}(y) = [x, y]$ for all $y \in \mathfrak{g}$.

**Example 1.2.** Let $\mathfrak{g}$ be any abelian Lie algebra, i.e., a Lie algebra such that $[x, y] = 0$ for all $x, y \in \mathfrak{g}$. Notice that bilinearity and alternativity ($[x, x] = 0$ for all $x \in \mathfrak{g}$) imply that any one-dimensional Lie algebra is abelian. The p-operation defined by $x^{[p]} = 0$ for all $x \in \mathfrak{g}$ gives $\mathfrak{g}$ the structure of a restricted Lie algebra. Notice that the condition that $\mathfrak{g}$ be abelian is necessary, for if we consider $\mathfrak{gl}_{n}$, the Lie algebra of $n \times n$ matrices with entries in $k$ whose bracket is given by commutation, it can be shown that the second and third conditions listed above are not satisfied by the p-operation $A^{[p]} = 0$ for all matrices $A \in \mathfrak{gl}_{n}$.

**Example 1.3.** Let $A$ be any associative, unital algebra over $k$ (from here on, unless otherwise specified, by algebra we mean an associative, unital algebra over $k$). Define a bracket and p-operation on elements of $A$ by $x^{[p]} := x^{p}$ and $[x, y] := xy - yx$ for all $x, y \in A$. We check that such definitions give $A$ the structure of a restricted Lie algebra. Let $x, y \in A$ and $a \in k$.

- $(ax)^{p} = a^{p}x^{p} = a^{p}x^{[p]}$, so the first condition above holds.
- $\text{ad}_{x^{[p]}}(y) = \text{ad}_{x^{p}}(y) = [x^{p}, y] = x^{p}y - yx^{p}$. Using the combinatorial identity $\dbinom{n}{i} + \dbinom{n}{i-1}$ along with induction, one can show that $\text{ad}_{x}^{p}(y) = \sum_{i=0}^{n}(-1)^{i}\dbinom{n}{i}x^{n-i}yx^{i}$.

Since $\dbinom{p}{i}$ is divisible by $p$ for all $i = 1, 2, \ldots, p-1$, it follows that $\text{ad}_{x}^{p}(y) = x^{p}y - yx^{p}$, and hence the second condition above holds.

- The third condition is difficult to check in generality. Using the above formula, we have that $\text{ad}_{x^{[p]}}^{p-1}(x) = \sum_{i=0}^{p-1}(-1)^{i}\dbinom{p-1}{i}(tx + y)^{p-1-i}(tx + y)^{i}$. I claim that the coefficient of $t^{j-1}$ in this expression is $j \sum_{\text{all words of length } p \text{ in } x \text{ and } y \text{ that have } j \text{ x's}}$. From the formula, it can be seen that the coefficient of $t^{j-1}$ is equal to $\sum_{i=0}^{p-1}(-1)^{j}\dbinom{p-1}{i} \sum_{\text{all words of length } p \text{ in } x \text{ and } y \text{ with } j \text{ x's, whose } (p-i)^{th} \text{ entry is } x \text{ }}$. Given a word of length $p$ in $x$ and $y$ with $j$ x's, we would like to know how many times this word is counted in the given sum. Fix a word $w$ of the desired
type and let \( J \subset \{0, 1, 2, \ldots, p-1\} \) be the subset of \( j \) elements such that for all \( i \in J \), \( w \) has an \( x \) in the \((p - i)^{\text{th}}\) position. Then this word is counted \( \sum_{i \in J} (-1)^i \binom{p-1}{i} \) many times. Since \((-1)^i \binom{p-1}{i} \equiv 1 \mod p\) for all \( i \in \{0, 1, 2, \ldots, p-1\} \) as can be checked with the above combinatorial identity, it follows that each word is counted \( j \) times, proving the claim. Now \((x + y)^p = (x + y)p = x^p + y^p + \sum \text{(words in } x \text{ and } y \text{ of length } p) = x^p + y^p + \sum_{i=1}^{p-1} \frac{s_i(x, y)}{i} \), and the third condition holds as well.

Denote by \( A_L \) the restricted Lie algebra associated to the algebra \( A \). We use the same notation for the Lie algebra (not restricted) associated to \( A \) (with bracket given by the commutator as defined above).

### 2. Enveloping Algebras

Here we desire to discuss the restricted enveloping algebra \( u(g) \) of a restricted Lie algebra \( g \). We first briefly review the definition of the universal enveloping algebra.

**Definition 2.1.** Let \( k \) be a field of any characteristic, and let \( g \) be a Lie algebra over \( k \). The universal enveloping algebra of \( g \) is an algebra \( U \) together with a map of Lie algebras \( h : g \to U_L \) satisfying the following universal property: given any algebra \( A \) and any map of Lie algebras \( f : g \to A_L \), there exists a unique map of algebras \( g : U \to A \) such that \( f = g \circ h \).

Note that the universal property described implies that if a universal enveloping algebra exists for \( g \), then it is unique up to unique isomorphism. That is, if \( U \) and \( U' \) both satisfy the universal property, then there is a unique algebra isomorphism \( U \to U' \). This can be seen as follows. Let \( h : g \to U_L \) and \( h' : g \to U'_L \) both satisfy the universal property. Hence, there exist unique maps \( g : U \to U' \) and \( g' : U' \to U \) satisfying \( h' = g \circ h \) and \( h = g' \circ h' \). Hence \( h = g' \circ g \circ h \). Since we also have \( h = id_U \circ h \), by uniqueness, it follows that \( g' \circ g = id_U \). The same argument applies to \( g \circ g' \), so that \( g \) and \( g' \) are algebra isomorphisms. We now show that the universal enveloping algebra always exists for any Lie algebra.

**Theorem 2.2.** Let \( g \) be a Lie algebra. The universal enveloping algebra of \( g \) always exists.

**Proof.** Let \( T(g) = \bigoplus_{n \geq 0} T^n(g) \) be the tensor algebra of \( g \) where \( T^n(g) = g \otimes \cdots \otimes g \) \( n \)-times, and multiplication is defined by concatenation of simple tensors. Notice that this multiplication turns \( T(g) \) into a graded algebra. Notice that \( g \hookrightarrow T(g) \) by taking \( x \in g \) to itself in \( T^1(g) = g \subset T(g) \). Next, let \( I \) be the two-sided ideal generated by elements of the form \( x \otimes y - y \otimes x - [x, y] \) where \( x, y \in g \), and let \( U = T(g)/I \). Let \( h : g \to U_L \) take \( x \in g \) to the coset \( x + I \) in \( U \). Notice this is a map of Lie algebras precisely because \( x \otimes y - y \otimes x = [x, y] \) in \( U \). We show that the pair \((U, h)\) satisfy the universal property described above.

Suppose \( A \) is an algebra, and \( f : g \to A_L \) is a map of Lie algebras. Define a map of algebras \( g : U \to A \) by mapping \( x + I \) to \( f(x) \) and extending linearly and multiplicatively. Thus,
\[ g \circ h(x) = g(x + I) = f(x), \text{ and } g \text{ is unique because any map of algebras } U \to A \text{ is determined by where it sends a set of generators, in this case, } \{x + I\}_{x \in \mathbb{g}} = T^1(\mathbb{g}). \]

The discussion before the proof justifies the notation \( U(\mathbb{g}) \) for the universal enveloping algebra of a Lie algebra \( \mathbb{g} \).

Let’s calculate some universal enveloping algebras for some specific Lie algebras.

**Example 2.3.** Let \( \mathbb{g} = \mathfrak{g}_m := k_L \), ie, \( \mathfrak{g}_m \) is a one dimensional \( k \) vector space with bracket given by the commutator in \( k \). Since \( \mathfrak{g}_m \) is one dimensional, it is necessarily abelian. Hence the universal enveloping algebra is commutative.

We have implicitly defined two functors in the preceding pages. The functor \( U(\cdot) : \{\text{Lie algebras}\} \to \{\text{algebras}\} \) takes a Lie algebra to its universal enveloping algebra. The functor \( (\cdot)_L : \{\text{algebras}\} \to \{\text{Lie algebras}\} \) takes an algebra to its associated Lie algebra. Notice that the universal property states that any \( f \in \text{Hom}_{\text{Lie alg}}(\mathbb{g}, A_L) \) uniquely defines a \( g \in \text{Hom}_{\text{alg}}(U(\mathbb{g}), A) \). Conversely, any algebra map \( U(\mathbb{g}) \to A \) uniquely defines a map of Lie algebras \( \mathbb{g} \to A_L \). Hence there is a bijection between the Hom sets \( \text{Hom}_{\text{Lie alg}}(\mathbb{g}, A_L) \) and \( \text{Hom}_{\text{alg}}(U(\mathbb{g}), A) \) for any Lie algebra \( \mathbb{g} \) and algebra \( A \). Moreover, this bijection is natural with respect to \( \mathbb{g} \) and \( A \), meaning the correspondence of Hom sets is consistent with Lie algebra maps \( \mathbb{h} \to \mathbb{g} \) and algebra maps \( B \to A \). In other words, for all maps \( \mathbb{g} \to \mathbb{h}, B \to A \), the following diagram commutes:

\[
\begin{array}{ccc}
\text{Hom}_{\text{Lie alg}}(\mathbb{g}, A_L) & \cong & \text{Hom}_{\text{alg}}(U(\mathbb{g}), A) \\
\uparrow & & \uparrow \\
\text{Hom}_{\text{Lie alg}}(\mathbb{h}, B_L) & \cong & \text{Hom}_{\text{alg}}(U(\mathbb{h}), B)
\end{array}
\]

Here the vertical arrows are induced by the maps \( \mathbb{g} \to \mathbb{h}, \text{ and } B \to A \). To see why this is true, start in the bottom right with a map of algebras \( U(\mathbb{h}) \to B \). Moving left gives us a map of Lie algebras \( \mathbb{h} \to B_L \) induced by restriction. Moving up then yields a map of Lie algebras \( \mathbb{g} \to \mathbb{h} \to B_L \to A_L \). If we initially move up, we have the map of algebras \( U(\mathbb{g}) \to U(\mathbb{h}) \to B \to A \), and then moving left, we restrict to \( \mathbb{g} \to U(\mathbb{g}) \), yielding \( \mathbb{g} \to \mathbb{h} \to B_L \to A_L \).

Functors that give such a correspondence on Hom sets are called adjoint functors, and are now defined in greater generality.

**Definition 2.4.** Let \( \mathcal{C} \) and \( \mathcal{D} \) be two categories, and \( G : \mathcal{C} \to \mathcal{D} \) and \( F : \mathcal{D} \to \mathcal{C} \) be two functors. Suppose for all objects \( X \in \mathcal{C} \) and \( Y \in \mathcal{D} \) there is a natural bijection \( \text{Hom}_\mathcal{C}(F(Y), X) \leftrightarrow \text{Hom}_\mathcal{D}(Y, G(X)) \), ie, a bijection such that for all morphisms \( Y \to Y' \) and \( X' \to X \) the following diagram commutes:

\[
\begin{array}{ccc}
\text{Hom}_\mathcal{D}(Y, G(X)) & \cong & \text{Hom}_\mathcal{C}(F(Y), X) \\
\uparrow & & \uparrow \\
\text{Hom}_\mathcal{D}(Y', G(X')) & \cong & \text{Hom}_\mathcal{C}(F(Y'), X')
\end{array}
\]

Then \( F \) is called left adjoint to \( G \) and \( G \) is said to be right adjoint to \( F \).
In our definition of adjoint functors, we recover the case just discussed if $C$ is the category of algebras, $D$ is the category of Lie algebras, $F = U(\cdot)$ and $G = (\cdot)L$. Having sufficiently reviewed the universal enveloping algebra of a Lie algebra, we now define the restricted enveloping algebra of a restricted Lie algebra. To do so, we need the notion of a map of restricted Lie algebras.

**Definition 2.5.** Let $g$ and $h$ be restricted Lie algebras. A $k$-linear map $f : g \to h$ is a homomorphism of restricted Lie algebras if:
\[ f([x, y]) = [f(x), f(y)] \quad \text{and} \]
\[ f(x^{[p]}) = f(x)^{[p]} \]
for all $x, y \in g$.

This is the clear definition of a homomorphism in any category respecting the algebraic structure. We now define the restricted enveloping algebra analogously to how we defined the universal enveloping algebra, through a universal property. As above, we will show if it exists, the restricted enveloping algebra is unique up to unique isomorphism, and we will construct it as a quotient of the universal enveloping algebra.

**Definition 2.6.** Let $g$ be a restricted Lie algebra. The restricted enveloping algebra of $g$ is an algebra $u$ together with a map of restricted Lie algebras $h : g \to u_L$ satisfying the following universal property: given any algebra $A$ and any map of restricted Lie algebras $f : g \to A_L$, there exists a unique map of algebras $g : u \to A$ such that $f = g \circ h$.

**Theorem 2.7.** The restricted enveloping algebra of a restricted Lie algebra $g$ exists, and is unique up to unique isomorphism.

**Proof.** The proof of uniqueness is no different than that for the universal enveloping algebra. To construct the restricted enveloping algebra, let $J \subset U(g)$ be the two-sided ideal generated by elements of the form $x \otimes x \otimes \ldots \otimes x - x^{[p]} + I$, where the tensor occurs $p$ times. Let $u = U(g)/J$. We can still think of $g$ as sitting inside of $u$ by sending $x \in g$ to the element $(x + I) + J \in u$. Notice that this embedding induces a map of restricted Lie algebras $h : g \to u_L$ precisely because quotienting by $J$ forces the $p$-operation in $u_L$ to agree with that of $g$ inside of $u_L$. We show that the pair $(u, h)$ satisfy the universal property described above.

Suppose $A$ is an algebra, and $f : g \to A_L$ is a map of restricted Lie algebras. Define a map of algebras $g : u \to A$ by mapping $(x + I) + J$ to $f(x)$ and extending linearly and multiplicatively. Thus, $g \circ h(x) = g((x + I) + J) = f(x)$, and $g$ is unique because any map of algebras $u \to A$ is determined by where it sends a set of generators, in this case, $\{(x + I) + J\}_{x \in g \to u}$.

Again, by uniqueness, we may use the notation $u(g)$ when speaking of the restricted enveloping algebra associated to $g$.

### 3. Representations

Before moving on to our desired discussion of the connection between restricted Lie algebras and height 1 infinitesimal group schemes, it makes sense that we discuss representations of Lie algebras and restricted Lie algebras, having just spent a considerable amount of time developing the concept of enveloping algebras.
Definition 3.1. Let \( \mathfrak{g} \) be a Lie algebra. A representation of \( \mathfrak{g} \) is a map of Lie algebras \( \rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V) \) where \( V \) is a \( k \) vector space. If \( \mathfrak{g} \) is a restricted Lie algebra, then a representation of \( \mathfrak{g} \) is a map of restricted Lie algebras \( \rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V) \) where the \( p \)-operation in \( \mathfrak{gl}(V) \) is given by \( p^th \)-powers of matrices.

We now show that a representation of \( \mathfrak{g} \) is equivalent to a module over the appropriate enveloping algebra. Working with modules is often easier than working with maps of Lie algebras, so this correspondence is quite useful.

Theorem 3.2. A representation of a (restricted) Lie algebra \( \mathfrak{g} \) defines a \( \mathfrak{u}(\mathfrak{g}) \)-module structure on \( V \). Similarly, a \( \mathfrak{u}(\mathfrak{g}) \)-module \( V \) defines a representation of \( \mathfrak{g} \).

Proof. We start with the case of a Lie algebra \( \mathfrak{g} \). Let \( \rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V) \) be a representation. Define a \( \mathfrak{u}(\mathfrak{g}) \)-module structure on \( V \) by \( x \cdot v := \rho(x)v \) for all \( x \in \mathfrak{g} \rightarrow \mathfrak{gl}(V) \) and all \( v \in V \), and extend multiplicatively and linearly. To show that this scalar multiplication is well-defined, we must show that \( x \otimes y - y \otimes x \) and \( [x, y] \) in \( \mathfrak{u}(\mathfrak{g}) \) yield the same action on \( v \) for all \( x, y \in \mathfrak{g} \). This follows from the fact that \( \rho \) is a map of Lie algebras, and that the bracket in \( \mathfrak{gl}(V) \) is given by commutation. Now suppose we are given a \( \mathfrak{u}(\mathfrak{g}) \)-module \( V \). Define a map \( \rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V) \) by \( \rho(x)v := x \cdot v \). Linearity follows from the module structure, and \( \rho \) preserves the bracket because \( x \otimes y - y \otimes x = [x, y] \) in \( \mathfrak{u}(\mathfrak{g}) \). For the case of restricted Lie algebras, everything from above holds, with one extra step to deal with the \( p \)-operation. The details are nearly identical to how we dealt with the bracket.

Example 3.3. Let \( \mathfrak{g} \) be a restricted Lie algebra. Consider the map:

\[
\rho : \mathfrak{g} \rightarrow \mathfrak{gl}(\mathfrak{g})
\]

\[
x \mapsto \text{ad}_x
\]

We check that this is indeed a map of restricted Lie algebras. Linearity follows from that of the bracket. The Jacobi identity shows that the above map is a map of Lie algebras (ie, the bracket is preserved). Since restricted Lie algebras satisfy \( \text{ad}_x[p] = \text{ad}_x^2 \), the above map also preserves the \( p \)-operation. Hence we have a representation of \( \mathfrak{g} \) called the adjoint representation. Notice that if we forget the \( p \)-operation, we still have a representation of a Lie algebra.

4. Hopf Algebra Structure

5. Infinitesimal Groups Schemes of Height 1

In this section we would like to establish an equivalence of categories between height 1 infinitesimal group schemes \( G \) and finite-dimensional restricted Lie algebras \( \mathfrak{g} \). Let \( \mathcal{C} \) be the category of height 1 infinitesimal group schemes, and let \( \mathcal{D} \) be the category of restricted Lie algebras. We begin by defining a functor \( E : \mathcal{C} \rightarrow \mathcal{D} \).

Let \( G \in \mathcal{C} \). There are many ways to define \( E \), and all such are naturally isomorphic. We take the view of \( k \)-linear \( \epsilon \)-derivations, ie, \( E(G) := \text{Der}(k[G], k) \), where for a commutative ring \( R \) and an \( R \)-module \( M \), \( \text{Der}(R, M) \) is all \( k \)-linear maps satisfying \( f(rs) = rf(s) + sf(r) \) for all \( r, s \in R \). Here we view \( k \) as a \( k[G] \)-module via the augmentation map \( \epsilon \). To give \( \text{Der}(k[G], k) \) the structure of a restricted Lie algebra, first notice that \( \text{Der}(k[G], k) \) is a \( k \)-space via pointwise addition and scalar multiplication. Turn \( \text{Der}(k[G], k) \) into a unital, associative \( k \)-algebra by defining a multiplication as follows: \( f * g := (f \otimes g) \circ \Delta \). It can be shown
that $\text{Der}(k[G], k)$ is closed under this multiplication. Having defined an algebra structure on $\text{Der}(k[G], k)$, we can now make it a restricted Lie algebra as in § 1 by defining the bracket to be the commutator and the $p$-operation to be $p^\text{th}$-powers.

Now we construct a functor $F : \mathcal{D} \to \mathcal{C}$. Let $g \in \mathcal{D}$. Then as shown previously, $u(g)^*$ is a local, commutative Hopf algebra, satisfying $x^p = 0$ for all $x \in \mathfrak{m}$ where $\mathfrak{m}$ is the unique maximal ideal in $u(g)^*$. Hence, $g$ defines a height one infinitesimal group scheme $G_g := \text{Hom}_{k\text{-alg}}(u(g)^*, \Box)$. Let $\phi : g \to \mathfrak{h}$ be a map of restricted Lie algebras.

We make explicit a number of computations to further clarify the above equivalence.

**Example 5.1.** Let $G = \mathbb{G}_{a(1)}$, the first Frobenius kernel of $\mathbb{G}_a$. Then $k[G] = \mathbb{G}_{a(1)} \cong k[T]/T^p$, where $T$ is a primitive element in the Hopf algebra structure. Using the properties of a $k$-linear $\epsilon$ derivation, it can be shown that in this case, if $f \in \text{Der}(k[G], k)$, then $f(a_0 + a_1 T + \ldots + a_{p-1} T^{p-1}) = a_1 f(T)$, and is thus completely determined by where it maps $T$. Thus, $\text{Der}(k[G], k)$ is a one-dimensional $k$-algebra. Now suppose $f(T) = a$ and $g(T) = b$ for $f, g \in \text{Der}(k[G], k)$. Then $(f * g)(T) = a + b$ so that both the bracket and $p$-operation are trivial. Hence we see that $E(G) = g_a$. In the other direction, let’s consider the trivial restricted Lie algebra, $g_a$, a one-dimensional (necessarily abelian) Lie algebra with trivial $p$-operation, i.e., $x^p = 0$ for all $x \in g_a$. I claim that the height one group scheme corresponding to $g_a$ is $\mathbb{G}_{a(1)}$, the first Frobenius kernel of $\mathbb{G}_a$. We have that $k[\mathbb{G}_{a(1)}] \cong k[T]/(T^p) \cong k\mathbb{G}_{m,(1)}$, ie, $k[T]/(T^p)$ is self-dual. The claim is a result of the computation of the restricted enveloping algebra of $g_a$ done above, which is $k[T]/(T^p)$.

**Example 5.2.** Generalizing the previous example, let us consider $g_m^{\otimes r}$, the $r$-dimensional trivial restricted Lie-algebra. $u(g_m^{\otimes r}) = k[x_1, \ldots, x_r]/(x_1^p, \ldots, x_r^p)$ as was shown above, and since this Hopf algebra is also self dual, we are looking for a height one group scheme whose coordinate algebra is $k[x_1, \ldots, x_r]/(x_1^p, \ldots, x_r^p)$. The desired group scheme is $\mathbb{G}^{x_r}_{a,(1)}$.

**Example 5.3.** Let $g = g_m := k_L$, ie, $g_m$ is a one dimensional $k$ vector space with bracket and $p$-operation given by commutator and $p^\text{th}$ powers respectively. The calculation of $u(g_m)$ was done above, yielding the result $u(g_m) \cong k[x]/(x^p - x)$. I claim that the height one group scheme corresponding to $g_m$ is $\mathbb{G}_{m,(1)}$, the first Frobenius kernel of $\mathbb{G}_m$. We have that $k[\mathbb{G}_{m,(1)}] \cong k[T]/(T^p - 1)$ and $k\mathbb{G}_{m,(1)} \cong k^{p/(p^2)}$ so to prove the claim, it suffices to exhibit a Hopf algebra isomorphism $f : k[x]/(x^p - x) \to k^{p/(p^2)}$. The appropriate map is given by $x \mapsto \sum_{i=1}^{p-1} i e_i$. Since algebra maps preserve multiplicative identities, we must have $1 \mapsto \sum_{i=0}^{p-1} e_i$.

Extending this map multiplicatively, we see that $x^n \mapsto \sum_{i=1}^{p-1} i^ne_i$ because the $e_i$ are mutually orthogonal idempotents. That $x^n - x$ maps to zero is a result of Fermat’s little theorem. It can also be shown that $f$ preserves the counit, comultiplication, and the antipode.

If we let $\{1, x, x^2, \ldots, x^{p-1}\}$ and $\{e_0, e_1, e_2, \ldots, e_{p-1}\}$ be ordered bases for $k[x]/(x^p - x)$ and $k^{p/(p^2)}$ respectively, then the matrix of $f$, viewed as a linear transformation is given by:
where the entries are to be reduced mod $p$. This matrix has a non-zero determinant because it has the same determinant as its $p - 1 \times p - 1$ Vandermonde sub-matrix excluding the first row and column. This sub-matrix has non-zero determinant because each row is generated by powers of the distinct numbers $1, 2, 3, ..., p - 1$. Thus, the matrix is invertible and $f$ is an isomorphism. The inverse is given by the following matrix:

\begin{equation}
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & -1 & -2 & -3 & -4 & \ldots & -(p - 1)^2 \\
0 & -1 & -2 & -3 & -4 & \ldots & -(p - 1)^3 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & -1 & -2 & -3 & -4 & \ldots & -(p - 1) \\
-1 & -1 & -1 & -1 & -1 & \ldots & -1 \\
\end{pmatrix}
\end{equation}

I’ve written the matrices with entries that suggest the pattern involved, neglecting to reduce mod $p$. Here I write out the matrices for the case $p = 5$, reducing the entries appropriately:

\begin{equation}
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 3 & 1 \\
1 & 3 & 4 & 2 & 1 \\
1 & 4 & 1 & 4 & 1 \\
\end{pmatrix} \quad \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 4 & 2 & 3 & 1 \\
0 & 4 & 1 & 1 & 4 \\
0 & 4 & 3 & 2 & 1 \\
4 & 4 & 4 & 4 & 4 \\
\end{pmatrix}
\end{equation}

Notice that $f^{-1}$ gives a system of $p$ mutually orthogonal idempotents in the $k[x]/(x^p - x)$ as the images of the $e_i$, a nontrivial result. To be explicit, we have:

\begin{equation}
e_0 \mapsto 1 - x^{p-1} \quad e_n \mapsto - \sum_{i=1}^{p-1} n^{i-1} x^{p-i} \quad n = 1, 2, ..., p - 1
\end{equation}

**Example 5.4.** Combining the previous examples, we see that if $\mathfrak{g} = \mathfrak{g}_{m,1}^{\otimes r}$, then $G_{\mathfrak{g}} = \mathbb{G}_{m,1}^{\times r}$.

**Example 5.5.** In this example we would like to make explicit the result suggested by notation, that is, that the restricted Lie algebras $\mathfrak{gl}_n$ and $\mathfrak{sl}_n$ correspond to the height one groups schemes $GL_{n,(1)}$ and $SL_{n,(1)}$ respectively. Here $k[GL_{n,(1)}] \cong k[x_{ij}]/(x_{ij} - \delta_{ij})$ and $k[SL_{n,(1)}] \cong k[GL_{n,(1)}]/(x_{ij} - \delta_{ij})$.