TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 355, Number 8, Pages 3291–3300
S 0002-9947(03)03314-2
Article electronically published on April 17, 2003

ON IDEMPOTENTS IN REDUCED ENVELOPING ALGEBRAS

GEORGE B. SELIGMAN

Abstract. Explicit constructions are given for idempotents that generate all projective indecomposable modules for certain finite-dimensional quotients of the universal enveloping algebra of the Lie algebra $s\ell(2)$ in odd prime characteristic. The program is put in a general context, although constructions are only carried through in the case of $s\ell(2)$.

§1. Introduction

We consider the Lie algebra $s\ell(2)$ with basis e, f, h, relations $[ef] = h$, $[eh] = 2e, [fh] = -2f$. A reduced enveloping algebra for the Lie algebra $\mathfrak{g} = s\ell(2)$ over a field F, assumed algebraically closed and of odd prime characteristic p, is determined by three parameters $\lambda, \mu, \nu \in F$. It is the algebra $\mathfrak{A}$ defined as the quotient of the universal enveloping algebra $\mathfrak{U} = \mathfrak{U}(s\ell(2))$ by the ideal generated by the (central) elements $h^p - h - \lambda$, $e^p - \mu$, $f^p - \nu$ of $\mathfrak{U}$. The dimension of $\mathfrak{A}$ is p^3. We identify e, f, h with their images in $\mathfrak{A}$ whenever there is no great danger of confusion.

The subalgebra $F[h]$ of $\mathfrak{A}$ is semisimple; since the minimum polynomial $X^p - X - \lambda$ of h factors as $\prod_{\alpha \in \mathbf{F}_p} (X - \tau - \alpha)$, where $\tau \in F$ is fixed with $\tau^p - \tau = \lambda$ (we fix $\tau = 0$ if $\lambda = 0$), we let $g_\alpha(X) = \frac{X^p - X - \lambda}{X - \tau - \alpha}$ for each $\alpha \in \mathbf{F}_p$. Then $h(\alpha) = g_\alpha(\tau + \alpha)^{-1} g_\alpha(h)$ is a nonzero idempotent in $F[h]$, and these $h(\alpha)$ form a complete system of orthogonal idempotents in $F[h]$: $h(\alpha)h(\beta) = 0$ if $\alpha \neq \beta$, $\sum_{\alpha \in \mathbf{F}_p} h(\alpha) = 1$, $h(\alpha)h = (\tau + \alpha)h(\alpha)$. A generalization in the case of the restricted enveloping algebra, yielding a complete set of idempotents in the enveloping algebra of a Cartan subalgebra, was given by Nielsen [N] in 1963. In that thesis, Nielsen also gives generators for minimal one-sided ideals in the restricted enveloping algebra of $\mathfrak{sl}(2)$.

We propose to refine this set of idempotents to a complete set of primitive idempotents in $\mathfrak{A}$. We work in the commutative subalgebra of $\mathfrak{A}$ generated by h and ef, and in the commutative subalgebra $\mathfrak{W}$ of $\mathfrak{U}$ generated by h, ef, e^p and f^p. (The subalgebra $\mathfrak{W}$ will only be involved in §5, where we shall recall that certain elements of $\mathfrak{W}$ satisfy relations, such as belonging to the ideal $\mathfrak{J}$ in $\mathfrak{W}$ generated by $e^p - \mu, f^p - \nu, h^p - h - \lambda$. For example, the elements $h^*(\alpha) = g_\alpha(\tau + \alpha)^{-1} g_\alpha(h)$, now regarded as elements of $\mathfrak{W}$, still satisfy $\sum_{\alpha \in \mathbf{F}_p} h^*(\alpha) = 1 \in \mathfrak{W}$, with $h^*(\alpha)h^*(\beta) - \delta_{\alpha_\beta} h^*(\beta)$ in the ideal in $\mathfrak{W}$ generated by $h^p - h - \lambda$, as is $h^*(\alpha)h - (\tau + \alpha)h^*(\alpha)$.)

Received by the editors August 14, 2002 and, in revised form, January 15, 2003.
2000 *Mathematics Subject Classification.* Primary 17B35, 16S30.

©2003 American Mathematical Society

The key to the construction is the following observation, easily proved by induction:

Lemma 1. *For any set of i or more indeterminates $X_1, \dots, X_k$, let $s_i[X_1, \dots, X_k]$ be the i-th elementary symmetric function* ($s_0 = 1$). *Then for every positive integer j, and each $\alpha \in \mathbf{F}_p$,*

$$(1)\quad h(\alpha)e^j f^j = \sum_{k=0}^{j-1} s_k(\alpha+\tau+2, 2(\alpha+\tau+3), \dots, (j-1)(\alpha+\tau+j))(h(\alpha)ef)^{j-k}.$$

We indicate a proof, with $h(\alpha)$ replaced by $h^*(\alpha)$, and working in $\mathfrak{U}$, that both sides of the relation are in $\mathfrak{W}$ and are congruent modulo the ideal in $\mathfrak{W}$ as above. The relation in $\mathfrak{A}$ then follows. For $j = 1$, there is nothing to prove. If one writes

$$h^*(\alpha)e^{j+1}f^{j+1} = h^*(\alpha)e^j f^j ef + \sum_{k=0}^{j} h^*(\alpha)e^j f^k[ef]f^{j-k}$$

and uses

$$[ef] = h, h^*(\alpha)e^j f^k h f^{j-k} = h^*(\alpha)he^j f^j + 2(j-k)h^*(\alpha)e^j f^j,$$

one deduces inductively that all $h^*(\alpha)e^m f^m$ are in $\mathfrak{W}$. Furthermore, all $e^m f^m$ are in $\mathfrak{W}$, so that $h^*(\alpha)he^j f^j$ is congruent, modulo our ideal $\mathfrak{J}$ in $\mathfrak{W}$, to $(\tau+\alpha)h^*(\alpha)e^j f^j$. Thus

$$h^*(\alpha)e^{j+1}f^{j+1} \equiv h^*(\alpha)e^j f^j ef + j(\alpha+\tau+j+1)h^*(\alpha)e^j f^j (\operatorname{mod} \mathfrak{J}),$$

giving the necessary inductive step. When $j = p$ (still working in $\mathfrak{W}$), we have $h^*(\alpha)e^p f^p \equiv \mu\nu h^*(\alpha)(\operatorname{mod} \mathfrak{J})$. If $b \in h^*(\alpha)\mathfrak{W}$, then $h^*(\alpha)b \equiv b(\operatorname{mod} \mathfrak{J})$, so that

$$\mu\nu h^*(\alpha) \equiv \sum_{k=0}^{p-1} s_k(\tau+\alpha+2, 2(\tau+\alpha+3), \dots, (p-1)(\tau+\alpha+p))(h^*(\alpha)ef)^{p-k} \quad (\operatorname{mod} \mathfrak{J}).$$

In the homomorphic image in $\mathfrak{A}$ of $\mathfrak{W}$, the image $h(\alpha)$ of $h^*(\alpha)$ is the unit element for the ideal it generates, and the element $h(\alpha)ef$ of this ideal satisfies the polynomial equation $f(X) = 0$ relative to the unit element $h(\alpha)$, where

$$f(X) = \prod_{\alpha \in \mathbf{F}_p} (X + i(\tau+\alpha+i+1)) - \mu\nu.$$

Changing the variable here to $Y = X - (\frac{\tau+\alpha+1}{2})^2$, we have

$$f(X) = g(Y) = \prod_{i \in \mathbf{F}_p} (Y + ((\frac{\tau+\alpha+1}{2}) + i)^2) - \mu\nu.$$

Now it is a straightforward exercise to verify that, for indeterminates Y and Z over $\mathbf{F}_p$,

$$\prod_{i \in \mathbf{F}_p} (Y + (i+Z)^2) = Y(Y^{\frac{p-1}{2}} + (-1)^{\frac{p+1}{2}})^2 + (Z^p - Z)^2.$$

Thus

$$(2)\quad \begin{aligned} g(Y) &= Y(Y^{\frac{p-1}{2}} + (-1)^{\frac{p+1}{2}})^2 + (\frac{\tau^p - \tau}{2})^2 - \mu\nu \\ &= Y(Y^{\frac{p-1}{2}} + (-1)^{\frac{p+1}{2}})^2 + (\frac{\lambda^2}{4} - \mu\nu). \end{aligned}$$

Here $g'(Y) = (-1)^{\frac{p+1}{2}} Y^{\frac{p-1}{2}} + 1$, so $g(Y)$ is semisimple if and only if no element $-\beta^2$ $(0 \neq \beta \in \mathbf{F}_p)$ is a root of $g(Y)$. One easily checks that

$$g(-\beta^2) = -\beta^2 + 2\beta^2 - \beta^2 + \tfrac{1}{4}\lambda^2 - \mu\nu = \tfrac{1}{4}\lambda^2 - \mu\nu.$$

That is, $g(Y)$ has repeated roots if and only if $\lambda^2 = 4\mu\nu$. We refer to $\lambda^2 - 4\mu\nu$ as the discriminant of $\mathfrak{A}$.

§2. The Semisimple Case

When the discriminant is nonzero, $f(X)$ has p distinct roots $\theta_1, \dots, \theta_p$. Lagrange interpolation may be applied once more to obtain $h(\alpha)$ (or $h^*(\alpha)$, modulo $\mathfrak{J}$) as a sum of p elements in $F[h(\alpha), h(\alpha)ef]$ that are nonzero orthogonal idempotents (with the same holding with $h(\alpha)$ replaced by $h^*(\alpha)$, if we work in $\mathfrak{W}$, modulo $\mathfrak{J}$). As α runs over $\mathbf{F}_p$, one obtains p^2 orthogonal idempotents in $\mathfrak{A}$, with sum 1. Typical for these is an element $E(\alpha, \theta_i) = h(\alpha)q(h(\alpha)ef)$, where $q(X)$ is a polynomial of degree $p-1$, depending on α and θ_i, with $E(\alpha, \theta_i)h(\alpha)ef = \theta_i E(\alpha, \theta_i)$ in $\mathfrak{A}$ (or with a corresponding congruence in $\mathfrak{W}$, modulo $\mathfrak{J}$).

Under these circumstances, it is easy to see that every irreducible $\mathfrak{A}$-module $\mathfrak{M}$ has dimension at least (indeed, equal to) p: If one of μ, ν is nonzero and if v is an eigenvector for h in $\mathfrak{M}$, then so are all ve^k, vf^k, and one of these families yields eigenvectors for p distinct eigenvalues. If $\mu = 0 = \nu, vh = \kappa v$, we may assume $ve = 0$. Then the usual treatment of $s\ell(2)$-modules shows that if the first integer $k > 0$ with $vf^k = 0$ is less than p, then $\kappa \in \mathbf{F}_p$ and $\lambda = 0$, a contradiction. Thus all $vf^k, 0 \leq k \leq p$, are linearly independent. (More detail on irreducible modules will be needed below; for a more thorough and extensive study of irreducible modules in all reductive cases, see [JCJ].)

It follows that the right ideals $E(\alpha, \theta_i)\mathfrak{A}$ have dimension at least p. But there are p^2 such ideals, and the algebra $\mathfrak{A}$, of dimension p^3, is their direct sum. Thus each $E(\alpha, \theta_i)\mathfrak{A}$ is a minimal right ideal in $\mathfrak{A}$, and $\mathfrak{A}$ is a semisimple algebra. From general principles, the modules $E(\alpha, \theta_i)\mathfrak{A}$ group into p blocks, each consisting of p isomorphic $\mathfrak{A}$-modules. We determine conditions for isomorphism in terms of the parameters α and θ_i.

First, the promised details on irreducible $\mathfrak{A}$-modules: If $\mathfrak{M}$ is such a module, then h and ef commute in their actions, so have a common eigenvector v. As above, if $\mu \neq 0$ or $\nu \neq 0$, then all ve^j or all vf^j, $0 \leq j < p$ are linearly independent. One readily verifies that their span is stable under the action of e, f, h, so is equal to $\mathfrak{M}$. If $\mu = \nu = 0$, then $ve^r \neq 0, ve^{r+1} = 0$ for some $r, 0 \leq r < p$. Let $w = ve^r$. Then $w, wf, \dots, wf^{p-1}$ form a basis for $\mathfrak{M}$. Having fixed τ (necessarily an eigenvalue of h), the eigenvalue of ef to which a τ-eigenvector for h belongs determines $\mathfrak{M}$ up to isomorphism.

In the present case, $E(\alpha, \theta)ef = E(\alpha, \theta)h(\alpha)ef = \theta E(\alpha, \theta)$, and there is some e^j or f^k (possibly both) with $E(\alpha, \theta)e^j$ or $E(\alpha, \theta)f^k$ an h-eigenvector of eigenvalue τ. The commutation relations then yield that the corresponding eigenvalue of ef is $\theta - \frac{\alpha}{2}(\tau + \frac{\alpha}{2} + 1)$. (Independently of whether we use $E(\alpha, \theta)ef$ or $E(\alpha, \theta)f^k$; for instance, if $0 \neq E(\alpha, \theta)f^k$ is an h-eigenvector belonging to the h-eigenvalue τ, then $2k = \alpha$ [in $\mathbf{F}_p$], and, inductively on m, $E(\alpha, \theta)f^m ef = (\theta - m\tau - m\alpha + m(m-1))E(\alpha, \theta)f^m$.)

Accordingly, we have $E(\alpha,\theta)\mathfrak{A} \cong E(\beta,\theta')\mathfrak{A}$ if and only if

$$\theta - \frac{\alpha}{2}(\tau + \frac{\alpha}{2} + 1) = \theta' - \frac{\beta}{2}(\tau + \frac{\beta}{2} + 1). \tag{3}$$

It may help to clarify this statement by noting that if θ is a root of $f(X) = \prod_{i \in \mathbf{F}_p} (X + i(\tau + \alpha + i + 1)) - \mu\nu$ as before, and if we make the change of variable

$$X = X' + \frac{\alpha}{2}(\tau + \frac{\alpha}{2} + 1) - \frac{\beta}{2}(\tau + \frac{\beta}{2} + 1),$$

then

$$\begin{aligned} f(X) = f^*(X') &= \prod_{i \in \mathbf{F}_p} (X' + (i + \frac{\alpha}{2} - \frac{\beta}{2})(\tau + \beta + (i + \frac{\alpha}{2} - \frac{\beta}{2}) + 1)) - \mu\nu \\ &= \prod_{j \in \mathbf{F}_p} (X' + j(\tau + \beta + j + 1)) - \mu\nu, \end{aligned}$$

so that $\theta' = \theta - \frac{\alpha}{2}(\tau + \frac{\alpha}{2} + 1) + \frac{\beta}{2}(\tau + \frac{\beta}{2} + 1)$ is a root of $f^*(X')$. For each $\beta \neq \alpha$ in $\mathbf{F}_p$, there is one such θ'. Thus, for given α, all $E(\alpha,\theta)\mathfrak{A}$ are non-isomorphic $\mathfrak{A}$-modules, while for each pair α, β ($\alpha \neq \beta$), the isomorphism classes of modules $E(\alpha,\theta)\mathfrak{A}$ and $E(\beta,\theta')\mathfrak{A}$ are the same when the relation (3) holds.

§3. The Degenerate, Non-restricted Case

When $\lambda^2 = 4\mu\nu$,

$$f(X) = (X - (\frac{\tau + \alpha + 1}{2})^2)((X - (\frac{\tau + \alpha + 1}{2})^2)^{\frac{p-1}{2}} + (-1)^{\frac{p+1}{2}})^2$$

(by (2)) is the minimum polynomial of $h(\alpha)ef$ relative to the unit element $h(\alpha)$. The roots in F of $Y^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}} = 0$ in F are the negatives of nonzero squares in $\mathbf{F}_p$. So

$$f(X) = (X - (\frac{\tau + \alpha + 1}{2})^2) \prod_{\gamma \in \mathbf{F}_p^{*2}} (X - (\frac{\tau + \alpha + 1}{2})^2 + \gamma)^2.$$

The following lemma, whose proof is left as an exercise, gives a resolution of each $h(\alpha)$ into orthogonal idempotents:

Lemma 2. *Let* $g_0(Y) = \prod_{\gamma \in \mathbf{F}_p^{*2}} (Y + \gamma)^2$, *and, for* $\beta \in \mathbf{F}_p^{*2}$, *let* $g_\beta(Y) = 2Y(Y - \beta) \prod_{\substack{\gamma \in \mathbf{F}_p^{*2} \\ \gamma \neq \beta}} (Y + \gamma)^2$. *Then*

$$g_0(Y) + \sum_{\beta \in \mathbf{F}_p^{*2}} g_\beta(Y) = 1, \text{ and} \tag{4}$$

$$g_\xi(Y) g_\eta(Y) \equiv \delta_{\xi\eta} g_\eta(Y) (\text{mod } f(Y + (\frac{\tau + \alpha + 1}{2})^2) = g(Y)).$$

It follows that the elements $E(\alpha, 0) = f_0(h(\alpha)ef)$, $E(\alpha, \beta) = f_\beta(h(\alpha)ef)$, where $f_\gamma(X) = g_\gamma(X - (\frac{\tau+\alpha+1}{2})^2)$, form a set of $\frac{p+1}{2}$ (nonzero) orthogonal idempotents in $F[h(\alpha), h(\alpha)ef] \subset \mathfrak{A}$, whose sum is the unit element $h(\alpha)$. (When $h(\alpha)$ is replaced by $h^*(\alpha)$, the corresponding relations hold $(\text{mod}\, \mathfrak{J})$ in the subalgebra $f[h^*(\alpha), h^*(\alpha)ef]$ of the commutative subalgebra $\mathfrak{W}$ of $\mathfrak{U}(\mathfrak{g})$.) As α runs over $\mathbf{F}_p$, we obtain a family of $\frac{p(p+1)}{2}$ orthogonal idempotents $E(\alpha,\beta)$ in $F[h,ef]\subset\mathfrak{A}$, whose sum is 1.

To see that these idempotents are *primitive*, one may reason as follows: Each $E(\alpha,0),\alpha\in\mathbf{F}_p$, generates a nonzero right $\mathfrak{A}$-module. If we assume not all of λ,μ,ν are 0, then as before, this module has dimension at least p, and dimension exactly p if and only if it is irreducible. *We defer the "restricted" case $\lambda=\mu=\nu=0$ to the next section.* When $\beta\in\mathbf{F}_p^{*2}$, left-multiplication by $h(\alpha)ef-(\frac{\tau+\alpha+1}{2})^2h(\alpha)+\beta h(\alpha)$ is a nonzero nilpotent $\mathfrak{A}$-endomorphism of $E(\alpha,\beta)\mathfrak{A}$ whose image lies in its kernel, and where each of the kernel and cokernel has dimension at least p. Thus $E(\alpha,\beta)\mathfrak{A}$ has dimension at least $2p$, and the dimension is exactly $2p$ only if both the image and kernel are irreducible. In that case the endomorphism above induces an isomorphism of the cokernel onto the kernel. The sum of the dimensions of all $E(\alpha,\beta)\mathfrak{A}$ is thus at least $p^2+p\cdot\frac{p-1}{2}\cdot 2p=p^3=\dim\mathfrak{A}$, with equality if and only if each $E(\alpha,0)\mathfrak{A}$ is irreducible and each $E(\alpha,\beta)\mathfrak{A},\beta\in\mathbf{F}_p^{*2}$ has dimension $2p$. From the above, the latter modules are indecomposable. We have the

Theorem 1. *If $\lambda^2=4\mu\nu$, not all of λ,μ,ν being equal to zero, fix a solution τ of $X^p-X-\lambda=0$, with $\tau=0$ if $\lambda=0$. Form elements $E(\alpha,\eta)$ for all $\eta\in\mathbf{F}_p^2$, $\alpha\in\mathbf{F}_p$, as above. Then these $\frac{p(p+1)}{2}$ elements of $F[h,ef]\subset\mathfrak{A}$ form a complete set of primitive idempotents in $\mathfrak{A}$. The right ideals $E(\alpha,0)\mathfrak{A}$ are isomorphic irreducible $\mathfrak{A}$-modules. The right ideals $E(\alpha,\beta)\mathfrak{A},\beta\in\mathbf{F}_p^{*2}$, are (projective) indecomposable $\mathfrak{A}$-modules of length 2, each with isomorphic composition factors. Two modules $E(\alpha,\eta)\mathfrak{A}$ and $E(\alpha',\eta')\mathfrak{A}$ are isomorphic if and only if $\eta=\eta'$.*

Proof. Only the assertions about isomorphisms remain to be proved. Here we may assume $\mu\neq 0$; the argument for $\nu\neq 0$ is analogous, and both cannot be zero because $\lambda^2=4\mu\nu$. (Some isomorphisms, e.g., those of all $E(\alpha,0)\mathfrak{A}$, follow from general theory, but our identification gives a little more detail.)

An element of the irreducible module $E(\alpha,0)\mathfrak{A}$ of h-eigenvalue τ is $E(\alpha,0)e^j$, where $2j$ represents $-\alpha(\bmod p)$, and

$$E(\alpha,0)e^jef=((\frac{\tau+\alpha+1}{2})^2+j(\tau+\alpha+j+1))E(\alpha,0)e^j.$$

But $j(\tau+\alpha+j+1)=-\frac{\alpha}{2}(\tau+\alpha-\frac{\alpha}{2}+1)$, so that $(\frac{\tau+\alpha+1}{2})^2+j(\tau+\alpha+j+1)=(\frac{\tau+1}{2})^2$, *independent of* α. Thus all $E(\alpha,0)\mathfrak{A}$ are isomorphic.

Similarly, the quotient of $E(\alpha,\beta)\mathfrak{A}$, for $\beta\in\mathbf{F}_p^{*2}$, by its unique maximal submodule has as h-eigenvector of eigenvalue τ the coset of $E(\alpha,\beta)e^j, 2j=-\alpha$ as above, and

$$E(\alpha,\beta)e^jef\equiv(-\beta+(\frac{\tau+1}{2})^2)E(\alpha,\beta)e^j,$$

as before, here modulo the maximal submodule. By [C-R], Theorem 54.11, if $\mathfrak{N}$ is the radical of $\mathfrak{A}, E(\alpha,\beta)\mathfrak{N}$ is the unique maximal submodule of $E(\alpha,\beta)\mathfrak{A}$, and $E(\alpha,\beta)\mathfrak{A}$ and $E(\alpha',\beta')\mathfrak{A}$ are isomorphic if and only if

$$E(\alpha,\beta)\mathfrak{A}/E(\alpha,\beta)\mathfrak{N}\cong E(\alpha',\beta')\mathfrak{A}/E(\alpha',\beta')\mathfrak{N}.$$

We have just seen that this last isomorphism holds if and only if $\beta=\beta'$. This completes the proof. □

§4. The Restricted Case

Now let $\lambda = \mu = \nu = 0$. In this case, the projective indecomposable $\mathfrak{A}$-modules are more complicated, but their structure is well known (see [P]). There is the irreducible Steinberg module, generated by an element v with $ve = 0, vh = -v$, and basis $v, vf, \ldots, vf^{p-1}$; and there are $p-1$ modules, each of dimension $2p$ and length 4. We assign to the Steinberg module, "$\mathfrak{M}_{p-1}$", the parameter $p-1$, and parameters $0, \ldots, p-2$ to the remaining modules, as follows:

The module $\mathfrak{M}_k$ has generator u_k, with $u_k h = k u_k$. To give further relations, and for future reference, we define, for $\alpha \in \mathbf{F}_p$, $\operatorname{res}(\alpha)$ to be the ordinary integer $j, 0 \leq j < p$, whose residue class $(\operatorname{mod} p)$ is α. Now let $k' = p - 2 - k$ ($\neq k \operatorname{mod} p$) and let $r_k = \operatorname{res}(\frac{k'-k}{2})$. Let $v_{k'} = u_k e^{r_k}$.

Then $v_{k'} \neq 0$ but $v_{k'} e = 0$, and

$$v_{k'} f^{r_k - 1} = (-1)^{r_k - 1} (r_k - 1)!^2 u_k e.$$

A basis for $\mathfrak{M}_k$ consists of the elements $\{u_k f^i, v_{k'} f^i\}, 0 \leq i < p$. The unique maximal submodule of $\mathfrak{M}_k$ is $\langle v_{k'} \rangle + \langle u_k f^{k+1} \rangle$, of codimension $k+1$.

Here $\tau = 0$, and again, we have $\frac{p(p+1)}{2}$ orthogonal idempotents $E(\alpha, \beta)$ in $\mathfrak{A}$, given as in §3. The algebra $\mathfrak{A}$ is a Frobenius algebra [Ber], indeed a symmetric algebra [S]. So the multiplicity of $\mathfrak{M}_k$ as an indecomposable summand of $\mathfrak{A}$ is equal to the dimension of the quotient of $\mathfrak{M}_k$ by its maximal submodule, or $k+1$ ([C-R], Theorem 61.13). It follows that the number of indecomposable summands of $\mathfrak{A}$ is

$$p + \sum_{k=0}^{p-2} (k+1) = \frac{p(p+1)}{2},$$

and therefore that all our (nonzero) $\frac{p(p+1)}{2}$ orthogonal idempotents are primitive, and all $E(\alpha, \beta)\mathfrak{A}$ are indecomposable.

Theorem 2. *When $\lambda = \mu = \nu = 0$, all $E(\alpha, 0)\mathfrak{A}$ are isomorphic for $\alpha \in \mathbf{F}_p$, and are the (irreducible) Steinberg module $\mathfrak{M}_{p-1}$. For $1 \leq j \leq \frac{p-1}{2}$, the modules $E(\alpha, j^2)\mathfrak{A}$ are indecomposable, with $E(\alpha, j^2)\mathfrak{A}$ isomorphic to $\mathfrak{M}_{\operatorname{res}(-2j-1)}$ or $\mathfrak{M}_{2j-1}$, according as $j \leq \operatorname{res}(-\frac{\alpha+1}{2}) < p - j$, or not. The $E(\alpha, \beta)$, $\alpha \in \mathbf{F}_p, \beta \in \mathbf{F}_p^2$, are a complete set of primitive idempotents in $\mathfrak{A}$.*

Proof. The last assertion has been established. If r is minimal with $E(\alpha, 0)e^{r+1} = 0$, then

$$0 = E(\alpha, 0)e^{r+1} f = (\frac{\alpha + 2r + 1}{2})^2 E(\alpha, 0) e^r.$$

So $\alpha \equiv -2r - 1 (\operatorname{mod} p)$, and $w = E(\alpha, 0)e^r$ has $wh = -w, we = 0$. It follows that $w, wf, \ldots, wf^{p-1}$ form a basis for an irreducible submodule isomorphic to $\mathfrak{M}_{p-1}$, with

$$wf^r = E(\alpha, 0)e^r f^r = (r!)^2 E(\alpha, 0) \neq 0.$$

Thus $E(\alpha, 0)\mathfrak{A} = \langle w \rangle \cong \mathfrak{M}_{p-1}$. □

For $1 \leq j \leq \frac{p-1}{2}$, we know that $E(\alpha, j^2)\mathfrak{A} \cong \mathfrak{M}_k$ for some $k, 0 \leq k \leq p-2$, and that in any such isomorphism the element $E(\alpha, j^2)$ cannot correspond to a member of the proper submodule $\langle v_{k'} \rangle + \langle u_k f^{k+1} \rangle$ of $\mathfrak{M}_k$. Thus $E(\alpha, j^2)$ must correspond to an element $\xi v_{k'} f^s + \eta u_k f^t$ where $\eta \neq 0, t \leq k$ and both $k' - 2s$ and $k - 2t$ represent $\alpha (\operatorname{mod} p)$. From the last remark, we have that $k' - 2s$ equal to one of $k - 2t, k - 2t \pm p$. If $k' - 2s = k - 2t$, then $k' - k$ is even, contrary to $k + k' = p - 2$.

If $k'-2s = k-2t+p$, then $p-k-2-2s = k-2t+p$, $2t = 2k+2s+2$, and $t > k$, a contradiction. Thus $p-2-k-2s = k'-2s = k-2t-p$, $2t = 2s+2(k-p+1) < 2s$, and $t < s$.

Applying f^{p-1-t} to our expression corresponding to $E(\alpha, j^2)$ gives

$$E(\alpha, j^2)f^{p-1-t} = \varepsilon u_k f^{p-1} \neq 0.$$

That is, $u_k f^{p-1}$ belongs to the eigenvalue $\alpha - 2(p-1-t)$ of h, and is annihilated by f. Its eigenvalue is evidently equal to $k-2(p-1) \equiv -k'$; so $\alpha+2+2t = -k'$ in $\mathbf{F}_p$.

In other words, for the nonnegative integer m such that $E(\alpha, j^2)f^m \neq 0$, $E(\alpha, j^2)f^{m+1} = 0$ determines k' by $k' = \operatorname{res}(2m-\alpha)$, and thereby the isomorphism class of $E(\alpha, j^2)\mathfrak{A}$: $E(\alpha, j^2)\mathfrak{A} \cong \mathfrak{M}_k$, where $k = \operatorname{res}(\alpha-2m-2)$. To determine this "$m$", we invoke the following:

Lemma 3. *Let*

$$g_{j^2}(X) = 2(X-j^2)X \prod_{\substack{i=1 \\ i\neq j}}^{\frac{p-1}{2}} (X+i^2)^2, \quad 1 \leq j \leq \frac{p-1}{2}.$$

Let $n(\alpha, j)$ be the largest value of k such that $f_{\alpha,k}(X) = \prod_{i=0}^{k-1}(X+i(\alpha+i+1))$ divides $g_{j^2}(X-(\frac{\alpha+1}{2})^2)$. Then $E(\alpha, j^2)\mathfrak{A}$ is the projective indecomposable module $\mathfrak{M}_{\operatorname{res}(\alpha+2n(\alpha,j))}$.

Proof of Lemma 3. With $n(\alpha, j)$ as defined,

$$g_{j^2}(X-(\frac{\alpha+1}{2})^2) = h_j(X-(\frac{\alpha+1}{2})^2) f_{\alpha,n(\alpha,j)}(X),$$

where $h_j(X-(\frac{\alpha+1}{2})^2)$ is a product of factors involving only $X+k^2-(\frac{\alpha+1}{2})^2$, $1 \leq k \leq \frac{p-1}{2}$; $X-(\frac{\alpha-1}{2})^2$; and $X-j^2-(\frac{\alpha+1}{2})^2$. In $\mathfrak{A}$, we have therefore

$$\begin{aligned} E(\alpha, j^2) &= h_j(h(\alpha)ef - (\frac{\alpha+1}{2})^2 h(\alpha)) f_{\alpha,n(\alpha,j)}(h(\alpha)ef) \\ &= h_j(h(\alpha)ef - (\frac{\alpha+1}{2})^2 h(\alpha)) h(\alpha)e^{n(\alpha,j)} f^{n(\alpha,j)}, \end{aligned}$$

by Lemma 1. Now $h(\alpha)ef$ commutes with all $h(\alpha)e^k f^k$, and the proof of Lemma 1 involves showing that

$$h(\alpha)e^k f^k ef = h(\alpha)e^{k+1}f^{k+1} - k(\alpha+k+1)h(\alpha)e^k f^k.$$

Thus

$$E(\alpha, j^2) = h(\alpha)e^{n(\alpha,j)} f^{n(\alpha,j)} (h_j(h(\alpha)ef - (\frac{\alpha+1}{2})^2 h(\alpha)))$$

and

$$\begin{aligned} &h(\alpha)e^{n(\alpha,j)} f^{n(\alpha,j)} h(\alpha)ef \\ &= h(\alpha)e^{n(\alpha,j)+1} f^{n(\alpha,j)+1} - n(\alpha,j)(\alpha+n(\alpha+n(\alpha,j)+1)h(\alpha)e^{n(\alpha,j)} f^{n(\alpha,j)}. \end{aligned}$$

By definition, $X+n(\alpha,j)(\alpha+n(\alpha,j)+1)$ is not among the factors of $g_{j^2}(X-(\frac{\alpha+1}{2})^2)$. Thus the coefficient of $h(\alpha)e^{n(\alpha,j)} f^{n(\alpha,j)}$ will not be zero when $E(\alpha, j^2)$ is expanded in terms of the form $h(\alpha)e^i f^i$, while the other values of "i" that occur will all be greater than $n(\alpha, j)$. Accordingly, $E(\alpha, j^2)f^{p-n(\alpha,j)-1} \neq 0$ while $E(\alpha, j^2)f^{p-n(\alpha,j)} = 0$. The lemma is proved. □

To complete the proof of the theorem: Note that $n(\alpha, j)$ is the first integer n with $n(\alpha+n+1) = j^2 - (\frac{\alpha+1}{2})^2$; so $n(\alpha, j) \equiv -(\frac{\alpha+1}{2}) \pm j (\operatorname{mod} p)$. If $j \leq \operatorname{res}(-(\frac{\alpha+1}{2})) < p-j$, then $n(\alpha, j) = \operatorname{res}(-j - \frac{\alpha+1}{2})$; otherwise, $n(\alpha, j) = \operatorname{res}(j - \frac{\alpha+1}{2})$. The remaining assertion of the theorem follows.

Remark. For example, if $j = \frac{p-1}{2}$, only $\alpha = 0$ satisfies the inequalities $\frac{p-1}{2} \leq \operatorname{res}(-\frac{\alpha+1}{2})) < \frac{p+1}{2}$, and $\mathfrak{M}_{\operatorname{res}(-2j-1)} = \mathfrak{M}_0$ occurs only *once*, while $\mathfrak{M}_{2j-1} = \mathfrak{M}_{p-2}$ occurs with multiplicity $p-1$.

§5. Some Generalizations

The remarks of this section apply generally. The case where the underlying Lie algebra is $s\ell(2)$ will be observed, from earlier constructions, to satisfy the conditions imposed on the idempotents. Application to that case enables us to recover, in somewhat more explicit form, some results of Christopher Bendel [Ben].

Here $\mathfrak{g}$ is an arbitrary Lie algebra of prime characteristic and finite dimension over a field F, assumed algebraically closed (although further assumptions avoid this constraint). Let $x_1, \ldots, x_n$ be a basis for $\mathfrak{g}$. For each x_i, let z_i be a p-polynomial in x_i that is central in $\mathfrak{U}(\mathfrak{g})$, say of degree p^{m_i}. Fix scalars $\lambda_1, \ldots, \lambda_n \in F$ and a nonnegative integer s. Let $\mathfrak{S}$ be the ideal in $\mathfrak{U}(\mathfrak{g})$ generated by the (central) elements $T_i^{p^s}, 1 \leq i \leq n$, where $T_i = z_i - \lambda_i$. Let $\mathfrak{T}$ be the ideal generated by the T_i. Then $\mathfrak{B} = \mathfrak{U}(\mathfrak{g})/\mathfrak{S}$ and $\mathfrak{A} = \mathfrak{U}(\mathfrak{g})/\mathfrak{T}$ are finite-dimensional algebras over F, of respective dimensions $p^{ns+\sum m_i}$ and $p^{\sum m_i}$ ([J], Chapter 6).

Suppose we have found elements $e_1, \ldots, e_t \in \mathfrak{U}(\mathfrak{g})$ such that:

i) $\sum_{j=1}^{t} e_j = 1$ in $\mathfrak{U}(\mathfrak{g})$;

ii) there is a commutative subalgebra $\mathfrak{W}$ of $\mathfrak{U}(\mathfrak{g})$, containing all e_j's and all T_i's, such that for all j, k, $e_j e_k - \delta_{jk} e_k$ is in the ideal in $\mathfrak{W}$ generated by the T_i.

These conditions guarantee that the homomorphic images $\bar{e}_j$ of the e_j in $\mathfrak{A}$ form a system of orthogonal idempotents whose sum is 1. The algebra "$\mathfrak{W}$" previously used guarantees that the polynomials in the $h^*(\alpha)ef$ yielding idempotents in the "$\mathfrak{A}$" of earlier sections satisfy i) and ii).

From i) and ii), $\sum_{j=1}^{t} e_j^{p^s} = 1$. If $e_j e_k - \delta_{jk} e_k = \sum_{n=1}^{n} w_i T_i, w_i \in \mathfrak{W}$, then

$$e_j^{p^s} e_k^{p^s} - \delta_{jk} e_k^{p^s} = \sum w_i^{p^s} T_i^{p^s}.$$

So the homomorphic images in $\mathfrak{B}$ of the $e_j^{p^s}$ are a system of orthogonal idempotents whose sum is 1. We denote the image of $e_j^{p^s}$ in $\mathfrak{B}$ by E_j. If $e_j \notin \mathfrak{T}$, then $e_j^{p^s} - e_j = \sum_{r=1}^{p^s-1} (e_j^{r+1} - e_j^r) \in \mathfrak{T}$, and so $e_j^{p^s} \notin \mathfrak{S}$ and $E_j \neq 0$ if $\bar{e}_j \neq 0$.

The central subalgebra $F[T_1, \ldots, T_n]$ of $\mathfrak{U}(\mathfrak{g})$ is a polynomial algebra on the T_i as generators. All monomials $T_1^{\nu_1} \ldots T_n^{\nu_n}$ with some $\nu_i \geq p^s$ are in $\mathfrak{S}$. We order the remaining monomials $\{M_i\}$ as follows: $M < N$ if degree $M <$ degree N, and the order is linear but otherwise arbitrary among monomials of the same degree. We label by subscripts indicating place in the order. Thus

$$1 = M_0 < M_1 < M_2 < \ldots < M_{p^{ns}-1} = T_1^{p^s-1} \ldots T_n^{p^s-1}.$$

Then the right ideal $E_j\mathfrak{B}$ in $\mathfrak{B}$ has descending filtration

$$E_j\mathfrak{B} = (E_j\mathfrak{B})_1 \supset \ldots \supset (E_j\mathfrak{B})_{p^{ns}} \supset 0,$$

where $(E_j\mathfrak{B})_r = \sum\limits_{q \geq r-1} E_j\mathfrak{B}M_q$.

In the right action of $\mathfrak{B}$ (or of $\mathfrak{U}(\mathfrak{g})$) on $E_j\mathfrak{B}$, $\mathfrak{T}$ maps each $(E_j\mathfrak{B})_r$ into $(E_j\mathfrak{B})_{r+1}$. So successive quotients in the filtration are right $\mathfrak{A}$-modules. Let φ be the canonical homomorphism of $\mathfrak{B}$ into $\mathfrak{A}$, ψ that of $\mathfrak{U}(\mathfrak{g})$ onto $\mathfrak{B}$, so that $\varphi \circ \psi$ is the canonical homomorphism of $\mathfrak{U}(\mathfrak{g})$ onto $\mathfrak{A}$. Then

$$(\varphi \circ \psi)(e_j^{p^s}\mathfrak{U}(\mathfrak{g})) = \varphi(E_j\mathfrak{B}) = (\varphi \circ \psi)(e_j^{p^s})\mathfrak{A} = (\varphi \circ \psi)(e_j)\mathfrak{A} = \bar{e}_j\mathfrak{A}.$$

The kernel of $\varphi \mid_{(E_j\mathfrak{B})}$ contains $(E_j\mathfrak{B})_2$. So φ induces a homomorphism of $(E_j\mathfrak{B})_1/(E_j\mathfrak{B})_2$ onto $\bar{e}_j\mathfrak{A}$ (as $\mathfrak{U}(\mathfrak{g})$-modules, or as $\mathfrak{A}$-modules). Now $\sum\limits_{r>0} \mathfrak{B}M_r =$ Ker φ (by Poincaŕe-Birkhoff-Witt - see [J], Chapter 5), and $E_j\mathfrak{B} \cap \sum\limits_{r>0} \mathfrak{B}M_r = \sum\limits_{r>0} E_j\mathfrak{B}M_r$, by left-multiplying with the idempotents E_k. Thus the kernel of the induced map of $(E_j\mathfrak{B})_1$ onto $\bar{e}_j\mathfrak{A}$ is exactly $(E_j\mathfrak{B})_2$. In particular, dim. $(E_j\mathfrak{B}/(E_j\mathfrak{B})_2) = \text{dim.}(\bar{e}_j\mathfrak{A})$.

For each $r, 1 \leq r < p^{ns}$, the multiplication-action of M_r sends $E_j\mathfrak{B}$ into $(E_j\mathfrak{B})_{r+1}$ and induces a map of $(E_j\mathfrak{B})/(E_j\mathfrak{B})_2$ *onto* $(E_j\mathfrak{B})_{r+1}/(E_j\mathfrak{B})_{r+2}$. (Here $(E_j\mathfrak{B})_{p^{ns}+1} = (0)$, by definition.) Thus

$$\dim((E_j\mathfrak{B})_r/(E_j\mathfrak{B})_{r+1}) \leq \dim \bar{e}_j\mathfrak{A}$$

for every r, every j. Summing over r and j gives

$$\dim \mathfrak{B} = \sum_{r,j} \dim((E_j\mathfrak{B})_r/(E_j\mathfrak{B})_{r+1}) \leq p^{ns} \dim \mathfrak{A} = \dim \mathfrak{B},$$

yielding equality at all stages. That is, we have proved:

Proposition 1. *With notation as above, the filtration* $(E_j\mathfrak{B}) \supset (E_j\mathfrak{B})_2 \supset \ldots \supset (E_j\mathfrak{B})_{p^{ns}} \supset 0$ *of* $E_j\mathfrak{B}$ *by right ideals has successive quotients which, as* $\mathfrak{A}$*-modules, are all isomorphic to* $\bar{e}_j\mathfrak{A}$.

Clearly the radical $\mathfrak{N}$ of the algebra $\mathfrak{B}$ contains all $\psi(T_i)$. So $E_j\mathfrak{B}/E_j\mathfrak{N}$ is a homomorphic image of $E_j\mathfrak{B}/(E_j\mathfrak{B})_2$, and the submodules of $E_j\mathfrak{B}/E_j\mathfrak{N}$ are in correspondence with the set of submodules of $\bar{e}_j\mathfrak{A}$ containing $\bar{e}_j\varphi(\mathfrak{N})$. Because $\varphi(\mathfrak{N})$ is a nilpotent ideal, $\bar{e}_j\varphi(\mathfrak{N}) \neq \bar{e}_j\mathfrak{A}$. If $\bar{e}_j$ is a primitive idempotent, $\bar{e}_j\mathfrak{A}$ has a unique maximal submodule ([C-R], §54), *a fortiori* a unique maximal submodule containing $\bar{e}_j\varphi(\mathfrak{N})$, and, by the same reference, this submodule is $\bar{e}_j\mathfrak{R}$, where $\mathfrak{R}$ is the radical of $\mathfrak{A}$. Thus $E_j\mathfrak{B}/E_j\mathfrak{N}$ has a unique maximal submodule. Because every maximal submodule of $E_j\mathfrak{B}$ must contain $E_j\mathfrak{N}, E_j\mathfrak{B}$ has a unique maximal submodule, and E_j is in turn a primitive idempotent. The converse is clear: If E_j is primitive, $E_j\mathfrak{B}$ has a unique maximal submodule, which must contain $(E_j\mathfrak{B})_2$; so $\bar{e}_j\mathfrak{A}$ has a unique maximal submodule. That is,

Proposition 2. *The idempotent* $\bar{e}_j$ *is primitive in* $\mathfrak{A}$ *if and only if* E_j *is primitive in* $\mathfrak{B}$.

To apply the above to $s\ell(2)$, with $z_i = h^p - h, e^p, f^p$ and the elements $\{e_j\}$ that are polynomials in the $h^*(\alpha)ef$ as in §§1-4, so that $\mathfrak{B}$ is the quotient of $\mathfrak{U}(\mathfrak{g})$ by the ideal generated by the $(h^p - h - \lambda)^{p^s}, (e^p - \mu)^{p^s}, (f^p - \nu)^{p^s}$, we find that the images in $\mathfrak{B}$ of the $e_j^{p^s}$ are a system of primitive orthogonal idempotents of sum 1. In the semisimple case, each of the corresponding projective indecomposable $\mathfrak{B}$-modules has a composition series of length p^{3s} with quotients all isomorphic to the irreducible $\mathfrak{A}$-module $\bar{e}_j\mathfrak{A}$. In the non-restricted case with $\lambda^2 = 4\mu\nu$, there are p projective indecomposable modules with composition series of length p^{3s} and quotients isomorphic to the $E(\alpha, 0)\mathfrak{A}(\alpha \in \mathbf{F}_p)$, while the remaining p.i.m.s have composition-length $2p^{3s}$, composition-factors all isomorphic to those of $E(\alpha, \beta)\mathfrak{A}, \beta \in \mathbf{F}_p^{*2}$. These p.i.m.s admit a filtration where successive quotients (p^{3s} of them) are all isomorphic to $E(\alpha, \beta)\mathfrak{A}$.

In the restricted case, there are p primitive idempotents with generated modules having composition series of length p^{3s} and the Steinberg module as quotient. The remaining $\frac{p(p-1)}{2}$ primitive idempotents each yield p.i.m.s of length $4p^{3s}$, dimension $2p^{3s+1}$, with filtrations having quotients all isomorphic to the $E(\alpha, \beta)\mathfrak{A}$ as in §4. These conclusions recover Bendel's results in [Ben] (§8).

It may be noted that, when F is algebraically closed, every finite-dimensional indecomposable $s\ell(2)$-module is a module for one of our algebras $\mathfrak{B}$, with suitable values of λ, μ, ν and s.

References

[Ben] C. Bendel, *Generalized reduced enveloping algebras for restricted Lie algebras*, Journal of Algebra **218** (1999), 373-411. MR **2000h:**17007

[Ber] A. Berkson, *The u-algebra of a restricted Lie algebra is Frobenius*, Proc. Amer. Math. Soc. **15** (1964), 14-15. MR **28:**2132

[C-R] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience (Wiley), New York (1962). MR **26:**2519

[J] N. Jacobson, *Lie Algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience (Wiley), New York (1962); Dover edition, Dover Publications, New York 1979. MR **26:**1345; MR **80k:**17001

[JCJ] J. C. Jantzen, *Representations of Lie algebras in prime characteristic*, In *Representation Theories and Algebaic Geometry*, A. Broer and A. Daigneault, eds., Kluwer, Dordrecht/Boston/London (1998), 185-235. MR **99h:**17026

[N] G. M. Nielsen, *A Determination of the Minimal Right Ideals in the Enveloping Algebra of a Lie Algebra of Classical Type*, Ph.D. dissertation, Madison, Wisconsin, 1963.

[P] R. D. Pollack, *Restricted Lie algebras of bounded type*, Bull. Amer. Math. Soc. **74** (1968), 326-331. MR **36:**2661

[S] J. Schue, *Symmetry for the enveloping algebra of a restricted Lie algebra*, Proc. Amer. Math. Soc. **16** (1965), 1123-1124. MR **32:**2515

Department of Mathematics, Yale University, P.O. Box 208283, New Haven, Connecticut 06520-8283

E-mail address: selig@math.yale.edu