# Linear Algebra over Z_p[[u]] and related rings <br> Xavier Caruso, David Lubicz 

## To cite this version:

Xavier Caruso, David Lubicz. Linear Algebra over Z_p[[u]] and related rings. LMS Journal of Computation and Mathematics, 2014, 17 (1), pp.302-344. 10.1112/S146115701300034X . hal-00759827

## HAL Id: hal-00759827

## https://hal.science/hal-00759827

Submitted on 3 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Linear Algebra over $\mathbb{Z}_{p}[[u]]$ and related rings 

Xavier Caruso, David Lubicz

December 3, 2012


#### Abstract

Let $\mathfrak{R}$ be a complete discrete valuation ring, $S=\mathfrak{R}[[u]]$ and $n$ a positive integer. The aim of this paper is to explain how to compute efficiently usual operations such as sum and intersection of sub- $S$-modules of $S^{d}$. As $S$ is not principal, it is not possible to have a uniform bound on the number of generators of the modules resulting of these operations. We explain how to mitigate this problem, following an idea of Iwasawa, by computing an approximation of the result of these operations up to a quasi-isomorphism. In the course of the analysis of the $p$-adic and $u$-adic precisions of the computations, we have to introduce more general coefficient rings that may be interesting for their own sake. Being able to perform linear algebra operations modulo quasi-isomorphism with $S$-modules has applications in Iwasawa theory and $p$-adic Hodge theory.


## Contents

1 Introduction ..... 1
2 Arithmetic of the rings $S_{\nu}$ ..... 3
2.1 Notations ..... 3
2.2 Definition and first properties of $S_{\nu}$ ..... 4
2.3 Division in $S_{\nu}$ ..... 6
3 Modules over $S_{\nu}$ ..... 8
3.1 Quasi-isomorphism and maximal modules ..... 9
3.2 An approach based on localisation ..... 12
3.3 A generalisation of Iwasawa's theorem and applications ..... 17
3.4 Comparing the two approaches ..... 29
4 Representation and precision ..... 30
4.1 Generality with precision ..... 31
4.2 Finite precision computation with elements of $S_{\nu}$ ..... 33
4.3 Finite precision computation with modules with coefficients in $S_{\nu}$ ..... 35

## 1 Introduction

Let $\Re$ be a complete discrete valuation ring (see $\S 2.1$ for a reminder of the definition) whose valuation is denoted by $v_{\Re}$. Let $K$ denote its fraction field with valuation $v_{K}$ and $\pi$ be a uniformizer of $\mathfrak{R}$. We set $S=\mathfrak{R}[[u]]$; it is the ring of formal series over $\mathfrak{R}$. Our aim is to provide efficient algorithms to deal with finitely generated modules over $S$. Since, we can always represent a torsion module as the quotient of two torsion-free modules, we shall focus on torsion-free modules.

Any finitely generated torsion-free $S$-module $\mathscr{M}$ can be considered as a submodule of $S^{d}$ for $d$ big enough. As a consequence, we can represent $\mathscr{M}$ by a matrix whose columns are the coefficients of generators of $\mathscr{M}$ in the canonical basis of $S^{d}$. Thus we can reformulate our problem as follows: given $M_{1}$ and $M_{2}$ two matrices representing respectively the $S$-modules $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ embedded in $S^{d}$, give algorithms to compute a matrix representing $\mathscr{M}_{1} \cap \mathscr{M}_{2}$ or $\mathscr{M}_{1}+\mathscr{M}_{2}$. We would like
also to be able to check membership, equality of sub- $S$-modules, inclusions, etc. As $S$ is not a principal ideal domain, in order to control the number of generators of the sub- $S$-modules of $S^{d}$, we propose, following an idea of Iwasawa, to compute approximations of the submodules resulting of aforementioned operations in the following sense: we say that a morphism $\mathscr{M}_{1} \rightarrow \mathscr{M}_{2}$ is a quasiisomorphism if its kernel and co-kernel have both finite length, and we want to make computations modulo quasi-isomorphisms. We propose two different approaches, each of them having its own advantages and disadvantages.

First, we notice that there exists a correspondence between the set of classes of modules modulo quasi-isomorphism and modules over the rings $S_{\pi}$ and $S_{u}$ defined respectively as the localization of $S$ with respect to $\pi$ and the completion of the localization of $S$ with respect to $u$. For $A=$ $S_{\pi}, S_{u}$, let Free ${ }_{A}^{d}$ be the set of free sub- $A$-modules of $A^{d}$, and denote by $\operatorname{Mod}_{S / \text { qis }}^{d}$ the set of quasiisomorphism classes of sub- $S$-modules of $S^{d}$, there is an injective morphism $\Psi^{\prime}: \operatorname{Mod}_{S / \text { qis }}^{d} \rightarrow$ $\operatorname{Free}_{S_{\pi}}^{d} \times \operatorname{Free}_{S_{u}}^{d}, \overline{\mathscr{M}} \mapsto\left(\mathscr{M} \otimes_{S} S_{\pi}, \mathscr{M} \otimes_{S} S_{u}\right)$, where $\mathscr{M}$ is any representative in the class $\overline{\mathscr{M}}$. The image of $\Psi^{\prime}$ can be precisely characterized (see Theorem 1.1 below). Using this correspondence, operations with modules with coefficients in $S$ reduces to the computation with modules over $S_{\pi}$ and $S_{u}$. As these two last rings are Euclidean, there exist classical canonical representations and algorithms to manipulate modules over these rings.

A second approach consists in finding a canonical representative in a class of modules modulo quasi-isomophism which is amenable to computations. Such a representative is provided by the maximal module of a $S$-module $\mathscr{M}$. It can be defined as the unique free module in the class of quasi-isomorphism of $\mathscr{M}$. We present an algorithm to compute the maximal module associated to a sub- $S$-module of $S^{d}$ which is inspired by a construction of Cohen, presented in [10, p. 131], to obtain a classification up to quasi-isomorphism of finitely generated $S$-modules. We can then compose this algorithm with algorithms to compute basic operations on free modules in order to compute with representatives up to quasi-isomorphisms.

In order to obtain real algorithms (i.e. something computable by a Turing machine) we have to consider the fact that elements of $S$ and its localized are not finite. In this paper we consider an approach in two steps in order to solve this problem. First, we give the ability to Turing machines, to manipulate, by the way of oracles, elements of $S, S_{\pi}, S_{u}$. More precisely, we suppose given oracles able to store elements of the base ring, compute valuation, multiplication, addition, inversion, and Euclidean division. We express the complexity of an algorithm with oracle by the number of calls to the oracles to compute ring operations. Once we have well defined algorithm with oracles to compute with modules, we study in a second time the problem of turning them into real algorithms.

Much in the same way as for floating point arithmetic, the actual computations with modules with coefficients in $S$ are done with approximations up to certain $\pi$-adic and $u$-adic precisions. It is important to ensure that the (truncated) outputs of our algorithms are correct which means that they do not depend on the $\pi$ or $u$ powers of the input that we have forgotten. In order to deal with this precision analysis, it is convenient to consider a generalisation of the family of ring coefficients $S$. Namely, given $\alpha, \beta$ relatively prime integers, we write $\nu=\beta / \alpha$ and set $S_{\nu}=\left\{\sum a_{i} u^{i} \in K[[u]] \mid v_{K}\left(a_{i}\right)+\nu i \geq 0, \forall i \in \mathbb{N}\right\}$. We have $S_{0}=S$. In this paper, we develop a theory of $S_{\nu}$-modules which encompass modules over $S$ and use it in order to obtain algorithm with complexity bounds and proof of correctness.

More precisely, we generalize the definition of a maximal module for finitely generated torsionfree $S_{\nu}$-modules. Denote by $\operatorname{Max}_{S_{\nu}}^{d}$ the set of maximal sub- $S_{\nu}$-modules of $S_{\nu}^{d}$. We prove the following theorem (see Theorem 3.12), which generalize the above mentioned decomposition:

## Theorem 1.1. The natural map

$$
\begin{aligned}
\Psi: \operatorname{Max}_{S_{\nu}}^{d} & \longrightarrow \operatorname{Free}_{S_{\nu, \pi}}^{d} \times \operatorname{Free}_{S_{\nu, u}}^{d} \\
\mathscr{M} & \mapsto\left(\mathscr{M}_{\pi}, \mathscr{M}_{u}\right) .
\end{aligned}
$$

is injective and its image consists of pairs $(A, B)$ such that $A$ and $B$ generate the same $\mathscr{E}$-vector space in $\mathscr{E}^{d}$. If a pair $(A, B)$ satisfies this condition, its unique preimage under $\Psi$ is given by $A \cap B$.

In the theorem, $\mathscr{E}$ is a field containing $S_{\nu}$ and its localized $S_{\nu, \pi}$ and $S_{\nu, u}$ which is precisely defined in Section 2.2. We give an algorithm with oracles to compute the maximal module associated to
a finitely generated torsion-free $S_{\nu}$-module. In general, it is not true that the maximal module of a torsion-free $S_{\nu}$-module is free, although this property holds when $\nu=0$. Nonetheless, by using the theory of continued fraction, it is possible to obtain a tight upper bound on the number of generators of a maximal module embedded in $S_{\nu}^{d}$. If $\nu$ is rational, it admits a unique finite development as a continued fraction that we denote by $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ (here, we suppose that $a_{n} \neq 1$ ). We can prove the following (see Theorem 3.32):

Theorem 1.2. Let $\nu=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. Let $\mathscr{M}$ be a sub- $S_{\nu}$-module of $S_{\nu}^{d}$. Then $\operatorname{Max}(\mathscr{M})$ is generated by at most $d \cdot\left(2+\sum_{i=1}^{\lceil n / 2\rceil} a_{2 i}\right)$ elements.

We provide some simple examples to show that a lot of basic operations that we need in order to compute with modules over $S_{\nu}$, such as the computation of the Gauss valuation, are not stable. This means that, in general, the computation with approximations of the input data does not yield approximation of the result. This is where it becomes interesting to use the possibility to change the slope $\nu$ of the base ring $S_{\nu}$. In the context of our computation, a bigger slope plays the role of a loss of precision in the computation of an approximation of a module over $S_{\nu}$. In this direction, we can prove the following theorem (see Theorem 4.7 for a precise statement):

Theorem 1.3. Let $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ be two finitely generated sub- $S_{\nu}$-modules of $S_{\nu}^{d}$ such that $\mathscr{M}_{2} \subset$ $1 / \pi^{c} \mathscr{M}_{1}$ for a positive integer $c$. Let $M_{1}$ and $M_{2}$ be the matrices with coefficients in $S_{\nu}$ of generators of $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ in the canonical basis of $S_{\nu}^{d}$. Suppose we are given approximations $M_{1}^{r}$ and $M_{2}^{r}$ of $M_{1}$ and $M_{2}$ respectively. Then, for a well chosen $\nu^{\prime}>\nu$, there exists a polynomial time algorithm in the length of the representation of $M_{1}^{r}$ and $M_{2}^{r}$ to compute a matrix $M_{3}^{r}$ which is an approximation of the maximal module associated to $\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+\left(\mathscr{M}_{2} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)$.

The organisation of the paper is as follows: in $\S 2$, we introduce the rings $S_{\nu}$, and their basic arithmetic and analytic properties. In $\S 3$, we generalize some classical results of Iwasawa to the case of finitely generated $S_{\nu}$-modules and then give an algorithm with oracle to compute the maximal module associated to a torsion-free $S_{\nu}$-module and obtain an upper bound on the number of generators of a maximal module. Note that $\S 2$ and $\S 3$, we only describe algorithms with oracles. In $\S 4$, we study the problem of $p$-adic and $u$-adic precisions and turn the algorithms with oracles obtained in the previous sections into real algorithms.

## 2 Arithmetic of the rings $S_{\nu}$

In order to compute with modules over $S_{\nu}$ we first have to study the basic arithmetic properties of their base ring. In this section, we show that its localized with respect to $u^{\alpha} / \pi^{\beta}$ and $\pi$ becomes Euclidean. We provide algorithms with oracles to compute the Euclidean division in these rings which will be very useful for our purpose along with their complexity expressed in term of the number of ring operations. They will be turned into real algorithms (i.e. working on a real Turing machine) in $\S 4$ where we study the problem of precision of computation in the rings $S_{\nu}$.

### 2.1 Notations

We fix the notations for the rest of the paper. Let $\mathfrak{R}$ be a ring equipped with a discrete valuation $v_{\Re}$, that is a map $v_{\Re}: \Re \rightarrow \mathbb{N}_{\geq 0} \cup\{+\infty\}$ satisfying the following conditions:

- for all $x \in \mathfrak{R}, v_{\mathfrak{R}}(x)=+\infty$ if and only if $x=0$;
- for all $x \in \mathfrak{R}, v_{\mathfrak{R}}(x)=0$ if and only if $x$ is invertible;
- for all $x, y \in \mathfrak{R}, v_{\mathfrak{R}}(x y)=v_{\mathfrak{R}}(x)+v_{\mathfrak{R}}(y)$;
- for all $x, y \in \mathfrak{R}, v_{\mathfrak{R}}(x+y) \geq \min \left(v_{\mathfrak{R}}(x), v_{\mathfrak{R}}(y)\right)$.

Let $a$ be a fixed real number in $(0,1)$. One can define a distance $d$ on $\mathfrak{R}$ by the formula $d(x, y)=$ $a^{v_{\mathfrak{R}}(x-y)}(x, y \in \mathfrak{R})$ where we use the convention that $a^{+\infty}=0$. For the rest of the paper, we assume that $\mathfrak{R}$ is complete with respect to $d$. We recall that $\mathfrak{R}$ is a local ring whose maximal ideal
is $\mathfrak{M}=\left\{x \in \mathfrak{R} \mid v_{\mathfrak{R}}(x)>0\right\}$. Up to renormalizing $v_{\mathfrak{R}}$, it is safe to assume that it is surjective, what we do. We denote by $\pi$ a uniformizer of $\mathfrak{R}$, that is an element of $\mathfrak{R}$ whose valuation is 1 . Every element $x$ in $\mathfrak{R}$ can then be written $x=\pi^{r} u$ where $r=v_{\mathfrak{R}}(x)$ and $u \in \mathfrak{R}$ is invertible. Here are several classical examples of such rings $\mathfrak{R}$ :

- the ring $\mathbb{Z}_{p}$ of $p$-adic integers equipped with the usual $p$-adic valuation;
- more generally, the ring of integers of any finite extension of $\mathbb{Q}_{p}$;
- for any field $k$, the ring $k[[u]]$ of formal power series with coefficients in $k$.

We now go back to a general $\Re$. It follows easily from the definition that the field of fractions of $\mathfrak{R}$ is just $\mathfrak{R}[1 / \pi]$. Let's denote it by $K$ and set $S=\mathfrak{R}[[u]]$, the ring of formal series over $\mathfrak{R}$. The valuation $v_{\Re}$ can be extended uniquely to a valuation $v_{K}$ on $K$.

### 2.2 Definition and first properties of $S_{\nu}$

Denote by $K[[u]]$ the power series ring with coefficients in $K$. It is classical to define the Gauss valuation of an element $\sum a_{i} u^{i} \in K[[u]]$ as the smallest $v_{K}\left(a_{i}\right)$ if it exists. The ring of elements of $K[[u]]$ with non negative Gauss valuation is nothing but $\mathfrak{R}[[u]]$. In this section, we are going to consider more generally a family of valuations parametrized by a slope $\nu \in \mathbb{Q}$ so as to define the subring of $K[[u]]$ of elements with positive valuation.

Definition 2.1. Let $\nu \in \mathbb{Q}$. We define the Gauss valuation $v_{\nu}: K[[u]] \rightarrow \mathbb{Q} \cup\{+\infty,-\infty\}$ by $v_{\nu}(x)=+\infty$ if $x=0, v_{\nu}\left(\sum a_{i} u^{i}\right)=\min \left\{v_{K}\left(a_{i}\right)+\nu i, i \in \mathbb{N}\right\}$ if $x \neq 0$ and this minimum exists and $v_{\nu}(x)=-\infty$ otherwise. The Weierstrass degree of $x$ denoted $\operatorname{deg}_{W}^{\nu}(x)$ is given by $\operatorname{deg}_{W}^{\nu}(0)=-\infty$, $\operatorname{deg}_{W}^{\nu}(x)=\min \left\{i \mid v_{K}\left(a_{i}\right)+\nu i=v_{\nu}(x)\right\}$ if $v_{\nu}(x) \neq-\infty$ and $\operatorname{deg}_{W}^{\nu}(x)=+\infty$ otherwise. When no confusion is possible, we will use the notation $\operatorname{deg}_{W}$ instead of $\operatorname{deg}_{W}^{\nu}$.


Figure 1: The Gauss valuation of $\pi^{2} \cdot u^{4}$ with $\nu=1 / 3$ is $10 / 3$.
The following lemma gives some basic properties of $v_{\nu}$ and $\operatorname{deg}_{W}$. In particular, it shows that $v_{\nu}$ has the usual properties of a valuation:

Lemma 2.2. For $x, y \in K[[u]]$ we have:

1. $v_{\nu}(x)=+\infty$ if and only if $x=0$;
2. $v_{\nu}(x \cdot y)=v_{\nu}(x)+v_{\nu}(y)$;
3. $v_{\nu}(x+y) \geq \min \left(v_{\nu}(x), v_{\nu}(y)\right)$.

Moreover for all $x, y \in K[[u]]$ with finite Gauss valuation, $\operatorname{deg}_{W}(x . y)=\operatorname{deg}_{W}(x)+\operatorname{deg}_{W}(y)$.
Proof. To prove 2., we first suppose that $x=\sum a_{i} u^{i}$ and $y=\sum b_{i} u^{i}$ have finite valuation. Let $z=x \cdot y=\sum c_{i} u^{i}$. We have $v_{K}\left(c_{i}\right)+\nu i=v_{K}\left(\sum_{j=0}^{i} a_{j} \cdot b_{i-j}\right)+\nu i \geq \min _{j}\left\{v_{K}\left(a_{j}\right)+\nu \cdot j+\right.$ $\left.v_{K}\left(b_{i-j}\right)+\nu \cdot(i-j)\right\} \geq v_{\nu}(x)+v_{\nu}(y)$. Moreover, by taking $i=\operatorname{deg}_{W}(x)+\operatorname{deg}_{W}(y)$ in the previous computation, we obtain that $v_{K}\left(c_{\operatorname{deg}_{W}}(x)+\operatorname{deg}_{W}(y)\right)=v_{\nu}(x)+v_{\nu}(y)$. If $v_{\nu}(x)=-\infty$ and $y \neq 0$, we can apply the previous result to the series obtained by truncating $x$ up to a certain power to show that $v_{\nu}(x \cdot y)=-\infty$. The proof of the rest of the lemma is left to the reader.

We let $S_{\nu}=\left\{x \in K[[u]] \mid v_{\nu}(x) \geq 0\right\}$. By definition, an element $x \in S_{\nu}$ can we written as a series

$$
x=\sum_{i \in \mathbb{N}} a_{i} u^{i},
$$

where $a_{i} \in K$ and $v_{K}\left(a_{i}\right) \geq-\nu i$.
Remark 2.3. It is clear that $S_{\nu}$ is complete for the valuation $v_{\nu}$. Nonetheless, the ring $S_{\nu}$ is not a valuation ring. In fact, although $v_{\nu}\left(u^{\alpha} / \pi^{\beta}\right)=0$ for $\nu \neq 0\left(\right.$ resp. $v_{\nu}(u)=0$ for $\left.\nu=0\right), u^{\alpha} / \pi^{\beta}$ (resp. u) is not invertible in $S_{\nu}$.

We let

$$
S_{\nu, \pi}=S_{\nu}[1 / \pi]=\left\{\sum_{i \in \mathbb{N}} a_{i} u^{i}, a_{i} \in K \text { such that } v_{K}\left(a_{i}\right)+\nu i \text { bounded below }\right\}
$$

In the same way, it is clear that one can extend the $v_{\nu}$ valuation of $S_{\nu}$ over $S_{\nu}\left[\pi^{\beta} / u^{\alpha}\right]$ and we let $S_{\nu, u}=S_{\nu} \widehat{\left[\pi^{\beta} / u^{\alpha}\right]}$ where the hat stands for the completion of $S_{\nu}\left[\pi^{\beta} / u^{\alpha}\right]$ with respect to the topology defined by $v_{\nu}$.

Put in another way,

$$
S_{\nu, u}=\left\{\sum_{i \in \mathbb{Z}} a_{i} u^{i}, a_{i} \in S_{\nu} \text { and } \lim _{i \rightarrow-\infty} v_{K}\left(a_{i}\right)+\nu i=+\infty\right\}
$$

We moreover define

$$
\mathscr{E}=\left\{\sum_{i \in \mathbb{Z}} a_{i} u^{i}, a_{i} \in K v_{K}\left(a_{i}\right)+\nu i \text { bounded below and } \lim _{i \rightarrow-\infty} v_{K}\left(a_{i}\right)+\nu i=+\infty\right\} .
$$

We have the following commutative diagram of inclusions:


As $S_{\nu, \pi}$ is a subring of $K[[u]]$, it is equipped with the $v_{\nu}$ valuation and the Weierstrass degree associated to $v_{\nu}$. Moreover, one can extend, in an obvious manner, the definition of $v_{\nu}$ and the Weierstrass degree for $S_{\nu, u}$ and $\mathscr{E}$.

We can interpret the ring $S_{\nu}$ in terms of the analytic functions on the $\pi$-adic disc. In order to explain this, for $\nu \in \mathbb{Q}$, we consider the open disk $D_{\nu}=\left\{x \in K \mid v_{K}(x)>\nu\right\}$. Denote by $\mathscr{O}_{\nu}$ the ring of convergent series $\mathscr{O}_{\nu}=\left\{\sum_{i \in \mathbb{N}} a_{i} u^{i} \mid a_{i} \in K, \lim _{\inf }^{i \rightarrow+\infty}, \frac{v_{K}\left(a_{i}\right)}{i} \geq-\nu\right\}$ in the disk $D_{\nu}$. It is clear that $S_{\nu, \pi}$ is exactly the set $\left\{f \in K[[u]] \mid v_{K}(f(x))\right.$ bounded below on $\left.D_{\nu}\right\}$ and $S_{\nu}$ can be described as $\left\{f \in K[[u]] \mid v_{K}(f(x))\right.$ bounded below by 0 on $\left.D_{\nu}\right\}$. Thus, there are obvious inclusions $S_{\nu} \subset S_{\nu, \pi} \subset \mathscr{O}_{\nu}$ but one should beware of the fact that the last inclusion is strict. Indeed for instance, for $\mathfrak{R}=\mathbb{Z}_{p}, \nu=0$ the series $\sum_{i>0} \frac{u^{i}}{i}$ which defines the function $\log (1-u)$ is convergent in the unity disk but is obviously not in $S_{0, \pi}$ since $v_{\pi}(1 / i)$ has no lower bound. Assuming that $\nu$ is rational (what we do), the following proposition gives another characterisation of elements of $\mathscr{O}_{\nu}$ that lies in $S_{\nu, \pi}$.
Proposition 2.4. An element $x \in \mathscr{O}_{\nu}$ is in $S_{\nu, \pi}$ if and only if $x$ has only a finite number of zeros in $\mathscr{O}_{\nu}$.

Proof. Let $x \in \mathscr{O}_{\nu}$. The number of zeros of $x \in D_{\nu}$ is equal to the length of the interval above which the Newton polygon of $x$ has a slope $<-\nu$. If this length is finite, it is clear that $v_{p}\left(a_{i}\right)$ is bounded below by a line of the form $-\nu i+c$ with $c$ a constant and as a consequence is an element of $S_{\nu, \pi}$.

Conversely, suppose that $x \in S_{\nu, \pi}$. This means that $v_{p}\left(a_{i}\right)+\nu i$ is bounded below and is contained in $\mathbb{Z}+\nu \mathbb{Z}$ which is a discrete subgroup of $\mathbb{R}$ (as $\nu$ is rational). Thus, the set $\left\{v_{p}\left(a_{i}\right)+\nu i, i \in\right.$ $N\}$ reaches a minimum for a certain index $i_{0}$. This means that for all $i>i_{0}$, the slope of the Newton polygon of $x$ is greater than $-\nu$ and $x$ has a finite number of zeros in $D_{\nu}$.

We end up this section, by remarking that up to an extension of the base ring $\mathfrak{R}$ all the $S_{\nu}$ 's are isomorphic to a $S_{0}$. Indeed, write $\nu=\beta / \alpha$ with $\alpha, \beta$ relatively prime numbers and let $\varpi$, in an algebraic closure of $K$, be such that $\varpi^{\alpha}=\pi$. Let $\mathfrak{R}^{\prime}=\mathfrak{R}[\varpi], K^{\prime}$ be the fraction field of $\mathfrak{R}^{\prime}$ (and a finite extension of $K$ ). The valuation on $\mathfrak{R}$ extends uniquely on $\mathfrak{R}^{\prime}$ by setting $v_{K^{\prime}}(\varpi)=1 / \alpha$. For $\mu=0, \nu$, let $S_{\mu}{ }^{\prime}=S_{\mu} \otimes_{\mathfrak{R}} \mathfrak{R}^{\prime}$. The valuation $v_{K^{\prime}}$ defines a Gauss valuation on $S_{\mu}{ }^{\prime}$ that we denote also by $v_{\mu}$.

Lemma 2.5. Keeping the notations from above, the morphism of ring $\rho: S_{0}{ }^{\prime} \rightarrow S_{\nu}^{\prime}$, defined by $\rho(1)=1$ and $\rho(u)=\frac{u}{\varpi^{\beta}}$ is an isomorphism. Moreover, if $x \in S_{0}{ }^{\prime}$ we have $v_{0}(x)=v_{\nu}(\rho(x))$ and $\operatorname{deg}_{W}^{0}(x)=\operatorname{deg}_{W}^{\nu}(\rho(x))$.
Proof. By definition, $S_{\nu}^{\prime}=\left\{\sum a_{i} u^{i} \mid v_{K^{\prime}}\left(a_{i}\right)+\nu i \geq 0\right\}=\left\{\sum a_{i}\left(u / \varpi^{\beta}\right)^{i} \mid v_{K^{\prime}}\left(a_{i}\right) \geq 0\right\}$ from which it is clear that $\rho$ is an isomorphism. The rest of the lemma is an easy verification.

### 2.3 Division in $S_{\nu}$

The Weierstrass degree allows us to describe an Euclidean division in $S_{\nu}$. Although, the existence of such a division is classical (see for instance [10]) at least over $S_{0}=\mathfrak{R}[[u]]$, we give here a proof for all $\nu$ which provides an algorithm with oracles to compute the Euclidean division.

In order to study divisibility in $S_{\nu}$, we have a first result:
Lemma 2.6. Let $x, z \in S_{\nu}$. We suppose that $\operatorname{deg}_{W}(x)=0$ then there exists $y \in S_{\nu}$ such that $x . y=z$ if and only if $v_{\nu}(x) \leq v_{\nu}(z)$.

Proof. We suppose that $\operatorname{deg}_{W}(x)=0$. If there exists $y \in S_{\nu}$ such that $x \cdot y=z$ then clearly $v_{\nu}(x) \leq v_{\nu}(z)$. Reciprocally, we suppose that $v_{\nu}(x) \leq v_{\nu}(z)$. Write $x=\sum_{i \in \mathbb{N}} a_{i} u^{i}$ and $z=$ $\sum_{i \in \mathbb{N}} c_{i} u^{i}$. Since $a_{0}$ is invertible in $K$ there exists $y \in K[[u]]$ such that $x . y=z$. We have to prove that $v_{\nu}(y) \geq 0$. For this, write $y=\sum_{i \in \mathbb{N}} b_{i} u^{i}$. We have $v_{K}\left(b_{0}\right)=v_{K}\left(c_{0}\right)-v_{K}\left(a_{0}\right) \geq 0$ by hypothesis. Then, for $j \geq 1$, we prove by induction that $v_{K}\left(b_{j}\right)+\nu j \geq 0$. We have $b_{j}=$ $a_{0}^{-1} \cdot c_{j}-a_{0}^{-1} \sum_{i=1}^{j} a_{i} \cdot b_{j-i}$. But $v_{K}\left(a_{0}^{-1} \cdot c_{j}\right)+\nu j \geq v_{\nu}(z)-v_{\nu}(x) \geq 0$ because $\operatorname{deg}_{W}(x)=0$. Moreover, for $i=1 \ldots j, v_{K}\left(a_{0}^{-1} \cdot a_{i} \cdot b_{j-i}\right)+\nu j=v_{K}\left(a_{i}\right)+\nu i-v_{\nu}(x)+v_{K}\left(b_{j-i}\right)+\nu(j-i)$. But by definition $v_{K}\left(a_{i}\right)+\nu i-v_{\nu}(x) \geq 0$ and by the induction hypothesis $v_{K}\left(b_{j-i}\right)+\nu(j-i) \geq 0$. Therefore, $v_{K}\left(b_{j}\right)+\nu j \geq 0$ and we are done.

Applying Lemma 2.6 to $z=1$, we get
Corollary 2.7. Let $x=\sum_{i \in \mathbb{N}} a_{i} x^{i} \in S_{\nu}$, then $x$ is invertible in $S_{\nu}$ if and only if $\operatorname{deg}_{W}(x)=0$ and $v_{\nu}(x)=0$.

We note that the corollary implies that $S_{\nu}$ is a local ring. Next, we introduce the following notations: for $x=\sum_{i \in \mathbb{N}} a_{i} u^{i} \in S_{\nu}$ and $d$ a positive integer, we let $\operatorname{Hi}(x, d)=\sum_{i \geq d} a_{i} u^{i}$ and $\mathrm{Lo}(x, d)=\sum_{i=0}^{d-1} a_{i} u^{i}$. It is clear that $x=\mathrm{Lo}(x, d)+\operatorname{Hi}(x, d)$.
Proposition 2.8. Let $x, y \in S_{\nu}$. Suppose that $v_{\nu}(y) \geq v_{\nu}(x)$ then there exist a unique couple $(q, r) \in S_{\nu} \times\left(K[u] \cap S_{\nu}\right)$ such that $\operatorname{deg}(r)<\operatorname{deg}_{W}(x)$ and $y=q \cdot x+r$.
Proof. First, we prove the existance of $(q, r)$. Let $d=\operatorname{deg}_{W}(x)$, we consider the sequences $\left(q_{i}\right)$ and $\left(r_{i}\right)$ defined by $q_{0}=0$ and $r_{0}=y$ and

$$
\begin{equation*}
q_{i+1}=q_{i}+\frac{\operatorname{Hi}\left(r_{i}, d\right)}{\operatorname{Hi}(x, d)}, r_{i+1}=r_{i}-\frac{\operatorname{Hi}\left(r_{i}, d\right)}{\operatorname{Hi}(x, d)} \cdot x \tag{2}
\end{equation*}
$$

We are going to prove by induction that $q_{i}$ and $r_{i}$ are convergent sequences (for the $v_{\nu}$ valuation) of elements of $S_{\nu}$. Let $e=v_{\nu}(\operatorname{Lo}(x, d))-v_{\nu}(\operatorname{Hi}(x, d))>0$. Our induction hypothesis is that $q_{i}$ and $r_{i}$ are elements of $S_{\nu}$, that $v_{\nu}\left(\operatorname{Hi}\left(r_{i}, d\right)\right) \geq e \cdot i+v_{\nu}(\operatorname{Hi}(y, d))$ and that $y=q_{i} \cdot x+r_{i}$. It is clearly true for $i=0$.

By the induction hypothesis, we have $v_{\nu}\left(\operatorname{Hi}\left(r_{i}, d\right)\right) \geq v_{\nu}(\operatorname{Hi}(y, d))$ and by hypothesis $v_{\nu}(\operatorname{Hi}(y, d)) \geq$ $v_{\nu}(y) \geq v_{\nu}(x)=v_{\nu}(\operatorname{Hi}(x, d))$ so that $v_{\nu}\left(\operatorname{Hi}\left(r_{i}, d\right)\right) \geq v_{\nu}(\operatorname{Hi}(x, d))$. Applying Lemma 2.6, we obtain $\frac{\mathrm{Hi}\left(r_{i}, d\right)}{\mathrm{Hi}(x, d)} \in S_{\nu}$ and then $q_{i+1}, r_{i+1} \in S_{\nu}$. Next writing $x=\operatorname{Hi}(x, d)+\operatorname{Lo}(x, d)$, we get

$$
\begin{equation*}
r_{i+1}=\operatorname{Lo}\left(r_{i}, d\right)-\frac{\operatorname{Hi}\left(r_{i}, d\right)}{\operatorname{Hi}(x, d)} \cdot \operatorname{Lo}(x, d) . \tag{3}
\end{equation*}
$$

Applying Lemma 2.2, we obtain that $v_{\nu}\left(\operatorname{Hi}\left(r_{i+1}, d\right)\right) \geq v_{\nu}\left(\operatorname{Hi}\left(r_{i}, d\right)\right)+v_{\nu}(\operatorname{Lo}(x, d))-v_{\nu}(\operatorname{Hi}(x, d))$. Using the induction hypothesis, we get that $v_{\nu}\left(\operatorname{Hi}\left(r_{i+1}, d\right)\right) \geq e \cdot(i+1)+v_{\nu}(\operatorname{Hi}(y, d))$. Finally, using the hypothesis that $y=q_{i} \cdot x+r_{i}$, we immediately check using (2) that $y=q_{i+1} \cdot x+r_{i+1}$.

From the induction, we deduce that $q_{i}$ and $r_{i}$ are convergent sequences of $S_{\nu}$ for the $v_{\nu}$ valuation. In fact, we have $q_{i+1}-q_{i}=\frac{\operatorname{Hi}\left(r_{i}, d\right)}{\operatorname{Hi}(x, d)}$ so that $v_{\nu}\left(q_{i+1}-q_{i}\right)=v_{\nu}\left(\operatorname{Hi}\left(r_{i}, d\right)\right)-v_{\nu}(\operatorname{Hi}(x, d)) \geq e \cdot i+$ $v_{\nu}(\operatorname{Hi}(y, d))-v_{\nu}(\operatorname{Hi}(x, d)) \geq e \cdot i$. The same argument works for $r_{i}$. Denote by $q$ and $r$ the limits. As for all $i \in \mathbb{N}, y=q_{i} \cdot x+r_{i}$, we have $y=q \cdot x+r$. Moreover, since $\operatorname{Hi}\left(r_{i}, d\right) \geq e \cdot i$, we have $\mathrm{Hi}(r, d)=0$, so that $r \in K[u]$ and $\operatorname{deg}(r)<\operatorname{deg}_{W}(x)$.

We prove the unicity of $(q, r)$. Let $\left(q^{\prime}, r^{\prime}\right) \in S_{\nu} \times\left(K[u] \cap S_{\nu}\right)$ such that $y=q^{\prime} \cdot x+r^{\prime}$. Then $\left(q-q^{\prime}\right) \cdot x=r^{\prime}-r$. We have $\operatorname{deg}_{W}\left(\left(q-q^{\prime}\right) \cdot x\right)=\operatorname{deg}_{W}\left(r^{\prime}-r\right)<\operatorname{deg}_{W}(x)$ which is only possible if $q=q^{\prime}$ and $r=r^{\prime}$.

From the proof of Proposition 2.8, we deduce Algorithm 1 to compute from the knowledge of $x, y$, the elements $q^{\prime}, r^{\prime} \in S_{\nu}$ such that $v_{\nu}\left(q-q^{\prime}\right) \geq$ prec and $v_{\nu}\left(r-r^{\prime}\right) \geq$ prec. Furthermore, by the proof of the proposition, the number of iterations of the while loop is bounded by $\lceil p r e c / e\rceil$. We deduce that Algorithm 1 needs one inversion and $3 \cdot\lceil p r e c / e\rceil$ multiplications in $S_{\nu}$.

```
Algorithm 1: EuclieanDivision
    input \(: x, y \in S_{\nu}\) with \(v_{\nu}(y) \geq v_{\nu}(x)\), prec \(\in \mathbb{N}\)
    output: \(q, r \in S_{\nu}\) such that \(y=q \cdot x+r\) and \(v_{\nu}\left(\operatorname{Hi}\left(r, \operatorname{deg}_{W}(x)\right)\right) \geq\) prec
    \(q \leftarrow 0 ;\)
    \(r \leftarrow y ;\)
    \(d \leftarrow \operatorname{deg}_{W}(x) ;\)
    while \(v_{\nu}(\operatorname{Hi}(r, d))<p r e c\) do
        \(q \leftarrow q+\frac{\mathrm{Hi}(r, d)}{\mathrm{Hi}(x, d)} ;\)
        \(r \leftarrow r-\frac{\mathrm{Hi}(r, d)}{\mathrm{Hi}(x, d)} \cdot x ;\)
    return \(q, r\);
```

Now, let $x \in S_{\nu}$, following [10] we say that $x$ is distinguished if $v_{\nu}(x)=0$. With this definition, we can state the classical Weierstrass preparation theorem:

Corollary 2.9 (Weierstrass preparation). Let $x \in S_{\nu}$ be a distinguished element and let $d=$ $\operatorname{deg}_{W}(x)$. Then we can write $x=q \cdot h$, where $q \in S_{\nu}$ is an invertible element and $h \in K[u] \cap S_{\nu}$ is of the form $h=\frac{u^{d}}{\pi^{\nu \cdot d}}+\sum_{i=0}^{d-1} b_{i} u^{i}$ with $v_{K}\left(b_{i}\right)+\nu i>0$.

Proof. We first notice that $d \nu$ is a nonnegative integer. Indeed, it is clearly nonnegative, and writing $x=\sum a_{d} u^{d}$, we have $v_{\mathfrak{R}}\left(a_{d}\right)+d \nu=0$ (since $x$ is assumed to be distinguished) and, consequently, $d \nu=-v_{\mathfrak{R}}\left(a_{d}\right) \in \mathbb{Z}$.

By proposition 2.8, there exist $q \in S_{\nu}$ and $r \in K[u] \cap S_{\nu}$ such that $\operatorname{deg} r<d$ and

$$
\frac{u^{d}}{\pi^{d \cdot \nu}}=q \cdot x+r
$$

Using Lemma 2.2, we obtain $v_{\nu}(q)=0$ and $\operatorname{deg}_{W}(q)=0$. Then, Corollary 2.7 implies that $q$ is invertible. To finish the proof it suffices to remark that $\operatorname{deg}_{W}\left(\frac{u^{d}}{\pi^{d \cdot \nu}}-r\right)=d$ and the result follows from the definition of $\operatorname{deg}_{W}$.

Remark 2.10. The previous proposition is closely related to the Proposition 2.4 since it says that an element of $\mathscr{O}_{\nu}$ is in $S_{\nu, \pi}$ if and only if it can be written as product of a polynomial times a function which does not have any zero in $D_{\nu}$.

The following proposition states that the rings $S_{\nu, \pi}$ and $S_{\nu, u}$ are Euclidean rings and provides algorithms with oracles to compute the division.

Proposition 2.11. The ring $S_{\nu, \pi}$ is Euclidean, the ring $S_{\nu, u}$ is a discrete valuation ring for the valuation $v_{\nu}$ (and as a consequence is also Euclidean). Moreover, $\mathscr{E}$ is a field.

Proof. Let $x, y \in S_{\nu, \pi}$. There exist $s, t \in \mathbb{N}$ such that $\pi^{s} x, \pi^{t} y \in S_{\nu}$ and $v_{\nu}\left(\pi^{t} \cdot y\right) \geq v_{\nu}\left(\pi^{s} \cdot x\right)$. Applying Proposition 2.8, yields $q \in S_{\nu}$ and $r \in K[[u]] \cap S_{\nu}$ such that $\operatorname{deg}(r)<\operatorname{deg}_{W}(x)$ and $y=\pi^{s-t} \cdot q \cdot x+\pi^{-t} \cdot r$ and we are done.

In order to prove that $S_{\nu, u}$ is a discrete valuation ring, we have to show that the set of invertible elements of $S_{\nu, u}$ is the set of elements $x \in S_{\nu, u}$ such that $v_{\nu}(x)=0$. Write $\nu=\beta / \alpha$, with $\alpha, \beta$ relatively prime numbers. Let $\mathfrak{m}$ be the ideal defined by $\left\{x \in S_{\nu, u}, v_{\nu}(x)>0\right\}$, it is clear that $S_{\nu, u} / \mathfrak{m}$ is isomorphic to the field $k\left(\left(u^{\alpha}\right)\right)$. As $S_{\nu, u}$ is complete for the $v_{\nu}$ valuation, the Hensel lift algorithm gives an algorithm with oracles to compute the inverse of an element whose valuation is zero. The Algorithm 2 uses a fast Newton iteration to perform this computation modulo $\mathfrak{m}^{n}$ at the expense of $O(\log (n))$ multiplications in $S_{\nu, u}$.

Let $x$ be a non zero element of $\mathscr{E}$, by dividing it by a power of $\pi$ we can suppose that $v_{\nu}(x)=0$ and by using the algorithm with oracle Algorithm 2, we can invert it.

```
Algorithm 2: Inverse
    input \(: x \in S_{\nu, u}\) such that \(v_{\nu}(x)=0, n \in \mathbb{N}\)
    output: \(y \in S_{\nu, u}\) such that \(x \cdot y=1 \bmod \mathfrak{m}^{n}\)
    if \(n=1\) then
        \(y \leftarrow 1 / \bar{x} \bmod \mathfrak{m} ;\)
    else
        \(y \leftarrow\) Inverse \((x,\lceil n / 2\rceil) ;\)
        \(y \leftarrow y+y(1-a y) \bmod \mathfrak{m}^{n}\);
```

Remark 2.12. One can use the usual Euclidean algorithm to compute the Bézout coefficients of $x, y \in S_{\nu, \pi}$. This algorithm outputs $g, k, l, m, n \in S_{\nu, \pi}$ such that $g$ is the greatest common divisor of $x$ and $y, k \cdot x+l \cdot y=g, m \cdot x+n \cdot y=0$ and $k \cdot n-l \cdot m=1$. It proceeds by using the fact that $g c d(x, y)=g c d(y, r)$ where $r$ is the rest of the division of $x$ by $y$ and uses $O\left(\operatorname{deg}_{W}(y)\right)$ calls to the Euclidean division Algorithm 1. We remark, as the rest of the division of two elements of $S_{\nu}$ is an element of $K[u]$, that starting from the second iteration of this algorithm all the divisions to be computed are the usual division between elements of $K[u]$. Unfortunately, we will see that in §4, that the Euclidean algorithm in general is not stable, so that we might need extra informations, about $x$ and $y$ in order to compute an approximation of their gcd from the knowledge of an approximation of $x$ and an approximation of $y$.

## 3 Modules over $S_{\nu}$

Let $d$ be a positive integer and fix $\nu \in \mathbb{Q}$. We want to compute with finitely generated torsion free $S_{\nu}$-modules. Any such module $\mathscr{M}$ can be embedded in $S_{\nu}^{d}$ for $d \in \mathbb{N}$ and can be represented by a matrix with coefficients in $S_{\nu}$ whose column vectors are the coordinates of generators of $\mathscr{M}$ in the canonical basis of $S_{\nu}^{d}$. Indeed, we can always embed $\mathscr{M}$ is $\mathscr{M} \otimes_{S_{\nu}} \operatorname{Frac}\left(S_{\nu}\right)$ and select a basis $\left(e_{1}, \ldots, e_{d}\right)$ of $\mathscr{M} \otimes_{S_{\nu}} \operatorname{Frac}\left(S_{\nu}\right)$ together with an element $D \in S_{\nu}$ such that the image of $\mathscr{M}$ in $\mathscr{M} \otimes_{S_{\nu}} \operatorname{Frac}\left(S_{\nu}\right)$ is contained in the free $S_{\nu}$-module generated by the $\frac{1}{D} \cdot e_{i}$ 's.

A first problem arises here: it is not possible to bound the number of generators of the submodules of $S_{\nu}^{d}$ that we have to compute with. For instance, for $d=1$ and $\nu=0$, choose a positive integer $k$ and consider the sub- $S_{0}$-module $\mathscr{M}_{k}$ of $S_{0}$ generated by the family $\left(\pi^{k-j} u^{j}\right)_{j=0, \ldots, k}$. Then $\mathscr{M}_{k}$ can not be generated by less than $k+1$ elements. Indeed, let $\left(e_{0}, \ldots, e_{n}\right) \in S_{0}^{n}$ be a family of generators of $\mathscr{M}_{k}$, and for $j \geq 0$ and define a filtration on $\mathscr{M}_{k}$ by letting $F^{j} \mathscr{M}_{k}=\mathscr{M}_{k} \cap u^{j} S_{0}$. We are going to prove by induction on $t \in\{0, \ldots, k\}$ that there exists a matrix $M_{t} \in M_{n \times n}\left(S_{0}\right)$ such that, if we set $\left(e_{0}^{\prime}, \ldots, e_{n}^{\prime}\right)=\left(e_{0}, \ldots, e_{n}\right) \cdot M_{t}$ then $\left(e_{0}^{\prime}, \ldots, e_{n}^{\prime}\right)$ is a family of generators of $\mathscr{M}_{k}$, for $j<t, e_{j}^{\prime}=u^{j} \pi^{k-j} \bmod F^{j+1} \mathscr{M}_{k}$ and $\left(e_{j}^{\prime}\right)_{j \geq t}$ is a family of generators of $F^{t} \mathscr{M}_{k}$. This is obviously true for $t=0$. Suppose that it is true for $t_{0} \in\{0, \ldots, k\}$. Let $\left(e_{0}^{\prime}, \ldots, e_{n}^{\prime}\right)=\left(e_{0}, \ldots, e_{n}\right) \cdot M_{t_{0}}$. As the morphism $\left(\sum_{j=t_{0}}^{k} S_{0} e_{j}^{\prime}\right) / F^{t_{0}+1} \mathscr{M}_{k} \rightarrow \pi^{k-t} \mathfrak{R}$, defined by $u^{t_{0}} \sum a_{i} u^{i} \mapsto a_{0}$ is an isomorphism, we can suppose if necessary by renumbering the family $\left(e_{i}^{\prime}\right)$ that $e_{t_{0}}^{\prime}=u^{t_{0}} \pi^{k-t_{0}} \bmod F^{t_{0}+1} \mathscr{M}_{k}$.

Then, by considering linear combinations of the form $e_{j}^{\prime}-\lambda e_{t_{0}+1}^{\prime}$ for $\lambda \in S_{0}$ for $j>t_{0}$, one can obtain a matrix $M_{t_{0}+1}$ satisfying the induction hypothesis for $t_{0}+1$. Finally, we get $n \geq k$.

A second problem comes from the fact that there is no unique way to represent a module by a set of generators. For computational purpose, in order to check equality between modules for instance, it is important to have a canonical representation, that is a bijective correspondence between mathematical objects and data structures. An example of such a canonical representation exists for finitely generated modules with coefficients in an Euclidean ring ([5]): it is the so-called Hermite Normal Form (HNF). It is given by a triangular matrix (with some extra conditions) that can be computed from an initial matrix $M$ by doing operations on column vectors of $M$. Even if $S_{\nu}$ is not Euclidean, we could have hoped that such representations still exist for free modules. Unfortunately, it turns out that it is not the case. Indeed, in general, there does not even exist a triangular matrix form for matrices over $S_{\nu}$. For instance, for $\nu=0$, take:

$$
M=\left(\begin{array}{ll}
u & \pi \\
\pi & u
\end{array}\right) \in M_{2 \times 2}\left(S_{0}\right)
$$

and assume that $M$ can be written as a product $L P$ where $L$ is lower-triangular and $P$ is invertible. Let $\alpha$ and $\beta$ be the diagonal entries of $L$. Then, $\alpha$ and $\beta$ belong to the maximal ideal of $S_{0}$ (since the coefficients of $M$ all belong to this ideal) and the product $\alpha \beta$ is equal to a unit times $u^{2}-\pi^{2}$. Hence, by multiplying $\beta$ by an invertible element in $S_{0}$ if necessary, we can assume that $\beta=u \pm \pi$ since $S_{0}$ is a unique factorisation domain. On the other hand, by hypothesis, there exist $a, b \in S_{0}$ such that $u a+\pi b=0$ and $\pi a+u b=\beta$. This equality implies that $\pi$ divides $a$ and therefore that $\beta=\pi a+u b \in u S_{0}+\pi^{2} S_{0}$. This is a contradiction.

In this section, we explain how to get around these problems. First, we recall the notion of quasi-isomorphism and study the localisation of the modules with respect to $\pi$ or $u^{\alpha} / \pi^{\beta}$ in order to obtain canonical representations well suited for the computation in the category of modules up to quasi-isomorphism. Then, we describe a generalisation of an algorithm of Cohen to compute the maximal module associated to a given torsion-free $S_{\nu}$-module and obtain a bound on the number of generators of a maximal $S_{\nu}$-module. We explain how to combine the different approaches in order to obtain a comprehensive algorithmic toolbox for modules over $S_{\nu}$.

### 3.1 Quasi-isomorphism and maximal modules

In order to be able to control the number of generators of a $S_{\nu}$-module, we are going to compute up to finite modules which will be considered as "negligible".

Definition 3.1. A finitely generated $S_{\nu}$-module is said to be finite if it has finite length. Let $\mathscr{M}$ and $\mathscr{M}^{\prime}$ be two finitely generated $S_{\nu}$-modules, let $f: \mathscr{M} \rightarrow \mathscr{M}^{\prime}$ be a $S_{\nu}$-linear morphism. We say that $f$ is a quasi-isomorphism if its kernel and its co-kernel are finite modules.

Remark 3.2. Since $\operatorname{ker} f$ and coker $f$ are finitely generated (because $S_{\nu}$ is a noetherian ring), it is easy to check that they have finite length if and only if they are canceled, at the same time, by a distinguished element of $S_{\nu}$ and a power of $\pi$. A quasi-isomorphism between torsion-free modules is always injective. Indeed, its kernel, being a submodule annihilated by a power of $u^{\alpha} / \pi^{\beta}$ and $\pi$ of a torsion free module, is zero.

Example 3.3. Let $\mathscr{M}$ be the submodule of $S_{0}$ generated by $\left(\pi^{2}, \pi u^{3}\right)$. The inclusion $\mathscr{M} \subset \pi S_{0}$ yields an injective morphism whose is annihilated by $\pi$ and $u^{3}$. As a consequence $\mathscr{M}$ is quasiisomorphic to the free module $\pi . S_{0}$ (see figure 2).

We have a canonical representative in a class of quasi-isomorphism which is given by the following definition.

Definition 3.4. Let $\mathscr{M}$ be a torsion-free finitely generated $S_{\nu}$-module. We say that $\mathscr{M}^{\prime}$ together with a quasi-isomorphism $f: \mathscr{M} \rightarrow \mathscr{M}^{\prime}$ is maximal for $\mathscr{M}$ if for every $\mathscr{N}$, torsion-free $S_{\nu}$-module, and quasi-isomorphism $f^{\prime}: \mathscr{M} \rightarrow \mathscr{N}$, there exists a morphism $g: \mathscr{N} \rightarrow \mathscr{M}^{\prime}$ which makes the following diagram commutative:


Figure 2: The module $\mathscr{M}$ is quasi-isomorphic to $\pi \cdot S_{0}$.


The morphism $g$ in the definition is unique and is in fact a quasi-isomorphism. Indeed, by the commutativity of the diagram, the image of $g$ contains the image of $f$. Thus, the cokernel of $g$ is finite. Moreover, since $f$ is injective, $g$ is injective on $\operatorname{Im} f^{\prime}$, which is cofinite in $\mathscr{N}$. It follows that ker $g$ is finite and $g$ is a quasi-isomorphism. Moreover, for every $x \in \mathscr{N}$, there exists a positive integer $n$ such that $\pi^{n} x$ is in the image of $f^{\prime}$. The image of $\pi^{n} x$ by $g$ is then uniquely defined by the commutativity of the diagram (4). The uniqueness of $g$ follows.

A maximal module for $\mathscr{M}$, if it exists, is unique up to isomorphism. Indeed, if $\mathscr{M}^{\prime}$ and $\mathscr{M}^{\prime \prime}$ are two maximal modules for $\mathscr{M}$ then there exist two quasi-isomorphisms $g_{1}: \mathscr{M}^{\prime} \rightarrow \mathscr{M}^{\prime \prime}$ and $g_{2}: \mathscr{M}^{\prime \prime} \rightarrow \mathscr{M}^{\prime}$ and the uniqueness of $g$ in the diagram (4) implies that $g_{1} \circ g_{2}=\operatorname{Id} \mathscr{M}^{\prime \prime}$ and $g_{2} \circ g_{1}=\operatorname{Id}_{\mathscr{M}^{\prime}}$. If it exists, we denote the maximal module of $\mathscr{M}$ by $\operatorname{Max}(\mathscr{M})$. We can rephrase the above by saying that if $\mathscr{M}^{\prime}$ is the maximal module for $\mathscr{M}$ then there is a quasi-isomorphism from $\mathscr{M}$ into $\mathscr{M}^{\prime}$ and any quasi-isomorphism $\mathscr{M}^{\prime} \rightarrow \mathscr{M}^{\prime \prime}$ is an isomorphism. In fact, this condition characterises maximal modules:

Lemma 3.5. Let $\mathscr{M}$ be a finitely generated torsion free $S_{\nu}$-module. Let $\mathscr{M}^{\prime}$ be a $S_{\nu}$-module such that there is a quasi-isomorphism $f: \mathscr{M} \rightarrow \mathscr{M}^{\prime}$. The following assertions are equivalent:

1. $\mathscr{M}^{\prime}$ is maximal;
2. any quasi-isomorphism $\mathscr{M}^{\prime} \rightarrow \mathscr{M}^{\prime \prime}$ is an isomorphism.

Proof. We only have to prove that the second property implies that $\mathscr{M}^{\prime}$ verifies the universal property of maximal modules. For this let $\mathscr{N}$ be a finite type $S_{\nu}$-module such that there is a quasi-isomorphism $f^{\prime}: \mathscr{M} \rightarrow \mathscr{N}$. Let $\Delta=f \oplus f^{\prime}: \mathscr{M} \rightarrow \mathscr{M}^{\prime} \oplus \mathscr{N}$ be the diagonal embedding and let $\mathscr{M}_{0}=\frac{\mathscr{M}^{\prime} \oplus \mathscr{N}}{\Delta(\mathscr{M})}$. It is clear that $\mathscr{M}_{0}$ is a finitely generated torsion free $S_{\nu}$-module.

There are canonical injections $i_{\mathscr{M}^{\prime}}: \mathscr{M}^{\prime} \rightarrow \mathscr{M}_{0}$ and $i_{\mathscr{N}}: \mathscr{N} \rightarrow \mathscr{M}_{0}$. We claim that $i_{\mathscr{M}^{\prime}}$ and $i_{\mathscr{N}}$ are quasi-isomorphisms. To see that, it suffices to show that the induced injection $i_{\mathscr{M}}=$ $\left(i_{\mathscr{M}^{\prime}}, i_{\mathscr{N}}\right) \circ \Delta: \mathscr{M} \rightarrow \mathscr{M}_{0}$ has a finite cokernel. But

$$
\operatorname{coker} i_{\mathscr{M}}=\frac{\operatorname{coker} f \oplus \operatorname{coker} f^{\prime}}{\Delta(\mathscr{M}) \cap\left(\operatorname{coker} f \oplus \operatorname{coker} f^{\prime}\right)}
$$

which has finite length being a quotient of coker $f \oplus \operatorname{coker} f^{\prime}$.
Next, by hypothesis $i_{\mathscr{M}^{\prime}}$ is in fact an isomorphism so that we have a quasi-isomorphism $g=$ $i_{\mathscr{M}^{\prime}}^{-1} \circ i_{\mathscr{N}}$ which sits in the following diagram:


It is clear that the lower left triangle of the diagram is commutative and we are done.

A theorem of Iwasawa [8] asserts that if $\mathscr{M}$ is a finitely generated module over $S_{0}$, then $\operatorname{Max}(\mathscr{M})$ exists and is free of finite rank over $S_{0}$. The main object of $\S 3.3$ is to extend this result to modules over $S_{\nu}$ : we shall provide a constructive proof of the existence of $\operatorname{Max}(\mathscr{M})$ for any finitely generated torsion-free module $\mathscr{M}$ over $S_{\nu}$. We will see however that this $\operatorname{Max}(\mathscr{M})$ is not free in general; nevertheless we shall provide an upper bound on the number of generators of $\operatorname{Max}(\mathscr{M})$.
Lemma 3.6. Let $f: \mathscr{M} \rightarrow \mathscr{M}^{\prime}$ be a quasi-isomorphism between torsion-free finitely generated $S_{\nu}$-modules. Suppose that $\mathscr{M}^{\prime}$ is free then $\mathscr{M}^{\prime}$ is maximal.

Proof. We use the criterion of Lemma 3.5. Let $\mathscr{N}$ be a finitely generated $S_{\nu}$-module such that there is a quasi-isomorphism $f^{\prime}: \mathscr{M}^{\prime} \rightarrow \mathscr{N}$ and we want to show that $f^{\prime}$ is an isomorphism. As $\mathscr{M}^{\prime}$ is torsion-free, we know that $f^{\prime}$ is injective. Now, suppose that there exists a non zero element in the cokernel of $f^{\prime}$. It means that there exists a non zero $x \in \mathscr{N}$ which is not in the image of $f^{\prime}$. As $f^{\prime}$ is a quasi-isomorphism there exists $n \in \mathbb{N}$ and $\lambda \in S_{\nu}$ a distinguished element with $\pi^{n} \cdot x \in \operatorname{Im} f^{\prime}$ and $\lambda \cdot x \in \operatorname{Im} f^{\prime}$. If we set $z_{1}=f^{\prime-1}\left(\pi^{n} \cdot x\right)$ and $z_{2}=f^{\prime-1}(\lambda \cdot x)$, we have the relation

$$
\begin{equation*}
\lambda z_{1}-\pi^{n} z_{2}=0 \tag{6}
\end{equation*}
$$

in $\mathscr{M}^{\prime}$. Let $\left(e_{i}\right)_{i \in I}$ be a basis of $\mathscr{M}^{\prime}$ and write $z_{i}=\sum \mu_{i}^{j} e_{j}$ for $i=1,2$. Putting this in (6), we obtain that $\lambda \mu_{1}^{j}=\pi^{n} \mu_{2}^{j}$ and thus $\pi^{n} \mid \mu_{1}^{j}$ for $j \in I$ since $\lambda$ is a distinguished element of $S_{\nu}$. But then $f^{\prime}\left(\sum \mu_{1}^{j} / \pi^{n} e_{j}\right)=1 / \pi^{n} . f\left(z_{1}\right)=x$ contradicting the fact that $x$ is not in the image of $f^{\prime}$.

Remark 3.7. One can rephrase Iwasawa's result in a more abstract way using the category language. Let $\underline{\operatorname{Mod}}_{S_{\nu}}$ be the category of finitely generated $S_{\nu}$-modules, that are torsion-free and let $\underline{\operatorname{Mod}}_{S_{\nu}}^{\mathrm{tf}}$ (resp. $\underline{\text { Free }}_{S_{\nu}}$ ) denote its full subcategory gathering all torsion-free modules (resp. all free modules). We also introduce the category $\operatorname{Mod}_{S_{\nu}}^{\text {qis }}$, which is by definition the category of finitely generated $S_{\nu}$-modules up to quasi-isomorphism, i.e. $\operatorname{Mod}_{S_{\nu}}^{\text {qis }}$ is obtained from $\underline{\operatorname{Mod}}_{S_{\nu}}$ by inverting formally quasi-isomorphisms. We have a natural functor $\underline{\operatorname{Mod}}_{S_{\nu}} \rightarrow \underline{\operatorname{Mod}}_{S_{\nu}}^{\text {qis }}$, whose restriction to $\underline{M o d}_{S_{\nu}}^{\mathrm{tf}}$ defines a pylonet in the sense of [2], §1. It follows from the results of loc. cit (see Corollary 1.2.2) that the Max construction is a functor: to a morphism $f: \mathscr{M} \rightarrow \mathscr{M}^{\prime}$ in $\underline{\operatorname{Mod}}_{S_{\nu}}^{\mathrm{tf}}$, one can attach a morphism $\operatorname{Max}(f): \operatorname{Max}(\mathscr{M}) \rightarrow \operatorname{Max}\left(\mathscr{M}^{\prime}\right)$. We recall briefly the construction of $\operatorname{Max}(f)$. Let $\mathscr{M}^{\prime \prime}$ be the pushout $\mathscr{M}^{\prime} \oplus \mathscr{M} \operatorname{Max}(\mathscr{M})$, that is the direct sum $\mathscr{M}^{\prime} \oplus \operatorname{Max}(\mathscr{M})$ divided by $\mathscr{M}$ (embedded diagonally). We have a natural morphism $\mathscr{M}^{\prime} \rightarrow \mathscr{M}^{\prime \prime}$ which turns out to be a quasiisomorphism. Hence, there exists a map $\mathscr{M}^{\prime \prime} \rightarrow \operatorname{Max}\left(\mathscr{M}^{\prime}\right)$ and we finally define $\operatorname{Max}(\mathscr{M})$ to be the compositum $\operatorname{Max}(\mathscr{M}) \rightarrow \mathscr{M}^{\prime \prime} \rightarrow \operatorname{Max}\left(\mathscr{M}^{\prime}\right)$ where the first map comes from the natural embedding $\operatorname{Max}(\mathscr{M}) \rightarrow \mathscr{M}^{\prime} \oplus \operatorname{Max}(\mathscr{M})$.

If $\mathscr{M}$ is a submodule of $S_{\nu}^{d}$ (for some positive integer $d$ ), the following proposition gives a very explicit description of $\operatorname{Max}(\mathscr{M})$.
Proposition 3.8. Write $\nu=\beta / \alpha$, with $\alpha, \beta$ relatively prime integers. Let $d$ be a positive integer and $\mathscr{M}$ be a submodule of $S_{\nu}^{d}$. Then $\operatorname{Max}(\mathscr{M})$ exists and

$$
\operatorname{Max}(\mathscr{M})=\left\{x \in S_{\nu}^{d} \quad \mid \quad \exists n \in \mathbb{N}, \pi^{n} x \in \mathscr{M} \text { and }\left(u^{\alpha} / \pi^{\beta}\right)^{n} \cdot x \in \mathscr{M}\right\} .
$$

Furthermore the morphism $i_{\mathscr{M}}: \mathscr{M} \rightarrow \operatorname{Max}(\mathscr{M})$ is the natural embedding.
Proof. Let $\mathscr{M}_{\text {max }}$ be the set of $x \in S_{\nu}^{d}$ such that there exists some $n$ such that $\pi^{n} x$ and $\left(u^{\alpha} / \pi^{\beta}\right)^{n} \cdot x$ belong to $\mathscr{M}$. We want to show that $\operatorname{Max}(\mathscr{M})$ exists and is equal to $\mathscr{M}_{\text {max }}$. It is clear that $\mathscr{M} \subset \mathscr{M}_{\max }$ and that the quotient $\mathscr{M}_{\max } / \mathscr{M}$ is canceled by a power of $\pi$ and a power of $u^{\alpha} / \pi^{\beta}$ which is a distinguished element. Hence it has finite length, and the inclusion $\mathscr{M} \rightarrow \mathscr{M}_{\max }$ is a quasi-isomorphism. Next, suppose that we are given a $S_{\nu}$-module $\mathscr{M}_{0}$ together with a quasiisomorphism $g: \mathscr{M}_{\max } \rightarrow \mathscr{M}_{0}$. Then there is a quasi-isomorphism $i_{\mathscr{M}}: \mathscr{M} \rightarrow \mathscr{M}_{0}$ that sits in the following diagram:


Note that $g$ is injective as it is a quasi-isomorphism. Moreover, we know that the cokernel of $\iota_{\mathscr{M}}$ is annihilated by a power of $u^{\alpha} / \pi^{\beta}$ and a power of $\pi$, which implies that $g$ is surjective. Thus, $g$ is an isomorphism and by Lemma $3.5, \operatorname{Max}(\mathscr{M})$ exists and $\operatorname{Max}(\mathscr{M})=\mathscr{M}_{\max }$ as claimed. The second part of the proposition is clear from the above diagram.

It follows directly from Proposition 3.8 that the intersection of two maximal modules is maximal. The same is however not true for the sum: in general the $S_{\nu}$-module $\mathscr{M}+\mathscr{M}^{\prime}$ is not maximal even if $\mathscr{M}$ and $\mathscr{M}^{\prime}$ are (take for example $\mathscr{M}=u S_{0}$ and $\mathscr{M}^{\prime}=\pi S_{0}$ ). This leads us to define the new operation $+_{\max }$ (which is much more pleasant than the usual sum of modules) on the set of maximal submodules of $S_{\nu}^{d}$ as follows:

$$
\mathscr{M}+{ }_{\max } \mathscr{M}^{\prime}=\operatorname{Max}\left(\mathscr{M}+\mathscr{M}^{\prime}\right)
$$

We also deduce from Proposition 3.8 that a $S_{0}$-module $\mathscr{M}$ is free if and only if $\mathscr{M}=\mathscr{M}_{\max }$. This gives a nice criterion to check if a $S_{0}$-module is free. It is not true in general for a sub- $S_{\nu^{-}}$ module $\mathscr{M}$ of $S_{\nu}^{d}$ that $\operatorname{Max}(\mathscr{M})$ is free (this will become apparent when we give the general shape of a maximal $S_{\nu}$-module in $\S 3.3$ ). However, by Lemma 2.5, every $S_{\nu}$ becomes isomorphic to $S_{0}$ over a finite extension $\mathfrak{R}^{\prime}=\mathfrak{R}[\varpi]$ (where $\varpi$ depends on $\nu$ ). Set $S_{\nu}^{\prime}=S_{\nu} \otimes_{\mathfrak{R}} \mathfrak{R}^{\prime}$. For all submodule $\mathscr{M}$ of $S_{\nu}^{d}$, we obtain that $\operatorname{Max}\left(\mathscr{M} \otimes S_{\nu}^{\prime}\right)$ is a free submodule of $\left(S_{\nu}^{\prime}\right)^{d}$. Denote by $\operatorname{Max}_{S_{\nu}}^{d}$ the set of maximal sub- $S_{\nu}$-modules of $S_{\nu}^{d}$ and by Free ${ }_{S_{\nu}^{\prime}}^{d}$ the set of free sub- $S_{\nu}^{\prime}$-module of $\left(S_{\nu}^{\prime}\right)^{d}$.

Proposition 3.9. The natural map

$$
\begin{array}{rlll}
\Phi \quad: \operatorname{Max}_{S_{\nu}}^{d} & \longrightarrow \operatorname{Free}_{S_{\nu}^{\prime}}^{d} \\
\mathscr{M} & \mapsto & \operatorname{Max}\left(\mathscr{M}_{S_{\nu}} S_{\nu}^{\prime}\right)
\end{array}
$$

is injective. A left inverse of $\Phi$ is given by $\mathscr{M}^{\prime} \mapsto \mathscr{M}^{\prime} \cap S_{\nu}^{d}$. Moreover, the image of $\Phi$ contains the subset of Free ${ }_{S_{\nu}^{\prime}}^{d}$ of free modules which admit a basis $\left(e_{i}\right)_{i \in I}$ where $e_{i} \in\left(S_{\nu}^{\prime}\right)^{d}$ and $e_{i}=\varpi^{\alpha_{i}} e_{i}^{\prime}$ with $e_{i}^{\prime} \in\left(S_{\nu}\right)^{d}$ and $\alpha_{i} \in \mathbb{N}$.

Remark 3.10. Actually, we will prove later (see Lemma 3.18) that the image of $\Phi$ is exactly the subset of Free ${ }_{S_{\nu}^{\prime}}^{d}$ verifying the condition of Proposition 3.9.
Proof. In order to prove that $\Phi$ is injective, it is enough to prove that $\Phi$ has a left inverse. For this, let $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ and let $\mathscr{M}^{\prime}=\operatorname{Max}\left(\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}\right) \in \operatorname{Free}_{S_{\nu}^{\prime}}^{d}$. Then it suffices to prove that $\mathscr{M}_{2}=\mathscr{M}^{\prime} \cap S_{\nu}^{d}$ is a maximal sub- $S_{\nu}$-module of $S_{\nu}^{d}$. Indeed, as it is clear that $\mathscr{M}_{2}$ contains $\mathscr{M}$ and that the injection $\mathscr{M} \rightarrow \mathscr{M}_{2}$ is a quasi-isomorphism since the injection $\mathscr{M} \rightarrow \mathscr{M}^{\prime}$ is a quasiisomorphism, we remark that by the maximality of $\mathscr{M}$ it would imply that $\mathscr{M}=\mathscr{M}_{2}$.

For this let $x \in S_{\nu}^{d}$ and suppose that there exists $n \in \mathbb{N}$ such that $\pi^{n} \cdot x \in \mathscr{M}_{2}$ and $\left(u^{\alpha} / \pi^{\beta}\right)^{n} \cdot x \in$ $\mathscr{M}_{2}$. As $\mathscr{M}^{\prime}$ is maximal and $\mathscr{M}_{2} \subset \mathscr{M}^{\prime}$, by Proposition 3.8, it means that $x \in \mathscr{M}^{\prime}$. hence $x \in \mathscr{M}_{2}$. Using again Proposition 3.8, we deduce that $\mathscr{M}_{2}$ is maximal.

Let us now prove the last claim of the proposition. Let $\mathscr{M}^{\prime} \in$ Free $_{S_{\nu}^{\prime}}^{d}$ which admits a basis $\left(e_{i}\right)_{i \in I}$ where $e_{i} \in\left(S_{\nu}^{\prime}\right)^{d}$ and $e_{i}=\varpi^{\alpha_{i}} e_{i}^{\prime}$ with $e_{i}^{\prime} \in\left(S_{\nu}\right)^{d}$ and $\alpha_{i} \in \mathbb{N}$. We have to find a sub- $S_{\nu^{-}}$ module $\mathscr{M}$ of $S_{\nu}^{d}$ such that $\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$ is quasi-isomorphic to $\mathscr{M}^{\prime}$. As $\mathscr{M}^{\prime}=\bigoplus e_{i} S_{\nu}^{\prime}$, it is enough to treat the case $d=1$. Let $0 \leq \alpha_{1}$ be an integer and let $\mathscr{M}^{\prime}$ be the sub- $S_{\nu}^{\prime}$-module of $S_{\nu}^{\prime}$ generated by $\varpi^{\alpha_{1}}$. Let $\lambda$ be a positive integer such that $\frac{\alpha_{1}}{\alpha}+\lambda \frac{\beta}{\alpha}=\gamma \in \mathbb{Z}$. Such a $\lambda$ exists because $\alpha$ and $\beta$ are relatively prime. Let $\mathscr{M}$ be the sub- $S_{\nu}$-module of $S_{\nu}$ generated by $\pi$ and $\frac{u^{\lambda}}{\pi^{\gamma}}$. Let $\mu=\varpi^{-\alpha_{1}} \frac{u^{\lambda}}{\pi^{\gamma}}$, it is clear that $v_{\nu}(\mu)=0$ so that $\mu$ is a distinguished element of $S_{\nu}^{\prime}$. Thus, we have $\varpi^{\alpha_{1}} . \mu \in \mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$ and $\varpi^{\alpha_{1}} \cdot \varpi^{\alpha-\alpha_{1}} \in \mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$ therefore $\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$ is quasi-isomorphic to $\mathscr{M}^{\prime}$.

### 3.2 An approach based on localisation

We have seen that in a class of quasi-isomorphism of a finite type torsion-free $S_{\nu}$-module $\mathscr{M}$ there exists a distinguished element $\operatorname{Max}(\mathscr{M})$. In this section, we use this fact in order to represent the quasi-isomorphism class of $\mathscr{M}$ by localizing with respect to $u^{\alpha} / \pi^{\beta}$ and $\pi$. We thus obtain a representation of finite type torsion-free $S_{\nu}$-modules amenable to computations.

### 3.2.1 A useful bijection

We keep our fixed positive integer $d$. We recall that

$$
\mathscr{E}=\left\{\sum_{i \in \mathbb{Z}} a_{i} u^{i}, a_{i} \in K, v_{K}\left(a_{i}\right)+\nu i \text { bounded below and } \lim _{i \rightarrow-\infty} v_{K}\left(a_{i}\right)+\nu i=+\infty\right\}
$$

is a field containing $S_{\nu, \pi}$ and $S_{\nu, u}$. If $\mathscr{M}$ is a sub- $S_{\nu}$-module of $\mathscr{E}$ d, we shall denote by $\mathscr{M}_{\pi}$ (resp. $\mathscr{M}_{u}$ ) the sub- $S_{\nu, \pi}$-module (resp. the sub- $S_{\nu, u}$-module) of $\mathscr{E} d$ generated by $\mathscr{M}$. For example, if $\mathscr{M}$ is free over $S_{\nu}$ with basis $\left(e_{1}, \ldots, e_{h}\right)$, then $\mathscr{M}_{\pi}$ (resp. $\left.\mathscr{M}_{u}\right)$ is also free over $S_{\nu, \pi}$ (resp. $\left.S_{\nu, u}\right)$ with the same basis. As $\mathscr{M}$ is torsion free, and as $S_{\nu, u}$ and $S_{\nu, \pi}$ are principal ideal domains, $\mathscr{M}_{\pi}$ and $\mathscr{M}_{u}$ are free. We denote by $\operatorname{Max}_{S_{\nu}}^{d}$ the set of maximal sub- $S_{\nu}$-modules of $S_{\nu}^{d}$ and for $A=S_{\nu}, S_{\nu, \pi}$ or $S_{\nu, u}$, let Free ${ }_{A}^{d}$ denote the set of sub- $A$-modules of $A^{d}$, which are free over $A$. Recall that $\operatorname{Max}_{S_{0}}^{d}=\operatorname{Free}_{S_{0}}^{d}$. Thus, the following lemma provides a useful description of maximal $S_{0}$-modules.

Lemma 3.11. Let $S=S_{0}$. The natural map

$$
\begin{aligned}
& \Psi^{\prime}: \operatorname{Free}_{S}^{d} \longrightarrow \operatorname{Free}_{S_{\pi}}^{d} \times \operatorname{Free}_{S_{u}}^{d} \\
& \mathscr{M} \mapsto \\
&\left(\mathscr{M}_{\pi}, \mathscr{M}_{u}\right) .
\end{aligned}
$$

is injective. If a pair $(A, B)$ is in the image of $\Psi^{\prime}$, its unique preimage under $\Psi^{\prime}$ is given by $A \cap B$.
Proof. From the descriptions of elements of $S, S_{\pi}, S_{u}$ and $\mathscr{E}$ in terms of series, it follows that $S=S_{\pi} \cap S_{u}$. If $\mathscr{M} \in$ Free ${ }_{S}^{d}$, it is isomorphic to $S^{h}$ for $h \leq d$ and, by applying the preceding remark component by component, we get $\mathscr{M}=\mathscr{M}_{\pi} \cap \mathscr{M}_{u}$. This implies the injectivity of $\Psi^{\prime}$ and the given formula for its left-inverse.

Using Lemma 3.11, we can prove:
Theorem 3.12. The natural map

$$
\begin{aligned}
\Psi: \operatorname{Max}_{S_{\nu}}^{d} & \longrightarrow \operatorname{Free}_{S_{\nu, \pi}}^{d} \times \operatorname{Free}_{S_{\nu, u}}^{d} \\
\mathscr{M} & \mapsto\left(\mathscr{M}_{\pi}, \mathscr{M}_{u}\right) .
\end{aligned}
$$

is injective and its image consists of pairs $(A, B)$ such that $A$ and $B$ generate the same $\mathscr{E}$-vector space in $\mathscr{E}^{d}$. If a pair $(A, B)$ satisfies this condition, its unique preimage under $\Psi$ is given by $A \cap B$.

Furthermore, we have the following equalities:

$$
\begin{aligned}
\Psi\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right) & =\left(\mathscr{M}_{\pi} \cap \mathscr{M}_{\pi}^{\prime}, \mathscr{M}_{u} \cap \mathscr{M}_{u}^{\prime}\right) \\
\Psi\left(\mathscr{M}+_{\max } \mathscr{M}^{\prime}\right) & =\left(\mathscr{M}_{\pi}+\mathscr{M}_{\pi}^{\prime}, \mathscr{M}_{u}+\mathscr{M}_{u}^{\prime}\right)
\end{aligned}
$$

for all $\mathscr{M}, \mathscr{M}^{\prime} \in \operatorname{Max}_{S_{\nu}}^{d}$.
Proof. Let $\varpi$ in an algebraic closure of $K$, be such that $\varpi^{\alpha}=\pi$. Let $\mathfrak{R}^{\prime}=\mathfrak{R}[\varpi]$ and $S_{\nu}^{\prime}=S_{\nu} \otimes_{\mathfrak{R}} \mathfrak{R}^{\prime}$. We know by Lemma 2.5 that $S_{\nu}^{\prime}$ is isomorphic to $\mathfrak{R}^{\prime}[[u]]$. Then, the map $\Psi$ sits in the following commutative diagram:

$$
\begin{align*}
& \operatorname{Max}_{S_{\nu}}^{d} \xrightarrow{\Psi} \operatorname{Free}_{S_{\nu, \pi}}^{d} \times \operatorname{Free}_{S_{\nu, u}}^{d}  \tag{8}\\
& \underset{\operatorname{Free}_{S_{\nu}^{\prime}}}{\operatorname{Max}\left(. \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)}{ }^{\Psi^{\prime}} \text { Free }_{S_{\nu, \pi}^{\prime}}^{d} \times \otimes_{S_{\nu}} S_{\nu}^{\prime} \\
& \operatorname{Free}_{S_{\nu, u}^{\prime}}^{d}
\end{align*}
$$

By Proposition 3.9, the map $\mathscr{M} \mapsto \operatorname{Max}\left(\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$ is injective and $\Psi^{\prime}$ is injective by Lemma 3.11, from which we deduce that $\Psi$ is injective by the commutativity of (8).

We want to prove now that if the pair $(A, B)$ belongs to Free ${ }_{S_{\nu, \pi}}^{d} \times$ Free $_{S_{\nu, u}}^{d}$ and satisfies the condition of the theorem, then $\mathscr{M}=A \cap B$ is maximal over $S_{\nu}$ and $\Psi(\mathscr{M}) \stackrel{( }{=}(A, B)$. We claim that there exists a basis $\left(e_{1}, \ldots, e_{h}\right)$ of $A$ (over $\left.S_{\nu, \pi}\right)$ such that $\mathscr{M}$ is included inside the $S_{\nu}$-module generated by the $e_{i}$ 's. Indeed, let us first consider $\left(e_{1}, \ldots, e_{h}\right)$ a basis of $A$ and denote by $\mathscr{M}^{\prime}$ the $S_{\nu}$-module generated by the $e_{i}$ 's. Now, remark that, by our assumption on the pair $(A, B)$, every
element $x \in B$ can be written as a $\mathscr{E}$-linear combination of the $e_{i}$ 's. Taking for $n$ the smallest valuation of the coefficients appearing in this writing, we get $x \in \pi^{-n} \mathscr{M}_{u}^{\prime}$. Moreover, since $B$ is finitely generated over $S_{\nu, u}$, we can choose a uniform $n$. Replacing $e_{i}$ by $\pi^{-n} e_{i}^{\prime}$ for all $i$, we then get $A=\mathscr{M}_{\pi}^{\prime}$ and $B \subset \mathscr{M}_{u}^{\prime}$. Thus $\mathscr{M}=A \cap B \subset \mathscr{M}_{\pi}^{\prime} \cap \mathscr{M}_{u}^{\prime}=\mathscr{M}^{\prime}$.

Since $S_{\nu}$ is a noetherian ring (recall that $\nu$ is rational), we find that $\mathscr{M}$ is finitely generated over $S_{\nu}$. Furthermore, one can compute $\operatorname{Max}(\mathscr{M})$ using Proposition 3.8: if $x$ is an element of $S_{\nu}^{d}$ for which there exists $n$ such that $\pi^{n} x$ and $\left(u^{\alpha} / \pi^{\beta}\right)^{n} x$ belong to $\mathscr{M}$, then $x \in A$ (since $\pi$ is invertible in $S_{\nu, \pi}$ ) and $x \in B$ (since $u^{\alpha} / \pi^{\beta}$ is invertible in $S_{\nu, u}$ ). Thus $x \in \mathscr{M}$ and $\operatorname{Max}(\mathscr{M})=\mathscr{M}$, i.e. $\mathscr{M}$ is maximal.

Let us prove now that $\Psi(\mathscr{M})=(A, B)$. By the same argument as before, we find that there exists a positive integer $n$ such that $\pi^{n} \mathscr{M}^{\prime} \subset \mathscr{M} \subset \mathscr{M}^{\prime}$, from what it follows that $\mathscr{M}_{\pi}=\mathscr{M}_{\pi}^{\prime}=A$. The method to prove that $\mathscr{M}_{u}=B$ is analogous: we first show that there exists a basis $\left(e_{1}, \ldots, e_{h}\right)$ of $B$ over $S_{\nu, u}$ and some elements $s_{1}, \ldots, s_{h} \in S_{\nu}$ such that:

- all $s_{i}$ 's are invertible in $S_{\nu, u}$, and
- we have $\sum s_{i} e_{i} S_{\nu} \subset \mathscr{M} \subset \sum e_{i} S_{\nu}$.

From these conditions, it follows that $\mathscr{M}_{u}$ is generated by the $e_{i}$ 's over $S_{u}$ and, consequently, that $\mathscr{M}_{u}=B$.

It remains to prove the claimed formulas concerning intersections and sums. For the intersection, we note that if $\mathscr{M} \cap \mathscr{M}^{\prime}=\left(\mathscr{M}_{\pi} \cap \mathscr{M}_{u}\right) \cap\left(\mathscr{M}_{\pi}^{\prime} \cap \mathscr{M}_{u}^{\prime}\right)=\left(\mathscr{M}_{\pi} \cap \mathscr{M}_{\pi}^{\prime}\right) \cap\left(\mathscr{M}_{u} \cap \mathscr{M}_{u}^{\prime}\right)$. Hence, we just need to justify that $\mathscr{M}_{\pi} \cap \mathscr{M}_{\pi}^{\prime}$ and $\mathscr{M}_{u} \cap \mathscr{M}_{u}^{\prime}$ are free over $S_{\nu, \pi}$ and $S_{\nu, u}$ respectively, and that they generate the same $\mathscr{E}$-vector space. The freedom follows from the classification theorem of finitely generated modules over principal rings, whereas the second property is a consequence of the flatness of $\mathscr{E}$ over $S_{\nu, \pi}$ and $S_{\nu, u}$.

For the sum, we have to justify that $\left(\mathscr{M}+_{\max } \mathscr{M}^{\prime}\right)_{\pi}=\mathscr{M}_{\pi}+\mathscr{M}_{\pi}^{\prime}$ and $\left(\mathscr{M}+_{\max } \mathscr{M}^{\prime}\right)_{u}=\mathscr{M}_{u}+\mathscr{M}_{u}^{\prime}$. It is clear that $\left(\mathscr{M}+\mathscr{M}^{\prime}\right)_{\pi}=\mathscr{M}_{\pi}+\mathscr{M}_{\pi}^{\prime}$ and $\left(\mathscr{M}+\mathscr{M}^{\prime}\right)_{u}=\mathscr{M}_{u}+\mathscr{M}_{u}^{\prime}$. Hence, it is enough to prove that, given a finitely generated $S_{\nu}$-module $N \in S_{\nu}^{d}$, we have $\operatorname{Max}(N)_{\pi}=N_{\pi}$ and $\operatorname{Max}(N)_{u}=N_{u}$. It is obvious by Proposition 3.8.

Reinterpretation in the language of categories We introduce the "fiber product" category Free $_{S_{\nu, \pi}} \otimes_{\text {Free }_{\delta}}$ Free $_{S_{\nu, u}}$ whose objects are triples $(A, B, f)$ where $A \in \underline{\text { Free }}_{S_{\nu, \pi}}, B \in \underline{\text { Free }}_{S_{\nu, u}}$ and $f: \mathscr{E} \otimes_{S_{\nu, \pi}} A \rightarrow \mathscr{E} \otimes_{S_{\nu, u}} B$ is an $\mathscr{E}$-linear isomorphism. We have natural functors in both directions between $\underline{\operatorname{Max}}_{S_{\nu}}$ and $\underline{\text { Free }}_{S_{\nu, \pi}} \otimes_{\text {Free }_{\mathscr{E}}}$ Free $_{S_{\nu, u}}$ : to an object $\mathscr{M}$ of $\operatorname{Max}_{S_{\nu}}^{d}$, we associate the triple $\left(S_{\nu, \pi} \otimes_{S} \mathscr{M}, S_{\nu, u} \otimes_{S} \mathscr{M}, f\right)$ where $f$ is the canonical isomorphism, and conversely, to a triple $\left(\mathscr{M}_{\pi}, \mathscr{M}_{u}, f\right)$, we associate the fiber product of the following diagram (which turns out to be free of finite rank over $S_{\nu}$ ):


Theorem 3.12 then says that these two functors are equivalences of categories inverse one to the other. Actually, this result can be generalized to non-free modules as follows.

Proposition 3.13. The functor $\underline{\operatorname{Mod}}_{S_{\nu}} \rightarrow \underline{\operatorname{Mod}}_{S_{\nu, \pi}} \otimes_{\underline{\operatorname{Mod}}_{\delta}} \underline{\operatorname{Mod}}_{S_{\nu, u}}, \mathscr{M} \mapsto\left(S_{\nu, \pi} \otimes_{S} \mathscr{M}, S_{\nu, u} \otimes_{S} \mathscr{M}\right)$ factors through $\operatorname{Mod}_{S_{\nu}}^{\text {qis }}$ and the resulting functor

$$
\underline{\operatorname{Mod}}_{S_{\nu}}^{\text {qis }} \rightarrow \underline{\operatorname{Mod}}_{S_{\nu, \pi}} \otimes_{\underline{\operatorname{Mod}}_{E}}^{\underline{\operatorname{Mod}}_{S_{\nu, u}}}
$$

is an equivalence of categories.
Proof. Left to the reader.

### 3.2.2 Normal forms for modules over $S_{\nu, \pi}$ and $S_{\nu, u}$

As $S_{\nu, \pi}$ and $S_{\nu, u}$ are Euclidean rings there exists a good notion of rank as well as Hermite Normal Forms for matrix over these rings. In this section, we state propositions giving the shape of Hermite Normal Form together with algorithms with oracles to compute them. We recall that an algorithm with oracle is a Turing machine which has access to oracles to store elements of the base ring and perform all usual ring operations: test equality, computation of the valuation, addition, opposite, multiplication and Euclidean division. We will measure the time complexity of the algorithms by counting the number of calls to the oracles. Classically, we then derive some consequences which will be used in this paper. For the complexity analysis, we denote by $\theta$ a real number such that product of two $d \times d$ matrices with coefficient in $S_{\nu}$ can be done in $O\left(d^{\theta}\right)$ ring operations. With a naive algorithm, we can take $\theta=3$ and with the current best known algorithm of Coppersmith and Winograd [6], $\theta=2.376$.

Proposition 3.14. Let $M=\left(m_{i j}\right) \in M_{d \times d^{\prime}}\left(S_{\nu, \pi}\right)$, let re the rank of $M$. Then, there exists an invertible matrix $P$ such that $M . P=T$ with
where

- for $i=1, \ldots, r, t_{i}=u^{d_{j}}+\sum_{i=0}^{d_{j}-1} b_{j} u^{j}$ with $v_{K}\left(b_{j}\right)+\nu\left(j-d_{j}\right)>0$;
- for $i=1, \ldots, r, T_{l(i), i}=t_{i}$ and $l$ is a scrictly increasing function from $\{1, \ldots r\}$ to $\{1, \ldots, d\}$ such that $l(1)=1$.

The matrix $T$ is said to be an echelon form of $M$. Let $d_{\max }$ be the maximal Weierstrass degree of the entries of $M$, an echelon form of $M$ can be computed in $O\left(d \cdot d^{\prime} \cdot d_{\max }+\max \left(d^{\theta} \cdot d^{\prime}, d^{\prime \theta} \cdot d\right) \log \left(2 d^{\prime} / d\right)\right)$ ring operations

If the echelon form moreover satisfies:

- all entries on the $l(i)^{t h}$-row are elements of $K[u]$ of degree $<d_{i}$.
then $T$ is unique with these properties and is called the Hermite Normal Form. The Hermite Normal form of $M$ can be computed from an echelon form of $M$ at the expense of an additional $O\left(r^{2}\right)$ ring operations.

Proposition 3.15. Let $M \in M_{d \times d^{\prime}}\left(S_{\nu, u}\right)$, let $r$ be the rank of $M$. Then there exists an invertible matrix $P$ such that $M . P=T$ and
where

- for $i=1, \ldots, r, T_{l(i), i}=\pi^{d_{i}}$ where $l$ is a strictly increasing function from $\{1, \ldots r\}$ to $\{1, \ldots, d\}$ such that $l(1)=1$.

The matrix $T$ is said to be an echelon form of $M$. An echelon form of $M$ can be computed in $\left.O\left(d . d^{\prime}\right)+\max \left(d^{\theta} \cdot d^{\prime}, d^{\prime \theta} \cdot d\right) \log \left(2 d^{\prime} / d\right)\right)$ ring operations.

If the echelon form moreover satisfies

- the entries on the $l(i)^{\text {th }}$-row are representatives modulo $\pi^{d_{i}}$.
then $T$ is unique with these properties and the called the Hermite Normal Form of M. The Hermite Normal form of $M$ can be computed at the expense of an additional $O\left(r^{2}\right)$ ring operations.

Proof. The proof of the previous propositions as well as algorithms to compute the echelon form of $M$ with the given complexity is an immediate consequence of [7, Theoreme 3.1] together with the fact that $S_{\nu, \pi}$ and $S_{\nu, u}$ are Euclidean rings. Moreover for all $x, y \in S_{\nu, \pi}$ one can compute the $\operatorname{gcd}(x, y)$ in $O\left(\operatorname{deg}_{W}(y)\right)$ ring operations. From its triangle form, one can then compute the Hermite Form of $M$ with coefficients in $S_{\nu, \pi}$ at the expense of $O\left(d \cdot r \cdot d_{\max }\right)$ ring operations.

Remark 3.16. We deduce from this proposition that if $M \in M_{d \times d^{\prime}}\left(S_{\nu, \pi}\right)$ is a full rank matrix, there exists $P$ such that $M \cdot P$ is a matrix of the form (10) with all coefficients in $K[u]$. In the same way, if $M \in M_{d \times d^{\prime}}\left(S_{\nu, u}\right)$ is a full rank matrix then there exists an invertible matrix $P$ such that $M \cdot P$ has the form (11) with all entries defined modulo $\pi^{\max \left\{d_{1}, \ldots, d_{r}\right\}}$.

Let $S_{\nu, l o c}$ be $S_{\nu, u}$ or $S_{\nu, \pi}$. We derive some consequences of the existence of triangle forms and Hermite Normal Form for the representation and computation with finitely generated sub- $S_{\nu, l o c}$ modules of $S_{\nu, l o c}^{d}$. We can represent a finitely generated sub- $S_{\nu, l o c}$-module $\mathscr{M}$ of $S_{\nu, l o c}^{d}$ by a $d \times d$ matrix $M$ giving $d$ generators of $\mathscr{M}$ in the canonical basis of $S_{\nu, l o c}^{d}$ since every sub-module of $S_{\nu, l o c}^{d}$ has dimension at most $d$. Keeping the same notations, one can compute the module of syzygies of $\mathscr{M}$. For this it is enough to compute $R$, a matrix of maximal rank such that $M \cdot R=0$ which can easily be done by computing an echelon form of $M$. Given a vector $\mathscr{V} \in S_{\nu, l o c}^{d}$ provided by its coordinates vector $V$ in the canonical basis, one can check efficiently if $\mathscr{V} \in \mathscr{M}$ by finding a vector $X$ such that $M . X=V$ which can also be done with the echelon form of $M$.

Let $M$ and $M^{\prime}$ representing the modules $\mathscr{M}$ and $\mathscr{M}^{\prime}$, one can compute a matrix representing the module $\mathscr{M}+\mathscr{M}^{\prime}$ by computing the echelon form of the matrix $\left(M M^{\prime}\right)$ and taking the $d$ first columns. One can compute the intersection of $\mathscr{M}$ and $\mathscr{M}^{\prime}$ in the same way by finding $R$ and $R^{\prime}$ such that $\left(M M^{\prime}\right)\binom{R}{R^{\prime}}=0$.

### 3.2.3 Consequences for algorithmics

In view of the results of $\S 3.2 .1$ and $\S 3.2 .2$, we shall represent a maximal $S_{\nu}$-module $\mathscr{M}$ living in some $S_{\nu}^{d}$ as a pair $(A, B)$ where $A$ (resp. $B$ ) is the matrix with coefficients in $S_{\nu, \pi}$ (resp. in $S_{\nu, u}$ ) in Hermite Normal Form representing $S_{\nu, \pi} \otimes_{S_{\nu}} \mathscr{M}$ (resp. $S_{\nu, u} \otimes_{S_{\nu}} \mathscr{M}$ ).

The second part of Theorem 3.12 tells us that it is very easy to compute intersections and "maximal-sums" of $S_{\nu}$-modules with this representation. Indeed, we just have to perform the same operations on each component, and we have already explained in $\S 3.2 .2$ how to do it efficiently. As the Hermite Normal Form is unique, it is also very easy to check the equality of two maximal sub- $S_{\nu}$-modules of $S_{\nu}^{d}$. Using only the echelon form of the matrices $A$ and $B$ it is also possible to test membership.

Even better, this representation is also very convenient for many other operations we would like to perform on $S_{\nu}$-modules. Below we detail three of them. First, let $\mathscr{M} \subset S_{\nu}^{d}$ be a maximal $S_{\nu}$-module. By definition, the saturation of $\mathscr{M}$ in $S_{\nu}^{d}$ is the module

$$
\mathscr{M}_{\mathrm{sat}}=\left\{x \in S_{\nu}^{d} \quad \mid \quad \exists n \in \mathbb{N}, \pi^{n} x \in \mathscr{M}\right\}
$$

It follows from Proposition 3.8 that $\mathscr{M}_{\text {sat }}$ is maximal over $S_{\nu}$, and we would like to compute it. For that, working with our representation, we need to compute $\left(\mathscr{M}_{\text {sat }}\right)_{\pi}$ and $\left(\mathscr{M}_{\text {sat }}\right)_{u}$. But, we have $\left(\mathscr{M}_{\text {sat }}\right)_{\pi}=\mathscr{M}_{\pi}$ and

$$
\left(\mathscr{M}_{\mathrm{sat}}\right)_{u}=\left\{x \in S_{\nu, u}^{d} \quad \mid \quad \exists n \in \mathbb{N}, \pi^{n} x \in \mathscr{M}_{u}\right\} .
$$

The computation of $\left(\mathscr{M}_{\text {sat }}\right)_{\pi}$ is then for free, whereas the computation of $\left(\mathscr{M}_{\text {sat }}\right)_{u}$ can be achieved using Smith forms, which is here quite efficient due to the fact that $S_{\nu, u}$ is a discrete valuation ring. An important special case is when $\mathscr{M}$ has rank $d$ over $S_{\nu}$. Then $\left(\mathscr{M}_{\text {sat }}\right)_{u}$ is always equal to $S_{\nu, u}^{d}$. Thus, in this case, if $\mathscr{M}$ is represented by the pair of matrices $(A, B)$, then $\mathscr{M}_{\text {sat }}$ is just represented by the pair $(A, I)$ where $I$ is the identity matrix.

More generally, one can consider the following situation. Let $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ and $\mathscr{M}^{\prime} \in \operatorname{Max}_{S_{\nu, \pi}}^{d}$. We want to compute $\mathscr{M} \cap \mathscr{M}^{\prime}$, which is a maximal module over $S_{\nu}$. As before, we need to determine $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{\pi}$ and $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{u}$ and one can check that:

$$
\begin{aligned}
\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{\pi} & =\mathscr{M}_{\pi} \cap \mathscr{M}_{\pi}^{\prime} \\
\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{u} & =\mathscr{M}_{u} \cap \mathscr{M}_{u}^{\prime} .
\end{aligned}
$$

Note that, here, $\mathscr{M}_{u}^{\prime}$ is vector space over $\mathscr{E}$. As before, the intersection $\mathscr{M}_{u} \cap \mathscr{M}_{u}^{\prime}$ can be computed using Smith forms and, if $\mathscr{M}^{\prime}$ has rank $d$ over $S_{\nu, \pi}$, we just have $\mathscr{M}_{u}^{\prime}=\mathscr{E}^{d}$ and so $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{u}=\mathscr{M}_{u}$.

The third example we would like to present is obtained from the previous one by inverting the roles of $S_{\nu, \pi}$ and $S_{\nu, u}$ : we take $\mathscr{M} \in \operatorname{Free}_{S_{\nu}}^{d}$ and $\mathscr{M}^{\prime} \in \operatorname{Free}_{S_{\nu, u}}^{d}$ and we want to compute $\mathscr{M} \cap \mathscr{M}^{\prime}$. We then have $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{\pi}=\mathscr{M}_{\pi} \cap \mathscr{M}_{\pi}^{\prime}$ and $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{u}=\mathscr{M}_{u} \cap \mathscr{M}^{\prime}$. Here a new difficulty occurs: $\mathscr{M}_{\pi}^{\prime}$ is a $\mathscr{E}$-vector space and so, in previous formulas, it appears an intersection between a free module over $S_{\nu, \pi}$ and a $\mathscr{E}$-vector space. Again, one can compute this Smith form. However, it is not so efficient as before since $S_{\nu, \pi}$ is just an Euclidean ring, and not a discrete valuation ring. Anyway, it remains true that, in the case where $\mathscr{M}^{\prime}$ has full rank, then $\mathscr{M}_{\pi}^{\prime}=\mathscr{E}^{d}$. So, in this case, $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{\pi}$ is just equal to $\mathscr{M}_{\pi}$ and the computation of $\left(\mathscr{M} \cap \mathscr{M}^{\prime}\right)_{\pi}$ becomes very easy.

### 3.2.4 Further localisations

We remark that the matrix appearing in Proposition 3.15 has coefficients in $S_{\nu, u}$ which is a discrete valuation ring while the matrix of Proposition 3.14 has coefficients in $S_{\nu, \pi}$ which is only Euclidean. For certain applications, it can be more convenient to compute with elements in a discrete valuation ring; for instance, the computation of the Smith Normal Form can be made faster in a discrete valuation ring.

It is actually possible to work only over discrete valuation rings by localising further. More precisely, for any element $a \in \bar{K}$ (where $\bar{K}$ is an algebraic closure $\bar{K}$ of $K$ ) with valuation $>\nu$, we have a canonical injective morphism $S_{\nu, \pi} \rightarrow \bar{K}[[u-a]]$ which maps a series to its Taylor expansion at $a$. Hence, if $\mathscr{M}_{p}$ is a sub- $S_{\nu, \pi}$-module of $S_{\nu, \pi}^{d}$, one can consider $\mathscr{M}_{p, a}=\mathscr{M}_{p} \otimes_{S_{\nu, \pi}} \bar{K}[[u-a]] \subset$ $\bar{K}[[u-a]]^{d}$ for all element $a$ as before. Moreover, if $\mathscr{M}_{p}$ has maximal rank, all $\mathscr{M}_{p, a}$ 's are trivial (i.e. equal to $\bar{K}[[u-a]]$ ) expect a finite number of them (which are those for which $a$ is a root of one of the $t_{i}$ 's of Proposition 3.14). In addition, the map:

$$
\begin{aligned}
\Xi \quad: \operatorname{Mod}_{S_{\nu, \pi}}^{d} & \longrightarrow \prod_{a \in \bar{\Re}^{\prime}} \operatorname{Mod}_{\bar{K}[[u-a]]}^{d} \\
\mathscr{M}_{p} & \mapsto\left(\mathscr{M}_{p, a}\right)_{a}
\end{aligned}
$$

is injective and commutes with sums and intersections. Hence, one can substitute to $\mathscr{M}_{p}$, the (finite) family consisting of all non trivial $\mathscr{M}_{p, a}$ 's. This way, we just have to work with modules defined over discrete valuation rings.

Note finally that there exist algorithms to compute one representation from the other. Indeed, remark first that computing the image of $\mathscr{M}_{p}$ by $\Xi$ is trivial if $\mathscr{M}_{p}$ is represented by a matrix of generators: it is enough to map all coefficients of this matrix to all $\bar{K}[[u-a]]$ 's. Going in the other direction is more subtle but is explained In [3], §2.3.

### 3.3 A generalisation of Iwasawa's theorem and applications

The aim of this subsection is to present an algorithm with oracle to compute the maximal module associated to a $S_{\nu}$-module. Moreover, as a byproduct of our study, we will derive an upper bound on the number of generators of a maximal sub- $S_{\nu}$-module of $S_{\nu}^{n}$.

The idea of our construction (inspired by an algorithm of Cohen) is to consider the matrix of relations of a module and to perform elementary operations preserving quasi-isomorphisms to put this matrix in a certain form. In order to do so, we first need a way to compute the matrix of relations of a module or at least a certain approximation of it. Let $\mathscr{M}$ be a torsion-free finitely generated $S_{\nu}$-module and let $\left(e_{1}, \ldots, e_{k}\right) \in \mathscr{M}^{k}$ be a family of generators of $\mathscr{M}$. We denote by $\mathscr{R}$ the module of relations of $\left(e_{1}, \ldots, e_{k}\right)$ that is the set of $\left(\lambda_{1}, \ldots, \lambda_{k}\right) \in S_{\nu}^{k}$ such that $\sum_{i=1}^{k} \lambda_{i} e_{i}=0$. Let $r$ be the rank of $\mathscr{M} \otimes_{S_{\nu}} S_{\nu, \pi}$. From the exact sequence

$$
\begin{equation*}
0 \rightarrow \mathscr{R} \otimes_{S_{\nu}} S_{\nu, \pi} \rightarrow S_{\nu, \pi}^{k} \rightarrow \mathscr{M} \otimes_{S_{\nu}} S_{\nu, \pi} \rightarrow 0 \tag{12}
\end{equation*}
$$

we deduce that $\mathscr{R} \otimes_{S_{\nu}} S_{\nu, \pi}$ is a free module over $S_{\nu, \pi}$ of rank $\ell=k-r$. Let $\left(f_{1}, \ldots, f_{\ell}\right)$ be a basis of $\mathscr{R} \otimes_{S_{\nu}} S_{\nu, \pi}$ and set $\mathscr{R}^{\prime}=\oplus_{i=1}^{\ell}\left(S_{\nu, \pi} \cdot f_{i} \cap S_{\nu}^{k}\right)$. Apparently, $\mathscr{R}^{\prime}$ is a sub- $S_{\nu}$-module of $\mathscr{R}$ which is free of rank $\ell$. Indeed, if $n_{i}$ denotes the smallest integer such that $\pi^{n_{i}} \cdot f_{i} \in S_{\nu}^{k}$, then the family $\left(\pi^{n_{i}} \cdot f_{i}\right)$ is a basis of $\mathscr{R}^{\prime}$. Moreover, we have the inclusion $\mathscr{R}^{\prime} \supset \pi^{N} \mathscr{R}$ for a certain $N$ since $\mathscr{R}^{\prime} \otimes_{S_{\nu}} S_{\nu, \pi}=\mathscr{R} \otimes_{S_{\nu}} S_{\nu, \pi}$. Now, from the knowledge of the matrix $M \in M_{d \times k}\left(S_{\nu}\right)$ whose column vectors are the coordinates of $e_{i}$ in the canonical basis of $S_{\nu}^{d}$, we can compute a matrix $R^{\prime} \in M_{k \times \ell}\left(S_{\nu}\right)$ of generators of $\mathscr{R}^{\prime}$ using the algorithms of $\S 3.2 .2$. We have by definition $M . R^{\prime}=0$. Of course in the above construction, we can replace, mutatis mutandis the localisation with respect to $\pi$ by the localisation with respect to $u^{\alpha} / \pi^{\beta}$.

### 3.3.1 An algorithm to compute the maximal module

We start with a couple of matrices $M=\left(m_{i, j}\right) \in M_{d \times k}\left(S_{\nu}\right)$ and $R=\left(r_{i, j}\right) \in M_{k \times \ell}\left(S_{\nu}\right)$ representing the generators of $\mathscr{M}$ embedded in $S_{\nu}^{d}$ and a sub-module of $\mathscr{R}$ containing $\pi^{N} \mathscr{R}$ for a certain $N$. We are going to prove by induction that we can put $R$ in triangular form by using elementary operations on the rows of $R$ and the columns of $M$ which preserve $\mathscr{M}$ up to quasi-isomorphism. We suppose that for a positive integer $i_{0}$ there is a strictly increasing function $t:\left[1, i_{0}\right] \rightarrow \mathbb{N}^{*}$ such that

- for all $i=1, \ldots, i_{0}-1$, for $j>i$, and $t(i) \leq m<t(i+1), r_{j, m}=0$;
- for all $i=1, \ldots, i_{0}$, for all $j>t(i), r_{i, j}=0$.

The matrix $R$ has the following shape:

$$
R=\left(\begin{array}{llll}
r_{1, t(1)} & & &  \tag{13}\\
& & \\
& r_{i_{0}, t\left(i_{0}\right)} & & \\
& & \star & \cdots \\
& & \star \\
& & & \\
& & & \vdots \\
& & & \star
\end{array}\right)
$$

where the blanks represent 0 entries.
We set $t\left(i_{0}+1\right)$ to be the first integer $t$ such that $t\left(i_{0}\right)<t \leq \ell$ and there exists a $j \geq i_{0}+1$ with $r_{j, t} \neq 0$. If no such integer exists then we have finished. In order to describe operations on rows (resp. columns) of a matrix $T$ of dimension $k \times \ell$ it is convenient to denote the row vectors of $T$ (resp. the column vectors of $T$ ) by $L_{i}(T)$ for $i=1, \ldots, k$ (resp. $C_{i}(T)$ for $i=1, \ldots, \ell$ ). We say that the condition Cond $(i)$ on $R$ is satisfied if there exist two different indices $j_{0}, j_{1} \in\{1, \ldots, k\}$ such that $r_{j_{0}, t(i)} \cdot r_{j_{1}, t(i)} \neq 0, v_{\nu}\left(r_{j_{0}, t(i)}\right) \leq v_{\nu}\left(r_{j_{1}, t(i)}\right)$ and $\operatorname{deg}_{W}\left(r_{j_{0}, t(i)}\right) \leq \operatorname{deg}_{W}\left(r_{j_{1}, t(i)}\right)$. We apply the algorithm ColumnReduction (see Algorithm 3) on $R, M, i_{0}+1, t\left(i_{0}+1\right)$.

It is clear that the matrix $M$ returned by Algorithm 3 represents the same module $\mathscr{M}$ since it modifies $M$ by performing elementary operations on the columns. Moreover, the algorithm preserves the relation $M \cdot R=0$. The effect of the operation of Step 5 of Algorithm 3 on the entry $r_{j_{1}, t(i)}$ of $R$ is either

- replace it by 0 ,
- or it decreases strictly its Weierstrass degree and it increases its Gauss valuation.

Hence, it is easily seen that after a finite number of loops the conditions $\operatorname{Cond}\left(t\left(i_{0}+1\right)\right)$ will no longer be satisfied on $R$. It may happen that there is only one nonzero entry on the $t\left(i_{0}+1\right)^{t h}$ column of $R$ and in this case, we are basically done: by permuting the rows of $R$ we can suppose that the non zero entry is $r_{i_{0}+1, t\left(i_{0}+1\right)}$. Next, we remark that the vector $v$ of $\mathscr{M}$ whose coordinates in the canonical basis of $S_{\nu}^{d}$ is given by the $\left(i_{0}+1\right)^{t h}$ column of $M$ verifies $r_{i_{0}+1, t\left(i_{0}+1\right)} \cdot v=0$ which means that $v=0$ and we can set $r_{i_{0}+1, j}=0$ for $j>t\left(i_{0}+1\right)$.

If there are several nonzero entries on the $t\left(i_{0}+1\right)^{t h}$ column of $R$ and the condition $\operatorname{Cond}\left(t\left(i_{0}+\right.\right.$ 1)) is not satisfied on $R$, we let $j_{0}$ be such that $v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right)=\min _{1 \leq j \leq k}\left\{v_{\nu}\left(r_{j, t\left(i_{0}+1\right)}\right)\right\}$. Note that we have $v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right)<v_{\nu}\left(r_{j, t\left(i_{0}+1\right)}\right)$ for $j \neq j_{0}$ because on the contrary, the condition $\operatorname{Cond}\left(t\left(i_{0}+1\right)\right)$ would be satisfied on $R$. By multiplying the $t\left(i_{0}+1\right)^{t h}$ column of $R$ by an element of $S_{\nu, \pi}$ with valuation $-v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right)$, we can moreover suppose that $v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right)=0$. Let $\delta=\min _{j \neq j_{0}}\left(v_{\nu}\left(r_{j, t\left(i_{0}+1\right)}\right)\right)$.

```
Algorithm 3: ColumnReduction (preliminary version)
    input :
        - \(M \in M_{d \times k}\left(S_{\nu}\right)\)
        - \(R \in M_{k \times \ell}\left(S_{\nu}\right)\) in the form (13),
        - \(i, t(i) \in \mathbb{N}\)
    output: \(R, M\) such that \(M \cdot R=0\) and \(R\) does not satisfy condition \(\operatorname{Cond}(t(i))\)
    while \(\operatorname{Cond}(t(i))\) is satisfied do
        Pick up \(j_{0}, j_{1} \in\{1, \ldots, k\}\) such that \(r_{j_{0}, t(i)} \cdot r_{j_{1}, t(i)} \neq 0, v_{\nu}\left(r_{j_{0}, t(i)}\right) \leq v_{\nu}\left(r_{j_{1}, t\left(i_{0}+1\right)}\right)\) and
        \(\operatorname{deg}_{W}\left(r_{j_{0}, t(i)}\right) \leq \operatorname{deg}_{W}\left(r_{j_{1}, t(i)}\right) ;\)
        \((q, r) \leftarrow\) EuclideanDivision \(\left(r_{j_{0}, t(i)}, r_{j_{1}, t(i)}\right)\);
        \(C_{j_{0}}(M) \leftarrow C_{j_{0}}(M)+q C_{j_{1}}(M) ;\)
        \(L_{j_{1}}(R) \leftarrow L_{j_{1}}(R)-q L_{j_{0}}(R) ;\)
    return \(M, R\);
```

The case $\nu=0$ First, we suppose that $\nu=0$ from which we deduce that $\delta$ is a positive integer. Denote by $e_{1}, \ldots, e_{k}$ the generators of $\mathscr{M}$ represented by the column vectors of the matrix $M$. Denote by $\mathscr{M}_{1}$ the module generated by $\left(e_{j}^{\prime}\right)_{j=1 \ldots k}$ with $e_{j}^{\prime}=e_{j}$ for $j \neq j_{0}$ and $e_{j_{0}}^{\prime}=\frac{1}{\pi} e_{j_{0}}$. The identity of $S_{\nu}^{d}$ induces an inclusion $f: \mathscr{M} \rightarrow \mathscr{M}_{1}$. It is clear that the cokernel of $f$ is annihilated by $\pi$. Moreover, we have

$$
\begin{equation*}
r_{j_{0}, t\left(i_{0}+1\right)} \cdot e_{j_{0}}^{\prime}=\sum_{j \neq j_{0}} \frac{r_{j, t\left(i_{0}+1\right)}}{\pi} e_{j} . \tag{14}
\end{equation*}
$$

As the right hand side of (14) is in $\mathscr{M}$ since $\frac{r_{j, t\left(i_{0}+1\right)}}{\pi} \in S_{\nu}$, the cokernel of $f$ is also annihilated by $r_{j_{0}, t\left(i_{0}+1\right)}$ which is a distinguished element of $S_{\nu}$. We conclude that $f$ is a quasi-isomorphism.

We denote by $O_{1}(j)$ the operation on the couple of matrices $(M, R)$ which consists in multiplying by $\frac{1}{\pi}$ the $(j)^{t h}$ column of $M$ and multiplying by $\pi$ the $(j)^{t h}$ row of $R$. Keeping the hypothesis and notations of the preceding paragraph, it is clear that if $(M, R)$ represents the module $\mathscr{M}$ and its relations, then the matrices resulting of the operation of $O_{1}\left(j_{0}\right)$ represents the module $\mathscr{M}_{1}$ which is quasi-isomorphic to $\mathscr{M}$. By repeating operations of the form $O_{1}(j)$ a finite number of time, we can suppose that $\delta=0$. But it means that the condition $\operatorname{Cond}\left(t\left(i_{0}+1\right)\right)$ is not satisfied on $R$ and we can call again Algorithm 3.

We thus obtain the algorithm ColumnReduction (final version) which takes a relation matrix of the form (13) for $i_{0}$ and returns a relation matrix of the same form for $i_{0}+1$. The algorithm MatrixReduction (final version), Algorithm 6, uses ColumnReduction in order to compute a new set of generators of a module quasi-isomorphic to $\mathscr{M}$ the relation matrix of which has a triangular form.

The general case We reduce the general case to the case $\nu=0$, by using Lemma 2.5. Let $\varpi$ in an algebraic closure of $K$ be such that $\varpi^{\alpha}=\pi$. Let $\mathfrak{R}^{\prime}=\mathfrak{R}[\varpi], S_{\nu}^{\prime}=S_{\nu} \otimes_{\mathfrak{R}} \mathfrak{R}^{\prime}$ and $\mathscr{M}^{\prime}=\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$. The valuation on $\mathfrak{R}$ (resp. the Gauss valuation on $S_{\nu}$ ) extends uniquely to $\mathfrak{R}^{\prime}$ (resp. to $S_{\nu}^{\prime}$ ). We have $v_{\nu}(\varpi)=1 / \alpha$. The algorithm for the general case is exactly the same as for the case $\nu=0$ up to the point when $\operatorname{Cond}\left(t\left(i_{0}+1\right)\right)$ is not satisfied. By multiplying the $t\left(i_{0}+1\right)^{t h}$ column of $R$ by $\varpi^{-v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right) \cdot \alpha}$, we can moreover suppose that $v_{\nu}\left(r_{j_{0}, t\left(i_{0}+1\right)}\right)=0$. Let $\delta=\min _{j \neq j_{0}}\left(v_{\nu}\left(r_{j, t\left(i_{0}+1\right)}\right)\right)$.

With this setting, we can define a quasi-isomorphism in the same manner as before. Namely, let $e_{1}, \ldots, e_{k}$ be the generators of $\mathscr{M}^{\prime}$ as a sub-module of ${S_{\nu}^{\prime}}^{d}$ represented by the column vectors of the matrix $M$. Denote by $\mathscr{M}_{1}^{\prime}$ the module generated by $\left(e_{j}^{\prime}\right)_{j=1 \ldots k}$ where $e_{j}^{\prime}=e_{j}$ for $j \neq j_{0}$ and $e_{j_{0}}^{\prime}=\frac{1}{\omega^{\delta}} e_{j_{0}}$. Then the natural injection $\mathscr{M}^{\prime} \rightarrow \mathscr{M}_{1}^{\prime}$ is a quasi-isomorphism. We denote by $O_{2}(j, \delta)$ the operation on the couple of matrices $(M, R)$ with coefficients in $S_{\nu}^{\prime}$ which consists in multiplying by $\frac{1}{\varpi^{\delta}}$ the $(j)^{t h}$ column of $M$ and multiplying by $\varpi^{\delta}$ the $(j)^{t h}$ row of $R$. With the hypothesis and notations of this paragraph (i.e. $M$ has the form (13)), if $(M, R)$ represents the module $\mathscr{M}^{\prime}$ and its

```
Algorithm 4: MatrixReduction for the case \(\nu=0\)
    input :
        - \(R \in M_{k \times \ell}\left(S_{\nu}\right)\),
        - \(M \in M_{d \times k}\left(S_{\nu}\right)\) such that \(M \cdot R=0\).
    \(i_{0} \leftarrow 0 ;\)
    \(t\left(i_{0}\right) \leftarrow 1 ;\)
    while \(i \leq k\) do
        \(t\left(i_{0}\right) \leftarrow \min \left\{t \mid t>t\left(i_{0}\right)\right.\) and \(\exists j>0\), with \(\left.r_{j, t} \neq 0\right\} ;\)
        \(i_{0} \leftarrow i_{0}+1\);
        \(M, R \leftarrow\) ColumnReduction \(\left(M, R, i_{0}, t\left(i_{0}\right)\right)\);
        for \(j \leftarrow t\left(i_{0}\right)+1\) to \(\ell\) do
            \(r_{i_{0}, j} \leftarrow 0\)
```

    output: \(R \in M_{k \times \ell}\left(S_{\nu}^{\prime}\right), M \in M_{d \times k}\left(S_{\nu}^{\prime}\right)\) such that \(M \cdot R=0\) and \(R\) is a triangular matrix.
    ```
Algorithm 5: ColumnReduction (final version) for \(\nu=0\)
    input :
        - \(M \in M_{d \times k}\left(S_{\nu}\right)\),
        - \(R \in M_{k \times \ell}\left(S_{\nu}\right)\) in the form (13),
        - \(i, t(i) \in \mathbb{N}\) the position of the last non zero "diagonal" entry of \(R\).
    output: \(R, M\) such that \(M . R=0\) and \(R\) is triangular up to the \(i+1\) row.
    while \(\exists j_{0}, j_{1}\) such that \(j_{0} \neq j_{1}\) and \(r_{j_{0}, t(i)} \cdot r_{j_{1}, t(i)} \neq 0\) do
        while \(\operatorname{Cond}(t(i))\) is satisfied do
            Pick up \(j_{0}, j_{1} \in\{1, \ldots, k\}\) such that \(r_{j_{0}, t(i)} \cdot r_{j_{1}, t(i)} \neq 0, v_{\nu}\left(r_{j_{0}, t(i)}\right) \leq v_{\nu}\left(r_{j_{1}, t(i)}\right)\) and
            \(\operatorname{deg}_{W}\left(r_{j_{0}, t(i)}\right) \leq \operatorname{deg}_{W}\left(r_{j_{1}, t(i)}\right)\);
            \((q, r) \leftarrow\) EuclideanDivision \(\left(r_{j_{0}, t(i)}, r_{j_{1}, t(i)}\right)\);
            \(C_{j_{0}}(M) \leftarrow C_{j_{0}}(M)+q C_{j_{1}}(M) ;\)
            \(L_{j_{1}}(R) \leftarrow L_{j_{1}}(R)-q L_{j_{0}}(R) ;\)
        Let \(j_{0}\) be such that \(\operatorname{deg}_{W}\left(r_{j_{0}, t(i)}\right)=\max _{1 \leq j \leq k}\left\{\operatorname{deg}_{W}\left(r_{j, t(i)}\right)\right\}\);
        \(\delta \leftarrow \min _{j \neq j_{0}}\left(v_{\nu}\left(r_{j, t(i)}\right)\right)-v_{\nu}\left(r_{j_{0}, t(i)}\right) ;\)
        \(C_{j_{0}}(M) \leftarrow \frac{1}{\pi^{\delta}} C_{j_{0}}(M) ;\)
        \(L_{j_{0}}(R) \leftarrow \pi^{\delta} L_{j_{0}}(R) ;\)
    return \(M, R\);
```

relations, then the matrices $\left(M^{\prime}, R^{\prime}\right)$ resulting of the operation of $O_{2}\left(j_{0}, \delta\right)$ represents the module $\mathscr{M}_{1}^{\prime}$ which have been shown to be quasi-isomorphic to $\mathscr{M}^{\prime}$ (as a $S_{\nu^{\prime}}^{\prime}$-module). Moreover, $R^{\prime}$ verifies the condition $\operatorname{Cond}\left(t\left(i_{0}+1\right)\right)$.

The matrix $M^{\prime}$ (resp. $R^{\prime}$ ), resulting of the operation $O_{2}(j, \delta)$ is made of column (resp. row) vectors with coefficients in $S_{\nu}$ multiplied by $\varpi^{\delta}$ for a certain $\delta \in \frac{1}{\alpha} \mathbb{Z}$. An important claim is that this structure will be kept intact in the course of the computations involving all the elementary operations introduced up to now. In fact, these operations on the rows of $R$ are:

- multiplication of a row by a $\varpi^{\alpha}$, for $\alpha$ an integer ;
- permutation of the rows ;
- for $j_{0}, j_{1} \in\{1, \ldots, k\}$, replacing $L_{j_{1}}(R)$ by $L_{j_{1}}(R)-q^{\prime} L_{j_{0}}(R)$ where $q^{\prime}$ is the quotient of $\varpi_{1}^{\alpha} \cdot y$ by $\varpi^{\alpha_{0}} \cdot x$ for $x, y \in S_{\nu}$ and $\alpha_{0}, \alpha_{1} \in \mathbb{N}$.

It is clear that the two first operations does not change the structure of $R$ and the same thing is true for the last operation. Indeed, let $q \in S_{\nu, \pi}$ and $r \in S_{\nu, \pi} \cap K[u]$ with $\operatorname{deg}(r) \leq \operatorname{deg}_{W}(x)$, be such that $y=q \cdot x+r$, then for $\alpha_{0}, \alpha_{1} \in \mathbb{N}$, we have $\varpi^{\alpha_{0}} \cdot y=\varpi^{\alpha_{0}-\alpha_{1}} q \cdot \varpi^{\alpha_{1}} x+\varpi^{\alpha_{0}} r$ so that we have $q^{\prime}=\varpi^{\alpha_{0}-\alpha_{1}} q$ with $q \in S_{\nu}$.

In order to prove formality this claim and take advantage of it to carry out all the computations in the smaller $S_{\nu}$ coefficient ring, we represent the couple of matrices $\left(M^{\prime}, R^{\prime}\right)$ with coefficients in $S_{\nu}^{\prime}$ by a triple $(M, R, L)$ where $M, R$ are matrices with coefficients in $S_{\nu}$ and $L=\left[\alpha_{1}, \ldots, \alpha_{k}\right]$ is a list of integers such that for $i=1, \ldots, k, C_{i}\left(M^{\prime}\right)=\varpi_{i}^{\alpha} C_{i}(M)$ and $L_{i}\left(R^{\prime}\right)=\varpi^{-\alpha_{i}} L_{i}(R)$. We say that the condition $\operatorname{Cond}^{\prime}(i)$ on $R$ is satisfied if there exists two different $j_{0}, j_{1} \in\{1, \ldots, k\}$ such that $r_{j_{0}, t(i)} \cdot r_{j_{1}, t(i)} \neq 0, v_{\nu}\left(r_{j_{0}, t(i)}\right)+\frac{\alpha_{j_{0}}}{\alpha} \leq v_{\nu}\left(r_{j_{1}, t(i)}\right)+\frac{\alpha_{j_{1}}}{\alpha}$ and $\operatorname{deg}_{W}\left(r_{j_{0}, t(i)}\right) \leq \operatorname{deg}_{W}\left(r_{j_{1}, t(i)}\right)$. With these notations, we can write the final version of the MatrixReduction algorithm (see Algorithm 6 ) which encode the matrices $M^{\prime}, R^{\prime}$ with coefficients in $S_{\nu}^{\prime}$ with a couple $M, R$ of matrices with coefficients in $S_{\nu}$ and a list of integers.

Example 3.17. We illustrate the operation of the algorithm on the module of example 3.3. Recall that $\mathscr{M}$ is the submodule of $S_{0}$ generated by $\left(\pi^{2}, \pi u^{3}\right)$. It is represented in the canonical basis of $S_{0}$ by the matrices $M$ of generators and $R$ of relation :

$$
M=\left(\begin{array}{ll}
\pi^{2} & \pi u^{3}
\end{array}\right), R=\binom{u^{3}}{-\pi}
$$

It is clear that $\operatorname{Cond}(1)$ is not verified on $R$ since there is no division possible between its entries. As a consequence, we apply operation $O_{1}(1)$ on the couple $(M, R)$ to obtain:

$$
M=\left(\begin{array}{ll}
\pi & \pi u^{3}
\end{array}\right), R=\binom{\pi u^{3}}{-\pi}
$$

Now, we have $\pi u^{3}=-u^{3} \cdot \pi$ and by applying on $M$ (resp. $R$ ) an elementary operation on the columns (resp. rows), we get finally:

$$
M=\left(\begin{array}{ll}
\pi & 0
\end{array}\right), R=\binom{0}{-\pi} .
$$

An we deduce that the maximal module associate to $\mathscr{M}$ is $\pi . S_{0}$.

### 3.3.2 Computation of $\operatorname{Max}(\mathscr{M})$

Let $M_{1}, R_{1}, L_{1}=\operatorname{MatrixReduction}(M, R, L=[0, \ldots, 0])$. Let $L_{1}=\left[\beta_{1}, \ldots, \beta_{k}\right]$. We denote by $\mathscr{M}_{1}^{\prime}$ the sub- $S_{\nu}^{\prime}$-module of $\left(S_{\nu}^{\prime}\right)^{d}$ generated by the vectors given in the canonical basis of $\left(S_{\nu}^{\prime}\right)^{d}$ by the column vectors $\varpi^{\beta_{i}} \cdot C_{i}\left(M_{1}\right)$ for $i \in\{1, \ldots, k\}$ such that $L_{i}\left(R_{1}\right)$ is the zero vector.

Lemma 3.18. We have $\mathscr{M}_{1}^{\prime}=\operatorname{Max}\left(\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$.

```
Algorithm 6: MatrixReduction
    input :
        - \(R \in M_{k \times \ell}\left(S_{\nu}\right)\),
        - \(M \in M_{d \times k}\left(S_{\nu}\right)\) such that \(M \cdot R=0\).
    output: \(R \in M_{k \times \ell}\left(S_{\nu}^{\prime}\right), M \in M_{d \times k}\left(S_{\nu}^{\prime}\right), L\) such that \(M \cdot R=0\) and \(R\) is a triangular
            matrix.
    \(i_{0} \leftarrow 0 ;\)
    \(t\left(i_{0}\right) \leftarrow 1 ;\)
    \(L \leftarrow[0, \ldots, 0] ;\)
    while \(i \leq k\) do
        \(i_{0} \leftarrow i_{0}+1 ;\)
        \(t\left(i_{0}\right) \leftarrow \min \left\{t \mid t>t\left(i_{0}\right)\right.\) and \(\exists j>0\), with \(\left.r_{j, t} \neq 0\right\}\);
        while \(\exists j_{0}, j_{1}\) such that \(j_{0} \neq j_{1}\) and \(r_{j_{0}, t\left(i_{0}\right)} \cdot r_{j_{1}, t\left(i_{0}\right)} \neq 0\) do
            while \(\operatorname{Cond}^{\prime}\left(t\left(i_{0}\right)\right)\) is satisfied do
            Pick up \(j_{0}, j_{1} \in\{1, \ldots, k\}\) such that \(r_{j_{0}, t\left(i_{0}\right)} \cdot r_{j_{1}, t\left(i_{0}\right)} \neq 0\),
            \(v_{\nu}\left(r_{j_{0}, t\left(i_{0}\right)}\right)+\frac{L\left[j_{0}\right]}{\alpha} \leq v_{\nu}\left(r_{j_{1}, t\left(i_{0}\right)}\right)+\frac{L\left[j_{1}\right]}{\alpha}\) and \(\operatorname{deg}_{W}\left(r_{j_{0}, t\left(i_{0}\right)}\right) \leq \operatorname{deg}_{W}\left(r_{j_{1}, t\left(i_{0}\right)}\right)\);
            if \(v_{\nu}\left(r_{j_{0}, t\left(i_{0}\right)}\right)>v_{\nu}\left(r_{j_{1}, t\left(i_{0}\right)}\right)\) then
                \(\delta_{0} \leftarrow\left\lceil v_{\nu}\left(r_{j_{0}, t\left(i_{0}\right)}\right)-v_{\nu}\left(r_{j_{1}, t\left(i_{0}\right)}\right)\right\rceil ;\)
                \(L_{j_{1}}(R) \leftarrow \pi^{\delta_{0}} L_{j_{1}}(R)\);
                \(C_{j_{1}}(M) \leftarrow \pi^{-\delta_{0}} C_{j_{1}}(M) ;\)
                \(L\left[j_{1}\right] \leftarrow L\left[j_{1}\right]+\alpha \cdot \delta_{0} ;\)
            \((q, r) \leftarrow\) EuclideanDivision \(\left(r_{j_{0}, t\left(i_{0}\right)}, r_{j_{1}, t\left(i_{0}\right)}\right) ;\)
            \(C_{j_{0}}(M) \leftarrow C_{j_{0}}(M)+q C_{j_{1}}(M) ;\)
            \(L_{j_{1}}(R) \leftarrow L_{j_{1}}(R)-q L_{j_{0}}(R) ;\)
            Let \(j_{0}\) be such that \(\operatorname{deg}_{W}\left(r_{j_{0}, t\left(i_{0}\right)}\right)=\max _{1 \leq j \leq k}\left\{\operatorname{deg}_{W}\left(r_{j, t\left(i_{0}\right)}\right)\right\}\);
            \(\delta \leftarrow \min _{j \neq j_{0}}\left(v_{\nu}\left(r_{j, t\left(i_{0}\right)}\right)\right)-v_{\nu}\left(r_{j_{0}, t\left(i_{0}\right)}\right)\);
            \(C_{j_{0}}(M) \leftarrow \frac{1}{\pi^{\delta \delta}} C_{j_{0}}(M)\);
            \(L_{j_{0}}(R) \leftarrow \pi^{\lfloor\delta\rfloor} L_{j_{0}}(R)\);
            \(L\left[j_{0}\right] \leftarrow L\left[j_{0}\right]+\delta-\lfloor\delta\rfloor ;\)
        for \(j \leftarrow t\left(i_{0}\right)+1\) to \(\ell\) do
            \(r_{i_{0}, j} \leftarrow 0\)
        Let \(j_{0} \in\{1, \ldots, k\}\) be such that \(r_{j_{0}, t\left(i_{0}\right)} \neq 0\);
        \(\left(C_{j_{0}}(M), C_{i_{0}}(M)\right) \leftarrow\left(C_{i_{0}}(M), C_{j_{0}}(M)\right) ;\)
        \(\left(L_{j_{0}}(R), L_{i_{0}}(R)\right) \leftarrow\left(L_{i_{0}}(R), L_{j_{0}}(R)\right) ;\)
```

Proof. Let $\mathscr{M}^{\prime}=\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}$ and let $\mathscr{M}_{1}$ be the sub- $S_{\nu}^{\prime}$-module of $\left(S_{\nu}^{\prime}\right)^{d}$ generated by the column vectors of $M_{1}$. It is clear that $\mathscr{M}_{1}=\mathscr{M}_{1}^{\prime}$ since for $i \in\{1, \ldots, k\}$ such that $L_{i}\left(R_{1}\right)$ is not the zero vector, we have $C_{i}\left(M_{1}\right)=0$ (because $\mathscr{M}_{1}$ is torsion free). As $\mathscr{M}_{1}$ is obtained from $\mathscr{M}^{\prime}$ by a sequence of quasi-isomorphisms, it means that there exists a quasi-isomorphism $q^{\prime}: \mathscr{M}^{\prime} \rightarrow \mathscr{M}_{1}^{\prime}$. If we prove that $\mathscr{M}_{1}^{\prime}$ is a free $S_{\nu}^{\prime}$-module, we are done by Lemma 3.6.

Consider the exact sequence $0 \rightarrow \mathscr{R} \rightarrow S_{\nu}^{k} \rightarrow \mathscr{M} \rightarrow 0$ associated to the family $\left(e_{1}, \ldots, e_{k}\right)$ of generators of $\mathscr{M}$. As $S_{\nu}^{\prime}$ is flat over $S_{\nu}$, and as $\mathscr{R}^{\prime} \otimes_{S_{\nu}} S_{\nu}^{\prime}[1 / \varpi]=\mathscr{R} \otimes_{S_{\nu}} S_{\nu}^{\prime}[1 / \varpi]$ by definition of $\mathscr{R}^{\prime}$, we have an exact sequence

$$
\begin{equation*}
0 \rightarrow \mathscr{R}^{\prime} \otimes_{S_{\nu}} S_{\nu}^{\prime}[1 / \varpi] \rightarrow\left({S_{\nu}^{\prime}}^{k}\right)[1 / \varpi] \rightarrow \mathscr{M}^{\prime}[1 / \varpi] \rightarrow 0 \tag{15}
\end{equation*}
$$

defined by the generators $\left(e_{1}, \ldots, e_{k}\right)$ of $\mathscr{M}^{\prime}[1 / \varpi]$. It is clear that at each step, the algorithm ReduceMatrix describes an exact sequence of the form (15) for a different map $\left(S_{\nu}^{\prime k}\right)[1 / \varpi] \rightarrow$ $\mathscr{M}^{\prime}[1 / \varpi]$ since it preserves the relation $M R=0$. From this and the definition of $M_{1}^{\prime}$, we deduce that if $\mathscr{R}_{1}$ is the module of relations of $\mathscr{M}_{1}^{\prime}$ then $\mathscr{R}_{1}[1 / \varpi]=0$ from which we deduce that $\mathscr{R}_{1}=0$ and we are done.

Remark 3.19. As a byproduct of the preceding proof, we see that the vectors given in the canonical basis of $\left(S_{\nu}^{\prime}\right)^{d}$ by the column vectors $\varpi^{\beta_{i}} \cdot C_{i}\left(M_{1}\right)$ for $i \in\{1, \ldots, k\}$ such that $L_{i}\left(R_{1}\right)$ is the zero vector form a basis of $\mathscr{M}_{1}^{\prime}$.
Corollary 3.20. Let $\mathscr{M}_{2}=\mathscr{M}_{1}^{\prime} \cap S_{\nu}^{d}$. Then, $\mathscr{M}_{2}=\operatorname{Max}(\mathscr{M})$.
Proof. The corollary is an immediate consequence of Proposition 3.9 and Lemma 3.18.

### 3.3.3 Computation with $S_{\nu}$-modules

Proposition 3.9 and Lemma 3.18 establish a one-to-one correspondence $\Phi: \operatorname{Max}_{S_{\nu}}^{d} \rightarrow$ Free $_{S^{\prime}}^{d}$, defined by $\mathscr{M} \mapsto \operatorname{Max}\left(\mathscr{M} \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$. Moreover, the image of $\Phi$ is exactly the set of free sub- $S_{\nu^{\prime}}^{\prime}$ modules of ${S_{\nu}^{\prime}}^{d}$ which admit a basis $\left(e_{i}\right)_{i \in I}$ where $e_{i} \in\left(S_{\nu}^{\prime}\right)^{d}$ and $e_{i}=\varpi^{\alpha_{i}} e_{i}^{\prime}$ with $e_{i}^{\prime} \in\left(S_{\nu}\right)^{d}$ and $0 \leq \alpha_{i} \leq \alpha$. We have seen that a $\mathscr{M} \in \Phi\left(\operatorname{Max}_{S_{\nu}}^{d}\right)$ can be represented by a couple ( $M, L$ ) where $M \in M_{d \times k}\left(S_{\nu}\right)$ and $L$ is a list of positive integers $\leq \alpha$.

From the data of a matrix representing an element of $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ the algorithm MatrixReduction computes the couple $(M, L)$ representing $\Phi(\mathscr{M})$. Moreover, if $\mathscr{M}^{\prime} \in \Phi\left(\operatorname{Max}_{S_{\nu}}^{d}\right)$, the Algorithm 7 allows to recover $\Phi^{-1}\left(\mathscr{M}^{\prime}\right)$. We see that we can easily go back and forth between the different representations. For most of the applications however, it is convenient to represent an element of $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ by a couple $(M, L)$. Indeed, we have the lemma:

Lemma 3.21. Let $\mathscr{M}_{1}, \mathscr{M}_{2} \in \operatorname{Max}_{S_{\nu}}^{d}$, then

$$
\begin{aligned}
\Phi\left(\mathscr{M}_{1} \cap \mathscr{M}_{2}\right) & =\Phi\left(\mathscr{M}_{1}\right) \cap \Phi\left(\mathscr{M}_{2}\right), \\
\Phi\left(\mathscr{M}_{1}+{ }_{\max } \mathscr{M}_{2}\right) & =\Phi\left(\mathscr{M}_{1}\right)+_{\max } \Phi\left(\mathscr{M}_{2}\right) .
\end{aligned}
$$

Proof. For the first claim, we have $\Phi^{-1}\left(\Phi\left(\mathscr{M}_{1}\right) \cap \Phi\left(\mathscr{M}_{2}\right)\right)=\Phi\left(\mathscr{M}_{1}\right) \cap \Phi\left(\mathscr{M}_{2}\right) \cap S_{\nu}^{d}=\left(\Phi\left(\mathscr{M}_{1}\right) \cap\right.$ $\left.S_{\nu}^{d}\right) \cap\left(\Phi\left(\mathscr{M}_{2}\right) \cap S_{\nu}^{d}\right)=\mathscr{M}_{1} \cap \mathscr{M}_{2}$.

Next, we prove the second claim. We have the following diagram of quasi-isomorphisms:


Thus, we have $\operatorname{Max}\left(\operatorname{Max}\left(\mathscr{M}_{1}+\mathscr{M}_{2}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)=\operatorname{Max}\left(\left(\mathscr{M}_{1}+\mathscr{M}_{2}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)=\operatorname{Max}\left(\operatorname{Max}\left(\mathscr{M}_{1} \otimes_{S_{\nu}}\right.\right.$ $\left.\left.S_{\nu}^{\prime}\right)+\operatorname{Max}\left(\mathscr{M}_{2} \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)\right)$ which is exactly the desired result.

Let $\mathscr{M}_{1}, \mathscr{M}_{2} \in \Phi\left(\operatorname{Max}_{S_{\nu}}^{d}\right)$ be represented respectively by the couples $\left(M_{1}, L_{1}\right)$ and $\left(M_{2}, L_{2}\right)$. Then, by Lemma 3.21 one can represent the sum $\mathscr{M}_{1}+_{\max } \mathscr{M}_{2}$ by applying the algorithm MatrixReduction on the couple $\left(\left(M_{1} M_{2}\right), L_{1}+L_{2}\right)$ (where $L_{1}+L_{2}$ is the concatenation of the lists $L_{1}$ and $L_{2}$ ). The representation as a couple $(M, L)$ is however not well suited to the computation of the intersection of modules, since it implies the computation of the kernel of a matrix with coefficient in $S_{\nu}$ which is not Euclidean.

### 3.3.4 The generators of a maximal module

In order to have a complete algorithm (with oracles) to compute $\operatorname{Max}(\mathscr{M})$, it remains to explain how to recover $\mathscr{M}_{2}=\mathscr{M}_{1}^{\prime} \cap S_{\nu}^{d}$ from the knowledge of $\mathscr{M}_{1}^{\prime}$ (see $\S 3.3 .2$ for the definition of $\mathscr{M}_{1}^{\prime}$ ). We would like also to obtain a bound on the number of generators of $\mathscr{M}_{2}$. By the construction of $\mathscr{M}_{1}^{\prime}$, there exists a basis $\left(e_{1}, \ldots, e_{k}\right) \in S_{\nu}^{d}$ and $\delta_{i} \in \mathbb{N}$ for $i=1, \ldots, k$, such that $\mathscr{M}_{1}^{\prime}=\bigoplus_{i=1}^{k} S_{\nu}^{\prime} \cdot \varpi^{\delta_{i}} e_{i}$. Then, we have $\mathscr{M}_{2}=\bigoplus_{i=1}^{k}\left(S_{\nu}^{\prime} \cdot \varpi^{\delta_{i}} \cap S_{\nu}\right) . e_{i}$. Hence, it is enough to explain how to compute $\mathscr{M}_{1}^{\prime} \cap S_{\nu}^{d}$ when $\mathscr{M}_{1}^{\prime}$ has dimension 1. In this case, $\mathscr{M}_{1}^{\prime}$ is generated by an element of the form $\frac{1}{\varpi^{\delta}} \cdot y$ where $y \in S_{\nu}$ and by definition, we want to find generators for the $S_{\nu}$-module $\left\{x \in S_{\nu} \left\lvert\, v_{\nu}(x) \geq v_{\nu}\left(\frac{1}{\varpi^{\delta}} \cdot y\right)\right.\right\}$. We are reduced to the problem of finding generators of the $S_{\nu}$-module $\mathscr{N}=\left\{x \in S_{\nu} \mid v_{\nu}(x) \geq-\delta / \alpha\right\}$.
Lemma 3.22. Let $\delta \in\{0, \ldots, \alpha-1\}$. We define inductively a sequence of couple of integers $\left(\alpha_{i}, \beta_{i}\right)$ by setting $\alpha_{0}=0, \beta_{0}=0$. Then for $i>0$, while $\beta_{i-1}+\alpha_{i-1} \nu>-\frac{\delta}{\alpha}$, we let $\left(\alpha_{i}, \beta_{i}\right)$ be the unique couple of integers such that

- $\beta_{i}+\alpha_{i} \nu \geq-\frac{\delta}{\alpha}$,
- for all $(x, y) \neq\left(\alpha_{i}, \beta_{i}\right) \in \mathbb{Z}^{2}$ such that $0 \leq x \leq \alpha_{i}$ and $y+x \nu \geq-\frac{\delta}{\alpha}$, we have $\beta_{i}+\alpha_{i} \nu<y+x \nu$,
- $\alpha_{i}$ is the smallest integer strictly greater than $\alpha_{i-1}$ such that there exists an integer $\beta_{i}$ with ( $\alpha_{i}, \beta_{i}$ ) satisfying the two conditions above.
The family $\left(\pi^{\beta_{i}} \cdot u^{\alpha_{i}}\right)$ has cardinality bounded by $\alpha$ and is a system of generators of the $S_{\nu^{-}}$ module $\mathscr{N}=\left\{x \in S_{\nu} \mid v_{\nu}(x) \geq-\delta / \alpha\right\}$.
Proof. First, it is clear by definition that all the $\pi^{\beta_{i}} \cdot u^{\alpha_{i}}$ are elements of $\mathscr{N}$. Moreover, it is clear that $\alpha_{i}$ is bounded by $-\delta / \beta \bmod \alpha$.

Denote by $\mathscr{N}_{0}$ the sub- $S_{\nu}$-module of $\mathscr{N}$ generated by the family $\left(\pi^{\beta_{i}} \cdot u^{\alpha_{i}}\right)$. Let $x \in \mathscr{N}$, we prove inductively on $\operatorname{deg}_{W}(x)$ that $x$ is in $\mathscr{N}_{0}$. If $\operatorname{deg}_{W}(x)=0$ then $v_{\nu}(x) \geq 0$ so that $x=x \cdot 1$ with $x \in S_{\nu}$. Suppose that $d=\operatorname{deg}_{W}(x)>0$. As $v_{\nu}(x) \geq-\delta / \alpha$, by applying Corollary 2.9, we can write $x=q \cdot h$, with $q \in S_{\nu}$ invertible and $h \in K[u]$ is a degree $d$ polynomial such that $v_{\nu}(h) \geq-\delta / \alpha$ and $\operatorname{deg}_{W}(h)=d$. We have to show that $h$ is in $\mathscr{N}_{0}$. Let $i_{0}$ be the greatest index such that $\alpha_{i_{0}} \leq d$. Then by construction of the family $\left(\alpha_{i}, \beta_{i}\right)$, we have $v_{\nu}\left(\pi^{\beta_{i}} \cdot u^{\alpha_{i_{0}}}\right) \leq v_{\nu}(h)$. Indeed, if $t$ is the term of $h$ of degree $d$ then $t \in \mathscr{N}$ and if we write $t=\pi^{\mu} \cdot u^{\chi}$, we have by construction $\beta_{i_{0}}+\alpha_{i_{0}} \nu \leq \mu+\chi \nu$. Thus we can write $h=q_{1} \cdot \pi^{\beta_{i}} \cdot u^{\alpha_{i_{0}}}+r$ where $q_{1} \in S_{\nu}, \operatorname{deg}_{W}(r)<\alpha_{i_{0}}$ and $v_{\nu}(r) \geq-\delta / \alpha$. We can then apply the induction hypothesis on $r$ to conclude.

From the above lemma, one can easily deduce an algorithm to compute the generators of $\mathscr{N}=\left\{x \in S_{\nu} \mid v_{\nu}(x) \geq-\delta / \alpha\right\}$ as well as an upper bound on the number of generators. In order to find the $\alpha_{i}$ we just run over all the values between 1 and $-\delta / \beta \bmod \alpha$ and check for each of them if it satisfies the conditions of Lemma 3.22. Nevertheless this algorithm is inefficient and the obtained bound is far from tight. In the following, we explain how to obtain a tight bound as well as an efficient algorithm to compute a family of generators of $\mathscr{N}$ by using the theory of continued fractions. In order to set up the notations, we briefly recall the results from this theory that we need (see [9]). For $a_{0}, \ldots, a_{n}$ integers, the notation $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ refers to the value of the continued fraction

$$
a_{0}+\frac{1}{a_{1}+\frac{1}{\ddots+\frac{1}{a_{n}}}} .
$$

We take the convention that $a_{n} \neq 1$ in $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ so that every rational number can be written uniquely as a finite continued fraction. Let $r=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. We let $p_{0}=a_{0}, q_{0}=1$, $p_{1}=a_{0} a_{1}+1, q_{1}=a_{1}$ and define inductively $p_{k}=a_{k} p_{k-1}+p_{k-2}, q_{k}=a_{k} q_{k-1}+q_{k-2}$. The fractions $p_{k} / q_{k}$ are called the $k^{t h}$ convergent of the continued fraction $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. We have the properties:

- the integers $p_{k}$ and $q_{k}$ are relatively prime (see [9, Th. 2]);
- $p_{k} / q_{k}=\left[a_{0} ; a_{1}, \ldots, a_{k}\right]$.

Definition 3.23. Let $r$ be a real number, and let $\gamma$ be a positive integer. We say that a fraction $\frac{a}{b}(b \geq \gamma)$ is $a$ best approximation (resp. a positive best approximation) of $r$ relatively to $\gamma$ if for all integers $c, d$ such that $\gamma \leq d \leq b$ and $c / d \neq a / b$ (resp. such that $\gamma \leq d \leq b, d r-c>0$ and $c / d \neq a / b$ ), we have $|d r-c|>|b r-a|$ (resp. $d r-c>b r-a>0$ ). We say simply that $\frac{a}{b}$ is $a$ best approximation (resp. a positive best approximation) of $r$ if $\frac{a}{b}$ is a best approximation (resp. a positive best approximation) relatively to 1 .

Remark 3.24. Our definition of best approximation corresponds to what is often called in the literature best approximation of second kind (see [9]).

Everything we need about continued fractions is contained in the following theorem (see $[9, \mathrm{Th}$. 15 and Th. 16]).
Theorem 3.25. Let $x=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$.

1. Every convergent $p_{k} / q_{k}$ is a best approximation of $x$.
2. Reciprocally, every best approximation of $x$ is a convergent, the only exceptions being the cases $x=a_{0}+\kappa$, with $\kappa \in\left[1 / 2,1\left[, \frac{p_{0}}{q_{0}}=\frac{a_{0}}{1}\right.\right.$.
Moreover, for $i=0, \ldots, n-1, x-\frac{p_{i}}{q_{i}}>0$ for $i$ even and $x-\frac{p_{i}}{q_{i}}<0$ for $i$ odd.
Let $r$ be a real number and $b$ an integer. In the following, it is convenient to denote by $\min (r, b)$ (resp. $\left.\min ^{+}(r, b)\right)$ the integer $a$ such that $|b \cdot r-a|=\min \{|b \cdot r-k|, k \in \mathbb{Z}\}$ (resp. such that $b \cdot r-a=\min \{b \cdot r-k, k \in \mathbb{Z}$ with $b \cdot r-k>0\})$. Then, for $r$ a real number and $b$ a positive integer, we let $\{b\}_{r}=b \cdot r-\min (r, b)$ and $\{b\}_{r}^{+}=b \cdot r-\min ^{+}(r, b)$.
Example 3.26. Let $r=0.9$ and $b=2$. Then we have $\min (r, b)=2, \min ^{+}(r, b)=1,\{b\}_{r}=-0.2$ and $\{b\}_{r}^{+}=0.8$.

We need the following lemma:
Lemma 3.27. We have:

- for all $j \in\{0, \ldots, n\},\left\{q_{j}\right\}_{x}>0$ if $j$ is even, $\left\{q_{j}\right\}_{x}<0$ if $j$ is odd;
- for $j \in\{1, \ldots, n-2\}$ for all $\zeta$ integer such that $0 \leq \zeta<a_{j+2}, \zeta \cdot\left\{q_{j+1}\right\}_{x}+\left\{q_{j}\right\}_{x}$ has the same sign has $\left\{q_{j}\right\}_{x}$.
Moreover for all $j \in\{1, \ldots, n-2\}$ and all $\zeta$ integer such that $0 \leq \zeta<a_{j+2}$,

$$
\left\{\zeta \cdot q_{j+1}+q_{j}\right\}_{x}=\zeta \cdot\left\{q_{j+1}\right\}_{x}+\left\{q_{j}\right\}_{x} .
$$

Proof. The fact that $\left\{q_{j}\right\}_{x}>0$ if $j$ is even, $\left\{q_{j}\right\}_{x}<0$ if $j$ is odd is an immediate consequence of Theorem 3.25.

If $\zeta=0$, there is nothing to prove. We suppose for instance that $\left\{q_{j}\right\}_{x}>0$ and $\left\{q_{j+1}\right\}_{x}<0$ (the other case can be treated in a similar manner). Suppose that for $0<\zeta<a_{j+2}$, we have

$$
\begin{equation*}
\left\{q_{j}\right\}_{x}+\zeta \cdot\left\{q_{j+1}\right\}_{x}<0 \tag{17}
\end{equation*}
$$

Let $\zeta$ be the smallest verifying (17), then $\zeta \geq 2$ since we have by definition of a best approximation $\left|\left\{q_{j}\right\}_{x}\right|>\left|\left\{q_{j+1}\right\}_{x}\right|$. Then, as $\left\{q_{j}\right\}_{x}+(\zeta-1) \cdot\left\{q_{j+1}\right\}_{x}>0$, we have $\left|\left\{q_{j}\right\}_{x}+\zeta \cdot\left\{q_{j+1}\right\}_{x}\right|<\left|\left\{q_{j+1}\right\}_{x}\right|$ which is a contradiction with the fact that there is no best approximation of $x$ the denominator of which is between $q_{j+1}$ and $q_{j+2}=a_{n+2} q_{j+1}+q_{j}>\zeta \cdot q_{j+1}+q_{j}$.

With our hypothesis, for all integer $\zeta$ such that $0<\zeta<a_{j+2}$, we have $\left\{q_{j}\right\}_{x}>\left\{q_{j}\right\}_{x}+\zeta \cdot\left\{q_{j+1}\right\}_{x}$. Thus we have we have $\left\{q_{j}\right\}_{x}>\zeta\left(q_{j+1} \cdot x-\min \left(x, q_{j+1}\right)\right)+q_{j} \cdot x-\min \left(x, q_{j}\right)>0$, so that $1 / 2>\left(\zeta q_{j+1}+\right.$ $\left.q_{j}\right) \cdot x-\zeta \min \left(x, q_{j+1}\right)-\min \left(x, q_{j}\right)>0$ (remember that as $\left.j \geq 1,\left\{q_{j}\right\}_{x} \leq 1 / 2\right)$. As a consequence, $\zeta \min \left(x, q_{j+1}\right)+\min \left(x, q_{j}\right)=\min \left(x, \zeta q_{j+1}+q_{j}\right)$ thus $\left\{\zeta \cdot q_{j+1}+q_{j}\right\}_{x}=\zeta \cdot\left\{q_{j+1}\right\}_{x}+\left\{q_{j}\right\}_{x}$.

For $x=\left[a_{0} ; a_{1}, \ldots, a_{n}\right] \in \mathbb{Q}$ and $\gamma$ a positive integer, we would like to be able to obtain the list of positive best approximations of $x$ relatively to $\gamma$. The lemma tells us that not only the convergents $p_{2 i} / q_{2 i}$ for $i \in\{0, \ldots,\lfloor n / 2\rfloor\}$ are positive best approximations of $x$ but also the $\min ^{+}\left(x, q_{2 i}+\mu q_{2 i+1}\right) /\left(q_{2 i}+\mu q_{2 i+1}\right)$ for $i \in\{0, \ldots,\lfloor(n-2) / 2\rfloor\}$ and $\mu$ integer such that $1<\mu<$ $a_{2 i+2}$. The following proposition states that these are all the positive best approximations of $x$ and gives a generalisation for the case of a positive $\gamma$.

Proposition 3.28. Let $x=a / b$ where $a, b$ are relatively prime integers. Write $x=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ and denote by $p_{k} / q_{k}$ the sequence of convergents associated to the continued fraction $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. Let $\gamma<b$ be a positive integer. Let $\gamma \leq d \leq b$ be an integer such that $\frac{\min ^{+}(x, d)}{d}$ is a positive best approximation of $x$ relatively to $\gamma$. Let $i$ be the biggest index such that $d-q_{2 i+1} \geq \gamma$ and let $\lambda$ be the biggest integer such that $d-q_{2 i+1}-\lambda \cdot q_{2 i+2} \geq \gamma$. Then

1) $\frac{\min ^{+}\left(x, d-q_{2 i+1}-\lambda \cdot q_{2 i+2}\right)}{d-q_{2 i+1}-\lambda \cdot q_{2 i+2}}$ is a positive best approximation of $x$ relatively to $\gamma$.
2) If $e$ is such that $d-q_{2 i+1}-\lambda \cdot q_{2 i+2}<e<d$ then $\min ^{+}(x, e) / e$ is not a positive best approximation of $x$ relatively to $\gamma$.

Moreover, we have

$$
\begin{equation*}
\left\{d-q_{2 i+1}-\lambda \cdot q_{2 i+2}\right\}_{x}^{+}-\{d\}_{x}^{+}=\lambda \cdot\left\{q_{2 i+2}\right\}_{x}-\left\{q_{2 i+1}\right\}_{x}>0 . \tag{18}
\end{equation*}
$$

Proof. Let $i$ and $\lambda$ be defined as in the statement. We remark that we have $\lambda<a_{2 i+3}$. Indeed, by hypothesis $d-q_{2 i+1}-\lambda \cdot q_{2 i+2} \geq \gamma$, but we have $q_{2 i+3}=a_{2 i+3} \cdot q_{2 i+2}+q_{2 i+1}$ and we know that $d-q_{2 i+3}<\gamma$. For $0 \leq \zeta<a_{2 i+3}$ an integer, let $\mu(\zeta)=q_{2 i+1}+\zeta . q_{2 i+2}, h=d-\mu(\lambda)$.

First, we prove that

$$
\begin{equation*}
\{d\}_{x}^{+}-\{\mu(\zeta)\}_{x}=\{d-\mu(\zeta)\}_{x}^{+} \tag{19}
\end{equation*}
$$

if $0 \leq \zeta<a_{2 i+3}$. Using Lemma 3.27, we obtain

$$
\begin{equation*}
0 \leq \min (x, \mu(\zeta))-\mu(\zeta) \cdot x<1 \tag{20}
\end{equation*}
$$

As $0 \leq d \cdot x-\min ^{+}(x, d)<1$, we have $0 \leq(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta))<2$. We have to prove that $(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta))<1$. Suppose, on the contrary, that $(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta)) \geq 1$, then because of (20), we have:

$$
\begin{equation*}
0 \leq(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta))-1<d \cdot x-\min ^{+}(x, d) \tag{21}
\end{equation*}
$$

If $\zeta \leq \lambda$ this is a contradiction with the hypothesis that $\frac{\min ^{+}(x, d)}{d}$ is a positive best approximation of $x$ relatively to $\gamma$. If $\zeta>\lambda$ then $(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta))<(d-\mu(\lambda)) \cdot x-$ $\min ^{+}(x, d)+\min (x, \mu(\lambda))$ because $\{\mu(\zeta)\}_{x}^{+}>\{\mu(\lambda)\}_{x}^{+}$by Lemma 3.27. Next, we remark that $(d-\mu(\lambda)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\lambda))<1$ by what we have just proved, so that we have $(d-\mu(\zeta)) \cdot x-\min ^{+}(x, d)+\min (x, \mu(\zeta))<1$. In any case, we are done.

Now, suppose that there exists $\gamma \leq e<d$ such that

$$
\begin{equation*}
\{d\}_{x}^{+}<\{e\}_{x}^{+} \leq\{h\}_{x}^{+} \tag{22}
\end{equation*}
$$

For $0 \leq \zeta<a_{2 i+3}$ a non negative integer, let $e(\zeta)=d-\mu(\zeta)$. Choose $\zeta$ so that $\left|\{e\}_{x}^{+}-\{e(\zeta)\}_{x}^{+}\right|$ is minimal. By (19), we know that $\{e(\zeta)\}_{x}^{+}=\{d\}_{x}^{+}-\{\mu(\zeta)\}_{x}$. As moreover $\{d\}_{x}^{+}-\left\{\mu\left(a_{2 i+3}\right)\right\}_{x} \leq$ $\{d\}_{x}^{+}$(following Lemma 3.27) and $\{e(\lambda)\}_{x}^{+}=\{h\}_{x}^{+}$, we deduce that $\lambda \leq \zeta<a_{2 i+3}$. Suppose that $\{e\}_{x}^{+}-\{e(\zeta)\}_{x}^{+} \neq 0$. As for all $\zeta \in\left\{\lambda, \ldots, a_{2 i+3}-1\right\},\left|\{e(\zeta+1)\}_{x}^{+}-\{e(\zeta)\}_{x}^{+}\right|=\mid\{\mu(\zeta)\}_{x}^{+}-$ $\{\mu(\zeta+1)\}_{x}^{+} \mid=\left\{q_{2 i+2}\right\}_{x}$, we deduce that $\left|\{e-e(\zeta)\}_{x}\right|<\left\{q_{2 i+2}\right\}_{x}$ and the fact that $|e-e(\zeta)|<$ $q_{2 i+3}$ contradicts the second statement of Theorem 3.25.

Thus, we have that $\{e\}_{x}^{+}=\{e(\zeta)\}_{x}^{+}$. Then, from (22), we can write $\{e\}_{x}^{+}=\{d\}_{x}^{+}-\{\mu(\zeta)\}_{x} \leq$ $\{h\}_{x}^{+}=\{d\}_{x}^{+}-\{\mu(\lambda)\}_{x}$ so that $\{\mu(\zeta)\}_{x} \geq\{\mu(\lambda)\}_{x}$. Suppose that $\{\mu(\zeta)\}_{x}>\{\mu(\lambda)\}_{x}$ then, as $\lambda \leq \zeta<a_{2 i+3}$, it means that $\zeta>\lambda$. But then, $e=e(\zeta)=d-\mu(\zeta)<\gamma$ which is a contradiction with the hypothesis $\gamma \leq e$. As a consequence, we have $\lambda=\zeta$ and $e=h$.

To finish the proof, we note that (18) is an immediate consequence of (19) and Lemma 3.27.
Let $x$ be a rational and $\gamma$ a positive integer. From the Proposition 3.28, we immediately obtain an algorithm (see Algorithm 7) to compute the reserve ordered list of the integers $q$ such that $\min ^{+}(x, q) / q$ is a positive best approximation of $x$ relatively to $\gamma$.

From Algorithm 7, it is possible to obtain a bound on the number of positive best approximations of a rational number $x$. In order to state the following corollary, we introduce a notation: for $(\mu, \rho, \chi) \in \mathbb{R}^{2} \times \mathbb{N}$, we denote by $L(\mu, \rho, \chi)$ the finite arithmetic sequence with first term $\mu$, common difference $\rho$ and length $\chi$ (if $\chi$ is zero then the sequence is considered as empty).

```
Algorithm 7: Reverse order list of positive best approximations
    input :
        - \(x=a / b=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]\) a rational number ;
        - the lists of integers \(p[k], q[k]\) for \(k=0, \ldots, n\), such that \(p[k] / q[k]\) are the convergents
        associated to \(\left[a_{0} ; a_{1}, \ldots, a_{n}\right]\);
        - \(\gamma \leq b\) a positive integer.
    output: \(L\) a reverse ordered list of the integers \(q\) such that \(\min ^{+}(x, q) / q\) is a positive best
                approximation of \(x\) relatively to \(\gamma\)
    \(\mathrm{L} \leftarrow[b]\);
    last \(\leftarrow b\);
    \(t \leftarrow n ;\)
    if \((t+1) \bmod 2=0\) then
        nextqk \(\leftarrow t-2\);
    else
        nextqk \(\leftarrow t-1\);
    while nextqk \(\geq 0\) do
        if last \(-q[\) nextqk \(] \geq \gamma\) then
            \(\lambda \leftarrow\) floor \(\left(\frac{\text { last }-q[\text { nextqk }]-\gamma}{q[\text { nextqk }+1]}\right)\);
            last \(\leftarrow\) last \(-\lambda . q[\) nextqk +1\(]\);
        while last \(-q[\) nextqk \(] \geq \gamma\) do
            last \(\leftarrow\) last \(-q[\) nextqk];
            \(\mathrm{L} \leftarrow\) last \(\cup \mathrm{L}\);
        nextqk \(\leftarrow\) nextqk -2 ;
    if \(L[1]>\gamma\) then
        \(L \leftarrow \gamma \cup L ;\)
    return \(L\);
```

Corollary 3.29. Let $x=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ be a rational number, denote by $p_{k} / q_{k}$ for $k=0, \ldots, n$ the associated sequence of convergents. Let $\gamma$ be a positive integer. The list a positive best approximations of $x$ relatively to $\gamma$ has cardinality bounded by $2+\sum_{i=1}^{\lfloor n / 2\rfloor} a_{2 i}$.

Denote by $L$ the finite sequence of increasing integers $q$ such that $\min ^{+}(x, q) / q$ is a positive best approximation relatively to $\gamma$. Let $I=\{0, \ldots,\lfloor(n-1) / 2\rfloor\}$. There exist two sequences $\left(\mu_{i}\right)_{i \in I}$ and $\left(\chi_{i}\right)_{i \in I}$ with coefficients respectively in $\mathbb{Q}$ and $\mathbb{N}$ such that $L=\cup_{i \in I} L\left(\mu_{i}, q_{2 i+1}, \chi_{i}\right)$. Moreover, for $i \in I$, the sequence $\left(\{q\}_{x}^{+}\right)_{q \in L\left(\mu_{i}, q_{2 i+1}, \chi_{i}\right)}$ is also an arithmetic sequence with common difference $\left\{q_{2 i+1}\right\}_{x}<0$.
Proof. To prove the first part of the statement, it suffices to show that the number of elements of the list generated by the loop beginning in line 12 of Algorithm 7 for a given value of nextqk is less than $a_{\text {nextqk+1 }}$. Indeed, it is clear from the initialisation of Algorithm 7 that nextqk is running through the odd indices in $\{0, \ldots, n-1\}$. Now the relation $q[$ nextqk +1$]=a_{\text {nextqk }+1}$. $q[$ nextqk $]+q[$ nextqk -1$]$ implies that the loop on line 12 is executed at most $a_{\text {nextqk }+1}$ times. Taking into account the first and last element in the list $L$, we obtain that its cardinality is bounded by $2+\sum_{i=1}^{\lfloor n / 2\rfloor} a_{2 i}$.

The second part of the statement is clear, since the while loop on line 12 build a (reverse ordered) arithmetic sequence of common difference $q[$ nextqk] and the last point is an immediate consequence of (18).
Remark 3.30. Denote by $L$ the output of Algorithm 7. By the corollary, $L$ is a union of arithmetic sequences each of which can be encoded by a triple of integers giving the first term of the sequence, its common difference and the number of terms of the sequence. Recall that $x=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. Using this encoding, the list $L$ can be represented (as a data structure) by $O(n)$ bits of information. Moreover, it is easy to modify Algorithm 7 so that it returns the list $L$ encoded in that way and have running time $O(n)$. For this, we just have to replace lines 12-14 by:

$$
\begin{aligned}
& \text { length } \leftarrow \text { floor }\left(\frac{\text { last }-\gamma}{\text { q[nextqk }]}\right) ; \\
& \text { first } \leftarrow \text { last }- \text { length } \cdot q[\text { nextqk }] ; \\
& L \leftarrow(\text { first, } q[\text { nextqk }], \text { length }) \cup L ; \\
& \text { last } \leftarrow \text { first }
\end{aligned}
$$

We have everything at hand in order to compute efficiently the generators of $\mathscr{N}=\{x \in$ $\left.S_{\nu} \mid v_{\nu}(x) \geq-\delta / \alpha\right\}$. Indeed, consider the line $\mathcal{L}$ given by the equation $y+x \cdot \frac{\beta}{\alpha}=-\frac{\delta}{\alpha}$. Let $\gamma=\frac{\delta}{\beta}$ $\bmod \alpha$, where $\frac{\delta}{\beta} \bmod \alpha$ is considered as a positive integer in $\{0, \ldots, \alpha-1\}$. Then $-\gamma$ is the abscissa of the first point of the line $\mathcal{L}$ with integer coordinates to the left of the origin point. Denote by $\left(q_{i}\right)_{i \in I}$ the list of integers $q_{i}$ such that $\min ^{+}\left(\beta / \alpha, q_{i}\right) / q_{i}$ is a positive best approximation of $\beta / \alpha$ relatively to $\gamma$. Then if we set $\alpha_{i}=q_{i}-\gamma$, it is easily seen that the $\alpha_{i}$ are precisely the same as the one defined in the Lemma 3.22.

Corollary 3.31. Let $\nu=\beta / \alpha=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. Let $\delta$ be an integer. Set $\mathscr{N}=\left\{x \in S_{\nu} \mid v_{\nu}(x) \geq\right.$ $-\delta / \alpha\}$. Then $\mathscr{N}$ is generated elements of the form $\left(\pi^{\beta_{i}} \cdot u^{\alpha_{i}}\right)_{i \in J}$ where the cardinality of $J$ is bounded by $2+\sum_{i=1}^{\lfloor n / 2\rfloor} a_{2 i}$. Let $I=\{1, \ldots,\lfloor n / 2\rfloor\}$. There exist two sequences $\left(\mu_{i}\right)_{i \in I}$ and $\left(\chi_{i}\right)_{i \in I}$ with coefficients respectively in $\mathbb{Q}$ and $\mathbb{N}$ such that $\left(\alpha_{i}\right)_{i \in J}=\cup_{i \in I} L\left(\mu_{i}, q_{2 i+1}, \chi_{i}\right)$. Moreover, the sequence $v_{\nu}\left(\pi^{\beta_{i}} . u^{\alpha_{i}}\right)_{\alpha_{i} \in L\left(\mu_{i}, q_{2 i+1}, \chi_{i}\right)}$ is also an arithmetic sequence.

By gathering all the results of this section, we obtain:
Theorem 3.32. Let $\nu=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$. Let $\mathscr{M}$ be a sub- $S_{\nu}$-module of $S_{\nu}^{d}$. Then a bound on the number of generators of $\operatorname{Max}(\mathscr{M})$ is $d .\left(2+\sum_{i=1}^{\lceil n / 2\rceil} a_{2 i}\right)$. These generators can be represented by $d$ vectors of $S_{\nu}^{d}$ and $d \cdot\lfloor n / 2\rfloor$ arithmetic sequences of the form $L(\mu, q, \chi)$ where $q$ is the denominator of a convergent of odd index associated to $\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$.

### 3.3.5 Application: scalar extension of $S_{\nu}$-modules

Let $\nu^{\prime}, \nu \in \mathbb{Q}$ such that $\nu^{\prime}>\nu$, there is a natural inclusion $\theta_{\nu, \nu^{\prime}}: S_{\nu} \rightarrow S_{\nu^{\prime}}$. Given a module $\mathscr{M}$ over $S_{\nu}$, We would like to compute the $\operatorname{module} \operatorname{Max}\left(\mathscr{M} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right) \in \operatorname{Max}_{S_{\nu^{\prime}}}^{d}$. If $M=\left(m_{i j}\right) \in M_{d \times k}\left(S_{\nu}\right)$
is a matrix representing $\mathscr{M}$, it can be done by calling the algorithm MatrixReduction on the matrix $\left(\theta_{\nu, \nu^{\prime}}\left(m_{i j}\right)\right)$.

Nevertheless, if $\mathscr{M}$ is maximal, there is another better way to carry out this computation. Assume that $\mathscr{M}$ is represented by a couple $\left(M^{\prime}, L^{\prime}\right)$ with $M^{\prime} \in M_{d \times k}\left(S_{\nu}\right)$ and $L^{\prime}=\left[\alpha_{1}, \ldots, \alpha_{k}\right]$ is a list of integers. Let $\left(f_{1}, \ldots, f_{k}\right)$ with $f_{i}=\varpi^{\alpha_{i}} \cdot e_{i}$ for $i=1, \ldots, k$ and $e_{i} \in S_{\nu}^{d}$ be the basis of $\Phi(\mathscr{M})$ given by the column vectors associated to the couple ( $M^{\prime}, L^{\prime}$ ) (see Remark 3.19). Then by definition $\mathscr{M}$ is generated by the sub- $S_{\nu}$-modules $F_{i}=f_{i} \cdot S_{\nu}^{\prime} \cap S_{\nu}^{d}$. Moreover, using Algorithm 7, one can recover a family of generators of $F_{i}$ which are of the form $s_{j} \cdot e_{i}$ with $s_{j} \in S_{\nu}$ and following Remark 3.30 it is possible to encode the generators of $F_{i}$ by a list of arithmetic sequences. As this representation is very compact, we would like take advantage of it in order to compute the scalar extension. By working component by component, we only have to consider the case of a sub- $S_{\nu^{-}}$ module of $S_{\nu}, \mathscr{N}=\left\{x \in S_{\nu} \mid v_{\nu}(x) \geq-\delta / \alpha\right\}$ for $\delta \in \mathbb{N}$. Then it has been seen in Corollary 3.31 that $\mathscr{N}$ is generated elements of the form $\left(\pi^{\beta_{i}} . u^{\alpha_{i}}\right)_{i \in J}$. More precisely, write $\nu=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$ and let $I=\{1, \ldots,\lfloor n / 2\rfloor\}$. Then, there exists three sequences $\left(\mu_{i}\right)_{i \in I}$, where $\left(\zeta_{i}\right)_{i \in I}$ and $\left(\chi_{i}\right)_{i \in I}$ with coefficients respectively in $\mathbb{Q}, \mathbb{N}$ and $\mathbb{N}$ such that $\left(\alpha_{j}\right)_{j \in J}=\cup_{i \in I} L\left(\mu_{i}, \zeta_{i}, \chi_{i}\right)$. Let $\mathscr{N}^{\prime}=\mathscr{N} \otimes_{S_{\nu}} S_{\nu^{\prime}}$. Of course, the sequence $\left(\pi^{\beta_{j}} \cdot u^{\alpha_{j}}\right)_{j \in J}$ has coefficients in $S_{\nu^{\prime}}$ and is a family of generators of $\mathscr{N}^{\prime}$. Hence, $\operatorname{Max}\left(\mathscr{N}^{\prime}\right)$ corresponds to the couple $\left(M^{\prime}, L^{\prime}\right)$ where the unique element of $L^{\prime}$ is given the minimum of all quantites $\beta_{j}+\nu^{\prime} \cdot \alpha_{j}$ when $j$ runs over $J$. Now, we remark that the sequence $\beta_{j}+\nu^{\prime} \cdot \alpha_{j}$ is arithmeric when $j$ runs over one subset $L\left(\mu_{i}, \zeta_{i}, \chi_{i}\right)$. On this subset, the minimum is reached for the first index or the last one. Thus, to compute $L^{\prime}$, it is enough to take the minimum over these particular indices. It yields an algorithm whose complexity is $O(n)$ - or $O(n d)$ for the $d$-dimensional case - where we recall that $n$ is the length of the continued fraction of $\nu$ (in particular $n=O(1+\min (\log |\alpha|, \log |\beta|))$ if $\nu=\frac{\alpha}{\beta}$.)

### 3.4 Comparing the two approaches

We have introduced two different ways to represent $S_{\nu}$-modules and compute with them. It is important to compare the two approaches since they are well suited for different kind of applications. We call the representation of $\S 3.2 .1$ the $\left(M_{\pi}, M_{u}\right)$-representation and the representation of $\S 3.3$ the ( $M, L$ )-representation.

First, we explain how to go back and forth between the two representations. Let $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ given with the $(M, L)$-presentation by the couple $(M, L)$ with $M \in M_{d \times k}\left(S_{\nu}\right)$ and $L$ is a list of integers. We can recover a matrix $M_{1}$ with coefficients in $S_{\nu}$ whose columns vectors gives generators of $\mathscr{M}$ in the canonical basis of $S_{\nu}^{d}$. Then to obtain the couple $\left(M_{\pi}, M_{u}\right)$ representing $\mathscr{M}$ we just have to compute the Hermite Normal Forms of $M_{1} \otimes_{S_{\nu}} S_{\nu, \pi}$ and $M_{1} \otimes_{S_{\nu}} S_{\nu, u}$.

We explain how to compute the $(M, L)$-representation associated to a $\left(M_{\pi}, M_{u}\right)$-representation in the case that the associated module $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ has full rank. Suppose we are given the couple $\left(M_{\pi}, M_{u}\right)$ representing $\mathscr{M}$ where $M_{\pi}=\left(m_{\pi, i, j}\right) \in M_{d \times k}\left(S_{\nu, \pi}\right)$ and $M_{u}=\left(m_{u, i, j}\right) \in M_{d \times k}\left(S_{\nu, u}\right)$. We can suppose, by multiplying $M_{\pi}$ by a certain power of $\pi$ (which is invertible in $S_{\nu, \pi}$ ), that all the $m_{\pi, i, j} \in S_{\nu}$. As the coefficients of $M_{u}$ are defined modulo a certain power of $\pi$ (namely the determinant of $M_{u}$ ), we can also suppose, by multiplying $M_{u}$ by a certain power of $u^{\alpha} / \pi^{\beta}$ (which is invertible in $S_{\nu, u}$ ), that all the coefficients of $M_{u}$ belongs to $S_{\nu}$. Let $D_{u}=\operatorname{det}\left(M_{u}\right) \in S_{\nu}$. On the other side, let $D_{\pi}=\operatorname{det}\left(M_{\pi}\right) / \varpi^{\alpha \cdot v_{\nu}\left(\operatorname{det}\left(M_{\pi}\right)\right)} \in S_{\nu}^{\prime}$. By definition, we have $v_{\nu}\left(D_{\pi}\right)=0$. Denote by $\mathscr{M}_{0}^{\pi}$ (resp. $\mathscr{M}_{0}^{u}$ ) the sub- $S_{\nu}^{\prime}$-module of $\left(S_{\nu}^{\prime}\right)^{d}$ generated by the column vectors of $D_{u} M_{\pi}$ (resp. $D_{\pi} M_{u}$ ), considered as matrices with coefficients in $S_{\nu}^{\prime}$. We can prove:

Lemma 3.33. Keeping the above notations, we have:

$$
\operatorname{Max}\left(\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)=\operatorname{Max}\left(\mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}\right) .
$$

Proof. Using the formula $\operatorname{adj}(M)=\operatorname{det}(M) \cdot M^{-1}$, it is clear that the column vectors of the matrix $D_{u} M_{\pi}$ (resp. $D_{\pi} M_{u}$ ) belong to the $S_{\nu, u}^{\prime}$-module generated by the column vectors of $M_{u}$ (resp. the $S_{\nu, \pi}^{\prime}$-module generated by the column vectors of $M_{\pi}$ ). As a consequence, we have $\mathscr{M}_{0}^{\pi} \subset$ $\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}$ and $\mathscr{M}_{0}^{u} \subset\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}$. We deduce that $\mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u} \subset\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}$. Thus, we have $\operatorname{Max}\left(\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right) \supset \operatorname{Max}\left(\left(\mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$.

Next, suppose that $x \in \operatorname{Max}\left(\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$. By Proposition 3.8, it means that there exists $n \in \mathbb{N}$ such that $\pi^{n} \cdot x \in\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}$ and $\left(u / \varpi^{\beta}\right)^{n} \cdot x \in\left(\mathscr{M}_{u} \cap \mathscr{M}_{\pi}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}$. Note
that $D_{u}$ is a power of $\pi$, as a consequence there exists $n_{0}>n$ such that

$$
\begin{equation*}
\pi^{n_{0}} \cdot x \in \mathscr{M}_{0}^{\pi} \subset \mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u} \tag{23}
\end{equation*}
$$

We would like to prove that there exists $n_{1} \in \mathbb{N}$ such that $\left(u / \varpi^{\beta}\right)^{n_{1}} x \in \mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}$. For this, it suffices to prove that $\left(u / \varpi^{\beta}\right)^{n_{1}} x \bmod \mathscr{M}_{0}^{\pi} \in \mathscr{M}_{0}^{u} /\left(\mathscr{M}_{0}^{\pi} \cap \mathscr{M}_{0}^{u}\right) \subset S_{\nu}^{\prime} / \mathscr{M}_{0}^{\pi}$. As $D_{\pi}$ is invertible in $S_{\nu, u}^{\prime}\left(\right.$ remember that $\left.v_{\nu}\left(D_{\pi}\right)=0\right)$ there exists $t \in S_{\nu}^{\prime}$ and $n_{2} \in \mathbb{N}$ such that $t . D_{\pi}=\left(u / \varpi^{\beta}\right)^{n_{2}}$ $\bmod \pi^{n_{0}} S_{\nu}^{\prime}$. Denote by $f_{1}, \ldots, f_{k}$ the vectors whose coordinates in the canonical basis of $\left(S_{\nu}^{\prime}\right)^{d}$ are given by the column vectors of $\mathscr{M}_{0}^{u}$. Now, as $\left(u / \varpi^{\beta}\right)^{n} \cdot x \in \mathscr{M}_{u}$ there exist $\lambda_{i} \in S_{\nu, u}^{\prime}$, for $i=1, \ldots, k$, such that

$$
\left(u / \varpi^{\beta}\right)^{n} \cdot x=\sum_{i=1}^{k} \lambda_{i} f_{i} .
$$

But we have $\left(u / \varpi^{\beta}\right)^{n} \cdot x \in \mathscr{M}_{\pi}$ so that $\left(u / \varpi^{\beta}\right)^{n} \cdot x \in\left(S_{\nu}^{\prime}\right)^{d}$ and using the triangular form of the matrix $M_{u}$ (see Proposition 3.15) we have that $\lambda_{i} \in S_{\nu}^{\prime}$ for $i=1, \ldots, k$. By multiplying the preceding equation by $t . D_{\pi}$, we obtain:

$$
\left(u / \varpi^{\beta}\right)^{n+n_{2}} \cdot x+\lambda\left(u / \varpi^{\beta}\right)^{n} \pi^{n_{0}} \cdot x=\sum_{i=1}^{k}\left(t \cdot \lambda_{i}\right)\left(D_{\pi} f_{i}\right)
$$

for $\lambda \in S_{\nu}^{\prime}$. Recall that we have seen that $\pi^{n_{0}} \cdot x \in \mathscr{M}_{0}^{\pi}$, thus $\left(u / \varpi^{\beta}\right)^{n+n_{2}} \cdot x \bmod \mathscr{M}_{0}^{\pi} \in$ $\mathscr{M}_{0}^{u} /\left(\mathscr{M}_{0}^{\pi} \cap \mathscr{M}_{0}^{\pi}\right)$. As a consequence by taking $n_{1}=n+n_{2}$, we have:

$$
\begin{equation*}
\left(u / \varpi^{\beta}\right)^{n_{1}} \cdot x \in \mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u} \tag{24}
\end{equation*}
$$

By (23) and (24), there exists a $m \in \mathbb{N}$ such that $\pi^{m} \cdot x \in \mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}$ and $\left(u / \varpi^{\beta}\right)^{m} \cdot x \in \mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}$. By applying Proposition 3.8, we deduce that $x \in \operatorname{Max}\left(\left(\mathscr{M}_{0}^{\pi}+\mathscr{M}_{0}^{u}\right) \otimes_{S_{\nu}} S_{\nu}^{\prime}\right)$ and we are done.
Remark 3.34. In the preceding construction, we need the extension $S_{\nu}^{\prime}$ of $S_{\nu}$ just to ensure that $v_{\nu}\left(D_{\pi}\right)=0$. Thus, if $v_{\nu}\left(\operatorname{det}\left(M_{\pi}\right)\right) \in \mathbb{Z}$, this extension is not necessary.

Now, let $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ be represented by a couple $\left(M_{\pi}, M_{u}\right)$. As $M_{\pi}$ and $M_{u}$ are given in Hermite Normal Form, we can easily compute $D_{\pi}$ and $D_{u}$. Let $M_{\pi}^{\prime}=D_{u} M_{\pi}$ and $M_{u}^{\prime}=D_{\pi} M_{u}$. Lemma 3.33 tells us that we can then obtain the $(M, L)$-representation of $\mathscr{M}$ by calling the MatrixReduction algorithm on the matrix $\left(M_{\pi}^{\prime} M_{u}^{\prime}\right)$.

The main advantage of the $\left(M_{\pi}, M_{u}\right)$-representation is that is provides unique representation of maximal modules over $S_{\nu}$, because of the same property for Hermite Normal Forms. Thus, it allows to test equality between modules. We have seen also that the echelon form is well suited to test whether $x \in S_{\nu}^{d}$ is an element of $\mathscr{M} \in \operatorname{Max}_{S_{\nu}}^{d}$ as well as to computation the intersection of two modules. On the other side the $(M, L)$-representation provides an actual basis of module in Max ${ }_{S_{\nu}}^{d}$. Moreover, the base change operation $\otimes_{S_{\nu}} S_{\nu^{\prime}}$ only makes sense in the ( $M, L$ )-representation and we will see in $\S 4$, an important application of this operation. Indeed, if $\nu^{\prime} \geq \nu$, altough there is a natural inclusion morphism $S_{\nu} \subset S_{\nu^{\prime}}$, the two sub-rings of $\mathscr{E}, S_{\nu, u}$ and $S_{\nu^{\prime}, u}$ are not comparable by the inclusion relation.

## 4 Representation and precision

In the previous sections, we have presented algorithms to compute with $S_{\nu}$-modules by using, as a black-box, the ring operations of $S_{\nu}$. As elements of $S_{\nu}$ can not be coded with a finite data structure, these procedures are not algorithms stricto sensus since they can not be implemented on a Turing machine for instance. In order to turn them into algorithms, we have to explain how to represent mathematical objects by finite data structures. Much in the same way as we compute with approximations of real numbers, we can represent power series with coefficients $\mathfrak{R}$ by truncating them up to a certain precision. Then we have to ensure the stability of the computations, i.e. that the result is independent of the part of the input that we ignore. In the following, we proceed in an incremental manner. First, we explain how to represent the elements of the coefficient ring $\mathfrak{R}$ of $S_{\nu}$ by a finite structure, then we deal with elements of $S_{\nu}$ and finally with more complex structures with coefficients in $S_{\nu}$ such as $S_{\nu}$-modules.

### 4.1 Generality with precision

We recall from the introduction that $\mathfrak{R}$ is a complete discrete valuation ring, and that for algorithmic applications we are mostly interested by:

- $\mathbb{Z}_{p}$ or more generally the ring a integer of a finite extension of $\mathbb{Q}_{p}$,
- the ring $k[[X]]$ of formal power series with coefficients in a (finite) field $k$.

In any case, if $\pi$ denote the uniformizer element of $\Re$ and $p_{\pi}$ is a positive integer, we shall represent an element of $\mathfrak{R}$ by its image in the quotient $\mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}$. We suppose that there exists algorithms to compute the arithmetic operations of the ring $\mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}$. We say that an element $\bar{x} \in \mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}$ is the data of element of $x \in \mathfrak{R}$ up to $\pi$-adic precision $p_{\pi}$ if $x \bmod \pi^{p_{\pi}}=\bar{x}$.

For the complexity analysis, we shall assume that we have efficient algorithms to perform all standard operations in quotients $\mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}$ for all integers $p_{\pi}$. We discuss briefly the validity of this assumption for the aforementioned classical examples of rings $\mathfrak{R}$. In the case that $\mathfrak{R}=k[[X]]$, we suppose that the operations in the field $k$ costs one unit of time and can be represented by one unit of memory. With that in mind, if $\Re=k[[X]]$ there exists a trivial algorithm to perform additions. It is optimal in the sense that its complexity is equal to the size of the inputs. The same thing is true if $\mathfrak{R}$ is the ring of integers of any finite extension of $\mathbb{Q}_{p}$. Things are more complicated for the multiplication of two elements of $\mathfrak{R} / \pi^{p_{\pi}} \Re$, whose time will be denoted by $T_{0}\left(p_{\pi}\right)$ in the rest of this paper. In the case $\mathfrak{R}=\mathbb{Z}_{p}$, using Strassen algorithm [11], we have $T\left(p_{\pi}\right)=\tilde{O}\left(p_{\pi}\right)$ where the soft-O notation means that we neglect logarithmic factors. If $\mathfrak{R}$ is the ring of integer of a degree $d$ finite extension of $\mathbb{Q}_{p}$, we can represent elements of $\mathfrak{R}$ with a degree $d-1$ polynomial with coefficients in $\mathbb{Z}_{p}$ and using again Strassen algorithm for polynomials, we have $T_{0}\left(p_{\pi}\right)=\tilde{O}\left(d \cdot p_{\pi}\right)$. If $\mathfrak{R}=k[[X]]$ using again Strassen algorithm for polynomials, we have $T\left(p_{\pi}\right)=\tilde{O}\left(p_{\pi}\right)$ (we suppose here that operation in $k$ costs one unit of time). We can summarize these results by saying that with the best known algorithms, the time $T_{0}\left(p_{\pi}\right)$ is quasi-linear $\log \left(\left|\mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}\right|\right)$.

An obvious way to obtain a finite approximation of an element of $\sum a_{i} u^{i} \in S_{\nu}$ is to consider a representative modulo a certain power $p_{u}$ of $u$. We, thus obtain a degree $p_{u}-1$ polynomial with coefficients in $\mathfrak{R}$ that we can represent by a vector of dimension $p_{u}$ with coefficients in $\mathfrak{R}$ up to precision $p_{\pi}$ as before. We call this representation the flat approximation of an element of $S_{\nu}$ with $u$-adic precision $p_{u}$ and $\pi$-adic precision $p_{\pi}$ or the ( $p_{u}, p_{\pi}$ )-flat approximation. The data of a representative with $\pi$-adic precision $p_{\pi}$ and $u$-adic precision $p_{u}$ of an element $x=\sum a_{i} u^{i} / \pi^{\lceil i \nu\rceil} \in S_{\nu}$ is given by a polynomial $\sum_{i=0}^{p_{u}} \bar{a}_{i} u^{i} / \pi^{\lceil i \nu\rceil}$ such that $\bar{a}_{i}=a_{i} \bmod \pi^{p_{\pi}}$. It should be remarked however that the flat approximation is not the only possible procedure to truncate an element of $S_{\nu}$ in order to obtain a finite structure. For instance, one can represent an element of $S_{\nu}$ up to a certain $u$-adic precision $p_{u}$ by a polynomial $\sum_{i=0}^{p_{u}-1} a_{i} u^{i}$ with coefficients in $\mathfrak{R}$ of degree $p_{u}-1$. Such a polynomial may itself be represented by the data of $a_{i} \bmod \pi^{p_{\pi}}$ for $i=0, \ldots, p_{u}-1$, as before but it is also possible to represent $\sum_{i=0}^{p_{u}-1} a_{i} u^{i}$ by coefficients with different $\pi$-adic precisions $a_{i} \bmod \pi^{p_{\pi, i}}$. Put in another way, we want to obtain a representative of $\sum_{i=0}^{p_{u}-1} a_{i} u^{i}$ modulo the $\mathfrak{R}$-module $\sum_{i=0}^{p_{u}-1} \pi^{p_{\pi_{i}}} u^{i} / \pi^{\lceil i \nu\rceil} . \mathfrak{R}$. We call this representation the jagged approximation. We can generalize even further the flat and jagged approximations. For instance, we remark that for $f=\sum a_{i} u^{i} \in S_{\nu}$ the flat and jagged approximations consist in the data of $f^{(i)}(0) / i$ ! for $i=0, \ldots, p_{u}-1$ but we could also provide the data of $f^{(i)}(x) / i$ ! for any $x \in K$ in the radius of convergence of $f$.

Taking into account the previous examples, we say that a data of precision is given by any sub- $\mathfrak{R}$-module $\mathscr{P}$ of $S_{\nu}$. Most of the time, but not always, we want $S_{\nu} / \mathscr{P}$ to be $\mathfrak{R}$-module of finite length. Indeed, it may happen that we compute with objects of $S_{\nu}$ that can be represented exactly with a finite structure. This is the case for instance, if the characteristic of $\mathfrak{R}$ is 0 , of any element $\mathbb{Z} \subset \mathfrak{R}$. In this special case, it makes sense to consider a data of precision $\mathscr{P}$ such that $S_{\nu} / \mathscr{P}$ is not of finite length in order to take into account the fact that we know certain elements of $S_{\nu}$ with "infinite precision". In general, in order to represent an element of $S_{\nu}^{d}$ by a finite data structure, one can consider a sub- $\mathfrak{R}$-module $\mathscr{P}$ of $S_{\nu}^{d}$ such that most of the time $S_{\nu}^{d} / \mathscr{P}$ has finite length.

Then, in order to compute a function $f: S_{\nu}^{d} \rightarrow S_{\nu}^{d}$, we would like to replace it by its approximation $f: S_{\nu}^{d} / \mathscr{P} \rightarrow S_{\nu}^{d} / f(\mathscr{P})$. This naive approach does not work in general since, as $f$ is not always $\mathfrak{R}$-linear, the image by $f$ of a data of precision is not a data of precision. Though, it is
possible to approximate $f(\mathscr{P})$ by the smallest possible data of precision. One way to do this is to consider a regular data precision which is a data of precision that is a $S_{\nu}$-module. Then for $x \in S_{\nu}^{d}$ and $h \in \mathscr{P}$, one can write the first order Taylor development of $f$ in $x$

$$
f(x+h)=f(x)+d f_{x}(h)+O\left(h^{2}\right) .
$$

Most of the time (but not always), $d f_{x}(\mathscr{P})$ will be the correct data of precision (see [1] for a full discussion about this). Note that any flat approximation is a regular data of precision but this is not always the case that a jagged approximation is a regular data of precision. The computation of the function $f$ reduces to the computation of the function on the representative up to the given precision and the computation of the precision of the result. A more general precision data is intuitively less convenient for computations since it involves more complex data structures. For instance, each coefficient of a polynomial representing an element of $S_{\nu}$ with the jagged approximation may have very unbalanced length so that it may be difficult to adapt asymptotically fast arithmetic for such objects. On the other side, we are going to see shortly that even for a very common operation in $S_{\nu}$ such as the computation of the Euclidean division, one may take advantage of the flexibility of the jagged approximation. Hence, the choice of a representation to compute with elements of $S_{\nu}$ is a non trivial trade off between space/time complexity on the one hand and the quantity of precision we accept to loss on the other hand.

It is convenient to represent a jagged precision by a series. For this, let $P_{\pi}=\sum_{i=0}^{\infty} a_{i} u^{i} / \pi^{\lfloor i \nu\rfloor} \in$ $S_{\nu}$. In the following, we denote by $\mathscr{P}\left(P_{\pi}\right)$ the sub- $\mathfrak{R}$-module of $S_{\nu}$ given by $\sum_{i=0}^{\infty} a_{i} u^{i} / \pi^{\lfloor i \nu\rfloor}$. $\mathfrak{R}$. Moreover, if $\mathscr{P}$ is sub- $\mathfrak{R}$-module of $S_{\nu}$, we denote by $\operatorname{repr}(\mathscr{P}): S_{\nu} \rightarrow S_{\nu} / \mathscr{P}$ the canonical projection of $\mathfrak{R}$-modules. It is clear that $\mathscr{P}\left(P_{\pi}\right)$ only depends on the valuation of the coefficients $a_{i}$ of $P_{\pi}=\sum_{i=0}^{\infty} a_{i} u^{i} / \pi^{\lfloor i \nu\rfloor} \in S_{\nu}$. If $p_{\pi}$ is an integer, we will use the notations $\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)$ for

$$
\mathscr{P}\left(\sum_{i=0}^{p_{u}-1} \pi^{p_{\pi}} u^{i} / \pi^{\lfloor i \nu\rfloor}+\sum_{p_{u}}^{\infty} u^{i} / \pi^{\lfloor i \nu\rfloor}\right)
$$

which corresponds to the $\left(p_{u}, p_{\pi}\right)$-flat approximation. If $\mathscr{P}^{\prime}$ and $\mathscr{P}$ are two sub- $\mathfrak{R}$-modules of $S_{\nu}$ such that $\mathscr{P}^{\prime} \subset \mathscr{P}$ then there is a canonical projection $S_{\nu} / \mathscr{P}^{\prime} \rightarrow S_{\nu} / \mathscr{P}$ that we denote also (by abuse of notation) by repr $(\mathscr{P})$. If $\lambda \in S_{\nu}$, and $\mathscr{P}$ is a sub- $\mathfrak{\Re}$-module of $S_{\nu}$, we denote by $\lambda . \mathscr{P}=\{\lambda . x, x \in \mathscr{P}\}$ the sub- $\mathfrak{R}$-module of $S_{\nu}$. If $\lambda$ is distinguished and $S_{\nu} / \mathscr{P}$ has finite length then $S_{\nu} /(\lambda \cdot \mathscr{P})$ has finite length. If $\mathscr{P}, \mathscr{P}^{\prime}$ are sub- $\mathfrak{R}$-modules of $S_{\nu}$, we denote by $\mathscr{P} \cdot \mathscr{P}^{\prime}$ the submodule generated by all products $x y$ for $(x, y) \in\left(\mathscr{P} \times \mathscr{P}^{\prime}\right)$. It is clear that if $S_{\nu} / \mathscr{P}$ and $S_{\nu} / \mathscr{P}^{\prime}$ have finite length then $S_{\nu} /\left(\mathscr{P} \cdot \mathscr{P}^{\prime}\right)$ also have finite length.
Lemma 4.1. For all $\mathscr{P}, \mathscr{P}^{\prime}$ sub- $\mathfrak{R}$-modules of $S_{\nu}$ such that $S_{\nu} / \mathscr{P}$ and $S_{\nu} / \mathscr{P}^{\prime}$ have finite length, for all $x, y \in S_{\nu}$ we have:

1. if $\mathscr{P}^{\prime} \supset \mathscr{P}$ then $\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(\operatorname{repr}(\mathscr{P})(x))=\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(x)$;
2. $\operatorname{repr}\left(\mathscr{P}+\mathscr{P}^{\prime}\right)(\operatorname{repr}(\mathscr{P})(x))+\operatorname{repr}\left(\mathscr{P}+\mathscr{P}^{\prime}\right)\left(\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(y)\right)=\operatorname{repr}\left(\mathscr{P}+\mathscr{P}^{\prime}\right)(x+y)$;
3. let $\mathscr{P}_{0}=y \cdot \mathscr{P}+x \cdot \mathscr{P}^{\prime}+\mathscr{P} \cdot \mathscr{P}^{\prime}$, then

$$
\operatorname{repr}\left(\mathscr{P}_{0}\right)(\operatorname{repr}(\mathscr{P})(x)) \cdot \operatorname{repr}\left(\mathscr{P}_{0}\right)\left(\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(y)\right)=\operatorname{repr}\left(\mathscr{P}_{0}\right)(x \cdot y)
$$

4. if $\mathscr{P}^{\prime} \supset \mathscr{P}$, then $\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(\operatorname{repr}(\mathscr{P})(x)) \cdot \operatorname{repr}\left(\mathscr{P}^{\prime}\right)(y)=\operatorname{repr}\left(\mathscr{P}^{\prime}\right)(x \cdot y)$

Proof. The fist claim is trivial. Then we have $(x+\mathscr{P})+\left(y+\mathscr{P}^{\prime}\right)=x+y+\left(\mathscr{P}+\mathscr{P}^{\prime}\right)$ and $(x+\mathscr{P}) \cdot\left(y+\mathscr{P}^{\prime}\right)=x \cdot y+x \cdot \mathscr{P}^{\prime}+y \cdot \mathscr{P}+\mathscr{P} \cdot \mathscr{P}^{\prime}$. The fourth claim, is an immediate consequence of 1 and 3 .

We discuss briefly the complexity of the elementary arithmetic operations in $S_{\nu}$ with the ( $p_{u}, p_{\pi}$ )flat approximation. First, we remark that the size of an element of $S_{\nu}$ with the ( $p_{u}, p_{\pi}$ )-flat approximation is in the order of $p_{\pi} \cdot p_{u}$. As before, the time of an addition in $S_{\nu}$ is linear in the size of a representative of $S_{\nu}$ since it reduces to the addition of two polynomials of degree $p_{u}-1$ with coefficients in $\mathfrak{R} / \pi^{p_{\pi}} \mathfrak{R}$. We denote by $T\left(p_{u}, p_{\pi}\right)$ the time cost of the multiplication of two elements of $S_{\nu}$ with the $\left(p_{u}, p_{\pi}\right)$-flat approximation. Again, by using a tweaked Strassen's algorithm, we have $T\left(p_{u}, p_{\pi}\right)=\tilde{O}\left(p_{u} \cdot T\left(p_{\pi}\right)\right)=\tilde{O}\left(p_{u} \cdot p_{\pi}\right)$. In the following, we study the precision of some important functions using the flat and jagged approximation.

### 4.2 Finite precision computation with elements of $S_{\nu}$

Most of the time, even for very elementary function dealing with elements of $S_{\nu}$, it is not possible to ensure the stability of the result without some extra assumption. We illustrate this fact with some important examples.

First, consider the Gauss valuation function $v_{\nu}: K[[u]] \rightarrow \mathbb{Q}$. A natural way to define $v_{\nu}$ on a representative modulo $\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)$, with $p_{u}, p_{\pi}$ positive integers, is to compute the valuation of the truncated representative in $S_{\nu}$. For instance let $x=\pi+u^{10}$, then $v_{0}\left(\operatorname{repr}\left(\mathscr{P}_{f}(9,2)\right)(x)\right)=$ $v_{0}(\pi)=1$. We denote also this function by $v_{\nu}$. But then we have $v_{0}\left(\operatorname{repr}\left(\mathscr{P}_{f}(9,2)\right)(x)\right)=1$ and $v_{0}\left(\operatorname{repr}\left(\mathscr{P}_{f}(10,2)\right)(x)\right)=0$. From the previous example, one can see that the Gauss valuation of an element $x \in S_{\nu, \pi}$ can not be computed in general from the knowledge of its approximation. Still, it is possible to obtain the Gauss valuation of an element $x \in S_{\nu, \pi}$ from the knowledge of its approximation if we are given some extra-information about $x$. For instance, if $v_{\nu}\left(\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)\right)(x)\right)=0$ and if we know furthermore that $x \in S_{\nu}$ then we are sure that $v_{\nu}(x)=0$. More generally, it may happen than we have a guaranty that $x \in 1 / \pi^{\lambda} . S_{\nu}$ for a $\lambda \in \mathbb{Z}$. Then, if $\nu$ is big enough, it is possible to compute the valuation of $x$ from the knowledge of $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)\right)(x)$.
Lemma 4.2. Let $x=\sum a_{i} u^{i} \in 1 / \pi^{\lambda} \cdot S_{\nu}$ for $\lambda$ a positive integer. Let $p_{u}$ be a positive integer and $\bar{x} \in K[u]$ be the unique representative of $x \bmod u^{p_{u}}$ of degree $<p_{u}$. We suppose that $x \neq 0$ and that $d=\operatorname{deg}_{W}(x)<p_{u}$.

Let $\nu^{\prime} \in \mathbb{Q}$ be such that

$$
\begin{equation*}
\nu^{\prime}-\nu \geq \frac{\lambda+v_{\nu}(x)}{p_{u}-d} \tag{25}
\end{equation*}
$$

then $v_{\nu^{\prime}}(x)=v_{\nu^{\prime}}(\bar{x})$.
Proof. Let $x=\sum a_{i} u^{i} \in 1 / \pi^{\lambda} \cdot S_{\nu}$. By definition, we have $v_{\nu^{\prime}}(\bar{x}) \leq v_{K}\left(a_{d}\right)+\nu^{\prime} \cdot d$ and on the other side we have of course $v_{\nu^{\prime}}(x) \leq v_{\nu^{\prime}}(\bar{x})$. Thus, in order to prove the lemma, we just have to check that for all $i \geq p_{u}$, we have

$$
\begin{equation*}
v_{K}\left(a_{i}\right)+\nu^{\prime} \cdot i \geq v_{K}\left(a_{d}\right)+\nu^{\prime} \cdot d \tag{26}
\end{equation*}
$$

But, using $x \in 1 / \pi^{\lambda} \cdot S_{\nu}$, we get

$$
\begin{equation*}
v_{K}\left(a_{i}\right)+\nu \cdot i \geq-\lambda \tag{27}
\end{equation*}
$$

for all $i \geq p_{u}$. From (26) and (27), we deduce that it is enough to prove that $-\lambda+i\left(\nu^{\prime}-\nu\right) \geq$ $v_{K}\left(a_{d}\right)+\nu^{\prime} . d$. Since $\nu^{\prime}-\nu \geq 0$ by hypothesis, it suffices to prove that $-\lambda+p_{u}\left(\nu^{\prime}-\nu\right) \geq v_{k}\left(a_{d}\right)+\nu^{\prime} . d$ for all $i \geq p_{u}$. This is equivalent to

$$
\begin{equation*}
\nu^{\prime} \geq \frac{v_{K}\left(a_{d}\right)+p_{u} \cdot \nu+\lambda}{p_{u}-d}, \tag{28}
\end{equation*}
$$

which is exactly (25).
This lemma, while totally elementary, shows the following very important fact: by increasing the $\nu$ parameter of the $S_{\nu}$-module, one can obtain guaranties on the valuation of a certain $x=$ $\sum a_{i} u^{i} \in S_{\nu}$ from the knowledge of its representative $x=\sum_{i=1}^{p_{u}-1} a_{i} u^{i}$ with bounded Weierstrass degree under the general hypothesis of a lower bound on the valuation of the coefficients $a_{i}$.

Another important operation for the arithmetic of $S_{\nu}$ is the inversion.
Lemma 4.3. Let $x \in S_{\nu}$ and suppose that $\operatorname{deg}_{W}(x)=0$ and that $v_{\nu}(x)=0$ so that by Corollary 2.7, $x$ is invertible. Let $p_{u}, p_{\pi}$ be positive integers. Then $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)\right)(x) \in S_{\nu} / \mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)$ is also invertible and we have $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)\right)(x)^{-1}=\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{u}, p_{\pi}\right)\right)\left(x^{-1}\right)$.
Proof. Write $x=\sum a_{i} u^{i} / \pi^{\lfloor i \nu\rfloor}, x^{-1}=\sum b_{i} u^{i} / \pi^{\lfloor i \nu\rfloor}$ and $c=1=\sum c_{i} u^{i} / \pi^{\lfloor i \nu\rfloor}$ with $c_{j}=\sum_{i=0}^{j} a_{i}$. $b_{j-i}$. We have $v_{K}\left(a_{0}\right)=0$ so that we can compute $a_{0}^{-1} \bmod p_{\pi}=b_{0} \bmod p_{\pi}$. Then, using the formula

$$
\frac{b_{j}}{\pi^{\lfloor j \nu\rfloor}}=\frac{1}{a_{0}} \cdot \sum_{i=0}^{j-1} \frac{a_{i} b_{j-i}}{\pi^{\lfloor i \nu\rfloor} \pi^{\lfloor(j-i) \nu\rfloor}},
$$

together with the remark that $\pi^{\lfloor j \nu\rfloor} /\left(\pi^{\lfloor i \nu\rfloor} \pi^{\lfloor(j-i) \nu\rfloor}\right)$ is equal to 1 or $\pi$, we obtain by induction for $j=1, \ldots, p_{u}-1, b_{j} \bmod p_{\pi}$.

Let $x, y \in S_{\nu}$. In order to be able to compute an approximation of the Euclidean division of $y$ by $x$, it is necessary to know that $v_{\nu}(y) \geq v_{\nu}(x)$. One way to have that guaranty is to be given $x$ with enough precision to know that it is distinguished. Then one can compute its Weierstrass degree. In the following proposition, we keep the notations of Proposition 2.8.

Proposition 4.4. Let $x, y \in S_{\nu}$. Suppose that $x$ is distinguished and let $d=\operatorname{deg}_{W}(x)$. Let $q \in S_{\nu}$ and $r \in K[u] \cap S_{\nu}$ be such that $\operatorname{deg}(r)<d$ and $y=q \cdot x+r$. Put $e=v_{\nu}(\operatorname{Lo}(x))>0$, let $p_{\pi}$ be a positive integer and $p_{x}=\left\lceil p_{\pi} / e\right\rceil d$. Let

$$
\begin{gathered}
P_{y}=\sum_{i=0}^{p_{x}-1} \pi^{\max \left\{p_{\pi}-\lfloor i / d\rfloor e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\right\}} u^{i}+\sum_{i=p_{x}}^{\infty} \frac{u^{i}}{\lfloor i \nu\rfloor}, \\
P_{q}=\sum_{i=0}^{p_{x}-d-1} \pi^{\max \left\{p_{\pi}-\lfloor i / d+1\rfloor e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\right\}} u^{i}+\sum_{i=p_{x}-d}^{\infty} \frac{u^{i}}{\lfloor i \nu\rfloor} .
\end{gathered}
$$

There exists an algorithm which takes as input $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}, p_{\pi}\right)\right)(x)$ and $\operatorname{repr}\left(\mathscr{P}\left(P_{y}\right)\right)(y)$ and outputs $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}, p_{\pi}\right)\right)(q)$ and $\operatorname{repr}\left(\mathscr{P}_{f}\left(\infty, p_{\pi}\right)\right)(r)$.


Figure 3: The form of the precision of $y$ in the Euclidean division for $d=2$ and $\nu=1 / 6$.

Proof. Recall that, from Proposition 2.8, $q, r$ are the limits of the sequences $\left(q_{j}, r_{j}\right)$ defined by $q_{0}=0$ and $r_{0}=y$ and

$$
\begin{gathered}
q_{j+1}=q_{j}+\frac{\operatorname{Hi}\left(r_{j}, d\right)}{\operatorname{Hi}(x, d)} \\
r_{j+1}=\operatorname{Lo}\left(r_{j}\right)-\frac{\operatorname{Hi}\left(r_{j}, d\right)}{\operatorname{Hi}(x, d)} \cdot \operatorname{Lo}(x)
\end{gathered}
$$

For $j=0, \ldots,\left\lceil p_{\pi} / e\right\rceil$, let

$$
P_{y, j}=\sum_{i=0}^{\left(\left\lceil p_{\pi} / e\right\rceil-j\right) \cdot d-1} \pi^{\max \left\{p_{\pi}-\lfloor i / d\rfloor e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\right\}} u^{i}+\sum_{i=\left(\left\lceil p_{\pi} / e\right\rceil-j\right) \cdot d}^{\infty} \pi^{\max \{j \cdot e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\}} u^{i},
$$

and let $t(j)=\operatorname{repr}\left(\mathscr{P}\left(P_{y, j}\right)\right)\left(r_{j}\right)$. It is clear that $t(0)=\operatorname{repr}\left(\mathscr{P}\left(P_{y}\right)\right)(y)$. We are going to prove that if we know $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}, p_{\pi}\right)\right)(x)$ and $t(j)$ then we can compute $t(j+1)$. Write $\operatorname{Hi}(x, d)=$ $u^{d} / \pi^{\nu d} \cdot x_{0}$, with $x_{0}$ an invertible element of $S_{\nu}$. Then from $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}, p_{\pi}\right)\right)(\operatorname{Hi}(x, d))$, we immediately obtain $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}-d, p_{\pi}\right)\right)\left(\operatorname{Hi}\left(x_{0}, d\right)\right)$, and by Lemma 4.3 , we can compute $\operatorname{repr}\left(\mathscr{P}_{f}\left(p_{x}-\right.\right.$ $\left.\left.d, p_{\pi}\right)\right)\left(1 /\left(\operatorname{Hi}\left(x_{0}, d\right)\right)\right) . \operatorname{As} \mathscr{P}_{f}\left(p_{x}-d, p_{\pi}\right) \subset \mathscr{P}\left(p_{x}-d \cdot j, P_{y, j}\right)$, applying Lemma 4.1, we deduce that

$$
\begin{align*}
\operatorname{repr}\left(\mathscr{P}\left(P_{y, j}\right)\right) & \left(\operatorname{Hi}\left(r_{j}, d\right) / \operatorname{Hi}\left(x_{0}, d\right)\right)= \\
& \operatorname{repr}\left(\mathscr { P } ( P _ { y , j } ) ( \operatorname { r e p r } ( \mathscr { P } _ { f } ( p _ { x } - d , p _ { \pi } ) ) ( 1 / ( \operatorname { H i } ( x _ { 0 } , d ) ) ) ) \cdot \operatorname { r e p r } \left(\mathscr{P}\left(P_{y, j}\right)\left(\operatorname{Hi}\left(r_{j}, d\right)\right) .\right.\right. \tag{29}
\end{align*}
$$

We remark that $\operatorname{repr}\left(\mathscr{P}\left(P_{y, j}\right)\left(\operatorname{Hi}\left(r_{j}, d\right)\right)=\operatorname{Hi}(t(j), d)\right.$ so that the left hand side of (29) can be computed from the known data. Dividing repr $\left(\mathscr{P}\left(P_{y, j}\right)\right)\left(\operatorname{Hi}\left(r_{j}, d\right) / H i\left(x_{0}, d\right)\right)$ by $u^{d} / \pi^{\lfloor d \nu\rfloor}$, we obtain $\operatorname{repr}\left(\mathscr{P}\left(P_{j}\right)\right)\left(\mathrm{Hi}\left(r_{j}, d\right) / \mathrm{Hi}(x, d)\right)$, where

$$
\begin{align*}
P_{j}= & \sum_{i=0}^{\left(\left\lceil p_{\pi} / e\right\rceil-(j+1)\right) \cdot d-1} \pi^{\max \left\{p_{\pi}-\lfloor i / d+1\rfloor e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\right.} u^{i} \\
& +\sum_{i=\left(\left\lceil p_{\pi} / e\right\rceil-(j+1)\right) \cdot d}^{\infty} \pi^{\max \{(j \cdot e-\lfloor i \nu\rfloor,-\lfloor i \nu\rfloor\}} u^{i} . \tag{30}
\end{align*}
$$

Next, as $v_{\nu}(\operatorname{Lo}(x))=e$, still be applying Lemma 4.1, and remarking that $t(j+1)=\pi^{e} \cdot P_{j}$, we obtain

$$
\begin{align*}
& \operatorname{repr}(\mathscr{P}(t(j+1)))\left(\frac{\operatorname{Hi}\left(r_{j}, d\right)}{\mathrm{Hi}(x, d)} \cdot \operatorname{Lo}(x)\right)= \\
& \quad \operatorname{repr}(\mathscr{P}(t(j+1)))\left(\operatorname{repr}\left(\mathscr{P}\left(P_{j}\right)\right)\left(\operatorname{Hi}\left(r_{j}, d\right) / \operatorname{Hi}(x, d)\right)\right) \cdot \operatorname{repr}\left(\mathscr{P}_{f}\left(\infty, p_{\pi}\right)\right)(\operatorname{Lo}(x)) . \tag{31}
\end{align*}
$$

From the above, we deduce by induction that we can compute $\operatorname{repr}\left(\mathscr{P}\left(P_{y,\left\lceil p_{\pi} / e\right\rceil}\right)\right)(r)$. But we have $\mathscr{P}\left(P_{y,\left\lceil p_{\pi} / e\right\rceil}\right)=\mathscr{P}_{f}\left(\infty, p_{\pi}\right)$ so that we can compute repr $\left(\mathscr{P}_{f}\left(\infty, p_{\pi}\right)\right)(r)$ as claimed. Moreover, as we can compute $\operatorname{repr}\left(\mathscr{P}\left(P_{j}\right)\right)\left(\mathrm{Hi}\left(r_{j}, d\right) / \mathrm{Hi}(x, d)\right)$, by Lemma 4.1, we can compute $\operatorname{repr}\left(\sum \mathscr{P}\left(P_{j}\right)\right)(q)=\operatorname{repr}\left(P_{0}\right)(q)$ and we are done.

Remark 4.5. In the preceding proposition, we see that in order to be able to compute $\operatorname{repr}\left(\mathscr{P}_{f}\left(d, p_{\pi}\right)\right)(r)$, we really use all the information contained in $\operatorname{repr}\left(\mathscr{P}\left(p_{y}, P_{y}\right)\right)(y)$. If we use the flat precision, then to obtain $\operatorname{repr}\left(\mathscr{P}\left(d, p_{\pi}\right)\right)$ we need to know $\operatorname{repr}\left(\mathscr{P}\left(\left\lceil p_{\pi} / e\right\rceil . d, p_{\pi}\right)\right)(y)$. This shows that the flat precision is not well adapted to the computation of the Euclidean division in $S_{\nu}$ since a lot of information about the operands is not useful for the computation.

The proposition shows that following the computations of Algorithm 1 on representatives modulo the given precision, we obtain the outputs with the guaranty that the result has the claimed precision.

The last operation in $S_{\nu}$ (actually in $S_{\nu, \pi}$ ) that we would like to consider is the gcd computation. To begin with, we consider some very simple examples, for elements of $S_{\nu}$ which are polynomials. Suppose that $\mathfrak{R}=\mathbb{Z}_{5}, \nu=0$ so that $S_{\nu}=\mathbb{Z}_{5}[[u]]$. Let $\overline{P_{1}}=\operatorname{repr}\left(\mathscr{P}_{f}(\infty, 2)\right)(u-1)$ and $\overline{P_{2}}=$ $\operatorname{repr}\left(\mathscr{P}_{f}(\infty, 2)\right)(u-2)$. Then it is clear that for all $P_{1}, P_{2} \in S_{\nu}$ such that $P_{1}=\overline{P_{1}} \bmod \mathscr{P}_{f}(\infty, 2)$ and $P_{2}=\overline{P_{2}} \bmod \mathscr{P}_{f}(\infty, 2)$ then $\operatorname{gcd}\left(P_{1}, P_{2}\right)=1$. This can be seen by using the Euclidean algorithm to compute the extended gcd of $\overline{P_{1}}$ and $\overline{P_{2}}$ in $S_{\nu} / \mathscr{P}_{f}(\infty, 2)$ which obviously returns 1. In this case, it is safe to claim that $\operatorname{gcd}\left(\overline{P_{1}}, \overline{P_{2}}\right)=1$.

Next, consider $\overline{P_{3}}=\operatorname{repr}\left(\mathscr{P}_{f}(\infty, 2)\right)(u-1)$ and $\overline{P_{4}}=\operatorname{repr}\left(\mathscr{P}_{f}(\infty, 2)\right)(u-1)$. In this case, it is very easy to find different representatives of $\overline{P_{3}}$ and $\overline{P_{4}}$ the gcd of which is not equal. For instance, we can take $P_{3}=P_{4}=u-1$ in this case $\operatorname{gcd}\left(P_{3}, P_{4}\right)=u-1$ but if we take $P_{3}=u-1$ and $P_{4}=u-6$ then $\operatorname{gcd}\left(P_{3}, P_{4}\right)=1$. If we compute the $\operatorname{gcd}$ of $\overline{P_{3}}$ and $\overline{P_{4}}$ using the Euclidean algorithm, we obtain $u-1$ and we do not have enough precision on the next remainder to decide whether it vanishes or not. This example shows that, in the case that the gcd of the representatives is not surely 1 it is not even clear how to define it since the result may change depending on the representatives in $S_{\nu}$ that we use in order to compute it.

### 4.3 Finite precision computation with modules with coefficients in $S_{\nu}$

Let $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ be two maximal sub- $S_{\nu}$-modules of $S_{\nu}^{d}$. In this section, we are interested by the computation of the maximal sum $\mathscr{M}_{1}+_{\max } \mathscr{M}_{2}$ of $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$. We would like to carry out computations with finite precision and have a guaranty on the precision of the results. The preceding example suggests that even in the case $d=1$, we can not hope much in that direction. Indeed, the computation of the maximal sum of two sub- $S_{\nu}$-modules of $S_{\nu, \pi}$ reduces to the computation of the gcd of two elements of $S_{\nu, \pi}$ and we have seen in $\S 4.2$, that unless this sum is $S_{\nu, \pi}$, we can not
guaranty that the result computed with finite precision is an approximation of the result computed on representatives in $S_{\nu, \pi}$.

As before, we need some extra-information, that we can get from the mathematical context of our computation, in order to guaranty the precision of the output. A very natural extra-information that can arise in practise is the following: let $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ be two sub- $S_{\nu}$-modules of $S_{\nu, \pi}^{d}$ and we know that there exists a positive integer $c$ such that $\mathscr{M}_{2} \subset 1 / \pi^{c} \mathscr{M}_{1}$. We recognize a generalisation of the hypothesis of Lemma 4.2 where we have shown in the case that $d=1$ that we can obtain a guaranty on the valuation $v_{\nu}$ of approximations of elements of $K[[u]]$ for well chosen $\nu$. This situation is also crucial in the paper [4]. We are going to see that, although we don't know how to compute an approximation of $\mathscr{M}_{1}+_{\text {max }} \mathscr{M}_{2}$, we can describe an algorithm which outputs an approximation of $\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(\mathscr{M}_{2} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)$ for a well chosen $\nu^{\prime}>\nu$.


Figure 4: The computation of $\nu^{\prime}$ from $p_{u}$ and $\nu$.
In order to compute $\mathscr{M}_{1}+_{\text {max }} \mathscr{M}_{2}$, it is enough to be able to compute $\mathscr{M}_{1}+{ }_{\text {max }} S_{\nu} \cdot t$ where $t \in \mathscr{M}_{2}$. Indeed, let $\left(t_{1}, \ldots, t_{h^{\prime}}\right)$ be a family of generators of $\mathscr{M}_{2}$, we have $\mathscr{M}_{1}+{ }_{\text {max }} \mathscr{M}_{2}=$ $\mathscr{M}_{1}+_{\max } S_{\nu} \cdot t_{1}+_{\max } \ldots+_{\max } S_{\nu} \cdot t_{h^{\prime}}$. Let $t \in \mathscr{M}_{2}$ and let $\left(e_{1}, \ldots, e_{h}\right)$ be a family of generators of $\mathscr{M}_{1}$. By our hypothesis, we know that there exists $\lambda_{i} \in 1 / \pi^{c} \cdot S_{\nu}$ such that $t=\sum \lambda_{i} e_{i}$. We remark that if all the $\lambda_{i}$ are in $S_{\nu}$ then $t \in \mathscr{M}_{1}$ so that $\mathscr{M}_{1}+S_{\nu} \cdot t=\mathscr{M}_{1}$ and there is nothing to do. Write $\lambda_{i}=\sum_{j \geq 0} a_{j}^{i} u^{j}$ with $v_{K}\left(a_{j}^{i}\right)+\nu \cdot j \geq-c$. Let $p_{u}$ a positive integer, we are going to choose $\nu^{\prime}$, as it is explained in figure 4 , such that $\sum_{j \geq p_{u}} a_{j}^{i} u^{i} \in S_{\nu^{\prime}}$. For this it is enough to take $\nu^{\prime} \geq \nu+c / p_{u}$. Let $t^{\prime}=\sum_{i} \lambda_{i}^{\prime} e_{i}$ with $\lambda_{i}^{\prime}=\sum_{j=0}^{p_{u}-1} a_{j}^{i} u^{j}$ and $t^{\prime \prime}=\sum_{i} \lambda_{i}^{\prime \prime} e_{i}$ with $\lambda_{i}^{\prime \prime}=\sum_{p_{u}}^{\infty} a_{j}^{i} u^{j}$. Using the same remark as above, we have:
$\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(t \cdot S_{\nu^{\prime}}\right)=\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(t^{\prime} \cdot S_{\nu^{\prime}}\right)+_{\max }\left(t^{\prime \prime} \cdot S_{\nu^{\prime}}\right)=\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(t^{\prime} \cdot S_{\nu^{\prime}}\right)$,
since $t^{\prime \prime} \cdot S_{\nu^{\prime}} \in \mathscr{M}_{1}$. Now, as $\lambda_{i}^{\prime}$ is a polynomial in $u$, we can obtain its valuation, greatest common divisor and all the operations that we need in order to compute $\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(t \cdot S_{\nu^{\prime}}\right)$.

We recall that we write $\nu=\beta / \alpha$ with $\alpha, \beta$ relatively prime numbers and let $\varpi$ in an algebraic closure of $K$, be such that $\varpi^{\alpha}=\pi$. Let $\mathfrak{R}^{\prime}=\mathfrak{R}[\varpi]$ and $S_{\nu}^{\prime}=S_{\nu} \otimes_{\mathfrak{R}} \mathfrak{R}^{\prime}$. The algorithm AddVector is an adaptation of the algorithm MatrixReduction.

In the preceding algorithm, $\operatorname{Cond}(\lambda, L)$ returns true if there exists $j_{0}, j_{1} \in\{1, \ldots, h\}$ such that $\lambda\left[j_{0}\right] \cdot \lambda\left[j_{1}\right] \neq 0, v_{\nu}\left(\lambda\left[j_{0}\right]\right)-\frac{L\left[j_{0}\right]}{\alpha} \leq v_{\nu}\left(\lambda\left[j_{1}\right]\right)-\frac{L\left[j_{1}\right]}{\alpha}$ and $\operatorname{deg}_{W}\left(\lambda\left[j_{0}\right]\right) \leq \operatorname{deg}_{W}\left(\lambda\left[j_{1}\right]\right)$

We want to give a consequence of this algorithm. We first need a definition.
Definition 4.6. Let $\mathscr{M}$ be a sub- $S_{\nu}$-module of $S_{\nu}^{d}$. Let $\mathscr{P}$ be a sub- $\mathfrak{R}$-module of $S_{\nu}$. We say that a matrix $M^{r}=\left(m_{i j}^{r}\right) \in M_{d \times d^{\prime}}\left(S_{\nu} / \mathscr{P}\right)$ is an $\mathscr{P}$-approximation of $\mathscr{M}$ is there exists a matrix $M=\left(m_{i j}\right) \in M_{d \times d^{\prime}}\left(S_{\nu}\right)$ whose columns are the coordinates of generators of $\mathscr{M}$ in the canonical basis of $S_{\nu}^{d}$ and such that $m_{i j}^{r}=\operatorname{repr}(\mathscr{P})\left(m_{i j}\right)$.

By iterating this algorithm AddVector on a set of $\left(t_{1}, \ldots, t_{h^{\prime}}\right)$ of generators of $\mathscr{M}_{2}$, we obtain the following theorem:

Theorem 4.7. Let $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ be two finitely generated sub- $S_{\nu}$-modules of $S_{\nu}^{d}$ such that $\mathscr{M}_{2} \subset$ $1 / \pi^{c} \mathscr{M}_{1}$ for a positive integer c. Let $M_{1}=\left(m_{i j}^{1}\right)$ and $M_{2}=\left(m_{i j}^{2}\right)$ be the matrices with coefficients in $S_{\nu}$ of generators of $\mathscr{M}_{1}$ and $\mathscr{M}_{2}$ in the canonical basis of $S_{\nu}^{d}$. Let $p_{u}, p_{\pi}$ be positive integers and

```
Algorithm 8: AddVector
    input :
        - \(M \in M_{d \times h}\left(S_{\nu}\right)\), a matrix whose column vectors \(C(i)\) for \(i=1, \ldots, h\) give generators of \(\mathscr{M}_{1}\)
        in the canonical basis of \(S_{\nu}^{d}\);
        - a list \(\lambda[1], \ldots, \lambda[h]\) such that \(\sum \lambda_{i} C_{i}(M)=t, \lambda[i] \in 1 / \pi^{c} \cdot S_{\nu} \cap K[u]\) and \(\operatorname{deg} \lambda[i] \leq p_{u}-1\)
        for \(i=1, \ldots, k\).
    output: \(M \in M_{d \times h}\left(S_{\nu}\right)\) and a list \(L\) a matrix such that the column vectors \(\varpi^{L[i]} \cdot C_{i}(M)\)
            give generators of \(\mathscr{M}_{1}+_{\text {max }} t\) in the canonical basis of \({S_{\nu}^{\prime}}^{d}\)
    \(L \leftarrow[0, \ldots, 0]\);
    while \(\exists j \in\{1, \ldots, h\}\) such that \(v_{\nu}(\lambda[j])-\frac{L[j]}{\alpha}<0\) do
        while \(\operatorname{Cond}(\lambda, L)\) is satisfied do
            Pick up \(j_{0}, j_{1} \in\{1, \ldots, h\}\) such that \(\lambda\left[j_{0}\right] \cdot \lambda\left[j_{1}\right] \neq 0\),
            \(v_{\nu}\left(\lambda\left[j_{0}\right]\right)-\frac{L\left[j_{0}\right]}{\alpha} \leq v_{\nu}\left(\lambda\left[j_{1}\right]\right)-\frac{L\left[j_{1}\right]}{\alpha}\) and \(\operatorname{deg}_{W}\left(\lambda\left[j_{0}\right]\right) \leq \operatorname{deg}_{W}\left(\lambda\left[j_{1}\right]\right)\);
            if \(v_{\nu}\left(\lambda\left[j_{0}\right]\right)>v_{\nu}\left(\lambda\left[j_{1}\right]\right)\) then
                \(\delta_{0} \leftarrow\left\lceil v_{\nu}\left(\lambda\left[j_{0}\right]\right)-v_{\nu}\left(\lambda\left[j_{1}\right]\right)\right\rceil ;\)
                \(\lambda\left[j_{0}\right] \leftarrow \pi^{-\delta_{0}} \lambda\left[j_{0}\right] ;\)
                \(L\left[j_{0}\right] \leftarrow L\left[j_{0}\right]-\alpha \cdot \delta_{0} ;\)
            \((q, r) \leftarrow\) EuclideanDivision \(\left(\lambda\left[j_{0}\right], \lambda\left[j_{1}\right]\right) ;\)
            \(\lambda\left[j_{1}\right] \leftarrow \lambda\left[j_{1}\right]-q \lambda\left[j_{0}\right] ;\)
            \(C_{j_{1}}(M) \leftarrow C_{j_{0}}(M)+q C_{j_{1}}(M) ;\)
            Let \(j_{0}\) such that \(\left.v_{\nu}\left(\lambda\left[j_{0}\right]\right)-\frac{L\left[j_{0}\right]}{\alpha}=\min _{j=1, \ldots, h}(\lambda[j])-\frac{L[j]}{\alpha}\right)\);
            Let \(j_{1}\) such that \(\left.v_{\nu}\left(\lambda\left[j_{1}\right]\right)-\frac{L\left[j_{1}\right]}{\alpha}=\min _{j \neq j_{0}}(\lambda[j])-\frac{L[j]}{\alpha}\right)\);
            \(L\left[j_{0}\right] \leftarrow L\left[j_{0}\right]+\alpha v_{\nu}\left(\lambda\left[j_{0}\right]\right)-L\left[j_{0}\right]-\alpha v_{\nu}\left(\lambda\left[j_{1}\right]\right)+L\left[j_{1}\right] ;\)
    return \(M, L\);
```

suppose that we are given $M_{1}^{r}=\left(\operatorname{repr}\left(\mathscr{P}_{0}\left(p_{u}, p_{\pi}\right)\right)\left(m_{i j}^{1}\right)\right)$ and $M_{2}^{r}=\left(\operatorname{repr}\left(\mathscr{P}_{0}\left(p_{u}, p_{\pi}\right)\right)\left(m_{i j}^{2}\right)\right)$. Let $e$ be the number of columns of $M_{2}$ and let $\nu^{\prime}=\nu+e c / p_{u}$. Then there exists a polynomial time algorithm in the length of the representation of $M_{1}^{r}$ and $M_{2}^{r}$ to compute a matrix $M_{3}^{r}=\left(M_{i j}^{3}\right)$ with coefficients in $S_{\nu^{\prime}} / \mathscr{P}_{0}\left(p_{u}, p_{\pi}\right)$ which is a $\mathscr{P}_{0}\left(p_{u}, p_{\pi}\right)$-approximation of

$$
\left(\mathscr{M}_{1} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)+_{\max }\left(\mathscr{M}_{2} \otimes_{S_{\nu}} S_{\nu^{\prime}}\right)
$$

Remark 4.8. If we suppose in the theorem that $\mathscr{M}_{2}$ is maximal, then by Theorem 3.32 we can take $e=d .\left(2+\sum_{i=1}^{\lceil n / 2\rceil} a_{2 i}\right)$ where $\nu=\left[a_{0} ; a_{1}, \ldots, a_{n}\right]$.

## References

[1] Xavier Caruso. p-adic precision. in preparation.
[2] Xavier Caruso. $F_{p}$-représentations semi-stables. Ann. Inst. Fourier (Grenoble), 61(4):16831747 (2012), 2011
[3] Xavier Caruso. Random matrix over a dvr and lu factorization. preprint, 2012.
[4] Xavier Caruso and David Lubicz. Semi-simplifiée modulo $p$ des représentations semi-stables : une approche algorithmique. in preparation.
[5] Henri Cohen. A course in computational algebraic number theory, volume 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993.
[6] Don Coppersmith and Shmuel Winograd. Matrix multiplication via arithmetic progressions. J. Symbolic Comput., 9(3):251-280, 1990.
[7] James L. Hafner and Kevin S. McCurley. Asymptotically fast triangularization of matrices over rings. SIAM J. Comput., 20(6):1068-1083, 1991.
[8] Kenkichi Iwasawa. On $\Gamma$-extensions of algebraic number fields. Bull. Amer. Math. Soc., 65:183-226, 1959.
[9] A. Ya. Khinchin. Continued fractions. The University of Chicago Press, Chicago, Ill.-London, 1964.
[10] Serge Lang. Cyclotomic fields. Springer-Verlag, New York, 1978. Graduate Texts in Mathematics, Vol. 59.
[11] Joachim von zur Gathen and Jürgen Gerhard. Modern computer algebra. Cambridge University Press, Cambridge, second edition, 2003.

