A pseudo-matrix approach to Prüfer domains

Gema M. Díaz-Toca* Henri Lombardi†

Abstract

In this extended abstract, we present the tools in order to construct an algorithm for computing the Hermite normal form of pseudo-matrices over Prüfer domains. This algorithm allows us to provide constructive proofs of the main theoretical results on finitely presented modules over Prüfer domains and to discuss the resolution of linear systems. We generalize the methodology developed by Henri Cohen for Dedekind domains in [Cohen, Chapter 1]. Finally, we present some results for Prüfer domains of dimension one. A full paper is found on `http://arxiv.org/abs/1508.00345`.

Introduction

The algorithmic solution of linear systems over fields or over PIDs is classical and it is equivalent to transforming the system via elementary manipulations (and Bezout manipulations for PIDs), in order to obtain a convenient reduced form (Hermite normal form or Smith normal form).

We use here a generalization of this kind of process for arbitrary Prüfer domains.

We adapt for an arbitrary Prüfer domain the generalized matrix computations given by Henri Cohen [Cohen, Chapter 1] for the algorithmics in rings of number fields (number rings).

We obtain a system of generalized matrix computations and as consequences the main "abstract" theorems for Prüfer domains. The generalization consists in replacing when necessary matrices over usual bases by matrices over decompositions of the modules as direct sums of rank one projective modules. These new matrices are called pseudo-matrices.

From a Computer Algebra viewpoint, computing with pseudo-matrices allows us to treat some examples inaccessible for usual methods: since our true computational tool is the inversion of finitely generated ideals, it is possible to work with number rings whose discriminant has no known complete factorization.

For Dedekind domains, and more generally for dimension one Prüfer domains, we obtain more precise results, similar to Smith reduction of usual matrices in PIDs.

General references for the constructive theory of Prüfer domains are found in [ACMC, CACM, Modules]. Many useful constructive proofs are also found in [MRR].

*Departamento de Matemática Aplicada, Universidad de Murcia, 30100 Murcia, Spain. `gemadiaz@um.es`

†Laboratoire de Mathématiques, Université de Franche-Comté, 25030 Besançon, France `henri.lombardi@univ-fcomte.fr`

1 Basic facts

1.1 Definitions

A ring $\mathbf{A}$ is ***zero-dimensional*** when

$$\forall a \in \mathbf{A},\ \exists n \in \mathbb{N}\ \exists x \in \mathbf{A},\ x^n(1-ax) = 0.$$

An integral domain $\mathbf{A}$ is ***of (Krull) dimension*** $\leqslant 1$ if for all $b \neq 0$ in $\mathbf{A}$, the quotient ring $\mathbf{A}/\langle b\rangle$ est zero-dimensional. E.g. number rings have dimension 1 because their quotients are finite, and consequently zero-dimensional.

Over an arbitrary ring $\mathbf{A}$ a finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ is ***locally principal*** if there exists $s_1, \ldots, s_n \in \mathbf{A}$ such that $\sum_{i\in[\![1..n]\!]} s_i = 1$ and $s_i\mathfrak{a} \subseteq \langle a_i\rangle$ for each s_i.

A ring $\mathbf{A}$ is ***arithmetic*** if all finitely generated ideals are locally principal.

A finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ is ***invertible*** if there exists a regular element c and an finitely generated ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \langle c\rangle$. Il other words, $\mathfrak{a}$ is locally principal an contains a regular element.

A ***Prüfer domain*** is an integral arithmetic ring. In other words, it is an integral domain whose all nonzero finitely generated ideal are invertible.

The ***determinantal ideal of order*** k of a matrix M is the ideal $\mathfrak{D}_k(M)$ generated by the minors of order k of M.

The ***Fitting ideal of order*** k of a finitely presented module P, coker of a matrix $M \in \mathbb{M}_{n,m}(\mathbf{A})$ is defined by $\mathfrak{F}_k(P) := \mathfrak{D}_{n-k}(M)$.

1.2 Computations with finitely generated ideals in a Prüfer domain

We work with an explicit Prüfer domain $\mathbf{Z}$. This means that for an arbitrary finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ we have an algorithm that computes $s_1, \ldots, s_n \in \mathbf{Z}$ such that $\sum_i s_i = 1$ and $s_i\mathfrak{a} \subseteq \langle a_i\rangle$ for each s_i. E.g. number rings are explicit Prüfer domains. We assume also that $\mathbf{Z}$ has a divisbility test, giving an x s.t. $ax = b$ when the test gives the answer "Yes" to the question "does a divise b?".

From these basic algorithms the following computations are shown to be easy. Note that by "computing an ideal", we mean to compute a generator set and a list $(s_1, \ldots, s_n)$ as in the previous explanation.

- For $\mathfrak{a}$ finitely generated, compute an ideal $\mathfrak{b}$ s.t. $\mathfrak{ab}$ is principal.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute s, t s.t. $s + t = 1$, $s\mathfrak{a} \subseteq \mathfrak{b}$ and $t\mathfrak{b} \subseteq \mathfrak{a}$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$, $\mathfrak{a} \cap \mathfrak{b}$ and $(\mathfrak{a} : \mathfrak{b})$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, test if $\mathfrak{a} \subseteq \mathfrak{b}$.

The following computations are more tricky. We assume that $\mathbf{Z}$ is moreover explicitly of dimension 1.

- For $\mathfrak{a}$ finitely generated and a nonzero in $\mathfrak{a}$, compute $b \in \mathfrak{a}$ s.t. $\mathfrak{a} = \langle a, b \rangle$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute an isomorphism between the modules $\mathfrak{a} \oplus \mathfrak{b}$ and $\mathbf{Z} \oplus \mathfrak{ab}$.

2 Pseudo-bases and pseudo-matrices

We note $\mathbf{K}$ the quotient field of $\mathbf{Z}$ and $\mathrm{Gfr}(\mathbf{Z})$ the (multiplicative) group of ***fractional ideals*** of $\mathbf{K}$. Such a fractional ideal is a sub-$\mathbf{Z}$-module of $\mathbf{K}$ equal to $\frac{\mathfrak{a}}{c}$ for a (usual) finitely generated ideal $\mathfrak{a} \subseteq \mathbf{Z}$ and c nonzero in $\mathbf{Z}$. A $\mathbf{Z}$-module E which is finitely generated and without torsion can be viewed as a sub-$\mathbf{Z}$-module of the $\mathbf{K}$-vector space $E' = \mathbf{K} \otimes_{\mathbf{Z}} E$.

A finitely generated projective $\mathbf{Z}$-module E can always be given as a direct sum $E = E_1 \oplus \cdots \oplus E_r$ with isomorphisms $E_i \simeq \mathfrak{e}_i \in \mathrm{Gfr}(\mathbf{A})$: $\mathfrak{e}_i \ni x \mapsto xe_i$ (where $e_i \in E'$). A ***pseudo-basis*** of E is by definition an r-tuple

$$\boxed{\big((e_1, \mathfrak{e}_1), \ldots, (e_r, \mathfrak{e}_r)\big)} \text{ s.t. } E = \mathfrak{e}_1 e_1 \oplus \cdots \oplus \mathfrak{e}_r e_r,$$

Note that $(e_1, \ldots, e_r)$ is a basis of the vector space E'.

Let $\varphi : E \to H$ a linear map between projective modules with pseudo-bases

$$\mathscr{E} = \big((e_1, \mathfrak{e}_1), \ldots, (e_m, \mathfrak{e}_m)\big) \text{ and } \mathscr{H} = \big((h_1, \mathfrak{h}_1), \ldots, (h_n, \mathfrak{h}_n)\big).$$

Extending the scalars to $\mathbf{K}$ we get a linear map $\varphi' : E' \to H'$ with a matrix $\underline{A}$ over the $\mathbf{K}$-bases $(e_1, \ldots, e_m)$ and $(h_1, \ldots, h_n)$.

- We call ***matrix of φ over pseudo-bases $\mathcal{E}$ and $\mathcal{H}$*** the data

  $$A = (\mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathfrak{e}_1, \ldots, \mathfrak{e}_m; \underline{A}) = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A}), \text{ where } \underline{A} = (a_{ij})_{ij} \in \mathbb{M}_{n,m}(\mathbf{K}).$$

  We have the inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. We note $\boxed{A = \mathscr{M}_{\mathcal{E},\mathcal{H}}(\varphi)}$.

intuitive visualization:

$$A = \begin{array}{c} \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \mathfrak{h}_3 \end{array} \begin{array}{c} \begin{array}{cccc} \mathfrak{e}_1 & \mathfrak{e}_2 & \mathfrak{e}_3 & \mathfrak{e}_4 \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} \end{array} \quad a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i.$$

- We call ***pseudo-matrix*** any data $(\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ of this kind, i.e. with inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. It can be viewed as the matrix of a $\mathbf{Z}$-linear map between sub-$\mathbf{Z}$-modules of $\mathbf{K}^n$ and $\mathbf{K}^m$.
- For fixed lists $\underline{\mathfrak{e}}$ et $\underline{\mathfrak{h}}$, the corresponding pseudo-matrices define a $\mathbf{Z}$-module $\boxed{\mathbb{M}_{\underline{\mathfrak{h}};\underline{\mathfrak{e}}}(\mathbf{A})}$ (isomorphic to the $\mathbf{Z}$-module of $\mathbf{Z}$-linear maps from E to H). The product of pseudo-matrices of convenient formats is defined in the natural way and corresponds to the composition of linear maps.

- For a square pseudo-matrix $A = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ we define its ***determinant (ideal)*** as being
$$\boxed{\mathbf{Z} \supseteq \mathfrak{Det}(A) := \det(\underline{A})\, \mathfrak{e}\, \mathfrak{h}^{-1}}, \text{ where } \mathfrak{e} = \prod_j \mathfrak{e}_j \text{ and } \mathfrak{h} = \prod_i \mathfrak{h}_i.$$
A square pseudo-matrix A is invertible if and only if $\mathfrak{Det}(A) = \mathbf{Z}$. For square pseudo-matrices A and B with convenient formats we have $\mathfrak{Det}(AB) = \mathfrak{Det}(A)\,\mathfrak{Det}(B)$.

- Let $\beta = [\beta_1, \ldots, \beta_r] \subseteq [\![1..n]\!]$ et $\alpha = [\alpha_1, \ldots, \alpha_r] \subseteq [\![1..m]\!]$ subsequences in increasing order. We note $A_{\beta,\alpha}$ the pseudo-matrix extracted on the rows β and columns α.
$$A_{\beta,\alpha} = (\mathfrak{h}_{\beta_1}, \ldots, \mathfrak{h}_{\beta_r}; \mathfrak{e}_{\alpha_1}, \ldots, \mathfrak{e}_{\alpha_r}, \underline{A}_{\beta,\alpha}).$$
The ideal
$$\mathfrak{m}_{\beta,\alpha}(A) := \mathfrak{Det}(A_{\beta,\alpha}) = \det(\underline{A}_{\beta,\alpha})(\prod_{i=0}^{r} \mathfrak{e}_{\alpha_i})(\prod_{j=0}^{r} \mathfrak{h}_{\beta_j})^{-1}$$
is called ***the minor (ideal) of order r of A extracted on rows β and columns α.***

- For an arbitrary pseudo-matrix and $r \leqslant \inf(m, n)$ the ***determinantal ideal of order r of*** A, noted $\mathfrak{D}_r(A)$, is the sum of minors of order r of A.
The pseudo-matrix A represents a surjective linear map if and only if $\mathfrak{D}_n(A) = \mathbf{Z}$.

- Let $s \in \mathbf{Z}^*$ s.t. the modules $E[1/s]$ and $H[1/s]$ are free over $\mathbf{Z}[1/s]$.
Let $\varphi_s : E[1/s] \to H[1/s]$ the extension of φ by $\mathbf{Z} \to \mathbf{Z}[1/s]$.
Then for each r we get $\mathfrak{D}_r(\varphi)\mathbf{Z}[1/s] = \mathfrak{D}_r(\varphi_s)$ (usual determinantal ideals).

- Let $(s_1, \ldots, s_n)$ be comaximal in $\mathbf{Z}$. A linear system $AX = B$ (with pseudo-matrices A, B, X) admits a solution in $\mathbf{Z}$ if and only if it admits a solution in each $\mathbf{Z}[1/s_i]$.

3 Computations with pseudo-matrices

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two finitely generated ideals of $\mathbf{Z}$ and M be a module with pseudo-basis $\mathcal{E} = \big((e_1, \mathfrak{a}), (e_2, \mathfrak{b})\big)$. If $s + t = 1$, $s\mathfrak{a} \subseteq \mathfrak{b}$ and $t\mathfrak{b} \subseteq \mathfrak{a}$, another pseudo-basis of M is $\mathcal{H} = \big((f_1, \mathfrak{a} + \mathfrak{b}), (f_2, \mathfrak{a} \cap \mathfrak{b})\big)$ where $f_1 = te_1 + se_2$ et $f_2 = -e_1 + e_2$. We get the following "Bezout pseudo-matrix " of change of pseudo-bases from $\mathcal{E}$ to $\mathcal{H}$.
$$B = \mathscr{M}_{\mathcal{H},\mathcal{E}}(\mathrm{Id}_M) = \begin{array}{c} \\ \mathfrak{a} \\ \mathfrak{b} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a}+\mathfrak{b} & \mathfrak{a}\cap\mathfrak{b} \end{array} \\ \begin{bmatrix} t & -1 \\ s & 1 \end{bmatrix} \end{array},$$
with inverse
$$\mathscr{M}_{\mathcal{E},\mathcal{H}}(\mathrm{Id}_M) = \begin{array}{c} \\ \mathfrak{a}+\mathfrak{b} \\ \mathfrak{a}\cap\mathfrak{b} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a} & \mathfrak{b} \end{array} \\ \begin{bmatrix} 1 & 1 \\ -s & t \end{bmatrix} \end{array}.$$

The Bezout pseudo-matrices and the analogues of Gauss pivoting matrices allow us to compute the reduction of pseudo-matrices to convenient "normal forms", analogous to HNF (Hermite normal form) for Prüfer domains and to SNF (Smith normal form) for Prüfer domains of dimension 1.

For dealing with pseudo-matrices over Prüfer domains of dimension 1 we use an algorithm in some zero-dimensional quotient rings: *a zero-dimensional arithmetic ring is a principal ideal ring and a matrix over it can be reduced to a Smith normal form by elementary row and column manipulations.*

Two kinds of easy consequences of these reductions of pseudo-matrices:

- The general discussion of linear systems over Prüfer domains (coefficients and unknowns in $\mathbf{Z}$)
- Theoretical results on the structure of finitely presented modules, finitely generated projective modules and linear maps between these modules: a finitely generated sub-$\mathbf{Z}$-module of $\mathbf{K}^n$ is finitely generated projective, a finitely generated projective module is a direct sum of rank one projective submodules, the kernel of a linear map between finitely generated projective modules is a direct summand, and so on...

References

[ACMC] Lombardi H. & Quitté C. *Algèbre Commutative. Méthodes constructives.* Calvage&Mounet (2011).

[CACM] Translated, revised and extended english version of [ACMC]. Springer (2015).

[Cohen] Cohen H. *Advanced topics in computational number theory.* Graduate texts in mathematics 193. Springer-Verlag (1999).

[Modules] Díaz-Toca G.-M., Lombardi H. & Quitté C. *Modules sur les anneaux commutatifs.* Calvage&Mounet (2014).

[MRR] Mines R., Richman F. & Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).