Linear Algebra over Z_p[[u]] and related rings

Xavier Caruso, David Lubicz

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

Let $\mathfrak{R}$ be a complete discrete valuation ring (see §2.1 for a reminder of the definition) whose valuation is denoted by $v_{\mathfrak{R}}$. Let K denote its fraction field with valuation v_K and π 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 $\mathscr{M}_1 \to \mathscr{M}_2$ is a quasi-isomorphism 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_π and S_u defined respectively as the localization of S with respect to π 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 $\mathrm{Mod}_{S/\mathrm{qis}}^d$ the set of quasi-isomorphism classes of sub-S-modules of S^d, there is an injective morphism $\Psi' : \mathrm{Mod}_{S/\mathrm{qis}}^d \to \mathrm{Free}_{S_\pi}^d \times \mathrm{Free}_{S_u}^d, \overline{\mathscr{M}} \mapsto (\mathscr{M} \otimes_S S_\pi, \mathscr{M} \otimes_S S_u)$, where $\mathscr{M}$ is any representative in the class $\overline{\mathscr{M}}$. The image of Ψ' 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_π 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_π, 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 π-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 π 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 α, β relatively prime integers, we write $\nu = \beta/\alpha$ and set $S_\nu = \{\sum a_i u^i \in K[[u]] | v_K(a_i) + \nu i \geq 0, \forall i \in \mathbb{N}\}$. We have $S_0 = S$. In this paper, we develop a theory of S_ν-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 torsion-free S_ν-modules. Denote by $\mathrm{Max}_{S_\nu}^d$ the set of maximal sub-S_ν-modules of S_ν^d. We prove the following theorem (see Theorem 3.12), which generalize the above mentioned decomposition:

Theorem 1.1. *The natural map*

$$\begin{array}{rcl} \Psi : \mathrm{Max}_{S_\nu}^d & \longrightarrow & \mathrm{Free}_{S_{\nu,\pi}}^d \times \mathrm{Free}_{S_{\nu,u}}^d \\ \mathscr{M} & \mapsto & (\mathscr{M}_\pi, \mathscr{M}_u). \end{array}$$

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 Ψ is given by $A \cap B$.

In the theorem, $\mathscr{E}$ is a field containing S_ν 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_ν-module. In general, it is not true that the maximal module of a torsion-free S_ν-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_ν^d. If ν is rational, it admits a unique finite development as a continued fraction that we denote by $[a_0; a_1, \ldots, a_n]$ (here, we suppose that $a_n \neq 1$). We can prove the following (see Theorem 3.32):

Theorem 1.2. *Let $\nu = [a_0; a_1, \ldots, a_n]$. Let $\mathscr{M}$ be a sub-S_ν-module of S_ν^d. Then* $\mathrm{Max}(\mathscr{M})$ *is generated by at most $d \cdot (2 + \sum_{i=1}^{\lceil n/2 \rceil} a_{2i})$ 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_ν, 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 ν of the base ring S_ν. 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_ν. 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_ν-modules of S_ν^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_ν of generators of $\mathscr{M}_1$ and $\mathscr{M}_2$ in the canonical basis of S_ν^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 $\nu' > \nu$, 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 $(\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) + (\mathscr{M}_2 \otimes_{S_\nu} S_{\nu'})$.*

The organisation of the paper is as follows: in §2, we introduce the rings S_ν, and their basic arithmetic and analytic properties. In §3, we generalize some classical results of Iwasawa to the case of finitely generated S_ν-modules and then give an algorithm with oracle to compute the maximal module associated to a torsion-free S_ν-module and obtain an upper bound on the number of generators of a maximal module. Note that §2 and §3, we only describe algorithms with oracles. In §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_ν

In order to compute with modules over S_ν 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^α/π^β and π 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 §4 where we study the problem of precision of computation in the rings S_ν.

2.1 Notations

We fix the notations for the rest of the paper. Let $\mathfrak{R}$ be a ring equipped with a discrete valuation $v_\mathfrak{R}$, that is a map $v_\mathfrak{R} : \mathfrak{R} \to \mathbb{N}_{\geq 0} \cup \{+\infty\}$ 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 $x, y \in \mathfrak{R}$, $v_\mathfrak{R}(xy) = v_\mathfrak{R}(x) + v_\mathfrak{R}(y)$;
- for all $x, y \in \mathfrak{R}$, $v_\mathfrak{R}(x + y) \geq \min(v_\mathfrak{R}(x), v_\mathfrak{R}(y))$.

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 $\mathfrak{M} = \{x \in \mathfrak{R} | v_{\mathfrak{R}}(x) > 0\}$. Up to renormalizing $v_{\mathfrak{R}}$, it is safe to assume that it is surjective, what we do. We denote by π 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 $\mathfrak{R}$. 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 $v_{\mathfrak{R}}$ can be extended uniquely to a valuation v_K on K.

2.2 Definition and first properties of S_ν

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 $v_K(a_i)$ 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 $v_\nu : K[[u]] \to \mathbb{Q} \cup \{+\infty, -\infty\}$ *by $v_\nu(x) = +\infty$ if $x = 0$, $v_\nu(\sum a_i u^i) = \min\{v_K(a_i) + \nu i, i \in \mathbb{N}\}$ if $x \neq 0$ and this minimum exists and $v_\nu(x) = -\infty$ otherwise. The* Weierstrass degree *of x denoted $\deg_W^\nu(x)$ is given by $\deg_W^\nu(0) = -\infty$, $\deg_W^\nu(x) = \min\{i | v_K(a_i) + \nu i = v_\nu(x)\}$ if $v_\nu(x) \neq -\infty$ and $\deg_W^\nu(x) = +\infty$ otherwise. When no confusion is possible, we will use the notation $\deg_W$ instead of $\deg_W^\nu$.*

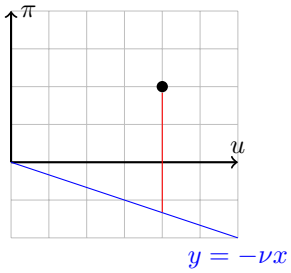


Figure 1: The Gauss valuation of $\pi^2 \cdot u^4$ with $\nu = 1/3$ is $10/3$.

The following lemma gives some basic properties of v_ν and $\deg_W$. In particular, it shows that v_ν 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. *$v_\nu(x + y) \geq \min(v_\nu(x), v_\nu(y))$.*

Moreover for all $x, y \in K[[u]]$ with finite Gauss valuation, $\deg_W(x.y) = \deg_W(x) + \deg_W(y)$.

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 $v_K(c_i) + \nu i = v_K(\sum_{j=0}^{i} a_j \cdot b_{i-j}) + \nu i \geq \min_j\{v_K(a_j) + \nu \cdot j + v_K(b_{i-j}) + \nu \cdot (i-j)\} \geq v_\nu(x) + v_\nu(y)$. Moreover, by taking $i = \deg_W(x) + \deg_W(y)$ in the previous computation, we obtain that $v_K(c_{\deg_W(x)+\deg_W(y)}) = v_\nu(x) + v_\nu(y)$. 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 $S_\nu = \{x \in K[[u]] | v_\nu(x) \geq 0\}$. 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 $v_K(a_i) \geq -\nu i$.

Remark 2.3. *It is clear that S_ν is complete for the valuation v_ν. Nonetheless, the ring S_ν is not a valuation ring. In fact, although $v_\nu(u^\alpha/\pi^\beta) = 0$ for $\nu \neq 0$ (resp. $v_\nu(u) = 0$ for $\nu = 0$), u^α/π^β (resp. u) is not invertible in S_ν.*

We let

$$S_{\nu,\pi} = S_\nu[1/\pi] = \big\{ \sum_{i \in \mathbb{N}} a_i u^i, a_i \in K \text{ such that } v_K(a_i) + \nu i \text{ bounded below} \big\}.$$

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

Put in another way,

$$S_{\nu,u} = \big\{ \sum_{i \in \mathbb{Z}} a_i u^i, a_i \in S_\nu \text{ and } \lim_{i \to -\infty} v_K(a_i) + \nu i = +\infty \big\}.$$

We moreover define

$$\mathscr{E} = \big\{ \sum_{i \in \mathbb{Z}} a_i u^i, a_i \in K \, v_K(a_i) + \nu i \text{ bounded below and } \lim_{i \to -\infty} v_K(a_i) + \nu i = +\infty \big\}.$$

We have the following commutative diagram of inclusions:

$$\begin{array}{ccccc} & & S_{\nu,\pi} & & \\ & \nearrow & & \searrow & \\ S_\nu & & & & \mathscr{E} \\ & \searrow & & \nearrow & \\ & & S_{\nu,u} & & \end{array} \tag{1}$$

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

We can interpret the ring S_ν in terms of the analytic functions on the π-adic disc. In order to explain this, for $\nu \in \mathbb{Q}$, we consider the open disk $D_\nu = \{x \in K | v_K(x) > \nu\}$. Denote by $\mathscr{O}_\nu$ the ring of convergent series $\mathscr{O}_\nu = \{\sum_{i \in \mathbb{N}} a_i u^i | a_i \in K, \liminf_{i \to +\infty} \frac{v_K(a_i)}{i} \geq -\nu\}$ in the disk D_ν. It is clear that $S_{\nu,\pi}$ is exactly the set $\{f \in K[[u]] |\, v_K(f(x)) \text{ bounded below on } D_\nu\}$ and S_ν can be described as $\{f \in K[[u]] |\, v_K(f(x)) \text{ bounded below by 0 on } D_\nu\}$. 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 ν 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 $v_p(a_i)$ 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 $v_p(a_i) + \nu i$ is bounded below and is contained in $\mathbb{Z}+\nu\mathbb{Z}$ which is a discrete subgroup of $\mathbb{R}$ (as ν is rational). Thus, the set $\{v_p(a_i)+\nu i, i \in N\}$ 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_ν. □

We end up this section, by remarking that up to an extension of the base ring $\mathfrak{R}$ all the S_ν's are isomorphic to a S_0. Indeed, write $\nu = \beta/\alpha$ with α, β relatively prime numbers and let ϖ, in an algebraic closure of K, be such that $\varpi^\alpha = \pi$. Let $\mathfrak{R}' = \mathfrak{R}[\varpi]$, K' be the fraction field of $\mathfrak{R}'$ (and a finite extension of K). The valuation on $\mathfrak{R}$ extends uniquely on $\mathfrak{R}'$ by setting $v_{K'}(\varpi) = 1/\alpha$. For $\mu = 0, \nu$, let ${S_\mu}' = S_\mu \otimes_{\mathfrak{R}} \mathfrak{R}'$. The valuation $v_{K'}$ defines a Gauss valuation on ${S_\mu}'$ that we denote also by v_μ.

Lemma 2.5. *Keeping the notations from above, the morphism of ring $\rho : {S_0}' \to S'_\nu$, defined by $\rho(1) = 1$ and $\rho(u) = \frac{u}{\varpi^\beta}$ is an isomorphism. Moreover, if $x \in {S_0}'$ we have $v_0(x) = v_\nu(\rho(x))$ and $\deg_W^0(x) = \deg_W^\nu(\rho(x))$.*

Proof. By definition, $S'_\nu = \{\sum a_i u^i | v_{K'}(a_i) + \nu i \geq 0\} = \{\sum a_i (u/\varpi^\beta)^i | v_{K'}(a_i) \geq 0\}$ from which it is clear that ρ is an isomorphism. The rest of the lemma is an easy verification. □

2.3 Division in S_ν

The Weierstrass degree allows us to describe an Euclidean division in S_ν. 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 ν which provides an algorithm with oracles to compute the Euclidean division.

In order to study divisibility in S_ν, we have a first result:

Lemma 2.6. *Let $x, z \in S_\nu$. We suppose that $\deg_W(x) = 0$ 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 $\deg_W(x) = 0$. 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 $v_K(b_0) = v_K(c_0) - v_K(a_0) \geq 0$ by hypothesis. Then, for $j \geq 1$, we prove by induction that $v_K(b_j) + \nu j \geq 0$. We have $b_j = a_0^{-1} \cdot c_j - a_0^{-1} \sum_{i=1}^{j} a_i \cdot b_{j-i}$. But $v_K(a_0^{-1} \cdot c_j) + \nu j \geq v_\nu(z) - v_\nu(x) \geq 0$ because $\deg_W(x) = 0$. Moreover, for $i = 1 \ldots j$, $v_K(a_0^{-1} \cdot a_i \cdot b_{j-i}) + \nu j = v_K(a_i) + \nu i - v_\nu(x) + v_K(b_{j-i}) + \nu(j-i)$. But by definition $v_K(a_i) + \nu i - v_\nu(x) \geq 0$ and by the induction hypothesis $v_K(b_{j-i}) + \nu(j-i) \geq 0$. Therefore, $v_K(b_j) + \nu j \geq 0$ 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_ν if and only if $\deg_W(x) = 0$ and $v_\nu(x) = 0$.*

We note that the corollary implies that S_ν 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 $\mathrm{Hi}(x,d) = \sum_{i\geq d} a_i u^i$ and $\mathrm{Lo}(x,d) = \sum_{i=0}^{d-1} a_i u^i$. It is clear that $x = \mathrm{Lo}(x,d) + \mathrm{Hi}(x,d)$.

Proposition 2.8. *Let $x, y \in S_\nu$. Suppose that $v_\nu(y) \geq v_\nu(x)$ then there exist a unique couple $(q, r) \in S_\nu \times (K[u] \cap S_\nu)$ such that $\deg(r) < \deg_W(x)$ and $y = q \cdot x + r$.*

Proof. First, we prove the existance of (q, r). Let $d = \deg_W(x)$, we consider the sequences (q_i) and (r_i) defined by $q_0 = 0$ and $r_0 = y$ and

$$q_{i+1} = q_i + \frac{\mathrm{Hi}(r_i, d)}{\mathrm{Hi}(x, d)}, r_{i+1} = r_i - \frac{\mathrm{Hi}(r_i, d)}{\mathrm{Hi}(x, d)} \cdot x. \tag{2}$$

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

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

$$r_{i+1} = \mathrm{Lo}(r_i, d) - \frac{\mathrm{Hi}(r_i, d)}{\mathrm{Hi}(x, d)} \cdot \mathrm{Lo}(x, d). \tag{3}$$

Applying Lemma 2.2, we obtain that $v_\nu(\mathrm{Hi}(r_{i+1},d)) \geq v_\nu(\mathrm{Hi}(r_i,d)) + v_\nu(\mathrm{Lo}(x,d)) - v_\nu(\mathrm{Hi}(x,d))$. Using the induction hypothesis, we get that $v_\nu(\mathrm{Hi}(r_{i+1},d)) \geq e\cdot(i+1) + v_\nu(\mathrm{Hi}(y,d))$. 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_ν for the v_ν valuation. In fact, we have $q_{i+1} - q_i = \frac{\mathrm{Hi}(r_i,d)}{\mathrm{Hi}(x,d)}$ so that $v_\nu(q_{i+1}-q_i) = v_\nu(\mathrm{Hi}(r_i,d)) - v_\nu(\mathrm{Hi}(x,d)) \geq e\cdot i + v_\nu(\mathrm{Hi}(y,d)) - v_\nu(\mathrm{Hi}(x,d)) \geq e\cdot i$. 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 $\mathrm{Hi}(r_i,d)\geq e\cdot i$, we have $\mathrm{Hi}(r,d) = 0$, so that $r\in K[u]$ and $\deg(r) < \deg_W(x)$.

We prove the unicity of (q,r). Let $(q',r')\in S_\nu\times(K[u]\cap S_\nu)$ such that $y = q'\cdot x + r'$. Then $(q-q')\cdot x = r'-r$. We have $\deg_W((q-q')\cdot x) = \deg_W(r'-r) < \deg_W(x)$ which is only possible if $q = q'$ and $r = r'$. □

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

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 $v_\nu(\mathrm{Hi}(r,\deg_W(x)))\geq prec$

```
q ← 0;
r ← y;
d ← deg_W(x);
while v_ν(Hi(r,d)) < prec do
    q ← q + Hi(r,d)/Hi(x,d);
    r ← r − Hi(r,d)/Hi(x,d) · 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 $d = \deg_W(x)$. 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 $v_K(b_i) + \nu i > 0$.*

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 $v_{\mathfrak{R}}(a_d) + d\nu = 0$ (since x is assumed to be distinguished) and, consequently, $d\nu = -v_{\mathfrak{R}}(a_d)\in\mathbb{Z}$.

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

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

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

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_ν.*

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_ν (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 $v_\nu(\pi^t \cdot y) \geq v_\nu(\pi^s \cdot x)$. Applying Proposition 2.8, yields $q \in S_\nu$ and $r \in K[[u]] \cap S_\nu$ such that $\deg(r) < \deg_W(x)$ 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 α, β relatively prime numbers. Let $\mathfrak{m}$ be the ideal defined by $\{x \in S_{\nu,u}, v_\nu(x) > 0\}$, it is clear that $S_{\nu,u}/\mathfrak{m}$ is isomorphic to the field $k((u^\alpha))$. As $S_{\nu,u}$ is complete for the v_ν 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 π 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 $x \cdot y = 1 \mod \mathfrak{m}^n$

```
if n = 1 then
    y ← 1/x̄ mod m;
else
    y ← Inverse(x, ⌈n/2⌉);
    y ← y + y(1 − ay) mod 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 $gcd(x, y) = gcd(y, r)$ where r is the rest of the division of x by y and uses $O(\deg_W(y))$ calls to the Euclidean division Algorithm 1. We remark, as the rest of the division of two elements of S_ν 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_ν

Let d be a positive integer and fix $\nu \in \mathbb{Q}$. We want to compute with finitely generated torsion free S_ν-modules. Any such module $\mathscr{M}$ can be embedded in S_ν^d for $d \in \mathbb{N}$ and can be represented by a matrix with coefficients in S_ν whose column vectors are the coordinates of generators of $\mathscr{M}$ in the canonical basis of S_ν^d. Indeed, we can always embed $\mathscr{M}$ is $\mathscr{M} \otimes_{S_\nu} \mathrm{Frac}(S_\nu)$ and select a basis $(e_1, \ldots, e_d)$ of $\mathscr{M} \otimes_{S_\nu} \mathrm{Frac}(S_\nu)$ together with an element $D \in S_\nu$ such that the image of $\mathscr{M}$ in $\mathscr{M} \otimes_{S_\nu} \mathrm{Frac}(S_\nu)$ is contained in the free S_ν-module generated by the $\frac{1}{D}.e_i$'s.

A first problem arises here: it is not possible to bound the number of generators of the submodules of S_ν^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 $(\pi^{k-j}u^j)_{j=0,\ldots,k}$. Then $\mathscr{M}_k$ can not be generated by less than $k+1$ elements. Indeed, let $(e_0, \ldots, e_n) \in S_0^n$ 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 $M_t \in M_{n\times n}(S_0)$ such that, if we set $(e'_0, \ldots, e'_n) = (e_0, \ldots, e_n) \cdot M_t$ then $(e'_0, \ldots, e'_n)$ is a family of generators of $\mathscr{M}_k$, for $j < t$, $e'_j = u^j\pi^{k-j} \mod F^{j+1}\mathscr{M}_k$ and $(e'_j)_{j\geq t}$ 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 $(e'_0, \ldots, e'_n) = (e_0, \ldots, e_n) \cdot M_{t_0}$. As the morphism $(\sum_{j=t_0}^k S_0 e'_j)/F^{t_0+1}\mathscr{M}_k \to \pi^{k-t}\mathfrak{R}$, 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 (e'_i) that $e'_{t_0} = u^{t_0}\pi^{k-t_0} \mod F^{t_0+1}\mathscr{M}_k$.

Then, by considering linear combinations of the form $e'_j - \lambda e'_{t_0+1}$ 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_ν 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_ν. For instance, for $\nu = 0$, take:

$$M = \begin{pmatrix} u & \pi \\ \pi & u \end{pmatrix} \in M_{2\times 2}(S_0)$$

and assume that M can be written as a product LP where L is lower-triangular and P is invertible. Let α and β be the diagonal entries of L. Then, α and β 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 β 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 $ua + \pi b = 0$ and $\pi a + ub = \beta$. This equality implies that π divides a and therefore that $\beta = \pi a + ub \in uS_0 + \pi^2 S_0$. 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 π or u^α/π^β 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_ν-module and obtain a bound on the number of generators of a maximal S_ν-module. We explain how to combine the different approaches in order to obtain a comprehensive algorithmic toolbox for modules over S_ν.

3.1 Quasi-isomorphism and maximal modules

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

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

Remark 3.2. *Since* $\ker f$ *and* $\operatorname{coker} f$ *are finitely generated (because S_ν 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_ν and a power of π. A quasi-isomorphism between torsion-free modules is always injective. Indeed, its kernel, being a submodule annihilated by a power of u^α/π^β and π of a torsion free module, is zero.*

Example 3.3. *Let $\mathscr{M}$ be the submodule of S_0 generated by $(\pi^2, \pi u^3)$. The inclusion $\mathscr{M} \subset \pi S_0$ yields an injective morphism whose is annihilated by π and u^3. As a consequence $\mathscr{M}$ is quasi-isomorphic 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_ν-module. We say that $\mathscr{M}'$ together with a quasi-isomorphism $f : \mathscr{M} \to \mathscr{M}'$ is* maximal *for $\mathscr{M}$ if for every $\mathscr{N}$, torsion-free S_ν-module, and quasi-isomorphism $f' : \mathscr{M} \to \mathscr{N}$, there exists a morphism $g : \mathscr{N} \to \mathscr{M}'$ which makes the following diagram commutative:*

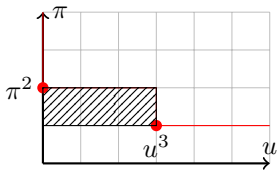
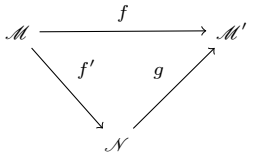


Figure 2: The module $\mathscr{M}$ is quasi-isomorphic to $\pi \cdot S_0$.



(4)

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 $\mathrm{Im} f'$, 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'. 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 $\mathscr{M}'$ and $\mathscr{M}''$ are two maximal modules for $\mathscr{M}$ then there exist two quasi-isomorphisms $g_1 : \mathscr{M}' \to \mathscr{M}''$ and $g_2 : \mathscr{M}'' \to \mathscr{M}'$ and the uniqueness of g in the diagram (4) implies that $g_1 \circ g_2 = \mathrm{Id}_{\mathscr{M}''}$ and $g_2 \circ g_1 = \mathrm{Id}_{\mathscr{M}'}$. If it exists, we denote the maximal module of $\mathscr{M}$ by $\mathrm{Max}(\mathscr{M})$. We can rephrase the above by saying that if $\mathscr{M}'$ is the maximal module for $\mathscr{M}$ then there is a quasi-isomorphism from $\mathscr{M}$ into $\mathscr{M}'$ and any quasi-isomorphism $\mathscr{M}' \to \mathscr{M}''$ is an isomorphism. In fact, this condition characterises maximal modules:

Lemma 3.5. *Let $\mathscr{M}$ be a finitely generated torsion free S_ν-module. Let $\mathscr{M}'$ be a S_ν-module such that there is a quasi-isomorphism $f : \mathscr{M} \to \mathscr{M}'$. The following assertions are equivalent:*

1. *$\mathscr{M}'$ is maximal;*
2. *any quasi-isomorphism $\mathscr{M}' \to \mathscr{M}''$ is an isomorphism.*

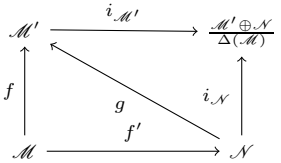
Proof. We only have to prove that the second property implies that $\mathscr{M}'$ verifies the universal property of maximal modules. For this let $\mathscr{N}$ be a finite type S_ν-module such that there is a quasi-isomorphism $f' : \mathscr{M} \to \mathscr{N}$. Let $\Delta = f \oplus f' : \mathscr{M} \to \mathscr{M}' \oplus \mathscr{N}$ be the diagonal embedding and let $\mathscr{M}_0 = \frac{\mathscr{M}' \oplus \mathscr{N}}{\Delta(\mathscr{M})}$. It is clear that $\mathscr{M}_0$ is a finitely generated torsion free S_ν-module.

There are canonical injections $i_{\mathscr{M}'} : \mathscr{M}' \to \mathscr{M}_0$ and $i_{\mathscr{N}} : \mathscr{N} \to \mathscr{M}_0$. We claim that $i_{\mathscr{M}'}$ and $i_{\mathscr{N}}$ are quasi-isomorphisms. To see that, it suffices to show that the induced injection $i_{\mathscr{M}} = (i_{\mathscr{M}'}, i_{\mathscr{N}}) \circ \Delta : \mathscr{M} \to \mathscr{M}_0$ has a finite cokernel. But

$$\mathrm{coker}\, i_{\mathscr{M}} = \frac{\mathrm{coker}\, f \oplus \mathrm{coker}\, f'}{\Delta(\mathscr{M}) \cap (\mathrm{coker}\, f \oplus \mathrm{coker}\, f')}$$

which has finite length being a quotient of $\mathrm{coker}\, f \oplus \mathrm{coker}\, f'$.

Next, by hypothesis $i_{\mathscr{M}'}$ is in fact an isomorphism so that we have a quasi-isomorphism $g = i_{\mathscr{M}'}^{-1} \circ i_{\mathscr{N}}$ which sits in the following diagram:



(5)

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 $\mathrm{Max}(\mathscr{M})$ exists and is free of finite rank over S_0. The main object of §3.3 is to extend this result to modules over S_ν: we shall provide a *constructive* proof of the existence of $\mathrm{Max}(\mathscr{M})$ for any finitely generated torsion-free module $\mathscr{M}$ over S_ν. We will see however that this $\mathrm{Max}(\mathscr{M})$ is not free in general; nevertheless we shall provide an upper bound on the number of generators of $\mathrm{Max}(\mathscr{M})$.

Lemma 3.6. *Let $f : \mathscr{M} \to \mathscr{M}'$ be a quasi-isomorphism between torsion-free finitely generated S_ν-modules. Suppose that $\mathscr{M}'$ is free then $\mathscr{M}'$ is maximal.*

Proof. We use the criterion of Lemma 3.5. Let $\mathscr{N}$ be a finitely generated S_ν-module such that there is a quasi-isomorphism $f' : \mathscr{M}' \to \mathscr{N}$ and we want to show that f' is an isomorphism. As $\mathscr{M}'$ is torsion-free, we know that f' is injective. Now, suppose that there exists a non zero element in the cokernel of f'. It means that there exists a non zero $x \in \mathscr{N}$ which is not in the image of f'. As f' is a quasi-isomorphism there exists $n \in \mathbb{N}$ and $\lambda \in S_\nu$ a distinguished element with $\pi^n \cdot x \in \mathrm{Im} f'$ and $\lambda \cdot x \in \mathrm{Im} f'$. If we set $z_1 = {f'}^{-1}(\pi^n \cdot x)$ and $z_2 = {f'}^{-1}(\lambda \cdot x)$, we have the relation

$$\lambda z_1 - \pi^n z_2 = 0, \tag{6}$$

in $\mathscr{M}'$. Let $(e_i)_{i\in I}$ be a basis of $\mathscr{M}'$ 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 $\pi^n | \mu_1^j$ for $j \in I$ since λ is a distinguished element of S_ν. But then $f'(\sum \mu_1^j/\pi^n e_j) = 1/\pi^n . f(z_1) = x$ contradicting the fact that x is not in the image of f'. □

Remark 3.7. *One can rephrase Iwasawa's result in a more abstract way using the category language. Let $\underline{\mathrm{Mod}}_{S_\nu}$ be the category of finitely generated S_ν-modules, that are torsion-free and let $\underline{\mathrm{Mod}}^{\mathrm{tf}}_{S_\nu}$ (resp. $\underline{\mathrm{Free}}_{S_\nu}$) denote its full subcategory gathering all torsion-free modules (resp. all free modules). We also introduce the category $\underline{\mathrm{Mod}}^{\mathrm{qis}}_{S_\nu}$, which is by definition the category of finitely generated S_ν-modules up to quasi-isomorphism,* i.e. *$\underline{\mathrm{Mod}}^{\mathrm{qis}}_{S_\nu}$ is obtained from $\underline{\mathrm{Mod}}_{S_\nu}$ by inverting formally quasi-isomorphisms. We have a natural functor $\underline{\mathrm{Mod}}_{S_\nu} \to \underline{\mathrm{Mod}}^{\mathrm{qis}}_{S_\nu}$, whose restriction to $\underline{\mathrm{Mod}}^{\mathrm{tf}}_{S_\nu}$ 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 $f : \mathscr{M} \to \mathscr{M}'$ in $\underline{\mathrm{Mod}}^{\mathrm{tf}}_{S_\nu}$, one can attach a morphism $\mathrm{Max}(f) : \mathrm{Max}(\mathscr{M}) \to \mathrm{Max}(\mathscr{M}')$. We recall briefly the construction of $\mathrm{Max}(f)$. Let $\mathscr{M}''$ be the pushout $\mathscr{M}' \oplus_{\mathscr{M}} \mathrm{Max}(\mathscr{M})$, that is the direct sum $\mathscr{M}' \oplus \mathrm{Max}(\mathscr{M})$ divided by $\mathscr{M}$ (embedded diagonally). We have a natural morphism $\mathscr{M}' \to \mathscr{M}''$ which turns out to be a quasi-isomorphism. Hence, there exists a map $\mathscr{M}'' \to \mathrm{Max}(\mathscr{M}')$ and we finally define $\mathrm{Max}(\mathscr{M})$ to be the compositum $\mathrm{Max}(\mathscr{M}) \to \mathscr{M}'' \to \mathrm{Max}(\mathscr{M}')$ where the first map comes from the natural embedding $\mathrm{Max}(\mathscr{M}) \to \mathscr{M}' \oplus \mathrm{Max}(\mathscr{M})$.*

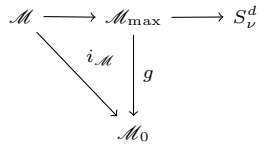
If $\mathscr{M}$ is a submodule of S_ν^d (for some positive integer d), the following proposition gives a very explicit description of $\mathrm{Max}(\mathscr{M})$.

Proposition 3.8. *Write $\nu = \beta/\alpha$, with α, β relatively prime integers. Let d be a positive integer and $\mathscr{M}$ be a submodule of S_ν^d. Then $\mathrm{Max}(\mathscr{M})$ exists and*

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

Furthermore the morphism $i_{\mathscr{M}} : \mathscr{M} \to \mathrm{Max}(\mathscr{M})$ is the natural embedding.

Proof. Let $\mathscr{M}_{\max}$ be the set of $x \in S_\nu^d$ such that there exists some n such that $\pi^n x$ and $(u^\alpha/\pi^\beta)^n \cdot x$ belong to $\mathscr{M}$. We want to show that $\mathrm{Max}(\mathscr{M})$ exists and is equal to $\mathscr{M}_{\max}$. 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 π and a power of u^α/π^β which is a distinguished element. Hence it has finite length, and the inclusion $\mathscr{M} \to \mathscr{M}_{\max}$ is a quasi-isomorphism. Next, suppose that we are given a S_ν-module $\mathscr{M}_0$ together with a quasi-isomorphism $g : \mathscr{M}_{\max} \to \mathscr{M}_0$. Then there is a quasi-isomorphism $i_{\mathscr{M}} : \mathscr{M} \to \mathscr{M}_0$ that sits in the following diagram:



(7)

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^α/π^β and a power of π, which implies that g is surjective. Thus, g is an isomorphism and by Lemma 3.5, $\mathrm{Max}(\mathscr{M})$ exists and $\mathrm{Max}(\mathscr{M}) = \mathscr{M}_{\max}$ 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_ν-module $\mathscr{M} + \mathscr{M}'$ is not maximal even if $\mathscr{M}$ and $\mathscr{M}'$ are (take for example $\mathscr{M} = uS_0$ and $\mathscr{M}' = \pi S_0$). 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_ν^d as follows:

$$\mathscr{M} +_{\max} \mathscr{M}' = \mathrm{Max}(\mathscr{M} + \mathscr{M}').$$

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_ν-module $\mathscr{M}$ of S_ν^d that $\mathrm{Max}(\mathscr{M})$ is free (this will become apparent when we give the general shape of a maximal S_ν-module in §3.3). However, by Lemma 2.5, every S_ν becomes isomorphic to S_0 over a finite extension $\mathfrak{R}' = \mathfrak{R}[\varpi]$ (where ϖ depends on ν). Set $S'_\nu = S_\nu \otimes_{\mathfrak{R}} \mathfrak{R}'$. For all submodule $\mathscr{M}$ of S_ν^d, we obtain that $\mathrm{Max}(\mathscr{M} \otimes S'_\nu)$ is a free submodule of $(S'_\nu)^d$. Denote by $\mathrm{Max}^d_{S_\nu}$ the set of maximal sub-S_ν-modules of S_ν^d and by $\mathrm{Free}^d_{S'_\nu}$ the set of free sub-S'_ν-module of $(S'_\nu)^d$.

Proposition 3.9. *The natural map*

$$\begin{array}{rccc} \Phi & : \mathrm{Max}^d_{S_\nu} & \longrightarrow & \mathrm{Free}^d_{S'_\nu} \\ & \mathscr{M} & \mapsto & \mathrm{Max}(\mathscr{M} \otimes_{S_\nu} S'_\nu) \end{array}$$

is injective. A left inverse of Φ is given by $\mathscr{M}' \mapsto \mathscr{M}' \cap S_\nu^d$. Moreover, the image of Φ contains the subset of $\mathrm{Free}^d_{S'_\nu}$ of free modules which admit a basis $(e_i)_{i\in I}$ where $e_i \in (S'_\nu)^d$ and $e_i = \varpi^{\alpha_i} e'_i$ with $e'_i \in (S_\nu)^d$ and $\alpha_i \in \mathbb{N}$.

Remark 3.10. *Actually, we will prove later (see Lemma 3.18) that the image of Φ is exactly the subset of $\mathrm{Free}^d_{S'_\nu}$ verifying the condition of Proposition 3.9.*

Proof. In order to prove that Φ is injective, it is enough to prove that Φ has a left inverse. For this, let $\mathscr{M} \in \mathrm{Max}^d_{S_\nu}$ and let $\mathscr{M}' = \mathrm{Max}(\mathscr{M} \otimes_{S_\nu} S'_\nu) \in \mathrm{Free}^d_{S'_\nu}$. Then it suffices to prove that $\mathscr{M}_2 = \mathscr{M}' \cap S_\nu^d$ is a maximal sub-S_ν-module of S_ν^d. Indeed, as it is clear that $\mathscr{M}_2$ contains $\mathscr{M}$ and that the injection $\mathscr{M} \to \mathscr{M}_2$ is a quasi-isomorphism since the injection $\mathscr{M} \to \mathscr{M}'$ is a quasi-isomorphism, 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 $(u^\alpha/\pi^\beta)^n \cdot x \in \mathscr{M}_2$. As $\mathscr{M}'$ is maximal and $\mathscr{M}_2 \subset \mathscr{M}'$, by Proposition 3.8, it means that $x \in \mathscr{M}'$. 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 $\mathscr{M}' \in \mathrm{Free}^d_{S'_\nu}$ which admits a basis $(e_i)_{i\in I}$ where $e_i \in (S'_\nu)^d$ and $e_i = \varpi^{\alpha_i} e'_i$ with $e'_i \in (S_\nu)^d$ and $\alpha_i \in \mathbb{N}$. We have to find a sub-S_ν-module $\mathscr{M}$ of S_ν^d such that $\mathscr{M} \otimes_{S_\nu} S'_\nu$ is quasi-isomorphic to $\mathscr{M}'$. As $\mathscr{M}' = \bigoplus e_i S'_\nu$, it is enough to treat the case $d = 1$. Let $0 \leq \alpha_1$ be an integer and let $\mathscr{M}'$ be the sub-S'_ν-module of S'_ν generated by ϖ^{α_1}. Let λ be a positive integer such that $\frac{\alpha_1}{\alpha} + \lambda\frac{\beta}{\alpha} = \gamma \in \mathbb{Z}$. Such a λ exists because α and β are relatively prime. Let $\mathscr{M}$ be the sub-S_ν-module of S_ν generated by π 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 μ is a distinguished element of S'_ν. Thus, we have $\varpi^{\alpha_1}.\mu \in \mathscr{M} \otimes_{S_\nu} S'_\nu$ and $\varpi^{\alpha_1} \cdot \varpi^{\alpha-\alpha_1} \in \mathscr{M} \otimes_{S_\nu} S'_\nu$ therefore $\mathscr{M} \otimes_{S_\nu} S'_\nu$ is quasi-isomorphic to $\mathscr{M}'$. □

3.2 An approach based on localisation

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

3.2.1 A useful bijection

We keep our fixed positive integer d. We recall that

$$\mathscr{E} = \Big\{ \sum_{i\in\mathbb{Z}} a_i u^i,\ a_i \in K,\ v_K(a_i) + \nu i \text{ bounded below and } \lim_{i\to-\infty} v_K(a_i) + \nu i = +\infty \Big\}$$

is a field containing $S_{\nu,\pi}$ and $S_{\nu,u}$. If $\mathscr{M}$ is a sub-S_ν-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_ν with basis $(e_1,\dots,e_h)$, then $\mathscr{M}_\pi$ (resp. $\mathscr{M}_u$) is also free over $S_{\nu,\pi}$ (resp. $S_{\nu,u}$) 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 $\mathrm{Max}^d_{S_\nu}$ the set of maximal sub-S_ν-modules of S_ν^d and for $A = S_\nu, S_{\nu,\pi}$ or $S_{\nu,u}$, let Free^d_A denote the set of sub-A-modules of A^d, which are free over A. Recall that $\mathrm{Max}^d_{S_0} = \mathrm{Free}^d_{S_0}$. Thus, the following lemma provides a useful description of maximal S_0-modules.

Lemma 3.11. *Let $S = S_0$. The natural map*

$$\begin{array}{rccc} \Psi' & : \mathrm{Free}^d_S & \longrightarrow & \mathrm{Free}^d_{S_\pi} \times \mathrm{Free}^d_{S_u} \\ & \mathscr{M} & \mapsto & (\mathscr{M}_\pi, \mathscr{M}_u). \end{array}$$

is injective. If a pair (A,B) is in the image of Ψ', its unique preimage under Ψ' is given by $A\cap B$.

Proof. From the descriptions of elements of S, S_π, S_u and $\mathscr{E}$ in terms of series, it follows that $S = S_\pi \cap S_u$. If $\mathscr{M} \in \mathrm{Free}^d_S$, it is isomorphic to S^h for $h \le d$ 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 Ψ' and the given formula for its left-inverse. □

Using Lemma 3.11, we can prove:

Theorem 3.12. *The natural map*

$$\begin{array}{rccc} \Psi & : \mathrm{Max}^d_{S_\nu} & \longrightarrow & \mathrm{Free}^d_{S_{\nu,\pi}} \times \mathrm{Free}^d_{S_{\nu,u}} \\ & \mathscr{M} & \mapsto & (\mathscr{M}_\pi, \mathscr{M}_u). \end{array}$$

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 Ψ is given by $A\cap B$.

Furthermore, we have the following equalities:

$$\begin{array}{rcl} \Psi(\mathscr{M} \cap \mathscr{M}') & = & (\mathscr{M}_\pi \cap \mathscr{M}'_\pi, \mathscr{M}_u \cap \mathscr{M}'_u) \\ \Psi(\mathscr{M} +_{\max} \mathscr{M}') & = & (\mathscr{M}_\pi + \mathscr{M}'_\pi, \mathscr{M}_u + \mathscr{M}'_u) \end{array}$$

for all $\mathscr{M}, \mathscr{M}' \in \mathrm{Max}^d_{S_\nu}$.

Proof. Let ϖ in an algebraic closure of K, be such that $\varpi^\alpha = \pi$. Let $\mathfrak{R}' = \mathfrak{R}[\varpi]$ and $S'_\nu = S_\nu \otimes_{\mathfrak{R}} \mathfrak{R}'$. We know by Lemma 2.5 that S'_ν is isomorphic to $\mathfrak{R}'[[u]]$. Then, the map Ψ sits in the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Max}^d_{S_\nu} & \xrightarrow{\Psi} & \mathrm{Free}^d_{S_{\nu,\pi}} \times \mathrm{Free}^d_{S_{\nu,u}} \\ \Big\downarrow{\scriptstyle \mathrm{Max}(.\otimes_{S_\nu} S'_\nu)} & & \Big\downarrow{\scriptstyle .\otimes_{S_\nu} S'_\nu} \\ \mathrm{Free}_{S'_\nu} & \xrightarrow{\Psi'} & \mathrm{Free}^d_{S'_{\nu,\pi}} \times \mathrm{Free}^d_{S'_{\nu,u}} \end{array} \tag{8}$$

By Proposition 3.9, the map $\mathscr{M} \mapsto \mathrm{Max}(\mathscr{M} \otimes_{S_\nu} S'_\nu)$ is injective and Ψ' is injective by Lemma 3.11, from which we deduce that Ψ is injective by the commutativity of (8).

We want to prove now that if the pair (A,B) belongs to $\mathrm{Free}^d_{S_{\nu,\pi}} \times \mathrm{Free}^d_{S_{\nu,u}}$ and satisfies the condition of the theorem, then $\mathscr{M} = A \cap B$ is maximal over S_ν and $\Psi(\mathscr{M}) = (A,B)$. We claim that there exists a basis $(e_1,\dots,e_h)$ of A (over $S_{\nu,\pi}$) such that $\mathscr{M}$ is included inside the S_ν-module generated by the e_i's. Indeed, let us first consider $(e_1,\dots,e_h)$ a basis of A and denote by $\mathscr{M}'$ the S_ν-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 $x \in \pi^{-n}\mathscr{M}'_u$. Moreover, since B is finitely generated over $S_{\nu,u}$, we can choose a uniform n. Replacing e_i by $\pi^{-n}e'_i$ for all i, we then get $A = \mathscr{M}'_\pi$ and $B \subset \mathscr{M}'_u$. Thus $\mathscr{M} = A \cap B \subset \mathscr{M}'_\pi \cap \mathscr{M}'_u = \mathscr{M}'$.

Since S_ν is a noetherian ring (recall that ν is rational), we find that $\mathscr{M}$ is finitely generated over S_ν. Furthermore, one can compute $\mathrm{Max}(\mathscr{M})$ using Proposition 3.8: if x is an element of S_ν^d for which there exists n such that $\pi^n x$ and $(u^\alpha/\pi^\beta)^n x$ belong to $\mathscr{M}$, then $x \in A$ (since π is invertible in $S_{\nu,\pi}$) and $x \in B$ (since u^α/π^β is invertible in $S_{\nu,u}$). Thus $x \in \mathscr{M}$ and $\mathrm{Max}(\mathscr{M}) = \mathscr{M}$, *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 $\pi^n\mathscr{M}' \subset \mathscr{M} \subset \mathscr{M}'$, from what it follows that $\mathscr{M}_\pi = \mathscr{M}'_\pi = A$. The method to prove that $\mathscr{M}_u = B$ is analogous: we first show that there exists a basis $(e_1, \dots, e_h)$ of B over $S_{\nu,u}$ and some elements $s_1, \dots, s_h \in S_\nu$ 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 $\mathscr{M} \cap \mathscr{M}' = (\mathscr{M}_\pi \cap \mathscr{M}_u) \cap (\mathscr{M}'_\pi \cap \mathscr{M}'_u) = (\mathscr{M}_\pi \cap \mathscr{M}'_\pi) \cap (\mathscr{M}_u \cap \mathscr{M}'_u)$. Hence, we just need to justify that $\mathscr{M}_\pi \cap \mathscr{M}'_\pi$ and $\mathscr{M}_u \cap \mathscr{M}'_u$ 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 $(\mathscr{M} +_{\max} \mathscr{M}')_\pi = \mathscr{M}_\pi + \mathscr{M}'_\pi$ and $(\mathscr{M} +_{\max} \mathscr{M}')_u = \mathscr{M}_u + \mathscr{M}'_u$. It is clear that $(\mathscr{M} + \mathscr{M}')_\pi = \mathscr{M}_\pi + \mathscr{M}'_\pi$ and $(\mathscr{M} + \mathscr{M}')_u = \mathscr{M}_u + \mathscr{M}'_u$. Hence, it is enough to prove that, given a finitely generated S_ν-module $N \in S_\nu^d$, we have $\mathrm{Max}(N)_\pi = N_\pi$ and $\mathrm{Max}(N)_u = N_u$. It is obvious by Proposition 3.8. □

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

$$\begin{array}{ccc} & & \mathscr{M}_u \\ & & \downarrow \\ \mathscr{M}_\pi & \longrightarrow \mathscr{E} \otimes_{S_{\nu,\pi}} \mathscr{M}_\pi & \longrightarrow \mathscr{E} \otimes_{S_{\nu,u}} \mathscr{M}_u \end{array} \tag{9}$$

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* $\underline{\mathrm{Mod}}_{S_\nu} \to \underline{\mathrm{Mod}}_{S_{\nu,\pi}} \otimes_{\underline{\mathrm{Mod}}_{\mathscr{E}}} \underline{\mathrm{Mod}}_{S_{\nu,u}}$, $\mathscr{M} \mapsto (S_{\nu,\pi} \otimes_S \mathscr{M}, S_{\nu,u} \otimes_S \mathscr{M})$ *factors through* $\underline{\mathrm{Mod}}^{\mathrm{qis}}_{S_\nu}$ *and the resulting functor*

$$\underline{\mathrm{Mod}}^{\mathrm{qis}}_{S_\nu} \to \underline{\mathrm{Mod}}_{S_{\nu,\pi}} \otimes_{\underline{\mathrm{Mod}}_{\mathscr{E}}} \underline{\mathrm{Mod}}_{S_{\nu,u}}$$

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 θ a real number such that product of two $d \times d$ matrices with coefficient in S_ν can be done in $O(d^\theta)$ 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 $M = (m_{ij}) \in M_{d\times d'}(S_{\nu,\pi})$, let r be the rank of M. Then, there exists an invertible matrix P such that $M.P = T$ with*

$$T = \begin{pmatrix} t_1 & & 0 & \cdots & 0 \\ \star & \ddots & & & \\ & t_r & & & \\ & \star & & & \\ \star & \cdots \ \star & 0 & \cdots & 0 \end{pmatrix}, \tag{10}$$

where

- *for $i = 1, \ldots, r$, $t_i = u^{d_j} + \sum_{i=0}^{d_j-1} b_j u^j$ with $v_K(b_j) + \nu(j - d_j) > 0$;*
- *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 $O(d\cdot d'\cdot d_{\max} + \max(d^\theta \cdot d', d'^\theta \cdot d)\log(2d'/d))$ ring operations

If the echelon form moreover satisfies:

- *all entries on the $l(i)^{th}$-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 $O(r^2)$ ring operations.

Proposition 3.15. *Let $M \in M_{d\times d'}(S_{\nu,u})$, let r be the rank of M. Then there exists an invertible matrix P such that $M.P = T$ and*

$$T = \begin{pmatrix} \pi^{d_1} & & 0 & \cdots & 0 \\ \star & \ddots & & & \\ & \pi^{d_r} & & & \\ & \star & & & \\ \star & \cdots \ \star & 0 & \cdots & 0 \end{pmatrix}, \tag{11}$$

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 $O(d.d') + \max(d^\theta \cdot d', d'^\theta \cdot d)\log(2d'/d))$ ring operations.

If the echelon form moreover satisfies

- *the entries on the $l(i)^{th}$-row are representatives modulo π^{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 $O(r^2)$ 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 $\gcd(x,y)$ in $O(\deg_W(y))$ 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 $O(d \cdot r \cdot d_{\max})$ ring operations. □

Remark 3.16. *We deduce from this proposition that if $M \in M_{d\times d'}(S_{\nu,\pi})$ 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 $M \in M_{d\times d'}(S_{\nu,u})$ 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 $\pi^{\max\{d_1,\ldots,d_r\}}$.*

Let $S_{\nu,loc}$ 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-$S_{\nu,loc}$-modules of $S^d_{\nu,loc}$. We can represent a finitely generated sub-$S_{\nu,loc}$-module $\mathscr{M}$ of $S^d_{\nu,loc}$ by a $d \times d$ matrix M giving d generators of $\mathscr{M}$ in the canonical basis of $S^d_{\nu,loc}$ since every sub-module of $S^d_{\nu,loc}$ 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 $\mathscr{V} \in S^d_{\nu,loc}$ 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' representing the modules $\mathscr{M}$ and $\mathscr{M}'$, one can compute a matrix representing the module $\mathscr{M} + \mathscr{M}'$ by computing the echelon form of the matrix (MM') and taking the d first columns. One can compute the intersection of $\mathscr{M}$ and $\mathscr{M}'$ in the same way by finding R and R' such that $(MM')\begin{pmatrix} R \\ R' \end{pmatrix} = 0$.

3.2.3 Consequences for algorithmics

In view of the results of §3.2.1 and §3.2.2, we shall represent a maximal S_ν-module $\mathscr{M}$ living in some S^d_ν 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_ν-modules with this representation. Indeed, we just have to perform the same operations on each component, and we have already explained in §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_ν-modules of S^d_ν. 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_ν-modules. Below we detail three of them. First, let $\mathscr{M} \subset S^d_\nu$ be a maximal S_ν-module. By definition, the *saturation* of $\mathscr{M}$ in S^d_ν is the module

$$\mathscr{M}_{\text{sat}} = \left\{ x \in S^d_\nu \quad | \quad \exists n \in \mathbb{N},\ \pi^n x \in \mathscr{M} \right\}.$$

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

$$(\mathscr{M}_{\text{sat}})_u = \left\{ x \in S^d_{\nu,u} \quad | \quad \exists n \in \mathbb{N},\ \pi^n x \in \mathscr{M}_u \right\}.$$

The computation of $(\mathscr{M}_{\text{sat}})_\pi$ is then for free, whereas the computation of $(\mathscr{M}_{\text{sat}})_u$ 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_ν. Then $(\mathscr{M}_{\text{sat}})_u$ is always equal to $S^d_{\nu,u}$. 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 $\mathscr{M} \in \mathrm{Max}^d_{S_\nu}$ and $\mathscr{M}' \in \mathrm{Max}^d_{S_{\nu,\pi}}$. We want to compute $\mathscr{M} \cap \mathscr{M}'$, which is a maximal module over S_ν. As before, we need to determine $(\mathscr{M} \cap \mathscr{M}')_\pi$ and $(\mathscr{M} \cap \mathscr{M}')_u$ and one can check that:

$$\begin{aligned}(\mathscr{M} \cap \mathscr{M}')_\pi &= \mathscr{M}_\pi \cap \mathscr{M}'_\pi \\ (\mathscr{M} \cap \mathscr{M}')_u &= \mathscr{M}_u \cap \mathscr{M}'_u.\end{aligned}$$

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

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 $\mathscr{M} \in \mathrm{Free}^d_{S_\nu}$ and $\mathscr{M}' \in \mathrm{Free}^d_{S_{\nu,u}}$ and we want to compute $\mathscr{M} \cap \mathscr{M}'$. We then have $(\mathscr{M} \cap \mathscr{M}')_\pi = \mathscr{M}_\pi \cap \mathscr{M}'_\pi$ and $(\mathscr{M} \cap \mathscr{M}')_u = \mathscr{M}_u \cap \mathscr{M}'$. Here a new difficulty occurs: $\mathscr{M}'_\pi$ 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 $\mathscr{M}'$ has full rank, then $\mathscr{M}'_\pi = \mathscr{E}^d$. So, in this case, $(\mathscr{M} \cap \mathscr{M}')_\pi$ is just equal to $\mathscr{M}_\pi$ and the computation of $(\mathscr{M} \cap \mathscr{M}')_\pi$ 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 $S_{\nu,\pi} \to \bar{K}[[u-a]]$ which maps a series to its Taylor expansion at a. Hence, if $\mathscr{M}_p$ is a sub-$S_{\nu,\pi}$-module of $S^d_{\nu,\pi}$, 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:

$$\begin{array}{rccc}\Xi & : \mathrm{Mod}^d_{S_{\nu,\pi}} & \longrightarrow & \prod_{a \in \overline{\mathfrak{R}}} \mathrm{Mod}^d_{\bar{K}[[u-a]]} \\ & \mathscr{M}_p & \mapsto & (\mathscr{M}_{p,a})_a\end{array}$$

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 Ξ 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_ν-module. Moreover, as a byproduct of our study, we will derive an upper bound on the number of generators of a maximal sub-S_ν-module of S^n_ν.

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_ν-module and let $(e_1, \ldots, e_k) \in \mathscr{M}^k$ be a family of generators of $\mathscr{M}$. We denote by $\mathscr{R}$ the module of relations of $(e_1, \ldots, e_k)$ that is the set of $(\lambda_1, \ldots, \lambda_k) \in S^k_\nu$ 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

$$0 \to \mathscr{R} \otimes_{S_\nu} S_{\nu,\pi} \to S^k_{\nu,\pi} \to \mathscr{M} \otimes_{S_\nu} S_{\nu,\pi} \to 0, \tag{12}$$

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 $(f_1, \ldots, f_\ell)$ be a basis of $\mathscr{R} \otimes_{S_\nu} S_{\nu,\pi}$ and set $\mathscr{R}' = \oplus_{i=1}^{\ell}(S_{\nu,\pi} \cdot f_i \cap S_\nu^k)$. Apparently, $\mathscr{R}'$ is a sub-S_ν-module of $\mathscr{R}$ which is free of rank ℓ. Indeed, if n_i denotes the smallest integer such that $\pi^{n_i} \cdot f_i \in S_\nu^k$, then the family $(\pi^{n_i} \cdot f_i)$ is a basis of $\mathscr{R}'$. Moreover, we have the inclusion $\mathscr{R}' \supset \pi^N \mathscr{R}$ for a certain N since $\mathscr{R}' \otimes_{S_\nu} S_{\nu,\pi} = \mathscr{R} \otimes_{S_\nu} S_{\nu,\pi}$. Now, from the knowledge of the matrix $M \in M_{d\times k}(S_\nu)$ whose column vectors are the coordinates of e_i in the canonical basis of S_ν^d, we can compute a matrix $R' \in M_{k\times\ell}(S_\nu)$ of generators of $\mathscr{R}'$ using the algorithms of §3.2.2. We have by definition $M.R' = 0$. Of course in the above construction, we can replace, *mutatis mutandis* the localisation with respect to π by the localisation with respect to u^α/π^β.

3.3.1 An algorithm to compute the maximal module

We start with a couple of matrices $M = (m_{i,j}) \in M_{d\times k}(S_\nu)$ and $R = (r_{i,j}) \in M_{k\times\ell}(S_\nu)$ representing the generators of $\mathscr{M}$ embedded in S_ν^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 $t : [1, i_0] \to \mathbb{N}^*$ 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:

$$R = \begin{pmatrix} r_{1,t(1)} & & & & \\ & \ddots & & & \\ & & r_{i_0,t(i_0)} & & \\ & & & \star \cdots \star & \\ & & & \vdots \quad \vdots & \\ & & & \star \cdots \star & \end{pmatrix}, \tag{13}$$

where the blanks represent 0 entries.

We set $t(i_0+1)$ to be the first integer t such that $t(i_0) < t \leq \ell$ 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 $\mathrm{Cond}(i)$ on R is satisfied if there exist two different indices $j_0, j_1 \in \{1, \ldots, k\}$ such that $r_{j_0,t(i)} \cdot r_{j_1,t(i)} \neq 0$, $v_\nu(r_{j_0,t(i)}) \leq v_\nu(r_{j_1,t(i)})$ and $\deg_W(r_{j_0,t(i)}) \leq \deg_W(r_{j_1,t(i)})$. We apply the algorithm ColumnReduction (see Algorithm 3) on $R, M, i_0 + 1, t(i_0 + 1)$.

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 $\mathrm{Cond}(t(i_0+1))$ will no longer be satisfied on R. It may happen that there is only one nonzero entry on the $t(i_0+1)^{th}$ 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 $r_{i_0+1,t(i_0+1)}$. Next, we remark that the vector v of $\mathscr{M}$ whose coordinates in the canonical basis of S_ν^d is given by the $(i_0+1)^{th}$ column of M verifies $r_{i_0+1,t(i_0+1)} \cdot v = 0$ which means that $v = 0$ and we can set $r_{i_0+1,j} = 0$ for $j > t(i_0 + 1)$.

If there are several nonzero entries on the $t(i_0+1)^{th}$ column of R and the condition $\mathrm{Cond}(t(i_0+1))$ is not satisfied on R, we let j_0 be such that $v_\nu(r_{j_0,t(i_0+1)}) = \min_{1\leq j\leq k}\{v_\nu(r_{j,t(i_0+1)})\}$. Note that we have $v_\nu(r_{j_0,t(i_0+1)}) < v_\nu(r_{j,t(i_0+1)})$ for $j \neq j_0$ because on the contrary, the condition $\mathrm{Cond}(t(i_0+1))$ would be satisfied on R. By multiplying the $t(i_0+1)^{th}$ column of R by an element of $S_{\nu,\pi}$ with valuation $-v_\nu(r_{j_0,t(i_0+1)})$, we can moreover suppose that $v_\nu(r_{j_0,t(i_0+1)}) = 0$. Let $\delta = \min_{j\neq j_0}(v_\nu(r_{j,t(i_0+1)}))$.

Algorithm 3: ColumnReduction (preliminary version)

input :

- $M \in M_{d\times k}(S_\nu)$
- $R \in M_{k\times \ell}(S_\nu)$ 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 Cond$(t(i))$

while Cond$(t(i))$ *is satisfied* **do**
  Pick up $j_0, j_1 \in \{1, \dots, k\}$ such that $r_{j_0,t(i)} \cdot r_{j_1,t(i)} \neq 0$, $v_\nu(r_{j_0,t(i)}) \leq v_\nu(r_{j_1,t(i_0+1)})$ and $\deg_W(r_{j_0,t(i)}) \leq \deg_W(r_{j_1,t(i)})$;
  $(q, r) \leftarrow \text{EuclideanDivision}(r_{j_0,t(i)}, r_{j_1,t(i)})$;
  $C_{j_0}(M) \leftarrow C_{j_0}(M) + qC_{j_1}(M)$;
  $L_{j_1}(R) \leftarrow L_{j_1}(R) - qL_{j_0}(R)$;
return M, R;

The case $\nu = 0$ First, we suppose that $\nu = 0$ from which we deduce that δ is a positive integer. Denote by $e_1, \dots, e_k$ the generators of $\mathscr{M}$ represented by the column vectors of the matrix M. Denote by $\mathscr{M}_1$ the module generated by $(e'_j)_{j=1\dots k}$ with $e'_j = e_j$ for $j \neq j_0$ and $e'_{j_0} = \frac{1}{\pi} e_{j_0}$. The identity of S_ν^d induces an inclusion $f : \mathscr{M} \to \mathscr{M}_1$. It is clear that the cokernel of f is annihilated by π. Moreover, we have

$$r_{j_0,t(i_0+1)} . e'_{j_0} = \sum_{j\neq j_0} \frac{r_{j,t(i_0+1)}}{\pi} e_j. \tag{14}$$

As the right hand side of (14) is in $\mathscr{M}$ since $\frac{r_{j,t(i_0+1)}}{\pi} \in S_\nu$, the cokernel of f is also annihilated by $r_{j_0,t(i_0+1)}$ which is a distinguished element of S_ν. 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 $(j)^{th}$ column of M and multiplying by π the $(j)^{th}$ 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 $O_1(j_0)$ 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 Cond$(t(i_0 + 1))$ 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 ϖ in an algebraic closure of K be such that $\varpi^\alpha = \pi$. Let $\mathfrak{R}' = \mathfrak{R}[\varpi]$, $S'_\nu = S_\nu \otimes_{\mathfrak{R}} \mathfrak{R}'$ and $\mathscr{M}' = \mathscr{M} \otimes_{S_\nu} S'_\nu$. The valuation on $\mathfrak{R}$ (resp. the Gauss valuation on S_ν) extends uniquely to $\mathfrak{R}'$ (resp. to S'_ν). 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 Cond$(t(i_0 + 1))$ is not satisfied. By multiplying the $t(i_0+1)^{th}$ column of R by $\varpi^{-v_\nu(r_{j_0,t(i_0+1)})\cdot\alpha}$, we can moreover suppose that $v_\nu(r_{j_0,t(i_0+1)}) = 0$. Let $\delta = \min_{j\neq j_0}(v_\nu(r_{j,t(i_0+1)}))$.

With this setting, we can define a quasi-isomorphism in the same manner as before. Namely, let $e_1, \dots, e_k$ be the generators of $\mathscr{M}'$ as a sub-module of ${S'_\nu}^d$ represented by the column vectors of the matrix M. Denote by $\mathscr{M}'_1$ the module generated by $(e'_j)_{j=1\dots k}$ where $e'_j = e_j$ for $j \neq j_0$ and $e'_{j_0} = \frac{1}{\varpi^\delta} e_{j_0}$. Then the natural injection $\mathscr{M}' \to \mathscr{M}'_1$ is a quasi-isomorphism. We denote by $O_2(j, \delta)$ the operation on the couple of matrices (M, R) with coefficients in S'_ν which consists in multiplying by $\frac{1}{\varpi^\delta}$ the $(j)^{th}$ column of M and multiplying by ϖ^δ the $(j)^{th}$ row of R. With the hypothesis and notations of this paragraph (*i.e.* M has the form (13)), if (M, R) represents the module $\mathscr{M}'$ and its

Algorithm 4: MatrixReduction for the case $\nu = 0$

input :

- $R \in M_{k\times\ell}(S_\nu)$,
- $M \in M_{d\times k}(S_\nu)$ such that $M \cdot R = 0$.

output: $R \in M_{k\times\ell}(S'_\nu)$, $M \in M_{d\times k}(S'_\nu)$ such that $M \cdot R = 0$ and R is a triangular matrix.

$i_0 \leftarrow 0$;
$t(i_0) \leftarrow 1$;
while $i \leq k$ **do**
  $t(i_0) \leftarrow \min\{t | t > t(i_0) \text{ and } \exists j > 0, \text{with } r_{j,t} \neq 0 \}$;
  $i_0 \leftarrow i_0 + 1$;
  $M, R \leftarrow \text{ColumnReduction}(M, R, i_0, t(i_0))$;
  for $j \leftarrow t(i_0) + 1$ **to** ℓ **do**
    $r_{i_0,j} \leftarrow 0$

Algorithm 5: ColumnReduction (final version) for $\nu = 0$

input :

- $M \in M_{d\times k}(S_\nu)$,
- $R \in M_{k\times\ell}(S_\nu)$ 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 Cond$(t(i))$ *is satisfied* **do**
    Pick up $j_0, j_1 \in \{1, \ldots, k\}$ such that $r_{j_0,t(i)} \cdot r_{j_1,t(i)} \neq 0$, $v_\nu(r_{j_0,t(i)}) \leq v_\nu(r_{j_1,t(i)})$ and $\deg_W(r_{j_0,t(i)}) \leq \deg_W(r_{j_1,t(i)})$;
    $(q, r) \leftarrow \text{EuclideanDivision}(r_{j_0,t(i)}, r_{j_1,t(i)})$;
    $C_{j_0}(M) \leftarrow C_{j_0}(M) + qC_{j_1}(M)$;
    $L_{j_1}(R) \leftarrow L_{j_1}(R) - qL_{j_0}(R)$;
  Let j_0 be such that $\deg_W(r_{j_0,t(i)}) = \max_{1\leq j\leq k}\{\deg_W(r_{j,t(i)})\}$;
  $\delta \leftarrow \min_{j\neq j_0}(v_\nu(r_{j,t(i)})) - v_\nu(r_{j_0,t(i)})$;
  $C_{j_0}(M) \leftarrow \frac{1}{\pi^\delta} C_{j_0}(M)$;
  $L_{j_0}(R) \leftarrow \pi^\delta L_{j_0}(R)$;
return M, R;

relations, then the matrices (M', R') resulting of the operation of $O_2(j_0, \delta)$ represents the module $\mathscr{M}'_1$ which have been shown to be quasi-isomorphic to $\mathscr{M}'$ (as a S'_ν-module). Moreover, R' verifies the condition $\mathrm{Cond}(t(i_0+1))$.

The matrix M' (resp. R'), resulting of the operation $O_2(j, \delta)$ is made of column (resp. row) vectors with coefficients in S_ν multiplied by ϖ^δ 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 ϖ^α, for α an integer ;
- permutation of the rows ;
- for $j_0, j_1 \in \{1, \ldots, k\}$, replacing $L_{j_1}(R)$ by $L_{j_1}(R) - q' L_{j_0}(R)$ where q' 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 $\deg(r) \leq \deg_W(x)$, 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 $q' = \varpi^{\alpha_0 - \alpha_1} q$ 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_ν coefficient ring, we represent the couple of matrices (M', R') with coefficients in S'_ν by a triple (M, R, L) where M, R are matrices with coefficients in S_ν and $L = [\alpha_1, \ldots, \alpha_k]$ is a list of integers such that for $i = 1, \ldots, k$, $C_i(M') = \varpi_i^\alpha C_i(M)$ and $L_i(R') = \varpi^{-\alpha_i} L_i(R)$. We say that the condition $\mathrm{Cond}'(i)$ on R is satisfied if there exists two different $j_0, j_1 \in \{1, \ldots, k\}$ such that $r_{j_0,t(i)} \cdot r_{j_1,t(i)} \neq 0$, $v_\nu(r_{j_0,t(i)}) + \frac{\alpha_{j_0}}{\alpha} \leq v_\nu(r_{j_1,t(i)}) + \frac{\alpha_{j_1}}{\alpha}$ and $\deg_W(r_{j_0,t(i)}) \leq \deg_W(r_{j_1,t(i)})$. With these notations, we can write the final version of the MatrixReduction algorithm (see Algorithm 6) which encode the matrices M', R' with coefficients in S'_ν with a couple M, R of matrices with coefficients in S_ν 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 $(\pi^2, \pi u^3)$. It is represented in the canonical basis of S_0 by the matrices M of generators and R of relation :*

$$M = \begin{pmatrix} \pi^2 & \pi u^3 \end{pmatrix}, R = \begin{pmatrix} u^3 \\ -\pi \end{pmatrix}.$$

It is clear that $Cond(1)$ 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:

$$M = \begin{pmatrix} \pi & \pi u^3 \end{pmatrix}, R = \begin{pmatrix} \pi u^3 \\ -\pi \end{pmatrix}.$$

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 :

$$M = \begin{pmatrix} \pi & 0 \end{pmatrix}, R = \begin{pmatrix} 0 \\ -\pi \end{pmatrix}.$$

An we deduce that the maximal module associate to $\mathscr{M}$ is $\pi.S_0$.

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

Let $M_1, R_1, L_1 = \mathrm{MatrixReduction}(M, R, L = [0, \ldots, 0])$. Let $L_1 = [\beta_1, \ldots, \beta_k]$. We denote by $\mathscr{M}'_1$ the sub-S'_ν-module of $(S'_\nu)^d$ generated by the vectors given in the canonical basis of $(S'_\nu)^d$ by the column vectors $\varpi^{\beta_i} \cdot C_i(M_1)$ for $i \in \{1, \ldots, k\}$ such that $L_i(R_1)$ is the zero vector.

Lemma 3.18. *We have $\mathscr{M}'_1 = \mathrm{Max}(\mathscr{M} \otimes_{S_\nu} S'_\nu)$.*

Algorithm 6: MatrixReduction

input :

- $R \in M_{k\times\ell}(S_\nu)$,
- $M \in M_{d\times k}(S_\nu)$ such that $M \cdot R = 0$.

output: $R \in M_{k\times\ell}(S'_\nu)$, $M \in M_{d\times k}(S'_\nu)$, L such that $M \cdot R = 0$ and R is a triangular matrix.

$i_0 \leftarrow 0$;
$t(i_0) \leftarrow 1$;
$L \leftarrow [0, \dots, 0]$;
while $i \leq k$ **do**
  $i_0 \leftarrow i_0 + 1$;
  $t(i_0) \leftarrow \min\{t | t > t(i_0) \text{ and } \exists j > 0, \text{with } r_{j,t} \neq 0 \}$;
  while $\exists j_0, j_1$ *such that* $j_0 \neq j_1$ *and* $r_{j_0,t(i_0)} \cdot r_{j_1,t(i_0)} \neq 0$ **do**
    while $\text{Cond}'(t(i_0))$ *is satisfied* **do**
      Pick up $j_0, j_1 \in \{1, \dots, k\}$ such that $r_{j_0,t(i_0)} \cdot r_{j_1,t(i_0)} \neq 0$,
      $v_\nu(r_{j_0,t(i_0)}) + \frac{L[j_0]}{\alpha} \leq v_\nu(r_{j_1,t(i_0)}) + \frac{L[j_1]}{\alpha}$ and $\deg_W(r_{j_0,t(i_0)}) \leq \deg_W(r_{j_1,t(i_0)})$;
      if $v_\nu(r_{j_0,t(i_0)}) > v_\nu(r_{j_1,t(i_0)})$ **then**
        $\delta_0 \leftarrow \lceil v_\nu(r_{j_0,t(i_0)}) - v_\nu(r_{j_1,t(i_0)}) \rceil$;
        $L_{j_1}(R) \leftarrow \pi^{\delta_0} L_{j_1}(R)$;
        $C_{j_1}(M) \leftarrow \pi^{-\delta_0} C_{j_1}(M)$;
        $L[j_1] \leftarrow L[j_1] + \alpha \cdot \delta_0$;
      $(q, r) \leftarrow \text{EuclideanDivision}(r_{j_0,t(i_0)}, r_{j_1,t(i_0)})$;
      $C_{j_0}(M) \leftarrow C_{j_0}(M) + qC_{j_1}(M)$;
      $L_{j_1}(R) \leftarrow L_{j_1}(R) - qL_{j_0}(R)$;
    Let j_0 be such that $\deg_W(r_{j_0,t(i_0)}) = \max_{1\leq j\leq k}\{\deg_W(r_{j,t(i_0)})\}$;
    $\delta \leftarrow \min_{j\neq j_0}(v_\nu(r_{j,t(i_0)})) - v_\nu(r_{j_0,t(i_0)})$;
    $C_{j_0}(M) \leftarrow \frac{1}{\pi^{\lfloor\delta\rfloor}} C_{j_0}(M)$;
    $L_{j_0}(R) \leftarrow \pi^{\lfloor\delta\rfloor} L_{j_0}(R)$;
    $L[j_0] \leftarrow L[j_0] + \delta - \lfloor\delta\rfloor$;
  for $j \leftarrow t(i_0) + 1$ **to** ℓ **do**
    $r_{i_0,j} \leftarrow 0$
  Let $j_0 \in \{1, \dots, k\}$ be such that $r_{j_0,t(i_0)} \neq 0$;
  $(C_{j_0}(M), C_{i_0}(M)) \leftarrow (C_{i_0}(M), C_{j_0}(M))$;
  $(L_{j_0}(R), L_{i_0}(R)) \leftarrow (L_{i_0}(R), L_{j_0}(R))$;

Proof. Let $\mathscr{M}' = \mathscr{M} \otimes_{S_\nu} S'_\nu$ and let $\mathscr{M}_1$ be the sub-S'_ν-module of $(S'_\nu)^d$ generated by the column vectors of M_1. It is clear that $\mathscr{M}_1 = \mathscr{M}'_1$ since for $i \in \{1, \ldots, k\}$ such that $L_i(R_1)$ is not the zero vector, we have $C_i(M_1) = 0$ (because $\mathscr{M}_1$ is torsion free). As $\mathscr{M}_1$ is obtained from $\mathscr{M}'$ by a sequence of quasi-isomorphisms, it means that there exists a quasi-isomorphism $q' : \mathscr{M}' \to \mathscr{M}'_1$. If we prove that $\mathscr{M}'_1$ is a free S'_ν-module, we are done by Lemma 3.6.

Consider the exact sequence $0 \to \mathscr{R} \to S_\nu^k \to \mathscr{M} \to 0$ associated to the family $(e_1, \ldots, e_k)$ of generators of $\mathscr{M}$. As S'_ν is flat over S_ν, and as $\mathscr{R}' \otimes_{S_\nu} S'_\nu[1/\varpi] = \mathscr{R} \otimes_{S_\nu} S'_\nu[1/\varpi]$ by definition of $\mathscr{R}'$, we have an exact sequence

$$0 \to \mathscr{R}' \otimes_{S_\nu} S'_\nu[1/\varpi] \to ({S'_\nu}^k)[1/\varpi] \to \mathscr{M}'[1/\varpi] \to 0 \tag{15}$$

defined by the generators $(e_1, \ldots, e_k)$ of $\mathscr{M}'[1/\varpi]$. It is clear that at each step, the algorithm ReduceMatrix describes an exact sequence of the form (15) for a different map $({S'_\nu}^k)[1/\varpi] \to \mathscr{M}'[1/\varpi]$ since it preserves the relation $MR = 0$. From this and the definition of M'_1, we deduce that if $\mathscr{R}_1$ is the module of relations of $\mathscr{M}'_1$ 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 $(S'_\nu)^d$ by the column vectors $\varpi^{\beta_i} \cdot C_i(M_1)$ for $i \in \{1, \ldots, k\}$ such that $L_i(R_1)$ is the zero vector form a basis of $\mathscr{M}'_1$.*

Corollary 3.20. *Let $\mathscr{M}_2 = \mathscr{M}'_1 \cap S_\nu^d$. Then, $\mathscr{M}_2 = \mathrm{Max}(\mathscr{M})$.*

Proof. The corollary is an immediate consequence of Proposition 3.9 and Lemma 3.18. □

3.3.3 Computation with S_ν-modules

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

From the data of a matrix representing an element of $\mathscr{M} \in \mathrm{Max}_{S_\nu}^d$ the algorithm MatrixReduction computes the couple (M, L) representing $\Phi(\mathscr{M})$. Moreover, if $\mathscr{M}' \in \Phi(\mathrm{Max}_{S_\nu}^d)$, the Algorithm 7 allows to recover $\Phi^{-1}(\mathscr{M}')$. 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 $\mathscr{M} \in \mathrm{Max}_{S_\nu}^d$ by a couple (M, L). Indeed, we have the lemma:

Lemma 3.21. *Let $\mathscr{M}_1, \mathscr{M}_2 \in \mathrm{Max}_{S_\nu}^d$, then*

$$\begin{aligned} \Phi(\mathscr{M}_1 \cap \mathscr{M}_2) &= \Phi(\mathscr{M}_1) \cap \Phi(\mathscr{M}_2), \\ \Phi(\mathscr{M}_1 +_{\max} \mathscr{M}_2) &= \Phi(\mathscr{M}_1) +_{\max} \Phi(\mathscr{M}_2). \end{aligned}$$

Proof. For the first claim, we have $\Phi^{-1}(\Phi(\mathscr{M}_1) \cap \Phi(\mathscr{M}_2)) = \Phi(\mathscr{M}_1) \cap \Phi(\mathscr{M}_2) \cap S_\nu^d = (\Phi(\mathscr{M}_1) \cap S_\nu^d) \cap (\Phi(\mathscr{M}_2) \cap S_\nu^d) = \mathscr{M}_1 \cap \mathscr{M}_2$.

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

$$\begin{array}{ccc} & (\mathscr{M}_1 + \mathscr{M}_2) \otimes_{S_\nu} S'_\nu & \\ \swarrow & & \searrow \\ \mathrm{Max}(\mathscr{M}_1 + \mathscr{M}_2) \otimes_{S_\nu} S'_\nu & & \mathrm{Max}(\mathscr{M}_1 \otimes_{S_\nu} S'_\nu) + \mathrm{Max}(\mathscr{M}_2 \otimes_{S_\nu} S'_\nu) \end{array} \tag{16}$$

Thus, we have $\mathrm{Max}(\mathrm{Max}(\mathscr{M}_1 + \mathscr{M}_2) \otimes_{S_\nu} S'_\nu) = \mathrm{Max}((\mathscr{M}_1 + \mathscr{M}_2) \otimes_{S_\nu} S'_\nu) = \mathrm{Max}(\mathrm{Max}(\mathscr{M}_1 \otimes_{S_\nu} S'_\nu) + \mathrm{Max}(\mathscr{M}_2 \otimes_{S_\nu} S'_\nu))$ which is exactly the desired result. □

Let $\mathscr{M}_1, \mathscr{M}_2 \in \Phi(\mathrm{Max}_{S_\nu}^d)$ be represented respectively by the couples (M_1, L_1) and (M_2, L_2). 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 $((M_1 M_2), L_1 + L_2)$ (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_ν which is not Euclidean.

3.3.4 The generators of a maximal module

In order to have a complete algorithm (with oracles) to compute $\mathrm{Max}(\mathscr{M})$, it remains to explain how to recover $\mathscr{M}_2 = \mathscr{M}_1' \cap S_\nu^d$ from the knowledge of $\mathscr{M}_1'$ (see §3.3.2 for the definition of $\mathscr{M}_1'$). We would like also to obtain a bound on the number of generators of $\mathscr{M}_2$. By the construction of $\mathscr{M}_1'$, there exists a basis $(e_1, \ldots, e_k) \in S_\nu^d$ and $\delta_i \in \mathbb{N}$ for $i = 1, \ldots, k$, such that $\mathscr{M}_1' = \bigoplus_{i=1}^k S_\nu'.\varpi^{\delta_i} e_i$. Then, we have $\mathscr{M}_2 = \bigoplus_{i=1}^k (S_\nu'.\varpi^{\delta_i} \cap S_\nu).e_i$. Hence, it is enough to explain how to compute $\mathscr{M}_1' \cap S_\nu^d$ when $\mathscr{M}_1'$ has dimension 1. In this case, $\mathscr{M}_1'$ 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_ν-module $\{x \in S_\nu | v_\nu(x) \geq v_\nu(\frac{1}{\varpi^\delta} \cdot y)\}$. We are reduced to the problem of finding generators of the S_ν-module $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$.

Lemma 3.22. *Let $\delta \in \{0, \ldots, \alpha - 1\}$. We define inductively a sequence of couple of integers (α_i, β_i) 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 (α_i, β_i) be the unique couple of integers such that*

- *$\beta_i + \alpha_i \nu \geq -\frac{\delta}{\alpha}$,*
- *for all $(x, y) \neq (\alpha_i, \beta_i) \in \mathbb{Z}^2$ such that $0 \leq x \leq \alpha_i$ and $y + x\nu \geq -\frac{\delta}{\alpha}$, we have $\beta_i + \alpha_i\nu < y + x\nu$,*
- *α_i is the smallest integer strictly greater than α_{i-1} such that there exists an integer β_i with (α_i, β_i) satisfying the two conditions above.*

The family $(\pi^{\beta_i} \cdot u^{\alpha_i})$ has cardinality bounded by α and is a system of generators of the S_ν-module $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$.

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 α_i is bounded by $-\delta/\beta \mod \alpha$.

Denote by $\mathscr{N}_0$ the sub-S_ν-module of $\mathscr{N}$ generated by the family $(\pi^{\beta_i} \cdot u^{\alpha_i})$. Let $x \in \mathscr{N}$, we prove inductively on $\deg_W(x)$ that x is in $\mathscr{N}_0$. If $\deg_W(x) = 0$ then $v_\nu(x) \geq 0$ so that $x = x \cdot 1$ with $x \in S_\nu$. Suppose that $d = \deg_W(x) > 0$. 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 $\deg_W(h) = d$. 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 (α_i, β_i), we have $v_\nu(\pi^{\beta_{i_0}} \cdot u^{\alpha_{i_0}}) \leq v_\nu(h)$. 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 $h = q_1 \cdot \pi^{\beta_{i_0}} \cdot u^{\alpha_{i_0}} + r$ where $q_1 \in S_\nu$, $\deg_W(r) < \alpha_{i_0}$ 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 $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$ as well as an upper bound on the number of generators. In order to find the α_i we just run over all the values between 1 and $-\delta/\beta \mod \alpha$ 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 $[a_0; a_1, \ldots, a_n]$ refers to the value of the continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

We take the convention that $a_n \neq 1$ in $[a_0; a_1, \ldots, a_n]$ so that every rational number can be written uniquely as a finite continued fraction. Let $r = [a_0; a_1, \ldots, a_n]$. 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^{th} convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$. We have the properties:

- the integers p_k and q_k are relatively prime (see [9, Th. 2]);
- $p_k/q_k = [a_0; a_1, \ldots, a_k]$.

Definition 3.23. *Let r be a real number, and let γ 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 γ if for all integers c, d such that $\gamma \leq d \leq b$ and $c/d \neq a/b$ (resp. such that $\gamma \leq d \leq b$, $dr - c > 0$ and $c/d \neq a/b$), we have $|dr - c| > |br - a|$ (resp. $dr - c > br - a > 0$). 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, Th. 15 and Th. 16]).

Theorem 3.25. *Let $x = [a_0; a_1, \ldots, a_n]$.*

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 $\kappa \in [1/2, 1[$, $\frac{p_0}{q_0} = \frac{a_0}{1}$.*

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. $\min^+(r, b)$) the integer a such that $|b \cdot r - a| = \min\{|b \cdot r - k|, k \in \mathbb{Z}\}$ (resp. such that $b \cdot r - a = \min\{b \cdot r - k, k \in \mathbb{Z} \,\text{with}\, b \cdot r - k > 0\}$). 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 $j \in \{0, \ldots, n\}$, $\{q_j\}_x > 0$ if j is even, $\{q_j\}_x < 0$ if j is odd;*
- *for $j \in \{1, \ldots, n-2\}$ for all ζ integer such that $0 \leq \zeta < a_{j+2}$, $\zeta \cdot \{q_{j+1}\}_x + \{q_j\}_x$ has the same sign has $\{q_j\}_x$.*

Moreover for all $j \in \{1, \ldots, n-2\}$ and all ζ integer such that $0 \leq \zeta < a_{j+2}$,

$$\{\zeta \cdot q_{j+1} + q_j\}_x = \zeta \cdot \{q_{j+1}\}_x + \{q_j\}_x.$$

Proof. The fact that $\{q_j\}_x > 0$ if j is even, $\{q_j\}_x < 0$ 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 $\{q_j\}_x > 0$ and $\{q_{j+1}\}_x < 0$ (the other case can be treated in a similar manner). Suppose that for $0 < \zeta < a_{j+2}$, we have

$$\{q_j\}_x + \zeta \cdot \{q_{j+1}\}_x < 0. \tag{17}$$

Let ζ be the smallest verifying (17), then $\zeta \geq 2$ since we have by definition of a best approximation $|\{q_j\}_x| > |\{q_{j+1}\}_x|$. Then, as $\{q_j\}_x + (\zeta - 1) \cdot \{q_{j+1}\}_x > 0$, we have $|\{q_j\}_x + \zeta \cdot \{q_{j+1}\}_x| < |\{q_{j+1}\}_x|$ 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 ζ such that $0 < \zeta < a_{j+2}$, we have $\{q_j\}_x > \{q_j\}_x + \zeta \cdot \{q_{j+1}\}_x$. Thus we have we have $\{q_j\}_x > \zeta(q_{j+1} \cdot x - \min(x, q_{j+1})) + q_j \cdot x - \min(x, q_j) > 0$, so that $1/2 > (\zeta q_{j+1} + q_j) \cdot x - \zeta \min(x, q_{j+1}) - \min(x, q_j) > 0$ (remember that as $j \geq 1$, $\{q_j\}_x \leq 1/2$). As a consequence, $\zeta \min(x, q_{j+1}) + \min(x, q_j) = \min(x, \zeta q_{j+1} + q_j)$ thus $\{\zeta \cdot q_{j+1} + q_j\}_x = \zeta \cdot \{q_{j+1}\}_x + \{q_j\}_x$. □

For $x = [a_0; a_1, \ldots, a_n] \in \mathbb{Q}$ and γ a positive integer, we would like to be able to obtain the list of positive best approximations of x relatively to γ. The lemma tells us that not only the convergents p_{2i}/q_{2i} for $i \in \{0, \ldots, \lfloor n/2 \rfloor\}$ are positive best approximations of x but also the $\min^+(x, q_{2i} + \mu q_{2i+1})/(q_{2i} + \mu q_{2i+1})$ for $i \in \{0, \ldots, \lfloor (n-2)/2 \rfloor\}$ and μ integer such that $1 < \mu < a_{2i+2}$. The following proposition states that these are all the positive best approximations of x and gives a generalisation for the case of a positive γ.

Proposition 3.28. *Let $x = a/b$ where a, b are relatively prime integers. Write $x = [a_0; a_1, \ldots, a_n]$ and denote by p_k/q_k the sequence of convergents associated to the continued fraction $[a_0; a_1, \ldots, a_n]$. 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 γ. Let i be the biggest index such that $d - q_{2i+1} \geq \gamma$ and let λ be the biggest integer such that $d - q_{2i+1} - \lambda \cdot q_{2i+2} \geq \gamma$. Then*

1) $\frac{\min^+(x,d-q_{2i+1}-\lambda\cdot q_{2i+2})}{d-q_{2i+1}-\lambda\cdot q_{2i+2}}$ is a positive best approximation of x relatively to γ.

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

Moreover, we have

$$\{d - q_{2i+1} - \lambda \cdot q_{2i+2}\}_x^+ - \{d\}_x^+ = \lambda \cdot \{q_{2i+2}\}_x - \{q_{2i+1}\}_x > 0. \tag{18}$$

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

First, we prove that

$$\{d\}_x^+ - \{\mu(\zeta)\}_x = \{d - \mu(\zeta)\}_x^+, \tag{19}$$

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

$$0 \leq \min(x, \mu(\zeta)) - \mu(\zeta) \cdot x < 1. \tag{20}$$

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:

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

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 γ. 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

$$\{d\}_x^+ < \{e\}_x^+ \leq \{h\}_x^+. \tag{22}$$

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

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 μ, common difference ρ and length χ (if χ is zero then the sequence is considered as empty).

Algorithm 7: Reverse order list of positive best approximations

input :

- $x = a/b = [a_0; a_1, \ldots, a_n]$ 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 $[a_0; a_1, \ldots, a_n]$;
- $\gamma \leq b$ 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 γ

```
1  L ← [b];
2  last ← b;
3  t ← n;
4  if (t + 1) mod 2 = 0 then
5  |  nextqk ← t − 2;
6  else
7  |  nextqk ← t − 1;
8  while nextqk ≥ 0 do
9  |  if last − q[nextqk] ≥ γ then
10 |  |  λ ← floor( (last − q[nextqk] − γ) / q[nextqk + 1] ) ;
11 |  |  last ← last − λ.q[nextqk + 1] ;
12 |  while last − q[nextqk] ≥ γ do
13 |  |  last ← last − q[nextqk];
14 |  |  L ← last ∪ L ;
15 |  nextqk ← nextqk − 2;
16 if L[1] > γ then
17 |  L ← γ ∪ L;
18 return L;
```

Corollary 3.29. *Let $x = [a_0; a_1, \ldots, a_n]$ be a rational number, denote by p_k/q_k for $k = 0, \ldots, n$ the associated sequence of convergents. Let γ be a positive integer. The list a positive best approximations of x relatively to γ has cardinality bounded by $2 + \sum_{i=1}^{\lfloor n/2 \rfloor} a_{2i}$.*

Denote by L the finite sequence of increasing integers q such that $\min^+(x, q)/q$ is a positive best approximation relatively to γ. Let $I = \{0, \ldots, \lfloor (n-1)/2 \rfloor\}$. There exist two sequences $(\mu_i)_{i \in I}$ and $(\chi_i)_{i \in I}$ with coefficients respectively in $\mathbb{Q}$ and $\mathbb{N}$ such that $L = \cup_{i \in I} L(\mu_i, q_{2i+1}, \chi_i)$. Moreover, for $i \in I$, the sequence $(\{q\}_x^+)_{q \in L(\mu_i, q_{2i+1}, \chi_i)}$ is also an arithmetic sequence with common difference $\{q_{2i+1}\}_x < 0$.

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 $a_{\texttt{nextqk}+1}$. 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 $q[\texttt{nextqk} + 1] = a_{\texttt{nextqk}+1} \cdot q[\texttt{nextqk}] + q[\texttt{nextqk} - 1]$ implies that the loop on line 12 is executed at most $a_{\texttt{nextqk}+1}$ times. Taking into account the first and last element in the list L, we obtain that its cardinality is bounded by $2 + \sum_{i=1}^{\lfloor n/2 \rfloor} a_{2i}$.

The second part of the statement is clear, since the while loop on line 12 build a (reverse ordered) arithmetic sequence of common difference $q[\texttt{nextqk}]$ 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 $x = [a_0; a_1, \ldots, a_n]$. 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:*

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

We have everything at hand in order to compute efficiently the generators of $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$. Indeed, consider the line $\mathcal{L}$ given by the equation $y + x.\frac{\beta}{\alpha} = -\frac{\delta}{\alpha}$. Let $\gamma = \frac{\delta}{\beta} \mod \alpha$, where $\frac{\delta}{\beta} \mod \alpha$ 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 $(q_i)_{i \in I}$ the list of integers q_i such that $\min^+(\beta/\alpha, q_i)/q_i$ is a positive best approximation of β/α relatively to γ. Then if we set $\alpha_i = q_i - \gamma$, it is easily seen that the α_i are precisely the same as the one defined in the Lemma 3.22.

Corollary 3.31. *Let $\nu = \beta/\alpha = [a_0; a_1, \ldots, a_n]$. Let δ be an integer. Set $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$. Then $\mathscr{N}$ is generated elements of the form $(\pi^{\beta_i}.u^{\alpha_i})_{i \in J}$ where the cardinality of J is bounded by $2 + \sum_{i=1}^{\lfloor n/2 \rfloor} a_{2i}$. Let $I = \{1, \ldots, \lfloor n/2 \rfloor\}$. There exist two sequences $(\mu_i)_{i \in I}$ and $(\chi_i)_{i \in I}$ with coefficients respectively in $\mathbb{Q}$ and $\mathbb{N}$ such that $(\alpha_i)_{i \in J} = \cup_{i \in I} L(\mu_i, q_{2i+1}, \chi_i)$. Moreover, the sequence $v_\nu(\pi^{\beta_i}.u^{\alpha_i})_{\alpha_i \in L(\mu_i, q_{2i+1}, \chi_i)}$ is also an arithmetic sequence.*

By gathering all the results of this section, we obtain:

Theorem 3.32. *Let $\nu = [a_0; a_1, \ldots, a_n]$. Let $\mathscr{M}$ be a sub-S_ν-module of S_ν^d. Then a bound on the number of generators of $\mathrm{Max}(\mathscr{M})$ is $d.(2 + \sum_{i=1}^{\lceil n/2 \rceil} a_{2i})$. These generators can be represented by d vectors of S_ν^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 $[a_0; a_1, \ldots, a_n]$.*

3.3.5 Application: scalar extension of S_ν-modules

Let $\nu', \nu \in \mathbb{Q}$ such that $\nu' > \nu$, there is a natural inclusion $\theta_{\nu,\nu'} : S_\nu \to S_{\nu'}$. Given a module $\mathscr{M}$ over S_ν, We would like to compute the module $\mathrm{Max}(\mathscr{M} \otimes_{S_\nu} S_{\nu'}) \in \mathrm{Max}_{S_{\nu'}}^d$. If $M = (m_{ij}) \in M_{d \times k}(S_\nu)$

is a matrix representing $\mathscr{M}$, it can be done by calling the algorithm MatrixReduction on the matrix $(\theta_{\nu,\nu'}(m_{ij}))$.

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 (M', L') with $M' \in M_{d\times k}(S_\nu)$ and $L' = [\alpha_1, \dots, \alpha_k]$ is a list of integers. Let $(f_1, \dots, f_k)$ with $f_i = \varpi^{\alpha_i} \cdot e_i$ for $i = 1, \dots, k$ and $e_i \in S_\nu^d$ be the basis of $\Phi(\mathscr{M})$ given by the column vectors associated to the couple (M', L') (see Remark 3.19). Then by definition $\mathscr{M}$ is generated by the sub-S_ν-modules $F_i = f_i.S'_\nu \cap S_\nu^d$. 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_ν-module of S_ν, $\mathscr{N} = \{x \in S_\nu | v_\nu(x) \geq -\delta/\alpha\}$ for $\delta \in \mathbb{N}$. Then it has been seen in Corollary 3.31 that $\mathscr{N}$ is generated elements of the form $(\pi^{\beta_i}.u^{\alpha_i})_{i\in J}$. More precisely, write $\nu = [a_0; a_1, \dots, a_n]$ and let $I = \{1, \dots, \lfloor n/2 \rfloor\}$. Then, there exists three sequences $(\mu_i)_{i\in I}$, where $(\zeta_i)_{i\in I}$ and $(\chi_i)_{i\in I}$ with coefficients respectively in $\mathbb{Q}$, $\mathbb{N}$ and $\mathbb{N}$ such that $(\alpha_j)_{j\in J} = \cup_{i\in I} L(\mu_i, \zeta_i, \chi_i)$. Let $\mathscr{N}' = \mathscr{N} \otimes_{S_\nu} S_{\nu'}$. Of course, the sequence $(\pi^{\beta_j}.u^{\alpha_j})_{j\in J}$ has coefficients in $S_{\nu'}$ and is a family of generators of $\mathscr{N}'$. Hence, $\mathrm{Max}(\mathscr{N}')$ corresponds to the couple (M', L') where the unique element of L' is given the minimum of all quantites $\beta_j + \nu' \cdot \alpha_j$ when j runs over J. Now, we remark that the sequence $\beta_j + \nu' \cdot \alpha_j$ is arithmeric when j runs over one subset $L(\mu_i, \zeta_i, \chi_i)$. On this subset, the minimum is reached for the first index or the last one. Thus, to compute L', it is enough to take the minimum over these particular indices. It yields an algorithm whose complexity is $O(n)$ — or $O(nd)$ for the d-dimensional case — where we recall that n is the length of the continued fraction of ν (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_ν-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 §3.2.1 the (M_π, M_u)-representation and the representation of §3.3 the (M, L)-representation.

First, we explain how to go back and forth between the two representations. Let $\mathscr{M} \in \mathrm{Max}_{S_\nu}^d$ given with the (M, L)-presentation by the couple (M, L) with $M \in M_{d\times k}(S_\nu)$ and L is a list of integers. We can recover a matrix M_1 with coefficients in S_ν whose columns vectors gives generators of $\mathscr{M}$ in the canonical basis of S_ν^d. Then to obtain the couple (M_π, M_u) 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 (M_π, M_u)-representation in the case that the associated module $\mathscr{M} \in \mathrm{Max}_{S_\nu}^d$ has full rank. Suppose we are given the couple (M_π, M_u) representing $\mathscr{M}$ where $M_\pi = (m_{\pi,i,j}) \in M_{d\times k}(S_{\nu,\pi})$ and $M_u = (m_{u,i,j}) \in M_{d\times k}(S_{\nu,u})$. We can suppose, by multiplying M_π by a certain power of π (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 π (namely the determinant of M_u), we can also suppose, by multiplying M_u by a certain power of u^α/π^β (which is invertible in $S_{\nu,u}$), that all the coefficients of M_u belongs to S_ν. Let $D_u = \det(M_u) \in S_\nu$. On the other side, let $D_\pi = \det(M_\pi)/\varpi^{\alpha \cdot v_\nu(\det(M_\pi))} \in S'_\nu$. By definition, we have $v_\nu(D_\pi) = 0$. Denote by $\mathscr{M}_0^\pi$ (resp. $\mathscr{M}_0^u$) the sub-S'_ν-module of $(S'_\nu)^d$ generated by the column vectors of $D_u M_\pi$ (resp. $D_\pi M_u$), considered as matrices with coefficients in S'_ν. We can prove:

Lemma 3.33. *Keeping the above notations, we have:*

$$\mathrm{Max}((\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu) = \mathrm{Max}(\mathscr{M}_0^\pi + \mathscr{M}_0^u).$$

Proof. Using the formula $\mathrm{adj}(M) = \det(M).M^{-1}$, it is clear that the column vectors of the matrix $D_u M_\pi$ (resp. $D_\pi M_u$) belong to the $S'_{\nu,u}$-module generated by the column vectors of M_u (resp. the $S'_{\nu,\pi}$-module generated by the column vectors of M_π). As a consequence, we have $\mathscr{M}_0^\pi \subset (\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu$ and $\mathscr{M}_0^u \subset (\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu$. We deduce that $\mathscr{M}_0^\pi + \mathscr{M}_0^u \subset (\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu$. Thus, we have $\mathrm{Max}((\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu) \supset \mathrm{Max}((\mathscr{M}_0^\pi + \mathscr{M}_0^u) \otimes_{S_\nu} S'_\nu)$.

Next, suppose that $x \in \mathrm{Max}((\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu)$. By Proposition 3.8, it means that there exists $n \in \mathbb{N}$ such that $\pi^n \cdot x \in (\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu$ and $(u/\varpi^\beta)^n \cdot x \in (\mathscr{M}_u \cap \mathscr{M}_\pi) \otimes_{S_\nu} S'_\nu$. Note

that D_u is a power of π, as a consequence there exists $n_0 > n$ such that

$$\pi^{n_0} \cdot x \in \mathscr{M}_0^\pi \subset \mathscr{M}_0^\pi + \mathscr{M}_0^u. \tag{23}$$

We would like to prove that there exists $n_1 \in \mathbb{N}$ such that $(u/\varpi^\beta)^{n_1} x \in \mathscr{M}_0^\pi + \mathscr{M}_0^u$. For this, it suffices to prove that $(u/\varpi^\beta)^{n_1} x \mod \mathscr{M}_0^\pi \in \mathscr{M}_0^u/(\mathscr{M}_0^\pi \cap \mathscr{M}_0^u) \subset S'_\nu/\mathscr{M}_0^\pi$. As D_π is invertible in $S'_{\nu,u}$ (remember that $v_\nu(D_\pi) = 0$) there exists $t \in S'_\nu$ and $n_2 \in \mathbb{N}$ such that $t.D_\pi = (u/\varpi^\beta)^{n_2} \mod \pi^{n_0} S'_\nu$. Denote by $f_1, \ldots, f_k$ the vectors whose coordinates in the canonical basis of $(S'_\nu)^d$ are given by the column vectors of $\mathscr{M}_0^u$. Now, as $(u/\varpi^\beta)^n \cdot x \in \mathscr{M}_u$ there exist $\lambda_i \in S'_{\nu,u}$, for $i = 1, \ldots, k$, such that

$$(u/\varpi^\beta)^n.x = \sum_{i=1}^{k} \lambda_i f_i.$$

But we have $(u/\varpi^\beta)^n.x \in \mathscr{M}_\pi$ so that $(u/\varpi^\beta)^n.x \in (S'_\nu)^d$ and using the triangular form of the matrix M_u (see Proposition 3.15) we have that $\lambda_i \in S'_\nu$ for $i = 1, \ldots, k$. By multiplying the preceding equation by $t.D_\pi$, we obtain:

$$(u/\varpi^\beta)^{n+n_2}.x + \lambda(u/\varpi^\beta)^n \pi^{n_0} \cdot x = \sum_{i=1}^{k} (t.\lambda_i)(D_\pi f_i),$$

for $\lambda \in S'_\nu$. Recall that we have seen that $\pi^{n_0} \cdot x \in \mathscr{M}_0^\pi$, thus $(u/\varpi^\beta)^{n+n_2} \cdot x \mod \mathscr{M}_0^\pi \in \mathscr{M}_0^u/(\mathscr{M}_0^\pi \cap \mathscr{M}_0^\pi)$. As a consequence by taking $n_1 = n + n_2$, we have:

$$(u/\varpi^\beta)^{n_1} \cdot x \in \mathscr{M}_0^\pi + \mathscr{M}_0^u \tag{24}$$

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 $(u/\varpi^\beta)^m \cdot x \in \mathscr{M}_0^\pi + \mathscr{M}_0^u$. By applying Proposition 3.8, we deduce that $x \in \mathrm{Max}((\mathscr{M}_0^\pi + \mathscr{M}_0^u) \otimes_{S_\nu} S'_\nu)$ and we are done. □

Remark 3.34. *In the preceding construction, we need the extension S'_ν of S_ν just to ensure that $v_\nu(D_\pi) = 0$. Thus, if $v_\nu(\det(M_\pi)) \in \mathbb{Z}$, this extension is not necessary.*

Now, let $\mathscr{M} \in \mathrm{Max}^d_{S_\nu}$ be represented by a couple (M_π, M_u). As M_π and M_u are given in Hermite Normal Form, we can easily compute D_π and D_u. Let $M'_\pi = D_u M_\pi$ and $M'_u = D_\pi M_u$. 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 $(M'_\pi M'_u)$.

The main advantage of the (M_π, M_u)-representation is that is provides unique representation of maximal modules over S_ν, 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 $\mathscr{M} \in \mathrm{Max}^d_{S_\nu}$ 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 $\mathrm{Max}^d_{S_\nu}$. Moreover, the base change operation $\otimes_{S_\nu} S_{\nu'}$ only makes sense in the (M, L)-representation and we will see in §4, an important application of this operation. Indeed, if $\nu' \geq \nu$, altough there is a natural inclusion morphism $S_\nu \subset S_{\nu'}$, the two sub-rings of $\mathscr{E}$, $S_{\nu,u}$ and $S_{\nu',u}$ are not comparable by the inclusion relation.

4 Representation and precision

In the previous sections, we have presented algorithms to compute with S_ν-modules by using, as a black-box, the ring operations of S_ν. As elements of S_ν 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_ν by a finite structure, then we deal with elements of S_ν and finally with more complex structures with coefficients in S_ν such as S_ν-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 π denote the uniformizer element of $\mathfrak{R}$ and p_π 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 $\overline{x} \in \mathfrak{R}/\pi^{p_\pi}\mathfrak{R}$ is the data of element of $x \in \mathfrak{R}$ up to π-adic precision p_π if $x \mod \pi^{p_\pi} = \overline{x}$.

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_π. 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 $\mathfrak{R} = k[[X]]$ 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 $\mathfrak{R}/\pi^{p_\pi}\mathfrak{R}$, whose time will be denoted by $T_0(p_\pi)$ in the rest of this paper. In the case $\mathfrak{R} = \mathbb{Z}_p$, using Strassen algorithm [11], we have $T(p_\pi) = \tilde{O}(p_\pi)$ 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 $T_0(p_\pi) = \tilde{O}(d \cdot p_\pi)$. If $\mathfrak{R} = k[[X]]$ using again Strassen algorithm for polynomials, we have $T(p_\pi) = \tilde{O}(p_\pi)$ (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 $T_0(p_\pi)$ is quasi-linear $\log(|\mathfrak{R}/\pi^{p_\pi}\mathfrak{R}|)$.

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_π as before. We call this representation the *flat approximation* of an element of S_ν with u-adic precision p_u and π-adic precision p_π or the (p_u, p_π)-flat approximation. The data of a representative with π-adic precision p_π 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 $\sum_{i=0}^{p_u} \overline{a}_i u^i/\pi^{\lceil i\nu \rceil}$ such that $\overline{a}_i = a_i \mod \pi^{p_\pi}$. It should be remarked however that the flat approximation is not the only possible procedure to truncate an element of S_ν in order to obtain a finite structure. For instance, one can represent an element of S_ν 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 $a_i \mod \pi^{p_\pi}$ 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 π-adic precisions $a_i \mod \pi^{p_{\pi,i}}$. 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 $\sum_{i=0}^{p_u-1} \pi^{p_{\pi_i}} u^i/\pi^{\lceil i\nu \rceil} \cdot \mathfrak{R}$. 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_ν. 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_ν 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_ν with "infinite precision". In general, in order to represent an element of S_ν^d by a finite data structure, one can consider a sub-$\mathfrak{R}$-module $\mathscr{P}$ of S_ν^d such that most of the time $S_\nu^d/\mathscr{P}$ has finite length.

Then, in order to compute a function $f : S_\nu^d \to S_\nu^d$, we would like to replace it by its approximation $f : S_\nu^d/\mathscr{P} \to S_\nu^d/f(\mathscr{P})$. 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_ν-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

$$f(x+h) = f(x) + df_x(h) + O(h^2).$$

Most of the time (but not always), $df_x(\mathscr{P})$ 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_ν 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_ν 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_ν 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 $\mathscr{P}(P_\pi)$ the sub-$\mathfrak{R}$-module of S_ν given by $\sum_{i=0}^{\infty} a_i u^i/\pi^{\lfloor i\nu \rfloor} \cdot \mathfrak{R}$. Moreover, if $\mathscr{P}$ is sub-$\mathfrak{R}$-module of S_ν, we denote by $\mathrm{repr}(\mathscr{P}) : S_\nu \to S_\nu/\mathscr{P}$ the canonical projection of $\mathfrak{R}$-modules. It is clear that $\mathscr{P}(P_\pi)$ 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_π is an integer, we will use the notations $\mathscr{P}_f(p_u, p_\pi)$ for

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

which corresponds to the (p_u, p_π)-flat approximation. If $\mathscr{P}'$ and $\mathscr{P}$ are two sub-$\mathfrak{R}$-modules of S_ν such that $\mathscr{P}' \subset \mathscr{P}$ then there is a canonical projection $S_\nu/\mathscr{P}' \to S_\nu/\mathscr{P}$ that we denote also (by abuse of notation) by $\mathrm{repr}(\mathscr{P})$. If $\lambda \in S_\nu$, and $\mathscr{P}$ is a sub-$\mathfrak{R}$-module of S_ν, we denote by $\lambda.\mathscr{P} = \{\lambda.x, x \in \mathscr{P}\}$ the sub-$\mathfrak{R}$-module of S_ν. If λ is distinguished and $S_\nu/\mathscr{P}$ has finite length then $S_\nu/(\lambda \cdot \mathscr{P})$ has finite length. If $\mathscr{P}, \mathscr{P}'$ are sub-$\mathfrak{R}$-modules of S_ν, we denote by $\mathscr{P} \cdot \mathscr{P}'$ the submodule generated by all products xy for $(x, y) \in (\mathscr{P} \times \mathscr{P}')$. It is clear that if $S_\nu/\mathscr{P}$ and $S_\nu/\mathscr{P}'$ have finite length then $S_\nu/(\mathscr{P} \cdot \mathscr{P}')$ also have finite length.

Lemma 4.1. *For all $\mathscr{P}, \mathscr{P}'$ sub-$\mathfrak{R}$-modules of S_ν such that $S_\nu/\mathscr{P}$ and $S_\nu/\mathscr{P}'$ have finite length, for all $x, y \in S_\nu$ we have:*

1. *if $\mathscr{P}' \supset \mathscr{P}$ then* $\mathrm{repr}(\mathscr{P}')(\mathrm{repr}(\mathscr{P})(x)) = \mathrm{repr}(\mathscr{P}')(x)$;
2. $\mathrm{repr}(\mathscr{P} + \mathscr{P}')(\mathrm{repr}(\mathscr{P})(x)) + \mathrm{repr}(\mathscr{P} + \mathscr{P}')(\mathrm{repr}(\mathscr{P}')(y)) = \mathrm{repr}(\mathscr{P} + \mathscr{P}')(x + y)$;
3. *let $\mathscr{P}_0 = y \cdot \mathscr{P} + x \cdot \mathscr{P}' + \mathscr{P} \cdot \mathscr{P}'$, then*

$$\mathrm{repr}(\mathscr{P}_0)(\mathrm{repr}(\mathscr{P})(x)) \cdot \mathrm{repr}(\mathscr{P}_0)(\mathrm{repr}(\mathscr{P}')(y)) = \mathrm{repr}(\mathscr{P}_0)(x \cdot y);$$

4. *if $\mathscr{P}' \supset \mathscr{P}$, then* $\mathrm{repr}(\mathscr{P}')(\mathrm{repr}(\mathscr{P})(x)) \cdot \mathrm{repr}(\mathscr{P}')(y) = \mathrm{repr}(\mathscr{P}')(x \cdot y)$

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

We discuss briefly the complexity of the elementary arithmetic operations in S_ν with the (p_u, p_π)-flat approximation. First, we remark that the size of an element of S_ν with the (p_u, p_π)-flat approximation is in the order of $p_\pi \cdot p_u$. As before, the time of an addition in S_ν is linear in the size of a representative of S_ν 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 $T(p_u, p_\pi)$ the time cost of the multiplication of two elements of S_ν with the $(p_u, p_\pi)-$flat approximation. Again, by using a tweaked Strassen's algorithm, we have $T(p_u, p_\pi) = \tilde{O}(p_u \cdot T(p_\pi)) = \tilde{O}(p_u \cdot p_\pi)$. 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_ν

Most of the time, even for very elementary function dealing with elements of S_ν, 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 $v_\nu : K[[u]] \to \mathbb{Q}$. A natural way to define v_ν on a representative modulo $\mathscr{P}_f(p_u, p_\pi)$, with p_u, p_π positive integers, is to compute the valuation of the truncated representative in S_ν. For instance let $x = \pi + u^{10}$, then $v_0(\mathrm{repr}(\mathscr{P}_f(9,2))(x)) = v_0(\pi) = 1$. We denote also this function by v_ν. But then we have $v_0(\mathrm{repr}(\mathscr{P}_f(9,2))(x)) = 1$ and $v_0(\mathrm{repr}(\mathscr{P}_f(10,2))(x)) = 0$. 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 $v_\nu(\mathrm{repr}(\mathscr{P}_f(p_u, p_\pi))(x)) = 0$ 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 ν is big enough, it is possible to compute the valuation of x from the knowledge of $\mathrm{repr}(\mathscr{P}_f(p_u, p_\pi))(x)$.

Lemma 4.2. *Let $x = \sum a_i u^i \in 1/\pi^\lambda \cdot S_\nu$ for λ a positive integer. Let p_u be a positive integer and $\overline{x} \in K[u]$ be the unique representative of $x \mod u^{p_u}$ of degree $< p_u$. We suppose that $x \neq 0$ and that $d = \deg_W(x) < p_u$.*

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

$$\nu' - \nu \geq \frac{\lambda + v_\nu(x)}{p_u - d}, \tag{25}$$

then $v_{\nu'}(x) = v_{\nu'}(\overline{x})$.

Proof. Let $x = \sum a_i u^i \in 1/\pi^\lambda \cdot S_\nu$. By definition, we have $v_{\nu'}(\overline{x}) \leq v_K(a_d) + \nu' \cdot d$ and on the other side we have of course $v_{\nu'}(x) \leq v_{\nu'}(\overline{x})$. Thus, in order to prove the lemma, we just have to check that for all $i \geq p_u$, we have

$$v_K(a_i) + \nu' \cdot i \geq v_K(a_d) + \nu' \cdot d. \tag{26}$$

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

$$v_K(a_i) + \nu \cdot i \geq -\lambda \tag{27}$$

for all $i \geq p_u$. From (26) and (27), we deduce that it is enough to prove that $-\lambda + i(\nu' - \nu) \geq v_K(a_d) + \nu'.d$. Since $\nu' - \nu \geq 0$ by hypothesis, it suffices to prove that $-\lambda + p_u(\nu' - \nu) \geq v_k(a_d) + \nu'.d$ for all $i \geq p_u$. This is equivalent to

$$\nu' \geq \frac{v_K(a_d) + p_u \cdot \nu + \lambda}{p_u - d}, \tag{28}$$

which is exactly (25). □

This lemma, while totally elementary, shows the following very important fact: by increasing the ν parameter of the S_ν-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_ν is the inversion.

Lemma 4.3. *Let $x \in S_\nu$ and suppose that $\deg_W(x) = 0$ and that $v_\nu(x) = 0$ so that by Corollary 2.7, x is invertible. Let p_u, p_π be positive integers. Then $\mathrm{repr}(\mathscr{P}_f(p_u, p_\pi))(x) \in S_\nu/\mathscr{P}_f(p_u, p_\pi)$ is also invertible and we have $\mathrm{repr}(\mathscr{P}_f(p_u, p_\pi))(x)^{-1} = \mathrm{repr}(\mathscr{P}_f(p_u, p_\pi))(x^{-1})$.*

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 $c_j = \sum_{i=0}^{j} a_i \cdot b_{j-i}$. We have $v_K(a_0) = 0$ so that we can compute ${a_0}^{-1} \mod p_\pi = b_0 \mod p_\pi$. 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 $\pi^{\lfloor j\nu \rfloor} / (\pi^{\lfloor i\nu \rfloor} \pi^{\lfloor (j-i)\nu \rfloor})$ is equal to 1 or π, we obtain by induction for $j = 1, \ldots, p_u - 1$, $b_j \mod p_\pi$. □

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 $d = \deg_W(x)$. Let $q \in S_\nu$ and $r \in K[u] \cap S_\nu$ be such that $\deg(r) < d$ and $y = q \cdot x + r$. Put $e = v_\nu(\mathrm{Lo}(x)) > 0$, let p_π be a positive integer and $p_x = \lceil p_\pi/e \rceil d$. Let*

$$P_y = \sum_{i=0}^{p_x-1} \pi^{\max\{p_\pi - \lfloor i/d \rfloor e - \lfloor i\nu \rfloor, -\lfloor i\nu \rfloor\}} u^i + \sum_{i=p_x}^{\infty} \frac{u^i}{\lfloor i\nu \rfloor},$$

$$P_q = \sum_{i=0}^{p_x-d-1} \pi^{\max\{p_\pi - \lfloor i/d+1 \rfloor e - \lfloor i\nu \rfloor, -\lfloor i\nu \rfloor\}} u^i + \sum_{i=p_x-d}^{\infty} \frac{u^i}{\lfloor i\nu \rfloor}.$$

There exists an algorithm which takes as input $\mathrm{repr}(\mathscr{P}_f(p_x, p_\pi))(x)$ *and* $\mathrm{repr}(\mathscr{P}(P_y))(y)$ *and outputs* $\mathrm{repr}(\mathscr{P}_f(p_x, p_\pi))(q)$ *and* $\mathrm{repr}(\mathscr{P}_f(\infty, p_\pi))(r)$.

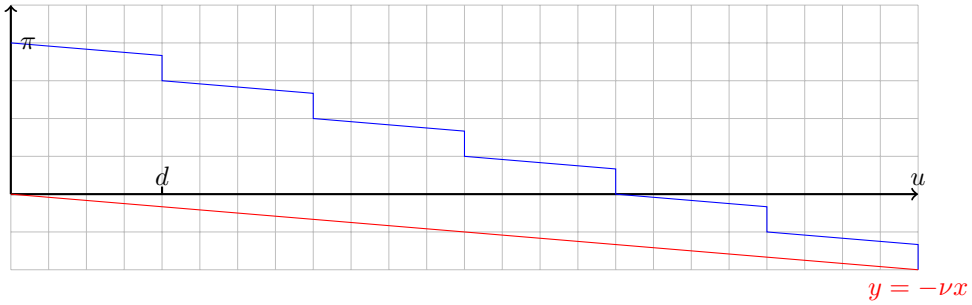


Figure 3: The form of the precision of y in the Euclidean division for $d = 2$ and $\nu = 1/6$.

Proof. Recall that, from Proposition 2.8, q, r are the limits of the sequences (q_j, r_j) defined by $q_0 = 0$ and $r_0 = y$ and

$$q_{j+1} = q_j + \frac{\mathrm{Hi}(r_j, d)}{\mathrm{Hi}(x, d)},$$

$$r_{j+1} = \mathrm{Lo}(r_j) - \frac{\mathrm{Hi}(r_j, d)}{\mathrm{Hi}(x, d)} \cdot \mathrm{Lo}(x).$$

For $j = 0, \ldots, \lceil p_\pi/e \rceil$, let

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

and let $t(j) = \mathrm{repr}(\mathscr{P}(P_{y,j}))(r_j)$. It is clear that $t(0) = \mathrm{repr}(\mathscr{P}(P_y))(y)$. We are going to prove that if we know $\mathrm{repr}(\mathscr{P}_f(p_x, p_\pi))(x)$ and $t(j)$ then we can compute $t(j+1)$. Write $\mathrm{Hi}(x, d) = u^d/\pi^{\nu d} \cdot x_0$, with x_0 an invertible element of S_ν. Then from $\mathrm{repr}(\mathscr{P}_f(p_x, p_\pi))(\mathrm{Hi}(x, d))$, we immediately obtain $\mathrm{repr}(\mathscr{P}_f(p_x - d, p_\pi))(\mathrm{Hi}(x_0, d))$, and by Lemma 4.3, we can compute $\mathrm{repr}(\mathscr{P}_f(p_x - d, p_\pi))(1/(\mathrm{Hi}(x_0, d)))$. As $\mathscr{P}_f(p_x - d, p_\pi) \subset \mathscr{P}(p_x - d \cdot j, P_{y,j})$, applying Lemma 4.1, we deduce that

$$\mathrm{repr}(\mathscr{P}(P_{y,j}))(\mathrm{Hi}(r_j, d)/\mathrm{Hi}(x_0, d)) = \mathrm{repr}(\mathscr{P}(P_{y,j})(\mathrm{repr}(\mathscr{P}_f(p_x - d, p_\pi))(1/(\mathrm{Hi}(x_0, d)))).\mathrm{repr}(\mathscr{P}(P_{y,j})(\mathrm{Hi}(r_j, d)). \quad (29)$$

We remark that $\mathrm{repr}(\mathscr{P}(P_{y,j})(\mathrm{Hi}(r_j,d)) = \mathrm{Hi}(t(j),d)$ so that the left hand side of (29) can be computed from the known data. Dividing $\mathrm{repr}(\mathscr{P}(P_{y,j}))(\mathrm{Hi}(r_j,d)/\mathrm{Hi}(x_0,d))$ by $u^d/\pi^{\lfloor d\nu\rfloor}$, we obtain $\mathrm{repr}(\mathscr{P}(P_j))(\mathrm{Hi}(r_j,d)/\mathrm{Hi}(x,d))$, where

$$P_j = \sum_{i=0}^{(\lceil p_\pi/e\rceil-(j+1))\cdot d-1} \pi^{\max\{p_\pi-\lfloor i/d+1\rfloor e-\lfloor i\nu\rfloor,-\lfloor i\nu\rfloor}u^i + \sum_{i=(\lceil p_\pi/e\rceil-(j+1))\cdot d}^{\infty} \pi^{\max\{(j\cdot e-\lfloor i\nu\rfloor,-\lfloor i\nu\rfloor\}}u^i. \quad (30)$$

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

$$\mathrm{repr}(\mathscr{P}(t(j+1)))(\frac{\mathrm{Hi}(r_j,d)}{\mathrm{Hi}(x,d)}\cdot \mathrm{Lo}(x)) = \mathrm{repr}(\mathscr{P}(t(j+1)))(\mathrm{repr}(\mathscr{P}(P_j))(\mathrm{Hi}(r_j,d)/\mathrm{Hi}(x,d))).\mathrm{repr}(\mathscr{P}_f(\infty,p_\pi))(\mathrm{Lo}(x)). \quad (31)$$

From the above, we deduce by induction that we can compute $\mathrm{repr}(\mathscr{P}(P_{y,\lceil p_\pi/e\rceil}))(r)$. But we have $\mathscr{P}(P_{y,\lceil p_\pi/e\rceil}) = \mathscr{P}_f(\infty,p_\pi)$ so that we can compute $\mathrm{repr}(\mathscr{P}_f(\infty,p_\pi))(r)$ as claimed. Moreover, as we can compute $\mathrm{repr}(\mathscr{P}(P_j))(\mathrm{Hi}(r_j,d)/\mathrm{Hi}(x,d))$, by Lemma 4.1, we can compute $\mathrm{repr}(\sum \mathscr{P}(P_j))(q) = \mathrm{repr}(P_0)(q)$ and we are done. □

Remark 4.5. *In the preceding proposition, we see that in order to be able to compute* $\mathrm{repr}(\mathscr{P}_f(d,p_\pi))(r)$*, we really use all the information contained in* $\mathrm{repr}(\mathscr{P}(p_y,P_y))(y)$*. If we use the flat precision, then to obtain* $\mathrm{repr}(\mathscr{P}(d,p_\pi))$ *we need to know* $\mathrm{repr}(\mathscr{P}(\lceil p_\pi/e\rceil.d,p_\pi))(y)$*. This shows that the flat precision is not well adapted to the computation of the Euclidean division in* S_ν *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_ν (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_ν which are polynomials. Suppose that $\mathfrak{R} = \mathbb{Z}_5$, $\nu = 0$ so that $S_\nu = \mathbb{Z}_5[[u]]$. Let $\overline{P_1} = \mathrm{repr}(\mathscr{P}_f(\infty,2))(u-1)$ and $\overline{P_2} = \mathrm{repr}(\mathscr{P}_f(\infty,2))(u-2)$. Then it is clear that for all $P_1,P_2 \in S_\nu$ such that $P_1 = \overline{P_1} \mod \mathscr{P}_f(\infty,2)$ and $P_2 = \overline{P_2} \mod \mathscr{P}_f(\infty,2)$ then $\gcd(P_1,P_2) = 1$. 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 $\gcd(\overline{P_1},\overline{P_2}) = 1$.

Next, consider $\overline{P_3} = \mathrm{repr}(\mathscr{P}_f(\infty,2))(u-1)$ and $\overline{P_4} = \mathrm{repr}(\mathscr{P}_f(\infty,2))(u-1)$. 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 $\gcd(P_3,P_4) = u-1$ but if we take $P_3 = u-1$ and $P_4 = u-6$ then $\gcd(P_3,P_4) = 1$. If we compute the 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_ν that we use in order to compute it.

4.3 Finite precision computation with modules with coefficients in S_ν

Let $\mathscr{M}_1$ and $\mathscr{M}_2$ be two maximal sub-S_ν-modules of S_ν^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_ν-modules of $S_{\nu,\pi}$ reduces to the computation of the gcd of two elements of $S_{\nu,\pi}$ and we have seen in §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_ν-modules of $S^d_{\nu,\pi}$ 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_ν of approximations of elements of $K[[u]]$ for well chosen ν. 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 $\mathscr{M}_1 +_{\max} \mathscr{M}_2$, we can describe an algorithm which outputs an approximation of $(\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (\mathscr{M}_2 \otimes_{S_\nu} S_{\nu'})$ for a well chosen $\nu' > \nu$.

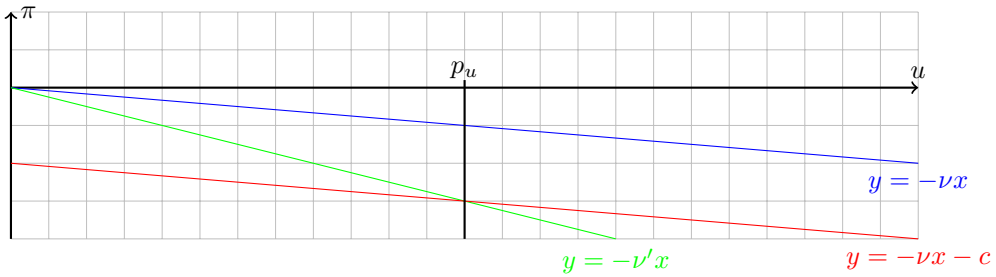


Figure 4: The computation of ν' from p_u and ν.

In order to compute $\mathscr{M}_1 +_{\max} \mathscr{M}_2$, it is enough to be able to compute $\mathscr{M}_1 +_{\max} S_\nu \cdot t$ where $t \in \mathscr{M}_2$. Indeed, let $(t_1, \dots, t_{h'})$ be a family of generators of $\mathscr{M}_2$, we have $\mathscr{M}_1 +_{\max} \mathscr{M}_2 = \mathscr{M}_1 +_{\max} S_\nu \cdot t_1 +_{\max} \dots +_{\max} S_\nu \cdot t_{h'}$. Let $t \in \mathscr{M}_2$ and let $(e_1, \dots, e_h)$ 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 λ_i are in S_ν 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 $\lambda_i = \sum_{j \geq 0} a^i_j u^j$ with $v_K(a^i_j) + \nu \cdot j \geq -c$. Let p_u a positive integer, we are going to choose ν', as it is explained in figure 4, such that $\sum_{j \geq p_u} a^i_j u^i \in S_{\nu'}$. For this it is enough to take $\nu' \geq \nu + c/p_u$. Let $t' = \sum_i \lambda'_i e_i$ with $\lambda'_i = \sum_{j=0}^{p_u - 1} a^i_j u^j$ and $t'' = \sum_i \lambda''_i e_i$ with $\lambda''_i = \sum_{p_u}^{\infty} a^i_j u^j$. Using the same remark as above, we have:

$$(\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (t \cdot S_{\nu'}) = (\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (t' \cdot S_{\nu'}) +_{\max} (t'' \cdot S_{\nu'}) = (\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (t' \cdot S_{\nu'}),$$

since $t'' \cdot S_{\nu'} \in \mathscr{M}_1$. Now, as λ'_i is a polynomial in u, we can obtain its valuation, greatest common divisor and all the operations that we need in order to compute $(\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (t \cdot S_{\nu'})$.

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

In the preceding algorithm, $Cond(\lambda, L)$ returns true if there exists $j_0, j_1 \in \{1, \dots, h\}$ such that $\lambda[j_0] \cdot \lambda[j_1] \neq 0$, $v_\nu(\lambda[j_0]) - \frac{L[j_0]}{\alpha} \leq v_\nu(\lambda[j_1]) - \frac{L[j_1]}{\alpha}$ and $\deg_W(\lambda[j_0]) \leq \deg_W(\lambda[j_1])$

We want to give a consequence of this algorithm. We first need a definition.

Definition 4.6. *Let $\mathscr{M}$ be a sub-S_ν-module of S^d_ν. Let $\mathscr{P}$ be a sub-$\mathfrak{R}$-module of S_ν. We say that a matrix $M^r = (m^r_{ij}) \in M_{d \times d'}(S_\nu/\mathscr{P})$ is an $\mathscr{P}$-approximation of $\mathscr{M}$ is there exists a matrix $M = (m_{ij}) \in M_{d \times d'}(S_\nu)$ whose columns are the coordinates of generators of $\mathscr{M}$ in the canonical basis of S^d_ν and such that $m^r_{ij} = \mathrm{repr}(\mathscr{P})(m_{ij})$.*

By iterating this algorithm AddVector on a set of $(t_1, \dots, t_{h'})$ 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_ν-modules of S^d_ν such that $\mathscr{M}_2 \subset 1/\pi^c \mathscr{M}_1$ for a positive integer c. Let $M_1 = (m^1_{ij})$ and $M_2 = (m^2_{ij})$ be the matrices with coefficients in S_ν of generators of $\mathscr{M}_1$ and $\mathscr{M}_2$ in the canonical basis of S^d_ν. Let p_u, p_π be positive integers and*

Algorithm 8: AddVector

input :

- $M \in M_{d\times h}(S_\nu)$, a matrix whose column vectors $C(i)$ for $i = 1, \dots, h$ give generators of $\mathscr{M}_1$ in the canonical basis of S_ν^d ;
- a list $\lambda[1], \dots, \lambda[h]$ such that $\sum \lambda_i C_i(M) = t$, $\lambda[i] \in 1/\pi^c \cdot S_\nu \cap K[u]$ and $\deg \lambda[i] \leq p_u - 1$ for $i = 1, \dots, k$.

output : $M \in M_{d\times h}(S_\nu)$ and a list L a matrix such that the column vectors $\varpi^{L[i]} \cdot C_i(M)$ give generators of $\mathscr{M}_1 +_{\max} t$ in the canonical basis of ${S'_\nu}^d$

$L \leftarrow [0, \dots, 0]$;
while $\exists j \in \{1, \dots, h\}$ *such that* $v_\nu(\lambda[j]) - \frac{L[j]}{\alpha} < 0$ **do**
  while Cond(λ, L) *is satisfied* **do**
    Pick up $j_0, j_1 \in \{1, \dots, h\}$ such that $\lambda[j_0] \cdot \lambda[j_1] \neq 0$,
    $v_\nu(\lambda[j_0]) - \frac{L[j_0]}{\alpha} \leq v_\nu(\lambda[j_1]) - \frac{L[j_1]}{\alpha}$ and $\deg_W(\lambda[j_0]) \leq \deg_W(\lambda[j_1])$;
    if $v_\nu(\lambda[j_0]) > v_\nu(\lambda[j_1])$ **then**
      $\delta_0 \leftarrow \lceil v_\nu(\lambda[j_0]) - v_\nu(\lambda[j_1]) \rceil$;
      $\lambda[j_0] \leftarrow \pi^{-\delta_0} \lambda[j_0]$;
      $L[j_0] \leftarrow L[j_0] - \alpha \cdot \delta_0$;
    $(q, r) \leftarrow$ EuclideanDivision$(\lambda[j_0], \lambda[j_1])$;
    $\lambda[j_1] \leftarrow \lambda[j_1] - q\lambda[j_0]$;
    $C_{j_1}(M) \leftarrow C_{j_0}(M) + qC_{j_1}(M)$;
  Let j_0 such that $v_\nu(\lambda[j_0]) - \frac{L[j_0]}{\alpha} = \min_{j=1,\dots,h}(\lambda[j]) - \frac{L[j]}{\alpha})$;
  Let j_1 such that $v_\nu(\lambda[j_1]) - \frac{L[j_1]}{\alpha} = \min_{j\neq j_0}(\lambda[j]) - \frac{L[j]}{\alpha})$;
  $L[j_0] \leftarrow L[j_0] + \alpha v_\nu(\lambda[j_0]) - L[j_0] - \alpha v_\nu(\lambda[j_1]) + L[j_1]$;
return M, L;

suppose that we are given $M_1^r = (\mathrm{repr}(\mathscr{P}_0(p_u, p_\pi))(m_{ij}^1))$ *and* $M_2^r = (\mathrm{repr}(\mathscr{P}_0(p_u, p_\pi))(m_{ij}^2))$. *Let* e *be the number of columns of* M_2 *and let* $\nu' = \nu + ec/p_u$. *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* $M_3^r = (M_{ij}^3)$ *with coefficients in* $S_{\nu'}/\mathscr{P}_0(p_u, p_\pi)$ *which is a* $\mathscr{P}_0(p_u, p_\pi)$*-approximation of*

$$(\mathscr{M}_1 \otimes_{S_\nu} S_{\nu'}) +_{\max} (\mathscr{M}_2 \otimes_{S_\nu} S_{\nu'}).$$

Remark 4.8. *If we suppose in the theorem that* $\mathscr{M}_2$ *is maximal, then by Theorem 3.32 we can take* $e = d.(2 + \sum_{i=1}^{\lceil n/2 \rceil} a_{2i})$ *where* $\nu = [a_0; a_1, \ldots, a_n]$.

References

[1] Xavier Caruso. p-adic precision. *in preparation.*

[2] Xavier Caruso. F_p-représentations semi-stables. *Ann. Inst. Fourier (Grenoble)*, 61(4):1683–1747 (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 Γ-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.