Towards Decidability of the Theory of Pseudo-Finite Dimensional Representations of $sl_2(k)$; I

Sonia L'Innocente[*]
Department of Mathematics
and Computer Science
University of Camerino
Camerino, Italy
sonia.linnocente@unicam.it

Angus Macintyre
School of Mathematics
Queen Mary University of London
London, England
angus@dcs.qmul.ac.uk

1 Introduction

In this paper, we refine the analysis begun in Ivo Herzog's paper [7] on representations of the Lie algebra $sl_2(k)$, where k is an algebraically closed field of characteristic 0. Our principal contribution is to bring out a connection to fundamental problems in the diophantine geometry of curves. We expect to show, in a subsequent paper, that the theory of finite dimensional representations of $sl_2(k)$ is decidable, modulo some widely believed conjectures in diophantine geometry. It should be noted that Prest and Puninski [13] showed that the theory of all $sl_2(k)$-modules is undecidable (this important result seems not to be well-known).

Our model theory and definability are relative to the formalism of left R-modules for a ring R [12]. In particular, we tacitly identify the theory of representations of the Lie algebra $sl_2(k)$ with the theory of modules over U_k, the universal enveloping algebra of $sl_2(k)$. We follow Herzog in calling a U_k-module M finite dimensional if it is finite dimensional over k. (Note that k is fixed throughout the paper. We discuss the effect of varying k in the sequel).
Then M is pseudo-finite dimensional (henceforward PFD) if it satisfies all sentences of the language of U_k-modules true in all finite dimensional modules. By classical model theory [4], M is PFD if and only if M is elementarily equivalent to an ultraproduct of finite dimensional modules.

The study of finite dimensional U_k-modules M is dominated by the classical result due to Lie and Study (see, for instance, [6], Theorem 8.7) showing that any such M is uniquely a finite direct sum of simple finite dimensional modules and there is exactly one of the latter for each finite dimension. We write V_λ for the unique simple finite dimensional module of dimension $\lambda + 1$, and recall that it has a beautiful presentation as the additive group of homogenous polynomials $F(X, Y)$ of degree λ in X, Y, with U_k acting as certain

[*] This research was carried out between October and December of 2006, when the first author visited the second in London with financial support from Indam, Istituto di Alta Matematetica "Francesco Severi", Roma, Italy

differential operators ([6], § 8.1). Part of the motivation for studying PFD-modules is to isolate the model-theoretic uniformities in the $V(\lambda)$, as $\lambda \to \infty$.

The ring U_k is left and right Ore domain (for instance, see [5] § 2.3), and thus belongs to a well-studied class. To understand PFD-modules, Herzog introduced an exotic epimorphic extension U_k' of U_k and showed:

1. U_k' is a von Neumann regular ring;

2. PFD-modules are naturally U_k'-modules;

3. the model theory of U_k'-modules is interpretable in that of U_k-modules;

4. there is an elegant axiomatization of the class of PFD-modules as a subclass of the class of U_k'-modules.

Unfortunately, the very abstract nature of the construction of U_k' leaves some basic questions unanswered. We remedy this by giving a "recursive" construction of U_k', building it from U_k in stages. This should enable us to prove decidability of the theory of PFD-modules (assuming some plausible conjectures about the decision problem for integer points on curves). We are obliged to describe the structure of the sets

$$\{\lambda : V(\lambda) \models \Phi\},$$

for Φ a sentence of the language of U_k-modules. In this paper we bring out some basic new information about the case when Φ concerns the nontriviality of certain kernels. This is where diophantine geometry is relevant.

For both of us it is an honour to dedicate a paper to the memory of Andrzej Mostowski. The junior author (S. L'I.) did not exist at the time of Mostowski's untimely death, and the model theory of modules was just beginning, but she is well aware of the lasting importance of his ideas (and we use essentially some of his work in this paper).

The senior author (A. M.) would like to make a more personal statement:

I began reading Mostowski's books and papers when I was an isolated teenager in Scotland, and was taken by their range and clarity. Throughout graduate school I continued to learn more of his work, and the paper with Andrzej Ehrenfeucht has remained one of my favourites. I first met Mostowski in 1968 (in Warsaw and in Italy), and was very much encouraged by the interest he showed in my work. We met a few times before 1975, and he became for me one of the most admired figures on logic, both for his work and for the strength and generosity of his personality. His death had many of us fearing for the future of logic in Poland, And yet, after thirty years, Poland is rich in young researchers, and the ideas of Mostowski's generation (and later mine) have evolved very far, exactly the right memorial to an outstanding teacher and researcher.

2 The basic structure and formalism

2.1 The Lie algebra $sl_2(k)$

Fix, for the rest of the paper, an algebraically closed field k of characteristic 0. $sl_2(k)$ is the Lie algebra (over k) of 2×2 matrices of trace 0. Throughout we consider the basis of

$sl_2(k)$ over k given by x, y, h where

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These satisfy the following relations:

$$\begin{aligned} [x,y] &= h\,, \\ [h,x] &= 2x\,, \\ [h,y] &= -2y. \end{aligned}$$

(and indeed all other Lie algebra relations are generated by these).

The study of left modules over the Lie algebra $sl_2(k)$ is naturally equivalent to the study of left modules over U_k the universal enveloping algebra [3]. U_k is well-understood. Via the natural embedding $sl_2(k) \to U_k$, we construe U_k as freely generated over k by elements x, y, h satisfying:

$$\begin{aligned} xy - yx &= h\,, \\ hx - xh &= 2x\,, \\ hy - yh &= -2y. \end{aligned}$$

U_k is a left and right Ore domain ([5] § 2.3), and so has a field of fractions. We follow Herzog in calling this field K. Its U_k-module structure turns out to be important.

Before looking at U_k-modules, we review the basics about the ring structure of U_k. Here, and in most of the paper, we are presenting, with a different emphasis, ideas from Herzog's paper [7].

Recall that U_k has a $\mathbb{Z}$-grading as k-algebra, induced by defining:

$$\begin{array}{rclcll} gr(h) & = & gr(\alpha) & = & 0 & \text{for all } \alpha \in k \\ gr(x) & = & 1\,, & & & \\ gr(y) & = & -1\,. & & & \end{array}$$

Let $U_{k,n}$ be the subalgebra of elements of grade n. We have

$$\begin{array}{rclcl} U_k & = & \bigoplus_{n\in\mathbb{Z}} U_{k,\,n}\,; & & \\ \text{for}\, n > 0,\ U_{k,\,n} & = & x^n U_{k,\,0} & = & U_{k,\,0} x^n\,; \\ \text{for}\, n < 0,\ U_{k,\,n} & = & y^n U_{k,\,0} & = & U_{k,\,0} y^n\,. \end{array}$$

These results are proved by simple manipulations of the basic relations connecting x, y and h.

Of fundamental importance is the *Casimir operator*, defined as

$$c = xy + yx + \frac{1}{2}h^2 \quad \in U_{k,\,0}\,.$$

Lemma 2.1 *c is central in U_k.*

Proof. It is enough to prove that c commutes with x, y and h.

i) $xc \;=\; x(xy + yx + \frac{1}{2}h^2) \;=\; xyx + x(yx + h) + \frac{1}{2}(hx - 2x)h \;=\; 2xyx + \frac{1}{2}hxh\,,$

$cx \;=\; (xy + yx + \frac{1}{2}h^2)x \;=\; xyx + (xy - h)x + \frac{1}{2}h^2x \;=\; 2xyx - hx + \frac{1}{2}h(xh + 2x) \;=$
$\;=\; 2xyx + \frac{1}{2}hxh \;=\; xc\,;$

ii) $yc = cy$ is proved similarly;

iii) $ch = \;(xy + yx + \frac{1}{2}h^2)h \;=\; (h + 2yx + \frac{1}{2}h^2)h \;=\; h^2 + \frac{1}{2}h^3 + 2yxh \;=$
$\;=\; h^2 + \frac{1}{2}h^3 + 2y(hx - 2x)\,,$

$hc = \;h(xy + yx + \frac{1}{2}h^2) \;=\; h(h + 2yx + \frac{1}{2}h^2) \;=\; h^2 + \frac{1}{2}h^3 + 2hyx \;=$
$\;=\; h^2 + \frac{1}{2}h^3 + 2(yh - 2y)x \;=\; ch\,.$

□

Lemma 2.2 *$U_{k,0} = k[h, c]$, the polynomial ring on the two commuting generators h, c.*

Proof. See [7] for a brief sketch, using the Poincaré-Birkhoff-Witt Theorem. □

Similarly, one can prove.

Lemma 2.3 *The center of U_k is $k[c]$.*

2.2 The simple finite dimensional modules

Let λ be an integer ≥ 1. Let V_λ be the k-vectorspace of homogenous polynomials of degree λ over k in the two variables X and Y. V_λ has dimension $\lambda + 1$, and a natural basis is given by the monomials

$$\{X^i \cdot Y^{\lambda - i}, \quad 0 \leq i \leq \lambda\}\,.$$

V_λ is given a U_k-module structure by having:

$$\begin{aligned} x &\quad \text{act as} \quad X\frac{\partial}{\partial Y} \\ y &\quad \text{act as} \quad Y\frac{\partial}{\partial X}\,, \\ h &\quad \text{act as} \quad X\frac{\partial}{\partial X} - Y\frac{\partial}{\partial Y}\,. \end{aligned}$$

See [6], § 8.1., for the details.

Lemma 2.4 *V_λ is a simple U_k module.*
Every simple finite dimensional U_k-module is isomorphic to a unique V_λ.
Furthermore, every finite dimensional U_k-module is isomorphic to a direct sum of simple modules, uniquely up to relabelling.

Proof. See [6], Theorem 8.2 and Theorem 8.5 for the first two statements and Theorem 8.7 for the last statement. □

Of crucial importance for us are the eigenvalues of h, c, x and y on a finite dimensional module M. Here, let us summarize the most basic definitions and facts that we will use later:

i) Any simple finite dimensional U_k-module V_λ decomposes as follows:

$$V_\lambda = \bigoplus_{0 \le i \le \lambda} V_{\lambda,\, i}\,,$$

where each $V_{\lambda,\, i}$ equals the one dimensional h-invariant subspace $\{v \in V_\lambda : hv = (\lambda - 2i)v\}$ of V_λ; more precisely, we have $V_{\lambda,\, i} = Ker(h - (\lambda - 2i) \cdot 1)$.

ii) On V_λ, c acts as scalar multiplication by $\frac{\lambda(\lambda+2)}{2}$.

iii) If we make the convention that $V_{\lambda,\, i} = \{0\}$ if $i \notin [-\lambda, \lambda]$, then:

$$x \text{ maps } V_{\lambda,\, i} \text{ to } V_{\lambda,\, i-1}\,,$$

and

$$y \text{ maps } V_{\lambda,\, i} \text{ to } V_{\lambda,\, i+1}\,.$$

iv) $Ker(x) \;=\; V_{\lambda,0}$, and
$Ker(y) \;=\; V_{\lambda,\lambda}$.

v) x and y act nilpotently.

vi) $V_\lambda = Ker(x) \oplus Image(y)$
$V_\lambda = Image(x) \oplus Ker(y)$.

The $V_{\lambda,\, i}$ are called the *weight spaces*, $V_{\lambda,\, 0}$ is called the *highest weight* space and $V_{\lambda,\, \lambda}$ is called the *lowest weight* space. (The terminology will be suitably adjusted once we deal with general U_k-module M).

vii) Let M be a finite dimensional U_k-module. For $\lambda \in k$, define $Cas(\lambda,\, M)$ to be $Ker(c - \frac{\lambda(\lambda+2)}{2} \cdot 1)$. Then

$$M = \bigoplus_{\lambda \in k} Cas(\lambda,\, M)\,,$$

with $Cas(\lambda,\, M) = \{0\}$ unless $\lambda \in \mathbb{N}$. Indeed, $Cas(\lambda,\, M)$ is isomorphic to some finite power of V_λ.
Note that for $\lambda \ge 0$, $\frac{\lambda(\lambda+2)}{2}$ determines λ.

viii) Define $Cas(M)$ as

$$\{\lambda : Cas(\lambda,\, M) \neq \{0\}\}\,.$$

2.3 Basic model theory and PFD modules

See [12] for all the basics on the formalism for model theory of modules. Our language is that of abelian groups, with a unary function symbol for (the endomorphism given by) each element of U_k.

We begin by noting the following:

Lemma 2.5 *If M is a U_k-module, then*

$$M \equiv M \oplus M\,.$$

Proof. By the Baur-Monk criteria for elementary equivalence [18] (generalizing that of Szmielew [16]), the elementary type of M is determined by the cardinality (modulo ∞) of all $\varphi(M)/\psi(M)$, where φ, ψ are pp-formulas defining subgroups of M. But since the infinite field k is in the center of U_k, these groups are k-subspaces, and so the above indices are always 1 or infinite. Thus M and $M \oplus M$ have the same elementary invariants. □

Corollary 2.6 *The class of finite dimensional U_k-modules is not closed under elementary equivalence.*

Proof. Lemma 2.5 shows that $M \equiv M^{(\omega)}$. □

One has already reached an interesting question.

Question 2.7 *Which U_k-modules are elementary equivalent to a finite dimensional module?*

It is worth noting that the theory of finite dimensional U_k -modules (for k a recursive algebraically closed field) is co-r.e. (that is, it has a recursively enumerable complement). The basic structure theory of finite dimensional modules gives a recursive enumeration of them using explicit matrix representations of the actions of h, x and y on the spaces V_λ. But for any fixed M of finite dimension we can test truth in M using this matrix representation and the decidability of the theory of algebraically closed fields. Thus if a sentence is not in the theory, it will be enumerated at some finite stage.

Herzog defines any U_k-module M to be pseudo-finite dimensional (PFD) if it is a model of the elementary theory of all finite dimensional modules. By general model theory, M is PFD if and only if M is elementary equivalent to an ultraproduct of finite dimensional modules (see [4], Exercise 4.1.18).

One should note that various “pseudo-finite” structures have been studied, notably fields and groups in [1] and [17] respectively. The flavour here is different (as described in § 2.2), as it is the dimension which is pseudo-finite, and not the cardinality.

Before entering on the more delicate details of the analysis, we discuss some fairly superficial aspects of ultraproducts of finite dimensional modules.

Lemma 2.8 *Let M be a PFD R-module. Then, the following properties hold:*

i) $Cas(\lambda, M) = \{0\}$ unless $\lambda \in \mathbb{N}$:

ii) If M is finite dimensional then $Cas(M)$ is finite.

iii) If $Cas(M)$ is finite, then M is elementary equivalent to a finite dimensional U_k-module if and only if

$$M = \sum_{\lambda \in Cas(M)} Cas(\lambda, M) \quad \left(= \bigoplus_{\lambda \in Cas(M)} Cas(\lambda, M) \right) ,$$

and this is a first order property of M, for fixed finite $Cas(M)$.

Proof. *i)* Obvious, since the property is expressible in the language and is true for finite dimensional M.

ii) This follows from the decomposition into a sum of V_λ.

iii) Suppose M is finite dimensional. So, $Cas(M) = E$ for some finite subset $E \subseteq \mathbb{N}$. Obviously, each $Cas(\lambda, M)$, for $\lambda \in E$, is definable, and so one can express by a first-order sentence that $M = \sum_{\lambda \in E} Cas(\lambda, M)$.
The direct sum representation follows.

Conversely, if M has this form, then

$$M \cong \bigoplus_{\lambda \in E} Cas(\lambda, M) \equiv \bigoplus_{\lambda \in E} V_\lambda \, ,$$

by Mostowski's Theorem [10] and the fact that in all finite dimensional M_0, for all λ and all sentences Φ

$$Cas(\lambda, M_0) \models \Phi \Leftrightarrow V_\lambda \models \Phi \, .$$

□

Corollary 2.9 *M is elementary equivalent to a finite dimensional M_0 if and only if $Cas(M)$ is finite and $M = \sum_{\lambda \in Cas(M)} Cas(\lambda, M)$*

Proof. This is immediate by Lemma 2.8 iii). □

Remarks 2.10 *1. For M a nonzero PFD module, $Cas(M)$ may be $\{0\}$. To see this, take M equal to the ultraproduct $\prod_{\lambda \in \mathbb{N}} V_\lambda / D$, where D is nonprincipal.*

We will show in a later paper that there are $2^{\aleph_0}$ complete theories of PFD U_k-modules M with $Cas(M) = \{0\}$.

2. For any $E \subseteq \mathbb{N}$ with $0 \in E$, there is a PFD M with $Cas(M) = E$. This is almost immediate from the compactness theorem, for if $\lambda_1, \ldots, \lambda_n \in E$ (with n a nonzero natural number) and $\mu_1, \ldots, \mu_m \in \mathbb{N} \backslash E$ (with m a nonzero natural number), then

$$V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_n}$$

is a finite dimensional module M with $\mu_1, \ldots, \mu_m \notin Cas(M)$ and $\lambda_1, \ldots, \lambda_n \in Cas(M)$.

3 The appropriate definable scalars

Let $FinDim$ be the class of all finite dimensional U_k-modules. We consider the ring U_k' of definable scalars attached to $FinDim$. In concrete terms, one consider pp-formulas $p(u, v)$ in two variables (modulo equivalence in all $M \in FinDim$) such that p defines a (necessarily additive) map $M \to M$ for all $M \in FinDim$. Addition and composition are defined in the obvious way, giving a ring structure on the equivalence classes. U_k' is the resulting ring (Herzog gives in [7] several equivalent definitions).

Remarks 3.1 *Some things are immediately clear.*

i) There is a natural ring homomorphism $U_k \to U_k'$;

ii) $FinDim$ is naturally a class of U_k'-modules;

iii) Each U_k'-module formula is naturally equivalent, for $M \in FinDim$, to a U_k-formula.

Less obvious is the result of Harish-Chandra.

Lemma 3.2 *$U_k \to U'_k$ is 1-1.*

Proof. See [5]. □

Understanding U'_k is naturally a prerequisite for understanding PFD modules. Herzog revealed some striking facts about U'_k, and in particular that it is von Neumann regular. Probably because of the rather abstract account he gave of U'_k, he did not answer the following questions:

Question 3.3 *What are the elementary types of PFD modules over U_k?*

Question 3.4 *Is the elementary theory of PFD modules decidable, if k is countable and given a natural recursive presentation?*

We hope to answer both questions. We will make full use of Herzog's work, but will reorganize the analysis so that U'_k is constructed in stages, and the diophantine information is used systematically.

3.1 Duality and the action of the Weyl group

The Weyl group of $sl_2(k)$ is cyclic of order 2 and its generator induces an involution σ on U_k via:

$$\begin{aligned}\sigma(x) &= -y;\\ \sigma(y) &= -x;\\ \sigma(h) &= -h.\end{aligned}$$

Herzog shows σ extends to an involution of U'_k. His argument, though expressed abstractly, is really quite concrete. He then considers a related canonical anti-isomorphism $\theta : U_k \to U_k^{opp}$ between U_k and U_k^{opp} defined by:

$$\begin{aligned}\theta(x) &= -x;\\ \theta(y) &= -y;\\ \theta(h) &= -h.\end{aligned}$$

$\theta\sigma$ induces an antihomomorphism of the lattice of pp subgroups of M, uniformly for all U_k-modules M. (Herzog states this in functorial terms). The action is written as $\varphi \to \varphi^-$, and is explicitly described in [7]. He goes on to show that it respects equivalence modulo $FinDim$, that is, $\varphi \to \psi$ on $FinDim$ implies $\varphi^- \to \psi^-$ on $FinDim$, and this becomes a key tool in his analysis. We remark that $\varphi \to \varphi^-$ is entirely constructive, uniformly in any k-scalars.

We note the following fact:

Lemma 3.5 *For $\alpha, \beta \in k$, with $\alpha \neq 0$, $\alpha + \beta \cdot x$ is invertible in U'_k.*

Proof. x acts nilpotently on each $M \in FinDim$, so $\alpha + \beta \cdot x$ acts invertibly on M, with inverse $\alpha^{-1} \cdot \sum_{m=0}^{\infty}(-1)^m(\alpha^{-1}\beta x)^m$, which is a finite sum, of length depending M. To see the inverse uniformly as a definable scalar, consider

$$\phi(u, v) \, : \, u = (\alpha + \beta \cdot x) \cdot v \, .$$

□

The above fact is given only as a simple example, and has no special place in the order of our analysis.

The heart of the matter is the generation of idempotents, and especially those corresponding to annihilators (which we prefer, for reasons connected to the duality of Section 3.1, to call kernels) of elements of $U_{k,0}$.

For $p \in U_k$, we consider the following k-subspace:

$$Ker(p)(M) = \{m \in M : p \cdot m = 0\}.$$

We want to have in U'_k an (associated) idempotent e_p corresponding to the projection from M to this subspace, but this has no real meaning in terms of definable scalars unless we have a pp complement for $Ker(p)$. It is not obvious that such exists, and Herzog's proof that it does depends on the anti-isomorphism $\varphi \to \varphi^-$ discussed above.

3.2 The centralizer of h

There is a direct (and obvious) connection between elements q of U'_k commuting with h, and elements of U'_k preserving weight spaces for M in $FinDim$.

Recall that such M are the direct sum of their pp-definable subspaces $Cas(\lambda, M)$. $Cas(\lambda, M)$ is isomorphic to a sum of copies of V_λ. Just as in V_λ we have the h-invariant weight spaces $V_{\lambda,i}$ $(0 \leq i \leq \lambda)$, where $V_{\lambda,i} = ker(h - (\lambda - 2i))$ (in the sense of V_λ), we can define $Cas(\lambda, M)_i$ as $Ker(h - (\lambda - 2i))$ (in the sense of $Cas(\lambda, M)$), and we have $Cas(\lambda, M) = \sum_i Cas(\lambda, M)_i$.

Now, if q commutes with h, each $Ker(h - (\lambda - 2i))$ is closed under q and, since the Casimir element c commutes with h, each $Cas(\lambda, M)_i$ is closed under q.

If $M \cong V_\lambda$ and $qh = hq$, q leaves each 1-dimensional weight space $V_{\lambda,i}$ invariant.

"Conversely", if q, on every V_λ, leaves the weight spaces $V_{\lambda,i}$ invariant then $hq - qh$ is the zero map on V_λ, for each λ. It follows that $hq - qh$ is the zero map on every $M \in FinDim$, so $hq - qh = 0 \in U'_k$.

We take Herzog's arguments, and add some number theory, to get the basic insight needed to answer Questions 3.3 and 3.4.

Note that on V_λ the elements of $U_{k,0}$ $(=k[h,c])$ have the common basis of eigenvectors $X^iY^{\lambda-i}$. In particular for each p in $U_{k,0}$, we have

$$V_\lambda = Ker(p) \oplus Image(p),$$

and then obviously $M = Ker(p) \oplus Image(p)$ for every $M \in FinDim$. Since $Image(p)$ is uniformly pp-definable, we thus see our first idempotent, $e_p \in U'_k$, for $p \in U_{k,0}$ defined by

$$e_p(m_1 + m_2) = m_1$$

where $m_1 \in Ker(p)$ and $m_2 \in Image(p)$.

So, e_p is the projection onto $Ker(p)$ relative to the decomposition $M = Ker(p) \oplus Image(p)$.

Remark 3.6 *$1 - e_p$ is the corresponding projection onto $Image(p)$.*

We note that all the e_p above commute with $U_{k,0}$ (they, too, have on V_λ the $X^iY^{\lambda-i}$ as eigenvectors).

Some are 0, for example e_c (where c is the Casimir element), since $Ker(c) = \{0\}$ on any $M \in FinDim$. Note that $e_h \neq 0$ in U'_k, since for even λ, h has a nonzero kernel in V_λ (and for odd λ it has not).

Note that for $p = c - \frac{\lambda(\lambda+2)}{2}$, e_p gives the projection onto $Cas(\lambda, M)$ for $M \in FinDim$.

3.3 Standard and nonstandard e_p

Here we go significantly beyond [7]. Let $p \in U_{k,0}$, so $p = p(c,h)$ where $p\,(u,v) \in k[u,v]$. As before, for $M \in FinDim$, $Ker(p)$ is a sum of eigenspaces $Cas(\lambda, M)_i$, where

$$Cas(\lambda, M)_i = \{\ m : c \cdot m = \frac{\lambda(\lambda+2)}{2} \cdot m,\ h \cdot m = (\lambda - 2i) \cdot m\}\,.$$

Then, as Herzog shows, $Cas(\lambda, M)_i \subseteq Ker(p)$ if and only if $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$.

The subsequent analysis in [7], essentially goes as follows.

Case 1. $p \notin k[u]$.

Then for all but finitely many λ ($\notin \{\lambda_1, \ldots, \lambda_r\}$) $p\,(\frac{\lambda(\lambda+2)}{2},\ v)$ is not the zero polynomial. If $p\,(\frac{\lambda(\lambda+2)}{2},\ v) \neq 0 \in k[v]$, then $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$ has no more than d solutions (λ, i), where d is the v-degree of p.
If however $\lambda \in \{\lambda_1, \ldots, \lambda_r\}$ and $p\,(\frac{\lambda(\lambda+2)}{2},\ v) = 0 \in k[v]$, then $p\,(\frac{\lambda(\lambda+2)}{2},\ \lambda - 2i) = 0$ has no more than $|\lambda|$ solutions with $0 \leq i \leq |\lambda|$, and there are no more than $2d$, such λ, where d, is the u-degree of p.

Case 2. $p \in k[u]$.

Then there are no more than $2d$ λ with $p\,(\frac{\lambda(\lambda+2)}{2}) = 0$, and for each such λ no more than $|\lambda|$ i with $0 \leq i \leq |\lambda|$. This proves the following fact.

Lemma 3.7 *If $p \neq 0$, $p \in U_{k,0}$ there is a bound $B(p)$, computable semi-algebraically from p, on the dimension of $V_\lambda \cap Ker(p)$, independently of λ.*

Proof. Done above (modifying slightly that in [7]). □

But much more is true!
Consider the affine plane curve $\mathcal{C}_p$ defined by $p\,(u,v) = 0$.

Suppose first p is an absolutely irreducible polynomial, and that $\mathcal{C}_p$ has genus ≥ 1. Then by Siegel's Theorem (see [8]) there are only finitely many pairs $(a,b) \in \mathbb{Z}^2$ such that $p\,(\frac{a}{2},\ b) = 0$. Thus there are only finitely many pairs (λ, i) so that $(\lambda, i) \in \mathbb{Z}^2$ and $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$. If follows that uniformly across all $M \in FinDim$, $Ker(p) \cap Cas(\lambda, M) = \{0\}$ except for λ in a finite set $supp(p)$ which is independent of M.
Moreover, there is a finite set I so that for $\lambda \in supp(p)$, $Cas(\lambda, M) \cap Ker(p) \subseteq \oplus_{i \in I} Cas(\lambda, M)_i$.
The existence of such a $supp(p)$ and I (which we will obtain below for p much more general than those just considered) will lead us to call p (and the e_p) standard.
We can relax the hypothesis on p significantly. First, factor p into absolutely irreducible factors p_r. The Herzog argument identifies $Ker(p)$ as $\oplus_{\lambda,\,i} Cas(\lambda, M)_i$, where the summation is over all (λ, i) in $\mathbb{Z}^2$, with $0 \leq i \leq \lambda$, and $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$. Thus we are reduced to considering for each r the condition $p_r(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$.

It may happen that p_r is not defined over $\mathbb{Q}$. But then suppose $(\lambda, i) \in \mathbb{Z}^2$ and

$p_r(\frac{\lambda(\lambda+2)}{2},\, \lambda - 2i) = 0.$

Then for any automorphism σ of k,

$p_r^{\sigma}(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0,$

where p_r^{σ} is got from p_r by acting on its coefficients by σ.

As far as $Ker(p_r)$ is concerned, we can assume that one of the coefficients of p_r is 1, and then if p_r is not defined over $\mathbb{Q}$, there exists σ so that $p_r^{\sigma} = 0$ defines a different curve. Then, by Bezout's Theorem, $\mathcal{C}_{p_r}$ and $\mathcal{C}_{p_r^{\sigma}}$ have an absolutely bounded number of points of intersection. So, for p_r not defined over $\mathbb{Q}$ (and even of genus 0) p_r is standard in the sense outlined before.

Thus, we can see that the interesting p are those for which one of the p_r is defined over $\mathbb{Q}$, and has infinitely many (λ, i) in $\mathbb{Z}^2$ with $p_r(\frac{\lambda(\lambda+2)}{2},\, \lambda - 2i) = 0$.
In particular, $\mathcal{C}_{p_r}$ must have genus 0.
But this is far from enough to guarantee infinitely many zeros (λ, i) from $\mathbb{Z}^2$ with $0 \leq i \leq \lambda$. Siegel himself showed (see [14] for a particularly clear treatment) that if p is an absolutely irreducible polynomial over $\mathbb{Q}$, with $p = 0$ defining a genus 0 curve with ≥ 3 points at infinity, then the curve has only finitely many points of the form $(\frac{a}{2},\, b)$, $(a,\, b) \in \mathbb{Z}^2$. A fairly recent subsequent literature has completely clarified which plane curves $\mathcal{C}_p$ have infinitely many points [11, 15].

In a later paper we will discuss the fine detail of this, in connection with decidability. For now, an example is provided to show that there are p which are not standard (and we call these *nonstandard*).

Example 3.8 *Let* $p\,(u,\, v) = u - v^2$.
Then, $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = \frac{(\lambda+1)^2-1}{2} - (\lambda - 2i)^2$.
So, $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0 \Leftrightarrow (\lambda + 1)^2 - 2(\lambda - 2i)^2 = 1$.

So, we are asking for infinitely many points $(\lambda + 1, \lambda - 2i)$ with $0 \leq i \leq \lambda$, on the genus zero curve corresponding to the Pell equation $X^2 - 2Y^2 = 1$.
The only thing to check is every integer solution (X, Y) with $X \geq 1$, $Y \leq 0$ is of the form $(\lambda + 1, \lambda - 2i)$ with $0 \leq i \leq \lambda$. This of course requires $X - Y$ to be odd, but this is automatic, since if $X - Y$ were even, that is $X - Y = 2W$ (for some integer W), we would have: $(Y + 2W)^2 - 2Y^2 - 1 = 4YW + 4W^2 - Y^2 - 1 \not\equiv 0 \quad mod\, 4$.
What we need is that for X and Y solutions with $X \geq 1$, $Y \leq -3$, we have

$0 \leq \frac{X-Y-1}{2} \leq X - 1,$
i.e $\quad 0 \leq X - Y - 1 \leq 2X - 2,$
i.e $\quad 0 \leq -Y - 1 \leq X - 2,$
i.e $\quad 3 + Y \leq 0 \leq X - Y,$

but this is automatic, proving that every nontrivial integer solution of $X^2 - 2Y^2 = 1$ with $X \geq 1$, $Y \leq -3$ is of the form $(\lambda + 1, \lambda - 2i)$ with $0 \leq i \leq \lambda$.

Let us consider p as in the Example 3.8, we can see that $e_p \cdot e_{c - \frac{\lambda(\lambda+2)}{2}} \neq 0$ for infinitely many λ, and the possible λ are determined by integer solutions of the Pell equation $X^2 - 2Y^2 = 1$, with $X \geq 1$.

Furthermore, we ask how many i exist for each λ with $0 \leq i \leq \lambda$ for which the following relations holds:

$\frac{\lambda(\lambda+2)}{2} = (\lambda - 2i)^2 \quad 0 \leq i \leq \lambda.$

In fact, there are two such i, say i_1, i_2, with $i_1 + i_2 = \lambda$, distinct unless $\lambda = \frac{\lambda}{2}$, when $\lambda = 0$ is the only possibility. Thus, when $e_p \cdot e_{c-\frac{\lambda(\lambda+2)}{2}} \neq 0$, its action on V_λ is to project onto a 2-dimensional sum of weight spaces $(V_\lambda)_i \oplus (V_\lambda)_{\lambda-i}$.

Now, we give a formal definition of "standard".

Definition 3.9 *i) $p \in U_{k,0}$ is standard if there is a finite set supp$(p) \subseteq \mathbb{N}$, such that $e_p \cdot e_{c-\frac{\lambda(\lambda+2)}{2}} = 0$ for $\lambda \notin$ supp(p);*

ii) The λ such that $e_p \cdot e_{c-\frac{\lambda(\lambda+2)}{2}} \neq 0$ form the support of p;

iii) p is nonstandard *if the support of p is infinite.*

We can note that by Herzog's argument, there is an absolute finite bound on the dimension of $e_p V_\lambda$.

4 Redundancy in the preceding construction of idempotents

Suppose $p\,(u,v) = \prod p_r(u,v)^{m_r}$ is the decomposition of p ($\in U_{k,0}$) into powers of distinct irreducible factors. Then, by Herzog's basic argument,

$$M \cap Ker(p) = \bigoplus_{\lambda, i} Cas(\lambda, M)_i\,,$$

where the direct sum is taken over all i such that, for some r, $p_r(\frac{\lambda(\lambda+2)}{2},\, \lambda - 2i) = 0$.

Note that $e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)}$ gives the projection onto $Cas(\lambda, M)_i$.

Now suppose each p_r is standard.

Then the different idempotents:

$e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)}$

are pairwise orthogonal, so the finite sum

$\sum_{\lambda,\, i} e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)}$

gives the projection onto $Ker(p)$.

So, $e_p = \sum_{\lambda,\, i} e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)}$. Note that $e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)}$ gives on any V_λ the projection onto a subspace of dimension ≤ 1, so these are what Herzog calls "pseudoweights".

Suppose however some p_r are nonstandard, say exactly $p_1, \ldots, p_l$ (with $l \in \mathbb{N}$). Our convention is that the p_r are distinct. There seems now no possibility of defining $e_{p_1}, \ldots, e_{p_l}$ ("nonstandard idempotents") in terms of pseudoweights.

We simply show how to define e_p in terms of the $e_{p_1}, \ldots, e_{p_l}$ and various pseudoweights.

Then $e_{p_1}, \ldots, e_{p_l}$ are not quite orthogonal to each other, but nearly so. Consider, for example, e_{p_1} and e_{p_2}, and the corresponding plane curves $\mathcal{C}_{p_1}$ and $\mathcal{C}_{p_2}$. These intersect in finitely many (algebraic) points, so there are only finitely many (λ, i) which are common zeros of $p_1(\frac{\lambda(\lambda+2)}{2},\, \lambda - 2i) = 0$ and $p_2(\frac{\lambda(\lambda+2)}{2},\, \lambda - 2i) = 0$.

By the same technique as above, one can write the projection onto $Ker(p_1) \cap Ker(p_2)$ as a finite sum of orthogonal pseudoweights. One does the same for all finite intersections of $p_1, \ldots, p_l$ and then by a routine formal argument with commuting idempotents writes the projection onto $Ker(p_1) + \ldots + Ker(p_l)$ as a polynomial in $c_{p_1}, \ldots, c_{p_l}$ and certain pseudoweights as above. Finally, taking account of the finitely (λ, i) so that $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$ but $p_j(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) \neq 0$ for $1 \leq j \leq l$, one easily writes e_p as a polynomial in $e_{p_1}, \ldots, e_{p_l}$ and definite pseudoweights.

We have shown that the ring generated over $U_{k,\,0}$ is generated by the various $e_{c-\frac{\lambda(\lambda+2)}{2}}$, $e_{h-(\lambda-2i)}$ and the e_p for p nonstandard. Obviously we will not understand U_k' till we understand the latter.

4.1 The elements of $U_{k,\,0}$ inverted in U_k'

Lemma 4.1 *$p\,(c, h)$ is invertible in U_k' if and only if $p\,(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$ has only the solution $(0, 0)$ with $0 \leq i \leq \lambda$.*

Proof. The condition just given is equivalent to $Ker(p) = \{0\}$, and is clearly equivalent to p being invertible on all $M \in FinDim$, hence to p being invertible in U_k'. □

Note that the condition just given is equivalent to $e_p = 0$.

Incorporating the inverses just considered we have a commutative ring generated over $U_{k,\,0}$ by the idempotents just discussed, together with all $\frac{1}{p}$ where $e_p = 0$.

One can go a bit further. Because of the decomposition $M = Ker(p) \oplus Image(p)$, we have in general "$p$ invertible modulo e_p" corresponding to the existence of a map which is the identity on $Ker(p)$, and the inverse of p on $Image(p)$.
It can be written naturally as $e_p + p^{-1}(1 - e_p)$, and it satisfies
$p \cdot (e_p + p^{-1}(1 - e_p)) = (1 - e_p)$.
Adding all of these gives as a commutative extension of $U_{k,\,0}$.
Note that $p \cdot (e_p + p^{-1}(1 - e_p)) \cdot p = p$. So, $e_p + p^{-1}(1 - e_p)$ "regularizes" p in the sense of making p satisfy the axiom for von Neumann regularity.

5 More on h-invariance

To go further, even before bringing x and y into the picture, one needs to consider not only U_k' but also the lattice (evidently modular) of pp-definable subgroups modulo equivalence in all $FinDim$. Herzog presents this in several ways, with emphasis on the lattice of finitely generated subobjects of the localization, corresponding to $FinDim$, of the element H (the forgetful functor) of the free abelian category over U_k [7]. Herzog uses crucially the anti-isomorphism of this lattice, $\varphi \to \varphi^-$, which we mentioned already in Section 3.1. It is very important that $\varphi \to \varphi^-$ is given completely explicitly.

In view of the basic importance of the above lattice in what follows, we should fix a suggestive notation for it. On the other hand, we do not wish to enter into a detailed discussion of Herzog's various equivalent definitions of the lattice. We have no doubt that the most elegant and fundamental approach is via categories of functors and localization, but, given our emphasis on decidability, our immediate purposes are best met by a "Lindenbaum algebra" formulation as in the first sentence of this section. We will simply take over Herzog's notation $Latt\, H_S$, where S is the Serre subcategory of coherent functors that vanish on all finite-dimensional representations of $sl_2(k)$. We will need also the extended notation $Latt\, \varphi_S$ for the lattice of subobjects of the localisation at this S of the subobject of H given by the formula φ. This of course has a perspicuous meaning in the Lindenbaum algebra formulation, in terms of equivalence modulo $FinDim$ of formulas intersected with φ.

For the above lattice, we have a natural notion of h-invariance, namely that φ is h-invariant if and only if $h\varphi \subseteq \varphi$ in $FinDim$. This is readily seen to be equivalent to φ being, in each simple finite dimensional U_k-module V_λ, a sum of weight spaces.

The fundamental result about h-invariance is the following result.

Lemma 5.1 *If φ is h-invariant, so is φ^- and $M = \varphi(M) \oplus \varphi^-(M)$ for all M in $FinDim$, so φ is complemented in the above lattice.*

Proof. See [7], page 260. □

This gives us more idempotents. For clearly if φ is h-invariant we can define the idempotent e_φ corresponding to the projection, with kernel φ^-, onto the subgroup (defined by) φ. Note however, that this is quite an abstract procedure. It is not clear at this stage how to tell if $e_\varphi = e_\psi$ in U_k'.

By the way, the preceding discussion is enough to show that the centralizer of h in U_k' is a commutative von Neumann regular ring. From r in U_k' and commuting with h, one passes to φ defining the image of r, and then to e_φ, which is h-invariant, and generates the same ideal in U_k' as r does.

The pseudoweights are the h-invariant elements φ of the lattice which in all V_λ they define spaces of dimension ≤ 1. (We have already see many of them). For such φ it follows that the lattice $Latt\,\varphi_S$ is not merely complemented (as follows from what said above) but actually uniquely complemented and is a Boolean algebra. (One should note that if φ is a pseudoweight and $\psi \subseteq \varphi$, then ψ is pseudoweight too).

Among the pseudoweights, some special ones arise as follows.
The highest weight space of V_λ is $Ker(x)$, which is of course h-invariant. We have e_x, the corresponding projection onto $Ker(x)$ (which is complemented by $Image(y)$). Herzog gives an important generalization for any idempotent e in the centralizer of h (in U_k'). He gives, explicitly in his Proposition 18, a definition of a pseudoweight e_0 corresponding to the projection of the highest weight subspace of the image of e. e_0 is called the *highest* pseudoweight of e. More precisely, on V_λ, $e_0 V_\lambda = \{0\}$ if $e = \{0\}$, and otherwise is $V_{\lambda,j}$ where j is minimal with $0 \leq j \leq \lambda$ such that $V_{\lambda,j} \subseteq eV_\lambda$.

6 Uniformly bounded φ

A pp-formula φ is said to be uniformly bounded if there is some n so that for all λ the dimension of φ in V_λ is bounded by n. (There is now no condition of h-invariance).

We have already seen some h-invariant examples, namely φ defining $Ker(p)$, for p in $U_{k,0}$. Now, (all this is in [7]) one generalizes to U_k. The basic result, with a constructive proof, is the following.

Lemma 6.1 *Suppose $q \in U_k$, $q \neq 0$. Then there is p in $U_{k,0}$ and a nonnegative integer such that*

$$Ker(q) \cap Image(y^n) \cap Image(p) \cap Image(x^n) = \{0\},$$

for all $M \in FinDim$,

Proof. See [7], page 265. □

Herzog's discussion brings into view further basic information connected to the standard/nonstandard distinction.

Suppose q, p, n are as in the preceding lemma, and $M \in FinDim$. Then $Image(p)$ is complemented by $Ker(p)$, $Image(x^n)$ is complemented by $Ker(y^n)$, and $Image(y^n)$ by $Ker(x^n)$.

We have already considered e_p, and now we consider e_{x^n}, e_{y^n} corresponding to the projections onto $Ker(x^n)$, $Ker(y^n)$ respectively. Note that $Ker(x^n)$ and $Ker(y^n)$ are h-invariant, so e_{x^n} and e_{y^n} are in the centralizer of h, and e_p, e_{x^n}, e_{y^n} pairwise commute. The idempotent $1-(1-e_p)(1-e_{x^n})(1-e_{y^n})$ gives the projection onto the complement of $Image(p) \cap Image(x^n) \cap Image(y^n)$, and this complement has dimension bounded by the sum of those of $Ker(p)$, $Ker(x^n)$ and $Ker(y^n)$.

In particular, if M is reduced, that is, is a sum of V_λ without repetitions (which is no restriction as far as elementary equivalence is concerned) both $Ker(x^n)$ and $Ker(y^n)$ have dimension $\leq n$ in each $Cas(\lambda,\, M) \neq \{0\}$, and then the above complement has dimension $\leq$ dimension of $Ker(p)+2n$.

By [7] Lemma 21, we know that the projection from $Ker(q)$ to the subspace given by $1-(1-e_p)(1-e_{x^n})(1-e_{y^n})$ is injective.

Now suppose p is standard. Then for all but finitely many λ, $Ker(p) \cap Cas(\lambda, M) = \{0\}$, and in this case, on $Cas(\lambda, M)$, the projection of $Ker(q)$ to $Ker(x^n)+Ker(y^n)$ is injective. For the other λ, one has only that the dimension of $Ker(p)$ in $Cas(\lambda, M)$ is uniformly bounded, giving the same result for $Ker(q)$.

When p is nonstandard, one has only the uniform boundedness result from the lemma above. In the sequel, we will look more closely at the nature of the kernels of general q.

For future reference, we note that Herzog's proof of the lemma above actually gives more useful information than he states.

Lemma 6.2 *Let $q = x^n a_n + x^{n-1}a_{n-1} + \ldots + xa_1 + c_0 + yb_1 + \ldots + y^m b_m$ where the a's, b's and c's are in $U_{k\,0}$. Let $w \in V_\lambda$ with $q \cdot w = 0$. For $0 \leq i \leq \lambda$, let w_i be the projection of w onto the i-th weight space.*
Let i_0 be the least i with $w_i \neq 0$, and let i_1 be the greatest i with $w_i \neq 0$. Then

i) If $a_n \neq 0$, either $a_n \cdot w_{i_0} = 0$ or $x^n \cdot w_{i_0} = 0$;

ii) If $b_m \neq 0$, either $b_m \cdot w_{i_1} = 0$ or $y^m \cdot w_{i_1} = 0$;

iii) If all $b_j = 0$ and $c_0 \neq 0$ and $a_n \neq 0$ then $q \cdot w \neq 0$;

iv) If all $a_j = 0$ and $c_0 \neq 0$ and $b_m \neq 0$ then $q \cdot w \neq 0$;

v) If all $a_j = 0$ and $c_0 = 0$, then $y^{m_1} \cdot w = 0$, where m_1 is minimal such that $b_{m_1} \neq 0$;

vi) If all $b_j = 0$ and $c_0 = 0$, then $x^{n_1} \cdot w = 0$, where n_1 is minimal such that $a_{n_1} \neq 0$.

Proof. (i) and (ii) are seen by inspection of what Herzog does on page 265. For (iii) and (iv) observe that in these cases q is $c_0 + (q - c_0)$, and $(q - c_0)$ acts nilpotently on the finite dimensional modules, so q is invertible. (v) and (vi) are done similarly, this time expressing q as a power of y (respectively x) times an invertible element. □

7 U'_k is von Neumann regular: rearranging the proof

We review the last stages of the proof quickly, indicating which points are less constructive. Firstly, Lemma 25 in [7] shows that if φ is an h-invariant uniformly bounded pp-formula, then $Latt\,\varphi_S$ (its corresponding lattice of subobjects modulo equivalence in $FinDim$) is complemented. The proof is by induction on the least n such that the dimension of $V_\lambda \cap \varphi$ $\leq n$, and is constructive in this n. By this we mean that once we know n there is an explicit recursive procedure of length n that allows us to write down complements for (formulas defining) subobjects of ϕ. But note that even for φ defining $Ker(p)$ with $p \in U_0$, it is not completely clear how constructive the exact bound n limiting the dimension is is, though in that special case a constructive upper bound for n is clear. If in the uniform boundedness of φ, an upper bound for the dimension n is given constructively, the rest of the proof is constructive, as is seen by inspection of what Herzog writes.

To complete the proof one has to drop the uniform boundedness assumption. This is done very beautifully by Herzog, using the duality and the model theory of one special U_k-module, K, the field of fractions of U_k.

K, as a left U'_k-module, is simple as a module over its endomorphism ring ([7], page 251), and thus induces a fundamental partition of the lattice of pp-definable subgroups. By the remark on simplicity, since each φ defines a module over the endomorphism ring, then either φ defines (0) in K or φ defines K in K. Moreover, the φ which define (0) form an ideal $\mathcal{I}$ in the lattice and those defining K form a complementary filter $\mathcal{F}$.

Herzog identifies $\mathcal{I}$ very neatly as given by the φ such that (modulo the theory of U_k-modules) φ is bounded by a (nontrivial) torsion condition $rv = 0$ (with $r \neq 0$).
With rather more work he shows ([7], page 253) that $\mathcal{F}$ can be characterized "dually" as the set of φ which contain a nontrivial divisibility condition, that is, contain a nontrivial $Image(r)$, with $r \in U'_k - \{0\}$.

If the field k is given recursively (as it can be if k is countable) one may combine these characterizations of $\mathcal{I}$ and $\mathcal{F}$ to show that $\mathcal{I}$, $\mathcal{F}$ and the theory of K are *recursive*.

Note that the preceding characterizations show that $\mathcal{I}$ consists of the uniformly bounded φ, and $\mathcal{F}$ consists of the φ whose codimension is uniformly bounded in the sense that the dimensions of the V_λ/φ are uniformly bounded.
Let us observe that despite its importance for the theory of PFD modules, K itself is not PFD. Indeed, $Ker(x) = \{0\}$ in K, since x is invertible in the ring K. But in every (nonzero) PFD U'_k-module, $Ker(x) \neq \{0\}$.

The proof ends by showing that each pp-formula φ has a complement in $Latt\,H_S$. There are two cases (decidable by the above discussion).

Case 1. $\varphi \in \mathcal{F}$. Even constructively, it suffices to find an h-invariant $\psi \in \mathcal{I}$ with $\varphi + \psi = H_S$. (This depends on the earlier proof that $Latt\,\psi_S$ is complemented). Herzog argues that one can assume that φ is a divisibility condition, and then the proof is routine using his Lemma 21 (our 6.2). In fact, it all works constructively. For φ contains a divisibility condition modulo the recursively enumerable theory of U_k-modules , and for any such divisibility condition we can effectively bound its codimension (and so that of φ) uniformly for all $V(\lambda)$.

Case 2. $\varphi \in \mathcal{I}$. This is done constructively, by duality.

We are still some distance from any "constructive presentation" of U'_k. For example, we have emphasized above the constructive aspects of the proof that $Latt\,H_S$ is complemented.

It is not quite immediate to get (von Neumann) regularity of U_k' (see Herzog's discussion on pages 254-256).

If we have constructed any element r in U_k', we need to explain the procedure for finding the element s with $rsr = r$ (and then it is formal to show that sr is idempotent and generates the same left ideal as r). What is needed is the following. Let e_1 correspond to projection onto $Image(r)$, and e_2 correspond to projection onto $Ker(r)$, and note that, unlike what happens when r is in the centralizer of h, in general $Image(r) \cap Ker(r) \neq \{0\}$. Let us define the element s as follows:

$$\begin{aligned} s(e_1(m)) &= (1-e_2)\cdot m_0, \quad \text{where } rm_0 = e_1(m)\,, \\ s((1-e_1)m) &= 0\,. \end{aligned}$$

Note that if $rm_0 = rm_1 = e_1(m)$, then $m_0 - m_1 \in Ker(r)$ so $(1-e_2)m_0 = (1-e_2)m_1$. So, s is a section of r. For,

$$\begin{aligned} r(s(e_1(m))) &= r((1-e_2)\cdot m_0) \\ &= rm_0 \;-\; r(e_2 m_0) \;= \\ &= rm_0 \;=\; e_1(m). \end{aligned}$$

Clearly, $rs((1-e_1)m) = 0$. So, we have $rsr = r$, and s is obtained constructively from r.

7.1 Building U_k'

It is should be clear from Herzog's analysis that the "fundamental" idempotents are the e_p ($p \in U_{k,0}$), followed first by the more general e_q ($q \in U_k$), and then by the e_{x^n}.

For generating more idempotents the highest weight idempotents e_0 associated to (previously constructed) e are crucial. Finally, the "sections" s (described above) are used systematically.

For a general $\varphi \in Latt\, H_S$, the corresponding e_φ is got relatively easily from the preceding using the test whether $\varphi \in \mathcal{I}$ or $\varphi \in \mathcal{F}$, and the corresponding dominating $Ker(q)$ or dominated $Image(q)$. So, we are now in a position to generate U_k' constructively, for k countable.

8 Constructive presentation of U_k'

Henceforward k is countable (although it is not hard to give a sensible meaning to what follows for general k). That U_k is a computable domain is clear, using the defining relations, the grading $\bigoplus_{n\in\mathbb{Z}} U_{k,n}$, and the unique representations of $U_{k,0}$ in terms of c and h, and of $U_{k,n}$ ($n \neq 0$) in terms of $x^n \cdot U_{k,0}$, $U_{k,0}\cdot x^n$, $y^n \cdot U_{k,0}$, $U_{k,0}\cdot y^n$ as before.

Now we add the idempotents e_p, corresponding to projection onto $Ker(p)$, for $p \in U_{k,0}$. Such p are written uniquely as $p(c,h)$, where $p(u,v) \in k[u,v]$.

Fix $p(u,v)$ and factor it constructively as a product of a constant and powers of monic irreducible $p_l(u,v)$ over k (for some positive integer l). It is clear ([7]) that $Ker(p)$ is the sum of the $Ker(p_l)$, and that e_p can be written equationally in terms of the (pairwise commuting) e_{p_l}. So, it is enough to add the e_{p_l}.

As in [7], we have to consider solutions in integers (λ, i) with $0 \leq i \leq \lambda$ of $p_l(\frac{\lambda(\lambda+2)}{2}, \lambda - 2i) = 0$.

There are only finitely many solutions if either:

i) p_l is not in $\mathbb{Q}[u,v]$ (the argument was given in Section 3.3),

or

ii) p_l defines a curve of genus ≥ 1 over $\mathbb{Q}$.

or

iii) p_l defines a curve of genus 0 over $\mathbb{Q}$ and certain suitable conditions are satisfied (see Section 3.3).

Now a moment's reflection shows that to decide such questions as $e_{p_l} = 0$ in the theory of PFD modules, we need to be able to decide compatibilities between the various e_p and to know, in the cases $i), ii), iii)$ above, what are the finitely many solutions. In Case (i), we can readily decide that p_l is not defined over $\mathbb{Q}$, exhibit constructively a normal number field E over which it is defined, together with a real subfield F so that $E = F(i)$. Moreover, we can obtain effectively an automorphism σ of E so that $p_l \neq {p_l}^{\sigma}$. Then Bezout applied to $C = R(i)$ gives us bounds for the absolute values of the common zeros of p_l and ${p_l}^{\sigma}$, in terms of the absolute values of the coefficients of p_l and ${p_l}^{\sigma}$, and so allows us to bound the common integral zeros, and thus the integral zeros of p_l.

For $ii)$, the problem is very profound, and no unconditional algorithm is known (though one is expected). For a thorough discussion, see [8]. It is known that if the Mordell-Weil Theorem can be constructivized then above problem is decidable [14]. Here we shall simply assume that the decision problem for curves of nonzero genus is decidable, in the sense that we can decide if a plane curve of nonzero genus over $\mathbb{Q}$ has an integer point (α, β) with α, $\beta > 0$, and then find the finitely many solutions.

Case $iii)$ involves subtleties not fully appreciated in earlier discussions [11, 15] of the genus 0 case. It is now known, using Baker's method, how to decide if a genus 0 curve has only finitely many points, and then how to find these points.

Henceforward we assume an algorithm for testing which irreducible monic p in $k[u,v]$ have only finitely many zeros $(\frac{\lambda(\lambda+2)}{2},\ \lambda - 2i)$ with $0 \leq i \leq \lambda$ (and λ, $i \in \mathbb{Z}$), and then listing those zeros.

In 3.3 we called a $p(u,v)$, which is monic, irreducible over $\mathbb{Q}$, and has only finitely many solutions $(\frac{\lambda(\lambda+2)}{2},\ \lambda - 2i)$ as above, *standard.* We now have some axioms about e_p, for p standard. An example is: $e_p = 0$, if there are no solutions $(\frac{\lambda(\lambda+2)}{2},\ \lambda - 2i)$. More generally, if $(\frac{\lambda_r(\lambda_r+2)}{2},\ \lambda_r - 2i_r)$, where $r = 1, \ldots, R$ (for some nonzero positive integer R) are all the solutions, one has an axiom: $e_p = \sum_{r=1}^{R} e_{c-\frac{\lambda_r(\lambda_r+2)}{2}} \cdot e_{h-(\lambda_r - 2i_r)}$.

So, in fact, one can define e_p for the very special idempotents on the right-hand side of the equation. For economy of notation, let us do so (that is, dispense with the general e_p as primitive).

We note that all e_p (p in $U_{k,0}$) pairwise commute. In addition, we have obvious orthogonality axioms. Firstly, $e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{c-\frac{\mu(\mu+2)}{2}} = 0$, for $\lambda \neq \mu$. Secondly, for distinct weight-spaces with $Cas(\lambda)$, we have: $e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot e_{h-(\lambda-2i)} \cdot e_{h-(\lambda-2j)} = 0$ for $i \neq j$.

The other dramatis personae at this stage are the e_p, where p is nonstandard. (We already know that there are interesting such e_p, connected to Pell equations). Such p are over $\mathbb{Q}$, monic and irreducible. Here is the first axiom:

$e_{p_1} \cdot e_{p_2} = 0$ for p_1, p_2 nonstandard if there is no $(\lambda,\ i)$ with $p_1(\frac{\lambda(\lambda+2)}{2},\ \lambda - 2i) =$

$p_2(\frac{\lambda(\lambda+2)}{2},\ \lambda-2i)=0$. More generally, for $p_1 \neq p_2$, $e_{p_1} \cdot e_{p_2} = \sum_{r=1}^{R} e_{c-\frac{\lambda_r(\lambda_r+2)}{2}} \cdot e_{h-(\lambda_r-2i_r)}$ if $(\frac{\lambda_1(\lambda_1+2)}{2},\ \lambda_1-2i_1),\ldots,(\frac{\lambda_R(\lambda_R+2)}{2},\ \lambda_R-2i_R)$ are the common zeros.
Finally, (because of the uniform boundedness phenomenon), we have $e_p \cdot e_{c-\frac{\lambda(\lambda+2)}{2}} = e_{c-\frac{\lambda(\lambda+2)}{2}} \cdot \sum_{i=1}^{s} e_{h-(\lambda-2i)}$ where $i_1,\ldots,i_s$ are the solutions of $p(\frac{\lambda(\lambda+2)}{2},\ \lambda-2i)=0$ (this includes $e_p \cdot e_{c-\frac{\lambda(\lambda+2)}{2}} = 0$ if there are no solutions). So, now we have a fragment of U'_k, generated by $U_{k,0}$ and the idempotents $e_{c-\frac{\lambda(\lambda+2)}{2}}$, the $e_{h-(\lambda-2i)}$, and the e_p for p nonstandard. Any element of this ring can be represented in the form

$$\begin{array}{lllllll}
\alpha_0 & + & \alpha_1 \cdot e_{c-\frac{\lambda_1(\lambda_1+2)}{2}} & + & \ldots & + & \alpha_m \cdot e_{c-\frac{\lambda_m(\lambda_m+2)}{2}} \quad + \\
 & + & \alpha_{m+1} \cdot e_{h-\mu_{m+1}} & + & \ldots & + & \alpha_{m+n} \cdot e_{h-\mu_{m+n}} \quad + \\
 & + & \alpha_{m+n+1} \cdot e_{c-\frac{\lambda_{m+n+1}(\lambda_{m+n+1}+2)}{2}} \cdot e_{h-\mu_{m+n+1}} & + & \ldots & + & \\
 & + & \alpha_{m+n+s} \cdot e_{c-\frac{\lambda_{m+n+s}(\lambda_{m+n+s}+2)}{2}} \cdot e_{h-\mu_{m+n+s}} & + & & & \\
 & + & \alpha_{m+n+s+1} \cdot e_{p_1} & + & \ldots & + & \alpha_{m+n+s} \cdot e_{p_t}
\end{array}$$

where the α are in $U_{k,0}$, the λ and μ are integers, $\lambda \geq 0$, and the $p_1,\ldots,p_t$ are nonstandard.

Using the relations we gave above one readily sees closure under multiplication. The crucial issue is uniqueness of the above representation. This has to be an essential part of our decision procedure. Note a slight ambiguity, as the $h-\mu$ are nonstandard according to our definition. So, we should assume that the $p_1,\ldots,p_t$ are not of this form. Note too that we should obviously assume that $\lambda_1,\ldots,\lambda_m$ are distinct and $\mu_{m+1},\ldots,\mu_{m+n}$ are distinct.
Suppose the sum above represents the zero element in U'_k.
First, suppose $\alpha_0 \neq 0$. Then let d be a bound on the dimension of $V_\lambda \cap Ker(\alpha_0)$. First restrict to (λ,μ) distinct from the (λ_r,μ_r) appearing in the sum. Then restrict further to the (λ,μ) such that $V_{\lambda,\mu}$ is not included in any of $Ker(p_1),\ldots,Ker(p_t)$. This leaves infinitely many λ to choose from. Again using uniform boundedness, one sees that there exists D so that if for some μ the pair (λ,μ) is not yet eliminated then there are $\geq \lambda - D$ such μ with (λ,μ) not yet eliminated. For any such (λ,μ) all terms except α_0 from the above sum vanish on $V_{\lambda,\mu}$. But then α_0 does too. But then if $\lambda - D > d$ we have a contradiction to uniform boundedness of α_0. So $\alpha_0 = 0$.

So now we put $\alpha_0 = 0$ in the above. As before restrict to (λ,μ) distinct from the (λ_r,μ_r) in the sum. The effect of this is that for such (λ,μ) the action of the sum on $V_{\lambda,\mu}$ is equal to that of $\alpha_{m+n+s+1} \cdot e_{p_1} + \ldots + \alpha_{m+n+s} \cdot e_{p_t}$.

Now, recall that the different $Ker(p_i)$ intersect in finite dimensional subspaces, and each $Ker(p_i)$ meets infinitely many $Cas(\lambda)$ nontrivially. Thus there are infinitely many λ so that $Ker(p_1)$ meets $Cas(\lambda)$ nontrivially, but no other $Ker(p_2)$ meets $Cas(\lambda)$ nontrivially. For each such λ choose a μ so that $p_1(\frac{\lambda(\lambda+2)}{2},\ \lambda-2\mu)=0$.
Now, $p_2(\frac{\lambda(\lambda+2)}{2},\ \lambda-2\mu) \neq 0,\ldots,p_t(\frac{\lambda(\lambda+2)}{2},\ \lambda-2\mu) \neq 0$, so $e_{p_1},\ldots,e_{p_t}$ vanish on $V_{\lambda\,\mu}$. So $\alpha_{m+n+s+1} \cdot e_{p_1}$ vanishes on $V_{\lambda,\mu}$. Thus, $\alpha_{m+n+s+1}$ and e_{p_1} have infinitely many common integer zeros, and so p_1 divides $\alpha_{m+n+s+1}$. But now we note that $p \cdot e_p = 0$ in general. This should be added to our defining relations, and so if p divides $q \in U_{k,0}$, then $q \cdot e_p = 0$. So now we should assume in our sum representation that no p_i divides $\alpha_{m+n+s+i}$. Then we conclude that each $\alpha_{m+n+s+i} = 0$ if the sum is zero.

So, finally we return to that sum under the assumption that $\alpha_0 = \alpha_{m+n+s+1} = \ldots = \alpha_{m+n+s+t} = 0$.

If λ is greater than all the λ_j that occur in the sum, then on V_λ the sum is equal to $\alpha_{m+1} \cdot e_{h-\mu_{m+1}} + \ldots + \alpha_{m+n} \cdot e_{h-\mu_{m+n}}$. Now assume, in addition, that λ is bigger than each of $|\mu_{m+1}|, \ldots, |\mu_{m+n}|$. This leaves, for each j, infinitely many λ such that $\lambda - \mu_{m+j}$ is even. It follows that for each j, $V_{\lambda, \frac{\lambda-\mu_{m+j}}{2}} \subseteq Ker\, \alpha_{m+j}$ for infinitely many λ such that $\lambda - \mu_{m+j}$ is even . By the same argument as for the nonstandard p above, $h - \mu_{m+j}$ divides α_{m+j}. So again we have an instance of $p \cdot e_p = 0$. As before we conclude that $\alpha_{m+1} = \ldots = \alpha_{m+j} = 0$ provided no $h - 2\mu_j$ divides α_{m+j}. We can in any case ignore such terms because of our defining relations, and so we come down to the case of a sum

$$\begin{array}{lllll} \alpha_1 \cdot e_{c-\frac{\lambda_1(\lambda_1+2)}{2}} & + \ \ldots \ + & \alpha_m \cdot e_{c-\frac{\lambda_m(\lambda_m+2)}{2}} & & + \\ & + \ \ldots \ + & \alpha_{m+n+1} \cdot e_{c-\frac{\lambda_{m+n+1}(\lambda_{m+n+1}+2)}{2}} \cdot e_{h-\mu_{m+n+1}} & & + \\ & + \ \ldots \ + & \alpha_{m+n+s} \cdot e_{c-\frac{\lambda_{m+n+s}(\lambda_{m+n+s}+2)}{2}} \cdot e_{h-\mu_{m+n+s}} & & \end{array}$$

which we suppose to be 0 (in U'_k). We can clearly assume $\lambda_1, \ldots, \lambda_m$ distinct, but perhaps not the distinctness of the list $\lambda_{m+n+1}, \ldots, \lambda_{m+n+s}$. There may be some overlap between the two lists. Suppose first λ_1 does not occur in the second list. Then the idempotent $e_{c-\frac{\lambda_1(\lambda_1+2)}{2}}$ is orthogonal to all the other $e_{c-\frac{\lambda(\lambda+2)}{2}}$ occurring, and we conclude that $\alpha_1 \cdot e_{c-\frac{\lambda_1(\lambda_1+2)}{2}} = 0$, But notice that this relation expresses exactly that $\alpha_1(\frac{\lambda_1(\lambda_1+2)}{2}, \lambda_1 - 2i) = 0$ for all i with $0 \leq i \leq \lambda_1$. And then the relation is simply a consequence, by our defining relations, of this fact about the number λ_1. Thus we may discard it.

So, provided we discard (as our relations permit) terms $\alpha \cdot e_{c-\frac{\lambda_i(\lambda_i+2)}{2}}$ with $c - \frac{\lambda_1(\lambda_1+2)}{2}$ dividing α_i, we can assume that all of $\lambda_1, \ldots, \lambda_m$ occur in second list too.

Dually, if some λ_{m+n+i} occurs in the second list , but not in first, we get $\alpha_{m+n+i} \cdot e_{c-\frac{\lambda_{m+n+i}(\lambda_{m+n+i}+2)}{2}} \cdot e_{h-\mu_{m+n+i}} = 0$. If μ_{m+n+i} is not of form $\lambda_{m+n+i} - 2\gamma_i$ with γ_i integral and $0 \leq \gamma_i \leq \lambda_{m+n+i}$, the above equation follows from an obvious relation on the e's, and so can be discarded . Thus we assume $\lambda_{m+n+i} - \mu_{m+n+i}$ even, with γ_i as above, and then the above equation says that $V_{\lambda_{m+n+i}\gamma_i} \subseteq Ker(\alpha_{m+n+i})$, and we can deduce that $(\frac{\lambda_{m+n+i}(\lambda_{m+n+i}+2)}{2}, \mu_{m+n+i})$ is a zero of $\alpha_{m+n+i}(u, v)$.
But conversely this forces, by an obvious relation, the equation. Thus we may discard the term $\alpha_{m+n+i} \cdot e_{c-\frac{\lambda_{m+n+i}(\lambda_{m+n+i}+2)}{2}} \cdot e_{h-\mu_{m+n+i}}$. The only remaining (notational) complication is that there may be repetitions in the second list, so that some λ_{m+n+i} occurs with both μ_{m+n+i} and at least one different μ_{m+n+j} attached.

Using orthogonality, this leads to m equations $(\alpha_i - \alpha_{m+n+i} \cdot e_{h-\mu_{m+n+i}}) \cdot e_{c-\frac{\lambda_i(\lambda_i+2)}{2}} = 0$. There are two cases (for each i).

Case 1. $\lambda_i - \mu_{m+n+i}$ even, say $= 2\gamma_i$, with $0 \leq \gamma_i \leq \lambda_i$, γ_i integral. Thus $V_{\lambda_i, \gamma_i} \subseteq Ker(\alpha_i - \alpha_{m+n+i})$ while $V_{\lambda, \gamma} \subseteq Ker(\alpha_i)$ if $\gamma \neq \gamma_i$. So we deduce that $(\frac{\lambda_i(\lambda_i+2)}{2}, \mu_{\lambda_i - 2\gamma_i})$ is a root of $(\alpha_i - \alpha_{m+n+i})(u, v)$, and for all γ with $0 \leq \gamma \leq \lambda_i$ and $\gamma \neq \gamma_i$, $(\frac{\lambda_i(\lambda_i+2)}{2}, \mu_{\lambda - 2\gamma})$ is a root of α_i.
Conversely, in Case 1, these two conditions imply the equation, using the obvious relations.

Case 2. Not Case 1.

Then the equation becomes $\alpha_i \cdot e_{c-\frac{\lambda_i(\lambda_i+2)}{2}} = 0$, and as usual this follows from formal relations.

Thus, after a long argument we have given a unique normal form for all elements of the ring generated by $U_{k,0}$ and the basic idempotents e_p for $p \in U_{k,0}$.

8.1 The centralizer of h again

The ring already described is a subring of the centralizer $Z'(h)$ of h in U'_k. Herzog has a fairly simple argument to show that $Z'(h)$ is a commutative von Neumann regular ring. He uses the notion of h-invariant pp-formula , that is pp-formula φ such that $h\varphi \subseteq \varphi$ for all $M \in FinDim$.

From the standpoint of constructivity there is a problem, for it is certainly not clear at this stage that the set of h-invariant formulas is recursively enumerable (its complement clearly is).

The basic examples of h-invariant formulas are (those defining) $Ker(p)$ and $Image(p)$ for p in $U_{k,0}$. For these we have $M = Ker(p) \oplus Image(p)$ for any $M \in FinDim$. This observation yielded the h-invariant e_p for projection onto $Ker(p)$ and $1 - e_p$ for projection onto $Image(p)$.

Other examples are $Ker(x^n)$, $Ker(y^n)$, $Image(x^n)$, $Image(y^n)$, with related decompositions

$$\begin{aligned} M &= Ker(x^n) \oplus Image(y^n) \\ &= Ker(y^n) \oplus Image(x^n) \end{aligned}$$

giving idempotents (in $Z'(h)$) e_{x^n}, e_{y^n}.

More generally we can use Lemma 6.1 to get information about $ker(q)$ for q in U. Let us use the notation of Lemma 6.1.

Then the point is that $Image(y^n) \cap Image(p) \cap Image(x^n)$ is h-invariant. Let φ be a pp-formula defining it. Since $Ker(p)$ is uniformly bounded, we have a uniform (constructive) bound on the codimension of the set defined by φ. Now by [7], Proposition 13, φ^- is also h-invariant, and $M = \varphi \oplus \varphi^-$.

Thus we have a pp-definable injection from $Ker(q)$ into φ^-, which is (constructively) uniformly bounded.

Now we can use Herzog's beautiful "highest pseudoweight" construction. Choose a bound d for the dimension of $V_\lambda \cap \varphi^-$ and construct $e_0, \ldots, e_{d-1}$ as follows. e is the idempotent for projection onto φ^- (one can write it down explicitly and constructively in terms of e_{x^n}, e_{y^n}, e_p).

By [7], Proposition 18, there is an explicit formula uniformly defining the highest weight space of φ^-, yielding an idempotent e_0 in $Z'(h)$ (in some model M for certain λ $e_0 Cas(\lambda) = \{0\}$).

Now replace φ^- by $(1 - e_0)\varphi^-$ and get e_1 defining the highest weight space for this. Again, $e_1 \in Z'(h)$. Repeat as far as the construction of e_{d-1}, and we have uniformly $\varphi^- = e_0 \cdot \varphi^- \oplus e_1 \cdot \varphi^- \oplus \ldots \oplus e_{d-1} \cdot \varphi^-$ (and the e_i are of course pairwise orthogonal).

Herzog adds a refinement, again entirely constructive. Namely, for any pseudoweight e, he writes down a pp injection from eM to $e_x M$, uniformly for $M \in FinDim$ (p. 269, end of proof of Theorem 30). This, in terms of U'_k, corresponds to having α, β, in $Z'(h)$, with

$$\begin{aligned} e_x \, \alpha \, e &= \alpha e \\ \beta \, e &= e \, . \end{aligned}$$

This implicitly contains a decomposition of the form $e_x = e_x \cdot (1 - e_\alpha) \oplus e_x \cdot e_\beta$.
Note too that it shows that e is in the ideal generated by e_x in $Z'(h)$, and so in both the left and right ideals generated by e_x in U'_k.

Thus we see that constructively we have for each $q \neq 0$ in U_k a pp injection of $Ker(q)$ into $Ker(x^n)$ (n, q as Lemma 8.2).

One can then generalize this to get, for a pp-formula φ in $\mathcal{I}$, constructively and uniformly a pp injection of φ into $Ker(x^n)$ for some n.

A crucial point now is the constructive content of Herzog's argument, which shows that the lattice of subobjects of an h-invariant $\varphi \in \mathcal{I}$ is complemented. The proof is by induction on a bound for the dimension in the uniform boundedness condition. To do this constructively is nontrival, as we still lack a proof that h-invariance is a recursively enumerable condition.

What we do is in fact quite reminiscent of the sort of unwindings pioneered in logic by Kreisel [9], although his unwindings are not generally associated to presentations of structures.

8.2 An enumeration of U'_k

We have repeatedly stressed that the theory of PFD is co-re, and that we have not yet improved this. We expect to do so in the sequel, by bringing more number theory to bear. What we have done, in the preceding, is to give a normal form, and in particular a recursive enumeration, for the elements of the ring generated by $U_{k,0}$ and the basic idempotents e_p for $p \in U_{k,0}$. The "enumeration" we now give of the whole of U'_k is much weaker, and we explain how.

The elements of U'_k are associated, not at all uniquely, to pp-formulas $\varphi(u, v)$ which satisfy the not obviously r.e condition of defining maps on each M in PFD. It is perfectly clear that there are recursive operations $+$, $-$ and $\cdot$ on the class of all pp-formulas $\varphi(u, v)$ which when restricted to those in U'_k give the operations of U'_k. That is, the ring operations on U'_k lift naturally to operations on the set of all $\varphi(u, v)$. What remains to be proved, hopefully in the sequel, is that the equality in U'_k lifts to a recursive operation on the set of all $\varphi(u, v)$. Thus, in this paper, when we talk of presenting U'_k we have in mind a set of pp-formulas, with recursive operations $+$, $-$ and $\cdot$ (and some other recursive operations with algebraic significance), but we make no assumptions about the equality. We do not wish to enter into formalities of recursive model theory here. What we intend should be clear from what follows. Any time we have an enumeration as above, with liftings of the ring operations (and maybe others) recursively enumerable, but the equality not assumed r.e, we say we have a weakly enumerated structure. Note, however, that we do not regard the lifted structures in our case as rings. They simply become so modulo an equivalence relation which can be very complicated. When we want to refer to the liftings of the ring operations we call our structure a pre-ring.

The ring generated by $U_{k,0}$ and the basic idempotents e_p for $p \in U_{k,0}$, for which we have given a genuine recursive presentation, is a subring of the centralizer $Z^{'}(h)$ of h in U'_k. Note that we have a recursive enumeration of certain pp formulas defining these elements (although we certainly do not have all such pp formulas).

Now, following Herzog, we construct a weakly enumerated structure which lifts, as above, a von Neumann regular ring $Z^+(h)$ which is a subring of $Z^{'}(h)$ and contains the ring generated by $U_{k,0}$ and the basic idempotents e_p for $p \in U_{k,0}$. Basically, we have to start with the latter ring (note that for it we have identified the collapsing congruence as recursively enumerable, and so we can without danger conflate the pre-ring and the ring) and close, in the sense of pre-rings under

1. going from r to $Image(r)$ to the idempotent (Herzog, page 261) corresponding to projection onto $Image(r)$;
2. the ring operations.

Note that these operations have clear meaning at the level of pp-formulas.

In this way we see clearly that $Z^{+}(h)$ is weakly presented. Moreover, it has a "section" operator as defined in Section 7. In this context this means that we have an operation taking an r to an s so that $(r - rsr, 0)$ is in the congruence, and this operation is recursive.

8.3 From $Z^{+}(h)$ towards the lifting of $U_k^{'}$, via lattice considerations

Here we follow Herzog's page 265. As we pointed out already, $\mathcal{I}$ and $\mathcal{F}$ are recursive. Indeed, his argument shows that we can recursively find, for φ in $\mathcal{I}$, a bound n so that $dim_k \varphi(V_\lambda) \leq n$ (enumerate the theory of U_k-modules to get φ bounded by a $Ker(q)$, for $q \in U_k$). There is of course a very serious issue of getting optimal n, but this can be bypassed, for now, by using Herzog's fundamental "highest pseudoweight space" operator, which is recursive at the pre-ring level, if suitably interpreted. First note that we can recursively bound the dimension of $Ker(q)$ using the workhorse Lemma 6.1 from the section on uniformly bounded φ.

We are going to make crucial use of the details of Herzog's work on his page 262 on the highest pseudoweight space construction. This takes one constructively from any (definition of an) idempotent e in $Z^{'}(h)$ to a definition, by an h-invariant pp-formula, of the highest weight space of eV_λ, uniformly in λ. Then in turn one gets (a pp definition of) the idempotent e_0 corresponding to projection onto this highest weight space. We will use the notation $hw(e)$ as being more memorable than e_0.

Now we first pass to a bigger pre-ring $Z^{++}(h)$, got from $Z^{+}(h)$ by closing off, in the obvious recursively enumerable way, under hw and all the operations previously used to construct $Z^{+}(h)$. Again we have a pre-ring which is weakly enumerated and, again, we have closure under the section operation, so that we have a lifting of a von Neumann regular subring of $U_k^{'}$.

Now we prove a constructive analogue of Herzog's Lemma 25. Suppose $\varphi(u)$ corresponds to an idempotent $1 - e$ in $Z^{++}(h)$, and $\varphi(u)$ is in $\mathcal{I}$. Find a recursive bound n for $dim_k \varphi(V(\lambda))$. Form successively:

$$f_0 = e - hw(e), f_1 = f_0 - hw(f_0), \ldots$$

proceeding through $n+1$ steps (the series may well stabilize before this, but it will stabilize by $n + 1$ steps). Each f_i is in $Z^{++}(h)$. An easy constructive argument (based on Herzog's proposition 16) shows that the lattice of subobjects (relative to $FinDim$) of each $Im(f_i)$ is a Boolean algebra, and then by easy and explicit Boolean algebra we get

Lemma 8.1 *The lattice of subobjects of φ as above is complemented and the corresponding idempotents are in $Z^{++}(h)$.*

One should really emphasize the constructive aspects of this prior to collapsing by the lattice congruence coming from $FinDim$. The lattice operations, and the complementation, are constructive at the level of pp-formulas. The congruence itself is not yet fully analyzed from a constructive viewpoint.

Now we consider a general φ. As in Herzog there are two cases.

Case 1. φ in $\mathcal{F}$. Get constructively $q \in U$ so that φ dominates $Image(q)$ in the theory of U-modules. Then, by Herzog's Lemma 21, get p in U_0, so that for all V in $FinDim$

$$Im(q) + Ker(x^n) + Ker(\theta\sigma(\rho)) + Ker(y^n) = 0$$

so that in Herzog's notation for the lattice of subobjects of H

$$\varphi + \psi = H\,,$$

where ψ is the sum of the three kernels in the above equation. But evidently ψ is in $Z^{++}(h)$, whence the lattice of subobjects of ψ is constructively complemented, by the preceding lemma. So, constructively, as in Herzog, we get a complement for φ in H.

Case 2. φ in $\mathcal{I}$. Now work with φ^- in $\mathcal{F}$.

What has been proved constructively? In terms analogous to those used on "liftings" of $U_k^{'}$, we have considered the set of pp-formulas in one free variable, and put on it recursive liftings of the lattice operations, the sum operation, and a relative complement operation, which, modulo the congruence associated to FinDim, become the Herzog operations on subobjects of H.

We stress that we are fully aware of the sketchy nature of our discussion. This is typical of the unwinding of proofs. We do not expect understanding from a reader who is not already familiar with Herzog's precise but non-effective construction. In the sequel we will be more precise, depending on the demands of the situation.

8.4 Reaching $U_k^{'}$ as a constructive von Neumann regular semiring

If one wants to proceed constructively, then the preceding arguments are not quite enough to get a presentation of a lifting of $U_k^{'}$. On page 266 of Herzog, he can conclude directly that $U_k^{'}$ is von Neumann regular. We have to do more, because we have used, as Herzog does without comment, only binary $\varphi(u, v)$ that define maps from H to H. We should, and can, get round the prima facie nonconstructive nature of this restriction.

Lemma 8.2 *We can attach constructively to every pp-formula φ in two free variables a pp-formula φ^f in the same variables such that*

- *φ^f does define a function on H;*
- *φ^f defines the same function as φ on H if φ defines a function on H.*

Proof. Let $\varphi(u, v)$ be pp-formula. Let $\chi(v)$ be $\varphi(0, v)$. Then $\varphi(u, v)$ fails to be the graph of a(partial) function only if $\chi(V) \neq 0$ for some V in FinDim. If $\varphi(u, v)$ does define a function then the function is total on V if and only if $\theta(V) = V$, where θ is $(\exists w)\varphi(v, w)$. Now we have constructively the (liftings of) definable idempotents e_χ and

e_θ corresponding to projection to the respective subspaces $\chi(V)$ and $\theta(V)$ (the projections got from constructive definable complements in the set of pp-formulas in one variable).

Now we define a pp-formula φ^{pf} in two variables by

$$(\exists w)(\varphi(u,v)(1-e_\chi(w))=v)\,.$$

Clearly this is the graph of a partial function, for if $\varphi(u,w_1)$ and $\varphi(u,w_2)$ and $(1-e_\chi)(w_1)=v_1$ and $(1-e_\chi)(w_2)=v_2$ in V then $\chi(w_1-w_2)$ and so $(1-e_\chi)(w_1)=(1-e_\chi)(w_2)$ since w_1-w_2 lives on χ.

Equally clearly, if φ is the graph of a partial function on V then e_χ annihilates V, so $1-e_\chi$ is the identity on V so φ and φ^{pf} define the same partial function. Finally, let $\varphi^f(u,v)$ be $\varphi^{pf}(e_\theta(u,v))$, and we clearly have the required conclusion. □

What we have done above replaces Herzog's terse argument. For now we can take as our domain for the lifting the set of all φ in two variables, replacing φ systematically by φ^f to get a prering structure which is obviously recursive. Moreover, by going from φ^f to its image (construed as in the set of all pp-formulas in one variable), we get, constructively, the section operator on our domain, and thus a proof that when we mod out the congruence coming from $FinDim$, we have a von Neumann regular ring, Herzog's $U_k^{'}$.

8.5 Concluding Remarks

Our ultimate goal is to exhibit $U_k^{'}$ as a genuine recursive von Neumann regular ring, and thereby to get decidability of the theory of $FinDim$, as well as a clear understanding of the algebra of sets

$$\{\lambda : V_\lambda \models \Phi\}\,,$$

for Φ a sentence of the language of U_k-modules. Till now we have considered in detail only the variation of kernels of p for p in U_0. In the next paper we will go on to consider the finer detail of the structure of the $Ker(q)$ for general q in U_k. Various uses will be made of deeper diophantine geometry. Thus we will give a normal form for the nonstandard p, and analyze, for pairs of nonstandard elements p_1 and p_2, the set of λ for which each has a nonzero kernel in V_λ. A deep theorem relating to this is that of Bilu and Tichy [2]. We expect that this analysis will lead us to a recursive presentation of $U_k^{'}$.

References

[1] J. Ax, The elementary theory of finite fields, *Annals of Math.*, 88 (1968), 239-271

[2] Y.F. Bilu, R.F. Tichy, The Diophantine equation $f(x) = g(y)$, *Acta Arith.* 95 (2000), no. 3, 261-288

[3] N. Bourbaki, *Lie groups and Lie Algebras*, Springer, 2002

[4] C.C. Chang, H.J. Keisler, *Model theory*, North-Hollad, Amsterdam, 1973

[5] J. Dixmier, *Enveloping Algebras*, North Holland, 1977

[6] K. Erdmann, M. Wildon, *Introduction to Lie algebras*, Springer, SUMS series, 2006

[7] I. Herzog, The pseudo-finite dimensional representations of $sl(2, k)$, *Selecta Mathematica* 7 (2001), 241-290

[8] M. Hindry, J. Silverman, *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, 201, Springer, 2000

[9] A. Macintyre, The mathematical significance of proof theory, *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* 363 (2005), no. 1835, 2419-2435

[10] A. Mostowski, On direct products of theories. *J. Symbolic Logic* 17 (1952), 1-31

[11] D. Poulakis, Affine curves with infinitely many integral points, *Proc. Amer. Math. Soc.* 131 (2003), no. 5, 1357-1359

[12] M. Prest, *Model theory and modules*, Cambridge UP, 1988

[13] M. Prest, G. Puninski, Pure injective envelopes of finite length modules over a Generalised Weyl Algebra, *J. Algebra* 251 (2002), 150-177

[14] J.P. Serre, *Lie algebras and Lie groups: 1964 Lectures given at Harvard University*, LNM 1500, Second Edition, 1992.

[15] J. Silverman, On the distribution of integer points on curves of genus zero, *Theoretical Computer Science* 235 (2000), 163-170

[16] W. Szmielew, Elementary properties of abelian groups, *Fund. Math.* 41 (1955), 203-271

[17] J.S. Wilson, On pseudofinite simple groups, *J. London Math. Soc.* (2) 51 (1995), 471-490

[18] M. Ziegler, Model theory of modules, *Ann. Pure Appl. Logic* 26 (1984), 149-213