

Table des matières

1	Introduction	2
2	Base régulière de $\text{Int}_n(E, D)$	4
2.1	Suite ordonnée	4
2.2	Base régulière dans le cas local	4
2.3	Base régulière	6
2.4	Calcul effectif pour $E = D$	8
2.4.1	Construction d'une suite P -ordonnée de D	8
2.4.2	Algorithme pour $\text{Int}_n(D)$	11
2.4.3	Exemples	12
2.4.4	Fonctions pour $\text{Int}_n(D)$	14
3	Base régulière du sous-module $\text{Int}_n^r(E, D)$	16
3.1	Le sous-module $\text{Int}_n^r(E, D)$	16
3.2	Suite (P, r) -ordonnée	17
3.3	Base régulière dans le cas local	17
3.4	Base régulière	20
3.5	Calcul effectif pour $E=D$	22
3.5.1	Construction d'une suite (P, r) -ordonnée de D	23
3.5.2	Algorithme pour $\text{Int}_n^r(D)$	25
3.5.3	Exemples	25
3.5.4	Fonctions pour $\text{Int}_n^r(D)$	27
4	Base régulière du sous-module $\text{Int}_n^M(E, D)$	28
4.1	Le sous-module $\text{Int}_n^M(E, D)$	28
4.2	Suite P^h -ordonnée	28
4.3	Base régulière dans le cas local	29
4.4	Base régulière	31
4.5	Calcul effectif pour $E = D$	33
4.5.1	Construction d'une suite P^h -ordonnée de D	33
4.5.2	Algorithme pour $\text{Int}_n^M(D)$	35
4.5.3	Exemples	35
4.5.4	Fonctions pour $\text{Int}_n^M(D)$	37

1 Introduction

Soit $P \in \mathbb{Q}[X]$. Il se peut qu'un tel polynôme, bien qu'à coefficients rationnels, ne prenne que des valeurs entières lorsqu'il est évalué sur des entiers. On dit alors que P est à valeurs entières. De tels exemples sont donnés par les polynômes binomiaux, définis par $\binom{X}{0} = 1$ et pour tout $n \geq 1$:

$$\binom{X}{n} = \frac{X(X-1)\dots(X-(n-1))}{n!}$$

En effet $n!$ divise tout produit de n entiers consécutifs par la formule du binôme de Newton.

Définition 1.1. On note $\text{Int}(\mathbb{Z})$ l'ensemble des polynômes à valeurs entières et $\text{Int}_n(\mathbb{Z})$ l'ensemble des éléments de $\text{Int}(\mathbb{Z})$ de degré au plus n .

Ce sont des \mathbb{Z} modules. Il s'avère que tout $f \in \text{Int}_n(\mathbb{Z})$ s'écrit comme \mathbb{Z} -combinaison linéaire unique des polynômes binomiaux $\binom{X}{k}_{k \leq n}$:

Preuve. Soit $f = \sum_{k=0}^n c_k \binom{X}{k}$ la décomposition de f sur la \mathbb{Q} -base $\binom{X}{k}_{k \leq n}$. Il s'agit de montrer que les c_k sont dans \mathbb{Z} . Par l'absurde, soit j le plus petit indice tel que $c_j \notin \mathbb{Z}$. Si $k > j$, $c_k \binom{X}{k}(j) = 0$ et si $k < j$, $c_k \binom{X}{k}(j) \in \mathbb{Z}$ par définition de j . Il vient $c_j = c_j \binom{X}{j}(j) = f(j) - \sum_{k=0}^{j-1} c_k \binom{X}{k}(j) \in \mathbb{Z}$, contradiction. \square

On a donc:

Proposition 1.1. $\text{Int}_n(\mathbb{Z})$ est un \mathbb{Z} module libre de rang $n+1$ et $\binom{X}{k}_{k \leq n}$ en est une base.

On peut naturellement généraliser la situation à un anneau de Dedekind D , et même à un sous-ensemble $E \subset D$. On a en tête l'anneau des entiers d'un corps de nombres ou un anneau de valuation discrète.

Définition 1.2. Soit D un anneau de Dedekind de corps des fractions K et $E \subset D$. On note $\text{Int}(E, D)$ l'ensemble des polynômes P de $K[X]$ tels que $P(E) \subset D$ et $\text{Int}_n(E, D)$ l'ensemble des éléments de $\text{Int}(E, D)$ de degré au plus n . Ce sont des D modules.

On peut alors se poser la question suivante :

Question 1. La Proposition 1.1 subsiste-t-elle dans ce cadre plus général ? Autrement dit, $\text{Int}_n(E, D)$ est-il un D module libre de rang $n+1$, et si oui, peut-on trouver une base $\{f_k\}_{k \leq n}$ telle que $\deg(f_k) = k$?

Même si $\text{Int}_n(E, D)$ est libre, il se peut qu'il n'existe pas de base $\{f_k\}_{k \leq n}$ vérifiant $\deg(f_k) = k$. Si une telle base existe, on dit que c'est une base régulière.

L'objectif du présent papier est de répondre à la Question 1 et de présenter un algorithme pour effectivement construire quand elle existe une base régulière de $\text{Int}_n(E, D)$ dans le cas $E = D$ où D est l'anneau des entiers d'un corps de nombre.

Il s'agira ensuite de généraliser cette construction à deux sous-modules de $\text{Int}_n(E, D)$ qui seront introduits en section 3 et 4, et de fournir à nouveau des algorithmes de construction de bases régulières pour ces sous-modules.

Ces algorithmes ont été implémentés en C en utilisant la bibliothèque pari/GP et réunis avec d'autres dans une librairie consultable à l'adresse:

<https://github.com/vilanele/libfact>

Les exemples présents dans ce papier ont été construits à l'aide de cette librairie, et quelques références de fonctions seront données à la fin des différentes parties. On renvoie à la documentation pour des descriptions détaillées.

Les principales sources sur lesquelles est basé ce document sont [Bha09] et [Joh10]. On généralise notamment certains résultats donnés sur \mathbb{Z} dans le deuxième papier à l'anneau des entiers d'un corps de nombres.

Dans l'ensemble de ce document, D est un anneau de Dedekind de corps des fractions K .

On note E un sous-ensemble infini de D , P un idéal premier de D , et $\pi \in P \setminus P^2$ une uniformisante.

2 Base régulière de $\text{Int}_n(E, D)$

2.1 Suite ordonnée

Dans le but de généraliser à $K[X]$ les polynômes binomiaux $\binom{X}{n} \in \mathbb{Q}[X]$, Bhargava a introduit la notion de *P-ordering* ([Bha97]) que l'on nommera en français *suite P-ordonnée*.

La définition d'une suite *P-ordonnée* est une généralisation à tout anneau de Dedekind de la remarque suivante: pour tout nombre premier p , la suite ordonnée $(0, 1, 2, 3, \dots) = (a_0, a_1, a_2, a_3, \dots)$ des entiers naturels est telle que pour tout $n \geq 0$, a_n réalise le minimum suivant:

$$\min_{x \in \mathbb{Z}} v_p \left(\prod_{i=0}^{n-1} (x - a_i) \right)$$

On est donc amené à la définition suivante:

Définition 2.1. On appelle suite *P-ordonnée* de E toute suite $(a_n)_{n \geq 0}$ d'éléments de E telle que pour tout $n \geq 0$, a_n vérifie:

$$\min_{x \in E} v_P \left(\prod_{i=0}^{n-1} (x - a_i) \right) = v_P \left(\prod_{i=0}^{n-1} (a_n - a_i) \right) = e_n$$

On appelle *P-séquence* associée à la suite *P-ordonnée* $(a_n)_{n \geq 0}$ la suite décroissante d'idéaux $(P^{e_0}, P^{e_1}, P^{e_2}, P^{e_3}, \dots)$.

On a alors le théorème d'indépendance suivant:

Théorème 2.1. *La P-séquence associée à une suite P-ordonnée δ de E est indépendante de δ .*

Le Théorème 2.1 sera démontré à la fin de la prochaine section.

2.2 Base régulière dans le cas local

Dans cette section, on montre que dans le cas où D est local, $\text{Int}_n(E, D)$ possède toujours une base régulière que l'on construit à l'aide d'une suite π -ordonnée de E par un procédé en tout point équivalent à celui présenté dans l'introduction pour $\text{Int}_n(\mathbb{Z})$. Ce résultat permet alors de démontrer le Théorème 2.1.

Nous avons vu que dans le cas $D = E = \mathbb{Z}$, la suite $(0, 1, 2, \dots)$ est une suite p -ordonnée de \mathbb{Z} pour tout premier p simultanément. Ce fait permet de définir les polynômes binomiaux $\binom{X}{n}$ qui permettent à leurs tour d'exprimer tout polynôme à valeurs entières comme \mathbb{Z} combinaison linéaire des $\binom{X}{n}$.

Si on essaye d'appliquer le même procédé à E et D quelconques, on se heurte rapidement à l'obstruction suivante: il n'existe pas toujours dans E de suite *P-ordonnée* pour tout P simultanément. En revanche, si D est local, toute suite π -ordonnée de E l'est pour tout premier simultanément puisque (π) est le seul idéal premier ! On peut alors reproduire le procédé présenté en introduction pour $\text{Int}_n(\mathbb{Z})$.

Jusqu'à la fin de cette section, sauf mention du contraire, D est local. Soit $\delta = (a_n)_{n \geq 0}$ une suite π -ordonnée de E .

Définition 2.2. Pour tout $n \geq 0$, on pose

$$n!_{\delta,E} = \prod_{i=0}^{n-1} (a_n - a_i)$$

Par construction, $(\pi)^{v_\pi(n!_{\delta,E})}$ est le n -ème terme de la π -séquence associée à δ .

Définition 2.3. Pour tout $n \geq 0$, on définit le n -ème polynôme binomial associé à E et δ par $\binom{X}{0}_{\delta,E} = 1$ et pour $n \geq 1$:

$$\binom{X}{n}_{\delta,E} = \frac{(X - a_0)(X - a_1) \dots (X - a_{n-1})}{n!_{\delta,E}}$$

Par définition de δ et $n!_{\delta,E}$, on a $\binom{X}{k}_{\delta,E} \in \text{Int}_n(E, D)$. Ces polynômes sont en tout point similaires aux polynômes $\binom{X}{n} \in \mathbb{Q}[X]$. Comme dans le cas de $\text{Int}_n(\mathbb{Z})$, on a:

Théorème 2.2. Pour tout n , le D -module $\text{Int}_n(E, D)$ est libre de rang $n + 1$ et la famille

$$\left(\binom{X}{k}_{\delta,E} \right)_{k \leq n}$$

en est une base régulière.

Preuve. Soit $f \in \text{Int}_n(E, D)$, $f = \sum_{i=0}^n c_i \binom{X}{i}_{\delta,E}$ sa décomposition sur la K -base $\left(\binom{X}{k}_{\delta,E} \right)_{k \leq n}$. Il s'agit de montrer que les c_i sont dans D . Par l'absurde, soit j le plus petit indice tel que c_j ne soit pas dans D . Si $k > j$, $c_k \binom{X}{k}_{\delta,E}(a_j) = 0$ et si $k < j$, $c_k \binom{X}{k}_{\delta,E}(a_j) \in D$ par définition de j .

Il vient $c_j = c_j \binom{X}{j}_{\delta,E}(a_j) = f(a_j) - \sum_{k=0}^{j-1} c_k \binom{X}{k}_{\delta,E}(a_j) \in D$, contradiction. \square

Corolaire 2.1. Un polynôme $f \in K[X]$ de degré n est à valeurs entières sur E si et seulement si il est à valeurs entières sur $\{a_0, a_1, \dots, a_n\}$.

Preuve. Si f est à valeur entière sur E , il l'est à fortiori sur $\{a_0, a_1, \dots, a_n\} \subset E$. Pour la réciproque, il suffit de remarquer que dans la preuve du Théorème 2.2 on utilise uniquement le fait que $f(\{a_0, a_1, \dots, a_n\}) \subset D$. \square

Corolaire 2.2. Soit δ une suite π -ordonnée de E . La π -séquence associée à δ ne dépend pas de δ .

Preuve. Le Théorème 2.2 implique que l'idéal fractionnaire formé par zéro et l'ensemble des coefficients dominants des éléments de $\text{Int}_n(E, D)$ de degré n est $(n!_{\delta,E})^{-1}D$ et cela pour tout δ . Ainsi l'entier $v_\pi(n!_{\delta,E})$ ne dépend pas de δ et par conséquent la π -séquence associée à δ non plus. \square

Remarque 2.1. On a donc $n!_{\delta_1,E}D = n!_{\delta_2,E}D$ pour tout δ_1, δ_2 . On peut donc noter simplement $n!_E D$.

Définition 2.4. On appelle fonction factorielle associée à E la fonction

$$n \rightarrow n!_E = n!_E D$$

Le Théorème 2.1 est conséquence immédiate du Corolaire 2.2:

Preuve du Théorème 2.1. Soit D quelconque, P un idéal premier de D , D_P le localisé de D en P et δ une suite P -ordonnée de E . La suite δ est aussi une suite π -ordonnée de $E \subset D_P$ et les exposants dans la π -séquence associée à δ sont les même que dans la P -séquence associée à δ . On applique alors le Corolaire 2.2. \square

2.3 Base régulière

D est quelconque (plus nécessairement local).

Dans cette section, on énonce une condition nécessaire et suffisante pour que $\text{Int}_n(E, D)$ admette une base régulière et lorsque c'est le cas, on explique comment construire une telle base à partir de suites P -ordonnée pour un nombre fini de P à l'aide du théorème chinois.

Les résultats obtenus dans le cas local suggèrent qu'en général les coefficients dominants des éléments de $\text{Int}_n(E, D)$ jouent un rôle important.

Définition 2.5. Pour tout n , on définit $\mathfrak{J}_n(E, D)$ comme l'ensemble formé de zéro et des coefficients dominants des éléments de $\text{Int}_n(E, D)$ de degré n .

Proposition 2.1. $\mathfrak{J}_n(E, D)$ est un idéal fractionnaire.

Preuve. Soit $f = \sum_{i=0}^n a_i X^i \in \text{Int}_n(E, D)$ de degré n et soient x_0, x_1, \dots, x_n des éléments distincts de E . En considérant les a_i comme des inconnus, les $f(x_i)$ forment un système de $n+1$ équations linéaires (à $n+1$ inconnues) à coefficients dans D . Le déterminant du système est le déterminant de Vandermonde $d = \prod_{0 \leq i < j \leq n} (x_i - x_j)$. D'après les fameuses formules de Cramer, $da_i \in D$ pour tout i . Autrement dit on a $\mathfrak{J}_n(E, D) \subset \frac{1}{d}D$. \square

On a alors la propriété centrale suivante qui lie l'existence d'une base régulière de $\text{Int}_n(E, D)$ à la principalité des idéaux fractionnaires $\mathfrak{J}_k(E, D)_{k \leq n}$

Théorème 2.3. $\text{Int}_n(E, D)$ possède une base régulière si et seulement si les idéaux fractionnaires $\mathfrak{J}_k(E, D)_{k \leq n}$ sont principaux.

Preuve. Supposons que pour tout $k \leq n$, $\mathfrak{J}_k(E, D) = a_k D$ avec $a_k \in K$. Par définition, il existe une suite $(f_k)_{k \leq n}$ dans $\text{Int}_n(E, D)$ telle que $\deg(f_k) = k$ et a_k soit le coefficient dominant de f_k . Soit $f \in \text{Int}_n(E, D)$ de degré $m \leq n$ et a son coefficient dominant. Par hypothèse il existe $\beta \in D$ tel que $a = \beta a_m$. Alors en posant $g = f - \beta f_m$, on a $g \in \text{Int}_n(E, D)$ et $\deg(g) < m$. En itérant le procédé (au plus m fois), on obtient une décomposition D -linéaire de f sur la famille $(f_k)_{k \leq n}$, nécessairement unique.

Réciproquement, supposons que $\text{Int}_n(E, D)$ admette une base régulière $(f_k)_{k \leq n}$ et soit a_k le coefficient dominant de f_k . Puisque $\text{Int}_n(E, D)$ est un D module, on a immédiatement $a_k D \subset \mathfrak{J}_k(E, D)$ pour tout k . Soit $f \in \text{Int}_n(E, D)$ de degré $m \leq n$ et $f = \lambda_0 f_0 + \dots + \lambda_m f_m$ sa décomposition sur la base $(f_k)_{k \leq n}$. Le coefficient dominant de f est donc $\lambda_m a_m \in a_m D$. Donc $\mathfrak{J}_m(E, D) \subset a_m D$ et finalement $\mathfrak{J}_m(E, D) = a_m D$ pour tout $m \leq n$. \square

Ainsi, lorsque les idéaux $\mathfrak{J}_k(E, D)_{k \leq n}$ sont principaux de générateurs β_k , il suffit pour construire une base régulière de trouver $n + 1$ polynômes $(f_k)_{k \leq n}$ de $K[X]$ tels que $\deg(f_k) = k$ et tels que le coefficient dominant de f_k soit β_k .

La proposition suivante permet de lier les idéaux fractionnaires $\mathfrak{J}_n(E, D)$ à ceux des localisés D_P puis de construire une factorielle généralisée $n!_E$ pour D quelconque à partir des $n!_{E_P}$.

Proposition 2.2 (Localisation).

$$\text{Int}_n(E, D_P) = \text{Int}_n(E, D)_P$$

Preuve. Soit $f \in \text{Int}_n(E, D)_P$. Pour tout $x \in E$, on a $f(x) \in D_P$ puisque les coefficients de f sont dans D_P et que $E \subset D \subset D_P$.

Réciproquement soit $f \in \text{Int}_n(E, D_P)$ et soit I le D -module engendré par ses coefficients. Pour $x \in E$, on a donc $f(x) \in I \cap D_P$. Puisque D est Noëtherien, $I \cap D_P$ est finiment engendré. Il existe donc $s \in D \setminus P$ tel que $sf \in \text{Int}_n(E, D)$, i.e $f \in \text{Int}_n(E, D)_P$. \square

Corolaire 2.3. Soit $n!_{E_P}$ la factorielle associée à $E \subset D_P$. On a $n!_{E_P} = D$ sauf pour un nombre fini de P

Preuve. $n!_{E_P} \neq D$ pour les P qui divisent $\mathfrak{J}_n^{-1}(E, D)$ qui sont en nombre fini. \square

La Proposition 2.2 permet naturellement d'étendre la fonction factorielle définie dans le cas local à D quelconque:

Définition 2.6. On appelle fonction factorielle associée à E la fonction

$$n \rightarrow n!_E = \mathfrak{J}_n^{-1}(E, D) = \prod_{(P, \pi)} P^{v_\pi(n!_{E_P})}$$

On présente maintenant un algorithme pour construire un polynôme $A_n \in D[X]$ de degré n tel que $A_n(D) \subset n!_E$.

Soient $n \in \mathbb{N}$ et $\{P_1, P_2, \dots, P_m\}$ les premiers qui divisent $n!_E$. Pour tout $1 \leq i \leq m$ soit $(u_{i,k})_{0 \leq k < n}$ les n premiers termes d'une suite P_i -ordonnée de E . On note également $e_{i,n} = v_{P_i}(n!_E)$.

Algorithme 2.1.

1. Pour tout $0 \leq k < n$, on construit à l'aide du théorème chinois un élément a_k vérifiant pour tout $1 \leq i \leq m$:

$$a_k \equiv u_{i,k} \pmod{P_i^{e_{i,n}+1}}$$

2. On retourne le polynôme $A_n = (X - a_0)(X - a_1) \dots (X - a_{n-1})$.

La suite $(a_k)_{k \leq n}$ est construite afin d'être P_i -ordonnée simultanément pour tout les $P_i \in \{P_1, P_2, \dots, P_m\}$.

Théorème 2.4. On a $A_n(E) \subset n!_E$.

Preuve. Soit $x \in E$. Il suffit de montrer que $v_P(A_n(x)) \geq v_P(n!_E)$ pour tout P . Si $P \notin \{P_1, P_2, \dots, P_m\}$, $v_P(n!_E) = 0$. On peut donc se restreindre à $P_i \in \{P_1, P_2, \dots, P_m\}$. Mais alors par construction

$$\begin{aligned} v_{P_i}(A_n(x)) &= \sum_{k=0}^{n-1} v_{P_i}(x - a_k) \\ &\geq \sum_{k=0}^{n-1} v_{P_i}(a_n - a_k) \quad \left(= \sum_{k=0}^{n-1} v_{P_i}(u_{i,n} - u_{i,k}) \right) \\ &= v_{P_i}(n!_E) \end{aligned}$$

□

Pour que $\text{Int}_n(E, D)$ admette une base régulière, il est nécessaire d'après le Théorème 2.3 que les idéaux $k!_E$ pour $k \leq n$ soient principaux. On suppose donc que c'est le cas et on note β_k un générateur de $k!_E$.

Soit $(A_k)_{0 \leq k \leq n}$ des polynômes de $D[X]$ tels que $A_k(D) \subset k!_D$, par exemple construits avec l'Algorithme 2.1. On pose $B_k = \frac{1}{\beta_k} A_k$.

Théorème 2.5 (Base régulière). *La famille $\{B_0, B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n(E, D)$*

Preuve. Pour tout k , B_k est un polynôme de degré k , à valeurs entières d'après le Théorème 2.4 et de coefficient dominant β_k par construction. D'après le Théorème 2.3, $\{B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n(E, D)$. □

2.4 Calcul effectif pour $E = D$

Pour construire en utilisant les résultats de la section précédente une base régulière de $\text{Int}_n(E, D)$ lorsque les $(k!_E)_{k \leq n}$ sont principaux, on a besoin de savoir:

1. déterminer les idéaux premiers qui divisent $n!_E$
2. construire les n premiers terme d'une suite P -ordonnée de E

Réaliser le deuxième point demande si on applique la définition d'une suite P -ordonnée de E de prendre un minimum sur un ensemble infini, ce qui n'est pas réalisable tel quel.

Cependant, dans le cas où $E = D$ et où D/P est de cardinal fini pour tout P , il est possible de construire effectivement les n premiers termes d'une suite P -ordonnée de D en utilisant la finitude de D/P et l'homogénéité de D . On peut également en déduire les idéaux qui divisent $n!_D$.

On présente un tel algorithme puis on l'applique dans le cas où D est un corps de nombres sur quelques exemples.

Dans cette partie, D/P est de cardinal fini pour tout P .

2.4.1 Construction d'une suite P -ordonnée de D

On propose un algorithme pour construire les n premiers termes d'une suite P -ordonnée de D . On utilise de manière cruciale le fait que D est réunion disjointe finie des différentes classes modulo P . On généralise notamment aux entiers d'un corps de nombres certains théorèmes donnés pour \mathbb{Z} dans [Joh10].

Le cardinale de D/P est noté q .

Soit $\{r_0, r_1, \dots, r_{q-1}\}$ un système de représentants modulo P . On note $D_{r_i} = \{x \in D : x \equiv r_i \pmod{P}\}$.

On montre que les D_{r_i} ont tous la même P -séquence

Proposition 2.3. *Pour tout r_i, r_j on a*

$$v_P(n!_{D_{r_i}}) = v_P(n!_{D_{r_j}})$$

Preuve. Soit $c \in D$ tel que $D_{r_i} + c = D_{r_j}$ et soit $(a_n)_n$ une suite P -ordonnée de D_{r_i} . Puisque pour tout $x, y, c \in D$ on a

$$v_P(x - y) = v_P((x + c) - (y + c))$$

la suite $(a_n + c)_n$ est une suite P -ordonnée de D_{r_j} et $v_P(n!_{D_{r_i}}) = v_P(n!_{D_{r_j}})$. □

On relie ensuite la P -séquence de D à celle des D_{r_i} .

Proposition 2.4. *L'application*

$$\theta_i : x \rightarrow x\pi + r_i$$

envoie une suite P -ordonnée de D sur une suite P -ordonnée de D_{r_i} .

Preuve. Soit $(a_n)_n$ une suite P -ordonnée de D . Pour tout $x, y \in D$, on a

$$v_P(\theta_i(x) - \theta_i(y)) = v_P(\pi(x - y)) = 1 + v_P(x - y)$$

Par récurrence sur $n \geq 0$, le minimum à la n -ème étape de construction d'une suite P -ordonnée de D_{r_i} est atteint par $\theta_i(a_n)$, ce qui fait de $(\theta_i(a_n))_n$ une suite P -ordonnée de D_{r_i} . □

Corolaire 2.4. *Pour tout $n \geq 0$ on a*

$$v_P(n!_{D_{r_i}}) = v_P(n!_D) + n$$

Preuve.

$$\begin{aligned} v_P(n!_{D_{r_i}}) &= \sum_{k=0}^{n-1} v_P(\theta_i(a_n) - \theta_i(a_k)) \\ &= \sum_{k=0}^{n-1} (v_P(a_n - a_k) + 1) = v_P(n!_D) + n \end{aligned}$$

□

On cherche désormais à construire une suite P -ordonnée de D à partir de suites P -ordonnées des D_{r_i} . On a besoin de la notion d'entrelacement de suites:

Définition 2.7. Soient (ϕ_1, \dots, ϕ_m) des applications de \mathbb{N} vers \mathbb{N} . On dit que (ϕ_1, \dots, ϕ_m) est un entrelacement si ϕ_i est strictement croissante et si $\cup_i \phi_i(\mathbb{N}) = \mathbb{N}$.

On dit qu'une suite $(b_n)_n$ est le (ϕ_1, \dots, ϕ_m) entrelacement des suites

$$((a_{i,n})_n)_{1 \leq i \leq m}$$

si pour tout i la suite $(a_{i,n})_n$ est une sous-suite de $(b_n)_n$ d'extractrice ϕ_i^{-1} .

On montre maintenant que l'entrelacement q -uniforme de suites P -ordonnée des D_{r_i} résulte en une suite P -ordonnée de D . On en tire notamment que $v_P(n!_D)$ ne dépend pas de P mais que du cardinal q de D/P , puis un algorithme pour construire une suite P -ordonnée de D .

Proposition 2.5. *Pour tout $0 \leq i < q$ et tout $n \geq 0$ soit*

$$\phi_i(n) = nq + i$$

La suite obtenue par $(\phi_i)_{0 \leq i < q}$ entrelacement de suites P -ordonnée des D_{r_i} est une suite P -ordonnée de D .

Preuve. Soit $(a_n)_n$ une telle suite et soit $qk \leq n < q(k+1)$ pour un certain k . Soit $D_{r_{i_0}}$ la classe contenant a_n . Par définition des ϕ_i , il y a exactement k éléments dans chaque classe parmi les qk premiers termes de la suite. Supposons par l'absurde qu'il existe $x \in D$ tel que

$$\sum_{j=0}^{n-1} v_P(x - a_j) < \sum_{j=0}^{n-1} v_P(a_n - a_j)$$

et soit $D_{r_{i_1}}$ la classe contenant x . Puisque $v_P(x - y) = 0$ dès que x et y sont dans des classes différentes, on a

$$\sum_{j=0}^{n-1} v_P(a_n - a_j) \geq v_P(k!_{D_{r_{i_0}}}) \text{ et } \sum_{j=0}^{n-1} v_P(x - a_j) \geq v_P(k!_{D_{r_{i_1}}})$$

Mais

$$v_P(k!_{D_{r_{i_1}}}) = v_P(k!_{D_{r_{i_0}}})$$

d'après la Proposition 2.3, contradiction. □

Corolaire 2.5. *Pour tout $n \geq 0$ on a*

$$v_P(n!_D) = v_P(\lfloor n/q \rfloor!_D) + \lfloor n/q \rfloor$$

Preuve. Le n -ème terme de la suite obtenue par $(\phi_i)_{0 \leq i < q}$ entrelacement de suites P -ordonnée des D_{r_i} est le $\lfloor n/q \rfloor$ -ème terme d'une suite P -ordonnée de l'un des $D_{r_i} = D_{r_{i_0}}$. On a donc

$$v_P(n!_D) = v_P(\lfloor n/q \rfloor!_{D_{r_{i_0}}})$$

On applique alors le Corolaire 2.4. □

Corolaire 2.6. *Pour tout $n \geq 0$ on a*

$$v_P(n!_D) = \sum_{k=1}^n \lfloor n/q^k \rfloor$$

En conséquence $v_P(n!_D)$ ne dépend pas de P mais uniquement du cardinal q de D/P .

Preuve. Il suffit d'itérer la formule du Corolaire 2.5. □

Notation 2.1. Pour tout $n \geq 0$ et $q \geq 2$ on pose

$$w_q(n) = \sum_{k=1}^n \lfloor n/q^k \rfloor$$

Corolaire 2.7. Pour tout $q \geq 2$, soit M_q le produit des idéaux premiers de norme q . Pour tout $n \geq 0$ on a

$$n!_D = \prod_{(P,q)} P^{w_q(n)} = \prod_{q=2}^n M_q^{w_q(n)}$$

Preuve. On a $w_q(n) = 0$ dès que $q > n$. □

On est en mesure de proposer un algorithme pour construire les n premiers termes d'une suite P -ordonnée de D .

Algorithme 2.2.

1. Les q premiers termes $(a_0, a_1, \dots, a_{q-1})$ sont simplement $(r_0, r_1, \dots, r_{q-1})$.

Puisque $v_P(r_i - r_j) = 0$ quelque soient $r_i \neq r_j$, on a pour tout $s < q$

$$\sum_{j=0}^{s-1} v_P(a_s - a_j) = 0$$

donc $(a_0, a_1, \dots, a_{q-1})$ forme bien les q premiers termes d'une suite P -ordonnée de D .

2. Les q^k premiers termes $(a_j)_{j < q^k}$ d'une suite P -ordonnée de D étant donnés, on construit pour chaque $0 \leq i < q$ la suite

$$u_{i,k} = (\theta_i(a_j))_{j < q^k}$$

D'après la Proposition 2.4, $u_{i,k}$ forme les q^k premiers termes d'une suite P -ordonnée de D_{r_i} .

On construit alors le $(\phi_i)_{0 \leq i < q}$ entrelacement des suites $u_{i,k}$. D'après la Proposition 2.5, la suite résultante forme les q^{k+1} premiers termes d'une suite P -ordonnée de D .

On itère ce procédé tant que $k \leq \lfloor \log_q(n) \rfloor$. Enfin on tronque (éventuellement) la suite résultante au n -ème terme. On obtient au final les n premiers termes d'une suite P -ordonnée de D .

2.4.2 Algorithme pour $\text{Int}_n(D)$

On résume maintenant la procédure pour construire lorsque les $(k!_D)_{k \leq n}$ sont principaux une base régulière de $\text{Int}_n(D)$:

1. Pour chaque $k \leq n$, on détermine les idéaux premiers T_k qui divisent $k!_D$. D'après le Corolaire 2.7 ce sont tout les idéaux premiers de norme $q \leq k$. On calcul également pour tout $q \leq n$ le produit M_q des idéaux premiers de norme q . Pour cela, on utilise les méthodes standards pour factoriser les premiers $p \leq n$ dans D .
2. On construit pour chaque $P \in \bigcup_{k \leq n} T_k$ les n premiers termes d'une suite P -ordonnée de D en utilisant l'Algorithme 2.2.

3. Pour chaque $k \leq n$ on utilise l'Algorithme 2.1 pour construire le polynôme A_k tel que $A_k(D) \subset k!_D$. On utilise pour $P \in T_k$ les k premiers termes des suites P -ordonnées construites à l'étape 2).
4. On calcul ensuite pour chaque $0 \leq k \leq n$ l'idéal $k!_D$ par la formule du Corolaire 2.7. On utilise alors les M_q calculés à l'étape 1).
5. Pour tout $k \leq n$, on calcul un générateur β_k de $k!_D$ par les méthodes standards puis $B_k = \frac{1}{\beta_k} A_k$.

La famille (B_0, B_1, \dots, B_k) ainsi construite est une base régulière de $\text{Int}_n(D)$.

2.4.3 Exemples

Exemple 1

Soit $K = \mathbb{Q}(i)$. L'anneau $\mathbb{Z}[i]$ est principal, donc tout les $n!_{\mathbb{Z}[i]}$ sont principaux et $\text{Int}_n(\mathbb{Z}[i])$ admet une base régulière pour tout n .

On construit ici une base régulière de $\text{Int}_5(\mathbb{Z}[i])$.

1. On détermine pour $q \leq 5$ les idéaux premiers T_q de norme q et le produit M_q des idéaux de norme q :

q	T_q	M_q
2	$(1 + i)$	(2)
5	$(2 + i), (-2 + i)$	(5)

2. On construit pour chaque idéal premier qui divise $5!_{\mathbb{Z}[i]}$ les 5 premiers termes d'une suite P -ordonnée de $\mathbb{Z}[i]$:

Ideal P	Suite P -ordonnée
$(1 + i)$	$(0, 1, 1 + i, 2 + i, 2, 1 + 2i)$
$(2 + i)$	$(0, 1, 2, 3, 4)$
$(-2 + i)$	$(0, 1, 2, 3, 4)$

3. On construit les A_k pour $k \leq 5$:

k	$A_k(X)$
0	1
1	X
2	$X^2 + X$
3	$X^3 + (2 + i)X^2 + (1 + i)X$
4	$X^4 - 2iX^3 + (i - 4)X^2 + (3 + i)X$
5	$X^5 + 40X^4 + (2160 + 1325i)X^3 + (54525 - 2775i)X^2 + (1450i - 56726)X$

4. et 5. On détermine $k!_{\mathbb{Z}[i]}$ et un générateur pour $k \leq 5$:

k	$k!_{\mathbb{Z}[i]}$	Gen
0	$\mathbb{Z}[i]$	1
1	$\mathbb{Z}[i]$	1
2	$(1+i)$	$(1+i)$
3	$(1+i)$	$(1+i)$
4	$(1+i)^3$	$(2+2i)$
5	$(1+i)^3(2+i)(-2+i)$	$(10+10i)$

On obtient la base suivante:

$$B_0(X) = 1 \quad B_1(X) = X \quad B_2(X) = \frac{1-i}{2}X^2 + \frac{1-i}{2}X$$

$$B_3(X) = \frac{1-i}{2}X^3 + \frac{3-i}{2}X^2 + X$$

$$B_4(X) = \frac{1-i}{4}X^4 + \frac{-1-i}{2}X^3 + \frac{-3+5i}{4}X^2 + \frac{2-i}{2}X$$

$$B_5(X) = \frac{1-i}{20}X^5 + (2-i)X^4 + \frac{697-167i}{4}X^3 + \frac{5175-5730i}{2}X^2 + \frac{-13819+14544}{5}X$$

Exemple 2

Soit $K = \mathbb{Q}(\zeta_5)$. L'anneau des entiers de K est $D = \mathbb{Z}[\zeta_5]$. On peut montrer que dans un corps cyclotomique, les idéaux factoriels $n!_D$ sont tous principaux ([Ler10, Proposition 1.40]). On donne une base régulière de $\text{Int}_6(\mathbb{Z}[\zeta_5])$:

$$B_0(X) = 1, \quad B_1(X) = X, \quad B_2(X) = X^2, \quad B_3(X) = X^3 \quad B_4(X) = X^4$$

$$B_5(X) = \frac{-4-3\zeta_5-2\zeta_5^2-\zeta_5^3}{5}X^5 + (2+2\zeta_5+\zeta_5^2)X^3 + \frac{-6-7\zeta_5-3\zeta_5^2+\zeta_5^3}{5}X$$

$$B_6(X) = \frac{-4-3\zeta_5-2\zeta_5^2-\zeta_5^3}{5}X^6 - \zeta_5^2X^5 + (2+2\zeta_5+\zeta_5^2)X^4 + (\zeta_5+3\zeta_5^2+\zeta_5^3)X^3 \\ + \frac{-6-7\zeta_5-3\zeta_5^+\zeta_5^3}{5}X^2 + (-\zeta_5-2\zeta_5^2-\zeta_5^3)X$$

Exemple 3

Soit $K = Q(\zeta_5)$ encore, et soit

$$f(X) = \frac{-3 - \zeta_5 - 4\zeta_5^2 - 2\zeta_5^3}{5}X^6 + \frac{6 - 18\zeta_5 - 2\zeta_5^2 + 4\zeta_5^3}{5}X^5 + (1 + \zeta_5 + 2\zeta_5^2 + \zeta_5^3)X^4 \\ + (2 + 13\zeta_5 + 3\zeta_5^2 + 2\zeta_5^3)X^3 + \frac{8 - 4\zeta_5 - 6\zeta_5^2 - 8\zeta_5^3}{5}X^2 \\ + \frac{16 - 37\zeta_5 - 28\zeta_5^2 - 4\zeta_5^3}{5}X + (2\zeta_5 + \zeta_5^2) = \sum_{i=0}^6 c_i f_i$$

un polynôme de $\mathbb{Q}(\zeta_5)[X]$ de degré 6.

On cherche à savoir si f est à valeurs entières et si oui, quelle est sa décomposition pour une base régulière donnée.

Considérons la base régulière B_r de $\text{Int}_6(Q(\zeta_5))$ de l'exemple précédent, et soit M la matrice de passage de cette base à la base canonique $C = \{1, X, X^2, X^3, X^4, X^5, X^6\}$ de $Q(\zeta_5)_6[X]$ (polynômes de $Q(\zeta_5)[X]$ de degré au plus 6). Soit F_C le vecteur de f sur la base canonique C .

Pour que f soit à valeurs entières, il faut et il suffit que le vecteur $M^{-1}F_C$ ait tout ses coefficients dans $\mathbb{Z}[\zeta_5]$. On a:

$$M^{-1}F_C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 + \zeta_5^2 + \zeta_5^3 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 + \zeta_5^2 + \zeta_5^3 \\ 0 & 0 & 0 & 1 & 0 & 2 - \zeta_5^2 - \zeta_5^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 - \zeta_5^2 - \zeta_5^3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 - \zeta_5 - 3\zeta_5^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 + \zeta_5 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{pmatrix} \\ = \begin{pmatrix} 2\zeta_5 + \zeta_5^2 \\ \zeta_5 \\ 2 - \zeta_5^3 \\ -3\zeta_5^2 + 2\zeta_5^3 \\ 0 \\ 5\zeta_5 - 4\zeta_5^2 \\ 1 + \zeta_5^2 \end{pmatrix}$$

Ainsi $f(X) \in \text{Int}_6(\mathbb{Z}[\zeta_5])$ et le vecteur $M^{-1}F_C$ donne ses coordonnées sur la base régulière B_r .

2.4.4 Fonctions pour $\text{Int}_n(D)$

Voici quelques fonctions utiles:

- la fonction `ispolyaupto(K, n)` teste si $\text{Int}_n(D)$ admet une base régulière
- la fonction `zkregbasis(K, n, "X")` retourne (si possible) une base régulière (d'indéterminée "X") de $\text{Int}_n(D)$
- la fonction `zkregbasis_dec(K, pol, "X")` retourne une matrice $(n+1) \times 2$ (où $n = \deg(\text{pol})$) avec une base régulière (d'indéterminée "X") dans la deuxième colonne et les coefficients de la K -décomposition de `pol` sur cette base dans la première.

Cette fonction permet aisément (comme dans l'exemple 3) de déterminer si un polynôme de $K[X]$ est à valeurs entières: il faut et il suffit que les coefficients de la première colonne soient tous dans D .

3 Base régulière du sous-module $\text{Int}_n^r(E, D)$

Dans cette section, on présente un sous-module de $\text{Int}_n(E, D)$ introduit par Bhargava ([Bha09]) qui dépend d'un nouveau paramètre $r \geq 0$ ainsi qu'une nouvelle notion de suite ordonnée associée qui permet d'appliquer la même stratégie que dans la partie 2.

On donnera une condition nécessaire et suffisante pour que ce sous-module admette une base régulière, puis un algorithme de construction d'une telle base quand elle existe. On fournira plusieurs exemples concrets en fin de partie.

Dans toute cette partie, r est un entier positif.

3.1 Le sous-module $\text{Int}_n^r(E, D)$

Un polynôme entier f (i.e $f \in D[X]$) est bien sûr à valeurs entières sur tout $E \subset D$. Un tel polynôme préserve les congruences, c'est à dire que l'on a $f(x) \equiv f(y) \pmod{P}$ dès que $x \equiv y \pmod{P}$. Autrement dit, le polynôme en deux variables

$$\phi^1 f(x, y) = \frac{f(x) - f(y)}{x - y}$$

est à valeurs entières. Un polynôme quelconque de $\text{Int}_n(E, D)$ ne possède pas nécessairement cette propriété.

La fonction $\phi^1 f$ est la première différence divisée de f . On peut itérer ce procédé et définir la n -ème différence divisée de f :

Définition 3.1. Pour tout $n \geq 0$ et tout $f \in K[X]$, on définit la n -ème différence divisée de f par $\phi^0 f(x_0) = f(x_0)$ et

$$\phi^{n+1} f(x_0, \dots, x_{n+1}) = \frac{\phi^n f(x_0, \dots, x_n) - \phi^n f(x_0, \dots, x_{n-1}, x_{n+1})}{x_n - x_{n+1}}$$

Remarque 3.1. $\phi^n f(x_0, \dots, x_n)$ est une fonction symétrique en (x_0, \dots, x_{n+1})

Remarque 3.2. Si f s'annule sur $\{a_0, \dots, a_n\}$, alors $\phi^n f(a_0, \dots, a_n) = 0$.

On a la formule d'interpolation de Newton suivante

Proposition 3.1. Soit (a_0, \dots, a_{n-1}) des éléments de E et $f \in K[X]$ de degré n . Alors

$$\begin{aligned} f(x) = & f(a_0) + \phi^1 f(a_0, a_1)(x - a_0) + \phi^2 f(a_0, a_1, a_2)(x - a_1)(x - a_0) + \dots \\ & + \phi^n f(a_0, \dots, x)(x - a_0) \dots (x - a_{n-1}) \end{aligned}$$

En conséquence, un polynôme f est à valeurs entières sur E si et seulement si ses n premières différences divisées sont à valeurs entières sur E . On en vient à la définition

Définition 3.2. Pour tout $r \geq 0$, on définit $\text{Int}_n^r(E, D)$ comme l'ensemble des $f \in \text{Int}_n(E, D)$ tels que $\phi^k f(x_0, x_1, \dots, x_k)$ est à valeurs entières pour tout $k \leq r$.

Par construction, $\text{Int}_n^r(E, D)$ est un sous- D -module de $\text{Int}_n(E, D)$. C'est l'ensemble des polynômes f de degré au plus n à valeurs entières sur E tels que le fait de savoir que ses r premières différences divisées soient à valeurs entières ne permet pas de déterminer si $f \in D[X]$.

3.2 Suite (P, r) -ordonnée

On définit dans cette section une nouvelle notion de suite ordonnée d'éléments de E ([Bha09], [CC16]) qui à vocation à jouer le même rôle pour $\text{Int}_n^r(E, D)$ qu'une suite P -ordonnée pour $\text{Int}_n(E, D)$

Définition 3.3. Soit $r \geq 0$ et $\delta_r = (a_n)_n$ une suite dans E . On dit que la suite $(a_n)_n$ est (P, r) -ordonnée si pour tout $n \geq r + 1$

$$\min_{\substack{S_r \in N(n, r) \\ x \in E}} v_P \left(\prod_{k \in S_r} (x - a_k) \right) = \min_{S_r \in N(n, r)} v_P \left(\prod_{k \in S_r} (a_n - a_k) \right) = e_{r, n}$$

où $N(n, r)$ est l'ensemble des sous-ensembles de $\{0, \dots, n-1\}$ de cardinal $n-r$.

On appelle P -séquence associée à δ_r la suite décroissante d'idéaux $\{P_1, P_2, P_3, \dots\}$ dont les r premiers termes sont D et pour $n \geq r + 1$, $P_n = P^{e_{r, n}}$.

Pour tout n , soit $S_r(n)$ l'un des S_r réalisant la condition de minimalité au rang n et $R_r(n) = \{n_1, \dots, n_r\} = \{0, \dots, n-1\} \setminus S_r(n)$ les indices des éléments étudiés correspondants.

Lorsqu'on se donne une suite (P, r) -ordonnée, on considère qu'on se donne implicitement des $S_r(n)$ et $R_r(n)$ pour tout n .

Contrairement aux suites P -ordonnées, un élément donné de E peut apparaître plusieurs fois dans une suite (P, r) -ordonnée. Il ne peut en revanche pas apparaître plus de $(r + 1)$ fois.

On a alors le même théorème d'indépendance que pour les suite P -ordonnée

Théorème 3.1. La P -séquence associée à une suite (P, r) -ordonnée δ_r de E ne dépend pas de δ_r .

La preuve du Théorème 3.1 sera donnée à la fin de la prochaine section.

3.3 Base régulière dans le cas local

Dans cette section, sauf mention du contraire, D est local. On montre que dans ce cas $\text{Int}_n^r(E, D)$ admet toujours une base régulière. Ce résultat permet ensuite de démontrer le Théorème 3.1.

Soit $\delta_r = (a_n)_n$ une suite (π, r) -ordonnée de E . On pose pour tout n

$$n!_{(\delta_r, E)}^r = \prod_{i \in S_r(n)} (a_n - a_i)$$

Définition 3.4. Pour tout $n \geq 0$, on définit le n -ème polynôme binomial associé à E et δ_r par $\binom{X}{0}_{\delta_r, E} = 1$ et pour $n \geq 1$

$$\binom{X}{n}_{\delta_r, E} = \frac{(X - a_0)(X - a_1) \dots (X - a_{n-1})}{n!_{(\delta_r, E)}^r}$$

Il n'est pas clair a priori que $\binom{X}{n}_{\delta_r, E} \in \text{Int}_n^r(E, D)$.

Pour le montrer, on aura besoin du lemme combinatoire suivant qui exprime pour tout (b_0, \dots, b_m) éléments de E la m -ème différence divisée $\phi^m f(b_0, \dots, b_m)$ d'un polynôme $f = (X - a_0) \dots (X - a_n)$ comme une somme de produits de la forme

$$\prod_{i \in I, j \in J} (b_j - a_i)$$

où I et J sont des sous-ensemble de $\{0, \dots, n-1\}$ de cardinal $n-m$.

L'objectif du lemme est de construire I et J de sorte que, à défaut d'avoir un terme constant pour les b_j , on puisse minorer la valuation de chaque produit par la valuation d'un produit de la forme

$$\prod_{i \in I} (b_k - a_i)$$

pour un certain k et cela pour venir attraper la propriété de minimalité que possède par construction la suite (P, r) -ordonnée $(a_n)_n$.

Notation 3.1. Soient (a_0, \dots, a_{n-1}) et (b_0, \dots, b_m) des éléments de E .

A toute suite $\mathbf{i} = (i_1, \dots, i_m)$ de la forme $0 \leq i_1 < i_2 < \dots < i_m < n$, on associe une suite $(s_i(k))_{0 \leq k \leq n-1}$ définie de la manière suivante.

Pour tout k , soit

$$I_k = \{0, \dots, m\} \setminus \{s_i(i_j) : i_j < k\}$$

Alors $s_i(k)$ est définie comme le plus petit élément de I_k qui maximise la quantité $v_\pi(b_{s_i(k)} - a_k)$.

Pour tout $\mathbf{i} = \{i_1, \dots, i_m\}$, l'ensemble $\{0, \dots, m\} \setminus \mathbf{i}$ est réduit à un élément que l'on note naturellement $s_i(n)$.

Remarque 3.3. La suite s_i est construite de sorte que

$$v_\pi(b_{s_i(k)} - a_k) \geq v_\pi(b_{s_i(n)} - a_k)$$

On en vient au lemme annoncé

Lemme 3.1. Avec les notations précédentes, on a

$$\phi^m f(b_0, \dots, b_m) = \sum_{\mathbf{i}} \left(\prod_{k \in \{0, \dots, n-1\} \setminus \mathbf{i}} (b_{s_i(k)} - a_k) \right) \quad (1)$$

Preuve. La preuve se fait par récurrence sur $m+n$.

Si $m+n=0$, l'énoncé se résume à $f=f$. En fait, le lemme est même trivialement vraie pour $m=0$ et n quelconque.

Soit $t > 0$. Supposons que le lemme soit vraie pour tout $m+n < t$ et soient m, n tels que $m+n=t$. Si $n > 1$, on pose $f_0(x) = \frac{f(x)}{x-a_0}$, $f_0(x) = 0$ sinon.

On a le lemme intermédiaire suivant

Lemme 3.2.

$$\begin{aligned} \phi^m f(b_0, \dots, b_m) = \\ (b_{s_i(0)} - a_0) \phi^m f_0(b_0, \dots, b_m) + \phi^{m-1} f(b_0, \dots, \widehat{b_{s_i(0)}}, \dots, b_m) \end{aligned}$$

Preuve. Une récurrence sur m pour f fixé permet immédiatement de conclure. \square

L'hypothèse de récurrence s'applique à $\phi^m f_0(b_0, \dots, b_m)$ et à $\phi^m f(b_0, \dots, \widehat{b_{s_i(0)}}, \dots, b_m)$. Le premier terme correspond aux \mathbf{i} tels que $i_1 = 0$ dans (1), tandis que le second correspond aux \mathbf{i} tels que $i_1 \neq 0$. Ceci achève la preuve. \square

On est en mesure de montrer que les $\binom{X}{n}_{\delta_r, E}$ sont à valeurs entières

Théorème 3.2. *Pout tout n*

$$\binom{X}{n}_{\delta_r, E} \in \text{Int}_n^r(E, D)$$

Preuve. Soient a_0, a_1, \dots, a_{n-1} les n premiers termes d'une suite (P, r) -ordonnée δ_r de E et b_0, \dots, b_m des éléments quelconques de E , $m \leq r$.

Pour tout $\mathbf{i} = (i_1, \dots, i_m)$ comme dans le Lemme 3.1, on a:

$$\begin{aligned} v_\pi \left(\prod_{k \in \{0, \dots, n-1\} \setminus \mathbf{i}} (b_{s_i(k)} - a_k) \right) &\geq v_\pi \left(\prod_{k \in \{0, \dots, n-1\} \setminus \mathbf{i}} (b_{s_i(n)} - a_k) \right) \geq v_\pi \left(\prod_{k \in \{0, \dots, n-1\} \setminus R_r(n)} (a_n - a_k) \right) \\ &= v_\pi \left(n!_{(\delta_r, E)}^r \right) \end{aligned}$$

Ainsi pour tout $m \leq r$, la m -ème différence divisée de $\binom{X}{n}_{\delta_r, E}$ est somme de termes qui sont dans D , donc est à valeurs entières. Ceci montre que $\binom{X}{n}_{\delta_r, E} \in \text{Int}_n^r(E, D)$. \square

Théorème 3.3. *La famille $\left(\binom{X}{k}_{\delta_r, E} \right)_{0 \leq k \leq n}$ est une base régulière de $\text{Int}_n^r(E, D)$.*

Preuve. Soit $f \in \text{Int}_n^r(E, D)$ de degré n et

$$f = \sum_{k=0}^n c_k \binom{X}{k}_{\delta_r, E}$$

sa décomposition sur la K -base $\left(\binom{X}{k}_{\delta_r, E} \right)_{0 \leq k \leq n}$. On souhaite montrer que les c_k sont dans D .

Par l'absurde, soit j le plus petit indice tel que $c_j \notin D$.

On rappelle que $R(j, r) = \{j_1, \dots, j_r\}$ est l'ensemble des indices des éléments étudiés pour réaliser le minimum à la j -ème étape du processus de construction de δ_r .

L'idée est de calculer $\phi^r f(a_{j_1}, \dots, a_{j_r}, a_j)$.

- Si $k > j$, on a immédiatement

$$\phi^r \left(c_k \binom{X}{k}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_r}, a_j) = 0$$

En effet, par définition de $\binom{X}{k}_{\delta_r, E}$, $\binom{X}{k}_{\delta_r, E}(a_{j_i}) = 0$ pour tout j_i et $\binom{X}{k}_{\delta_r, E}(a_j) = 0$ aussi.

- Si $k < j$, on a

$$\phi^r \left(c_k \binom{X}{k}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_r}, a_j) \in D$$

En effet, $c_k \binom{X}{k}_{\delta_r, E}(x) \in D$ pour tout $x \in E$ par définition de j .

- On a

$$\phi^r \left(c_j \binom{X}{j}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_r}, a_j) = \frac{\phi^{r-1} \left(c_j \binom{X}{j}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_{r-1}}, a_j)}{a_j - a_{j_r}}$$

En itérant, on obtient

$$\begin{aligned} \phi^r \left(c_j \binom{X}{j}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_r}, a_j) &= c_j \frac{\binom{X}{j}_{\delta_r, E}(a_j)}{\prod_{k \in R(j, r)} (a_j - a_k)} = c_j \frac{(a_j - a_0) \dots (a_j - a_{j-1})}{\prod_{k \in R(j, r) \cup S(j, r)} (a_j - a_k)} \\ &= c_j \frac{(a_j - a_0) \dots (a_j - a_{j-1})}{(a_j - a_0) \dots (a_j - a_{j-1})} \\ &= c_j \end{aligned}$$

Finalement

$$c_j = \left(\phi^r f(a_{j_1}, \dots, a_{j_r}, a_j) - \sum_{k=0}^{j-1} \phi^r \left(c_j \binom{X}{k}_{\delta_r, E} \right) (a_{j_1}, \dots, a_{j_r}, a_j) \right) \in D$$

contradiction. \square

Corolaire 3.1. *La π -séquence associée à une suite (π, r) -ordonnée δ_r de E ne dépend pas de δ_r .*

Preuve. Le Théorème 3.3 implique que l'idéal fractionnaire formé par zéro et l'ensemble des coefficients dominants des éléments de $\text{Int}_n^r(D, E)$ de degré n est

$$\left(n!_{(\delta_r, E)}^r \right)^{-1} D$$

et cela pour toute suite (π, r) -ordonnée δ_r de E . Ainsi l'entier $v_\pi(n!_{\delta_r, E}^r)$ ne dépend pas de δ_r et par conséquent la π -séquence associée à δ_r non plus. \square

Remarque 3.4. *On a donc $n!_{(\delta_r, E)}^r D = n!_{(\delta'_r, E)}^r D$ pour tout δ_r, δ'_r . On peut donc noter simplement $n!_E^r D$.*

Notation 3.2. *On appelle fonction factorielle associée à E et r la fonction*

$$n \rightarrow n!_E^r = n!_E^r D$$

Le Théorème 3.1 est conséquence immédiate du Corolaire 3.1:

Preuve du Théorème 3.1. Soit D quelconque, D_P le localisé de D en P , et δ_r une suite (P, r) -ordonnée de E . La suite δ_r est aussi une suite (π, r) -ordonnée de $E \subset D_P$ et les exposants dans la π -séquence associée à δ_r sont les même que dans la P -séquence associée à δ_r . On applique alors le Corolaire 3.1. \square

3.4 Base régulière

D est quelconque (plus nécessairement local).

Dans cette section, on énonce une condition nécessaire et suffisante pour que $\text{Int}_n^r(E, D)$ admette une base régulière et lorsque c'est le cas, on présente un algorithme qui construit une telle base à partir de suites (P, r) -ordonnée pour un nombre fini de P à l'aide du théorème chinois.

Le procédé, les preuves et l'algorithme sont en tout point similaires à ceux utilisés dans la partie précédente pour $\text{Int}_n(E, D)$ et les suites P -ordonnée.

Définition 3.5. Pour tout n , on définit $\mathfrak{J}_n^r(E, D)$ comme l'ensemble formé de zéro et des coefficients dominants des éléments de $\text{Int}_n^r(E, D)$ de degré n .

Proposition 3.2. $\mathfrak{J}_n^r(E, D)$ est un idéal fractionnaire.

Preuve. Identique à la preuve de la Proposition 2.1 pour $\mathfrak{J}_n(E, D)$. \square

Théorème 3.4. $\text{Int}_n^r(E, D)$ possède une base régulière si et seulement si les idéaux fractionnaires $\mathfrak{J}_k^r(E, D)_{k \leq n}$ sont principaux.

Preuve. Identique à la preuve du Théorème 2.3 pour $\text{Int}_n(E, D)$. \square

Proposition 3.3 (Localisation).

$$\text{Int}_n^r(E, D_P) = \text{Int}_n^r(E, D)_P$$

Preuve. Soit $f \in \text{Int}_n^r(E, D)_P$. Pour tout $k \leq r$ et tout $x_0, \dots, x_k \in E$, on a $\phi^k f(x_0, \dots, x_k) \in D_P$ puisque $f(x_i) \in D_P$ d'après la Proposition 2.2.

Réciproquement, soit $f \in \text{Int}_n^r(E, D_P)$ et soit I le D -module engendré par ses coefficients. Pour tout $k \leq r$ et tout $x_0, \dots, x_k \in E$, $\phi^k f(x_0, \dots, x_k) \in I \cap D_P$. Puisque D est Noétherien, il existe $s \in D \setminus P$ tel que $s\phi^k f(x_0, \dots, x_k) \in D$, et donc $f \in \text{Int}_n^r(E, D)_P$. \square

Corolaire 3.2. Soit $n!_{E_P}^r$ la factoriel associée à $E \subset D_P$. On a $n!_{E_P}^r = D$ sauf pour un nombre fini de P

Preuve. $n!_{E_P}^r \neq D$ pour les P qui divisent $\mathfrak{J}_n^r(E, D)^{-1}$ qui sont en nombre fini. \square

La Proposition 3.3 permet naturellement d'étendre la fonction factorielle définie dans le cas local à D quelconque:

Définition 3.6. On appelle fonction factoriel associée à E et r la fonction

$$n \rightarrow n!_E^r = \mathfrak{J}_n^r(E, D)^{-1} = \prod_{(P, \pi)} P^{v_\pi(n!_{E_P}^r)}$$

On présente maintenant un algorithme pour construire un polynôme $A_n \in D[X]$ de degré n tel que $A_n(D) \subset n!_E^r$.

Soient $n \in \mathbb{N}$ et $\{P_1, P_2, \dots, P_m\}$ les premiers qui divisent $n!_E^r$. Pour tout $1 \leq i \leq m$ soit $(u_{i,k})_{0 \leq k < n}$ les n premiers termes d'une suite (P_i, r) -ordonnée de E . On note également $e_{i,n} = v_{P_i}(n!_E^r)$.

Algorithme 3.1.

1. Pour tout $0 \leq k < n$, on construit à l'aide du théorème chinois un élément a_k vérifiant pour tout $1 \leq i \leq m$:

$$a_k \equiv u_{i,k} \pmod{P_i^{e_{i,n}+1}}$$

2. On retourne le polynôme $A_n = (X - a_0)(X - a_1) \dots (X - a_{n-1})$.

La suite $(a_k)_{k \leq n}$ est construite afin d'être (P_i, r) -ordonnée simultanément pour tout les $P_i \in \{P_1, P_2, \dots, P_m\}$.

Théorème 3.5. *On a $A_n(E) \subset n!_E^r$.*

Preuve. Soit $x \in E$. Il suffit de montrer que $v_P(A_n(x)) \geq v_P(n!_E^r)$ pour tout P . Si $P \notin \{P_1, P_2, \dots, P_m\}$, $v_P(n!_E^r) = 0$. On peut donc se restreindre à $P_i \in \{P_1, P_2, \dots, P_m\}$. Mais alors par construction

$$\begin{aligned} v_{P_i}(A_n(x)) &= \sum_{k=0}^{n-1} v_{P_i}(x - a_k) \geq \sum_{k \in S(n,r)} v_{P_i}(x - a_k) \\ &\geq \sum_{k \in S(n,r)} v_{P_i}(a_n - a_k) \quad \left(= \sum_{k \in S(n,r)} v_{P_i}(u_{i,n} - u_{i,k}) \right) \\ &= v_{P_i}(n!_E^r) \end{aligned}$$

□

Pour que $\text{Int}_n^r(E, D)$ admette une base régulière, il est nécessaire que les idéaux $k!_E^r$ pour $k \leq n$ soient principaux. On suppose donc que c'est le cas et on note β_k un générateur de $k!_E^r$.

Soit $(A_k)_{0 \leq k \leq n}$ des polynômes de $D[X]$ tels que $A_k(D) \subset k!_D^r$. On pose $B_k = \frac{1}{\beta} A_k$.

Théorème 3.6. *La famille $\{B_0, B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n^r(E, D)$*

Preuve. Pour tout k , B_k est un polynôme de $\text{Int}_n^r(E, D)$ de degré k et de coefficient dominant β_k par construction. D'après la preuve du Théorème 3.4, $\{B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n^r(E, D)$. □

3.5 Calcul effectif pour $E=D$

Pour construire en utilisant les résultats de la section précédente une base régulière de $\text{Int}_n^r(E, D)$ lorsque les $(k!_E^r)_{k \leq n}$ sont principaux, on a besoin de savoir:

1. déterminer les idéaux premiers qui divisent $n!_E^r$
2. construire les n premiers termes d'une suite (P, r) -ordonnée de E

Réaliser le deuxième point demande si on applique la définition d'une suite (P, r) -ordonnée de E de prendre un minimum sur un ensemble infini, ce qui n'est pas réalisable tel quel.

Cependant, dans le cas où $E = D$ et où D/P est de cardinal fini pour tout P , il est possible de construire effectivement les n premiers termes d'une suite (P, r) -ordonnée de D en utilisant la finitude de D/P et l'homogénéité de D . On peut également en déduire les idéaux qui divisent $n!_D^r$.

On montre en fait que les n termes produits par l'Algorithme 2.2 servant à construire une suite P -ordonnée de D forment aussi les n premiers termes d'une suite (P, r) -ordonnée de D et cela pour tout r !

Dans cette partie, D/P est de cardinal fini pour tout P .

3.5.1 Construction d'une suite (P, r) -ordonnée de D

On propose un algorithme pour construire les n premiers termes d'une suite (P, r) -ordonnée de D . On utilise de manière cruciale le fait que D est réunion disjointe finie des différentes classes modulo P . On généralise notamment aux entiers d'un corps de nombres certains théorèmes donnés pour \mathbb{Z} dans [Joh10]. Le cardinal de D/P est noté q .

Soit $\{r_0, r_1, \dots, r_{q-1}\}$ un système de représentants modulo P . On note $D_{r_i} = \{x \in D : x \equiv r_i \pmod{P}\}$.

On montre que les D_{r_i} ont tous la même P -séquence.

Proposition 3.4. *Pour tout r_i, r_j et $n \geq 0$:*

$$v_P(n!_{D_{r_i}}^r) = v_P(n!_{D_{r_j}}^r)$$

Autrement dit les P -séquences associées aux suites (P, r) -ordonnées des D_{r_i} sont les mêmes.

Preuve. Soit $c \in D$ tel que $D_{r_i} + c = D_{r_j}$. Soit $(a_n)_n$ une suite (P, r) -ordonnée de D_{r_i} . Pour tout n, m

$$v_P((a_n - c) + (a_m - c)) = v_P(a_n - a_m)$$

Ainsi $(a_n - c)_n$ est une suite (P, r) -ordonnée de D_{r_j} et $v_P(n!_{D_{r_i}}^r) = v_P(n!_{D_{r_j}}^r)$ □

Proposition 3.5. *L'application $\theta_i : x \rightarrow x\pi + r_i$ envoie une suite (P, r) -ordonnée de D sur une suite (P, r) -ordonnée de D_{r_i} .*

Preuve. Soit $(a_n)_n$ une suite (P, r) -ordonnée de D . Pour tout $x, y \in D$

$$v_P(\theta(x) - \theta(y)) = v_P(\pi(x - y)) = 1 + v_P(x - y)$$

Par récurrence sur $n \geq r + 1$, le minimum à la n -ème étape de construction d'une suite (P, r) -ordonnée de D_{r_i} est donc atteint pour $\theta(a_n)$ ce qui fait de $(\theta(a_n))_n$ une suite (P, r) -ordonnée de D_{r_i} . □

Corolaire 3.3. *Pour tout $0 \leq i < q$ et pour $n \geq r + 1$*

$$v_P(n!_{D_{r_i}}^r) = v_P(n!_D^r) + n - r$$

Preuve.

$$\begin{aligned} v_P(n!_{D_{r_i}}^r) &= \sum_{k \in S_r(n)} (v_P(\theta(a_n) - \theta(a_k))) \\ &= \sum_{k \in S_r(n)} (v_P(a_n - a_k) + 1) = v_P(n!_D^r) + n - r \end{aligned}$$

□

On cherche désormais à construire une suite (P, r) -ordonnée de D à partir de suites (P, r) -ordonnées des D_{r_i} . On rappelle que la notion d'entrelacement de suites a été introduite dans la Définition 2.7.

On montre que l'entrelacement q -uniforme de suites (P, r) -ordonnées des D_{r_i} résulte en une suite (P, r) -ordonnée de D .

Proposition 3.6. Pour tout $0 \leq i < q$ et tout $n \in \mathbb{N}$ soit

$$\phi_i(n) = nq + i$$

La suite obtenue par $(\phi_i)_{0 \leq i < q}$ entrelacement de suites (P, r) -ordonnée des D_{r_i} est une suite (P, r) -ordonnée de D .

Preuve. Identique à la preuve de la Proposition 2.5 pour les suites P -ordonnée. \square

Corolaire 3.4. Pour $n \geq q(r+1)$

$$v_P(n!_D^r) = v_P(\lfloor n/q \rfloor!_D^r) + \lfloor n/q \rfloor - r$$

Preuve. Remarquons d'abord que $n \geq q(r+1)$ implique $\lfloor n/q \rfloor \geq r+1$.

Soit $(a_n)_n$ la suite obtenue par $(\phi_i)_{1 \leq i < q}$ entrelacement de suites (P, r) -ordonnée des D_{r_i} . Par définition des ϕ_i , a_n est le $\lfloor n/q \rfloor$ -ème terme d'une suite (P, r) -ordonnée de l'un des $D_{r_i} = D_{r_{i_0}}$. Puisque $v_P(a_n - a_k) = 0$ dès que $a_k \notin D_{r_{i_0}}$, on a

$$v_P(n!_D^r) = v_P(\lfloor n/q \rfloor!_{D_{r_{i_0}}}^r)$$

On peut alors appliquer le Corolaire 3.3 puisque $\lfloor n/q \rfloor \geq r+1$. \square

Théorème 3.7. Pour tout $n \geq 0$ on a

$$v_P(n!_D^r) = \sum_{i=1}^k \lfloor n/q^i \rfloor - kr$$

où $k = \lfloor \log_q(n/(r+1)) \rfloor$.

Preuve. Pour $n < q(r+1)$, la formule est trivialement vraie.

Rappelons la formule du Corolaire 3.4 valable pour $n \geq q(r+1)$

$$v_P(n!_D^r) = v_P(\lfloor n/q \rfloor!_D^r) + \lfloor n/q \rfloor - r$$

On peut itérer cette relation pour obtenir

$$v_P(n!_D^r) = v_P(\lfloor n/q^j \rfloor!_D^r) + \sum_{i=1}^j \lfloor n/q^i \rfloor - jr$$

et cela tant que $n/q^{j-1} \geq q(r+1)$. La dernière valeur de j pour laquelle on peut appliquer le Corolaire 3.4 est donc $j = \lfloor \log_q(n/(r+1)) \rfloor - 1$. Le résultat suit puisqu' alors $v_P(\lfloor n/q^j \rfloor!_D^r) = 0$. \square

Définition 3.7. Soit $k = \lfloor \log_q(n/(r+1)) \rfloor$. Pour $n < q(r+1)$, on pose $w_{q,r}(n) = 0$ et pour $n \geq q(r+1)$

$$w_{q,r}(n) = v_P(n!_D^r) = w_q(n) - w_q(\lfloor n/q^k \rfloor) - kr$$

Corolaire 3.5. Pour tout $q \geq 2$ soit M_q le produit des idéaux premiers de D de norme q . On a

$$n!_D^r = \prod_{(P,q)} P^{w_{q,r}(n)} = \prod_{q=2}^n M_q^{w_{q,r}(n)}$$

Preuve. $v_P(n!_D^r) = w_{q,r}(n)$ ne dépend que du cardinal q de D/P et $w_{q,r}(n) = 0$ dès que $q > n$. \square

Les Proposition 3.5 et Proposition 3.6 impliquent que l'Algorithme 2.2 servant à construire une suite P -ordonnée de D peut être utilisé pour construire les n premiers termes d'une suite (P, r) -ordonnée de D à condition de prendre pour q premiers termes à l'étape 1) les q premiers termes d'une suite (P, r) -ordonnée de D . Mais il est immédiat que les q premiers termes $(r_0, r_1, \dots, r_{q-1})$ utilisés dans l'algorithme sont aussi les q premiers termes d'une suite (P, r) -ordonnée de D quelque soit r . En conséquence:

Théorème 3.8. *La suite P -ordonnée de D produite par l'Algorithme 2.2 est aussi une suite (P, r) -ordonnée de D pour tout $r \geq 0$.*

3.5.2 Algorithme pour $\text{Int}_n^r(D)$

On résume maintenant la procédure pour construire lorsque les $(k!_D^r)_{k \leq n}$ sont principaux une base régulière de $\text{Int}_n^r(D)$:

1. On détermine les idéaux premiers T_k qui divisent $k!_D^r$ pour $k \leq n$. D'après le Corolaire 3.5, ce sont tout les idéaux premiers de norme $q \leq k$. On calcul également pour tout $q \leq n$ le produit M_q des idéaux premiers de norme q .

Pour cela, on utilise les méthodes standards pour factoriser les premiers $p \leq n$ dans D .

2. On construit pour chaque $P \in \cup_{k \leq n} T_k$ les $n+1$ premiers termes d'une suite (P, r) -ordonnée de D en utilisant l'Algorithme 2.2.
3. Pour chaque $k \leq n$ on utilise l'Algorithme 3.1 pour construire le polynôme A_k tel que $A_k(D) \subset n!_D^r$. On utilise pour cela les $k+1$ premiers termes des suites (P, r) -ordonnée pour $P \in T_k$ construites à l'étape 2).
4. On calcul ensuite pour chaque $0 \leq k \leq n$ l'idéal $k!_D^r$ par la formule du Corolaire 3.5. On utilise alors les M_q calculés à l'étape 1).
5. Pour tout $k \leq n$, on calcul un générateur β_k de $k!_D^r$ par les méthodes standards puis $B_k = \frac{1}{\beta_k} A_k$.

La famille (B_0, B_1, \dots, B_k) ainsi construite est une base régulière de $\text{Int}_n^r(D)$.

3.5.3 Exemples

Exemple 1

Soit $K = \mathbb{Q}[i]$. L'anneau des entiers $\mathbb{Z}[i]$ est principal, donc $\text{Int}_n^r(\mathbb{Z}[i])$ admet une base régulière pour tout n et r .

Voici une base régulière de $\text{Int}_6^1(\mathbb{Z}[i])$:

$$\begin{aligned} B_0(X) &= 1, \quad B_1(X) = X, \quad B_2(X) = X^2 + X, \quad B_3(X) = X^3 + 2X^2 + X \\ B_4(X) &= \frac{1-i}{2}X^4 + (1-i)X^3 + \frac{1-i}{2}X^2 \\ B_5(X) &= \frac{1-i}{2}X^5 + (2+3i)X^4 - \frac{27+13i}{2}X^3 + (19-i)X^2 - (8+2i)X \end{aligned}$$

$$B_6(X) = \frac{1}{2}X^6 + \frac{1-20i}{2}X^5 - \frac{159+10i}{2}X^4 + \frac{-1+600i}{2}X^3 + (485-140i)X^2 - (406+145i)X$$

Soit $f \in \text{Int}_6^1(\mathbb{Z}[i])$ le polynôme dont les coordonnées sur la base $(B_i(X))_{i \leq 6}$ sont:

$$\begin{pmatrix} 1+i \\ 0 \\ 2-i \\ 3+5i \\ -2 \\ i \\ 1 \end{pmatrix}$$

et soit $g(x, y) = \phi^1 f(x, y)$ la première différence divisée de f .

Puisque $f \in \text{Int}_6^1(\mathbb{Z}[i])$, on a $g(x, a) \in \text{Int}_5(\mathbb{Z}[i])$ quelque soit $a \in \mathbb{Z}[i]$. Soit R la base régulière de $\text{Int}_5(\mathbb{Z}[i])$ construite dans l'exemple 1. de la partie 2. Dans le tableau suivant, on donne pour quelques valeurs de a la décomposition du polynôme $g(a, x)$ sur la base R :

a	0	i	$1+i$
$(g(a, x))_R$	$\begin{pmatrix} -399 - 149i \\ 55093 - 3153i \\ 629966 - 21543i \\ -442 - 1847i \\ -19 - 57i \\ 5 + 5i \end{pmatrix}$	$\begin{pmatrix} -296 + 118i \\ 54881 - 3073i \\ -29897 - 21639i \\ -435 - 1838i \\ -20 - 56i \\ 5 + 5i \end{pmatrix}$	$\begin{pmatrix} -224 + 113i \\ 54895 - 2926i \\ 629975 - 21707i \\ -426 - 1844i \\ -19 - 55i \\ 5 + 5i \end{pmatrix}$

Table 1: Les coordonnées de $g(a, x)$ sur la base R en fonction de a

Exemple 2

Soit $K = \mathbb{Q}(j)$. On donne dans le tableau suivant les 15 premiers termes d'une suite $((2), r)$ -ordonnée ainsi que les exposants de la (2) -séquence associée pour $0 \leq r \leq 2$:

r	Suite $((2), r)$ -ordonnée et exposants
0	$(0, 1, j, j + 1, 2, 3, 2 + j, 3 + j, 2j, 1 + 2j, 3j, 1 + 3j, 2 + 2j, 3 + 2j, 2 + 3j)$
	$(0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3)$
1	$(0, 2, 1, 3, j, 2 + j, 1 + j, 3 + j, 2, 3, 2 + j, 3 + j, 2j, 1 + 2j, 3j)$
	$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2)$
2	$(0, 2, 2j, 1 + j, 1 + j, 1 + j, 1, 3, 1 + 2j, j, 2 + j, 3j, 3 + j, 2, 3)$
	$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$

Table 2: Suites $((2), r)$ -ordonnée pour $r = 0, 1, 2$

3.5.4 Fonctions pour $\text{Int}_n^r(D)$

Voici quelques fonctions utiles:

- la fonction `ispolyaupto_rem(K, r, n)` teste si $\text{Int}_n^r(D)$ admet une base régulière
- la fonction `zkremregbasis(K, r, n, "X")` retourne (si possible) une base régulière (d'indéterminée "X") de $\text{Int}_n^r(D)$.
- la fonction `zkremregbasis_dec(K, pol, 1, "X")` retourne une matrice $(n + 1) \times 2$ (où $n = \deg(\text{pol})$) avec une base régulière de $\text{Int}_n^r(D)$ (d'indéterminée "X") dans la deuxième colonne et les coefficients de la K -décomposition de `pol` sur cette base dans la première.

4 Base régulière du sous-module $\text{Int}_n^M(E, D)$

Dans cette section, on présente un sous-module de $\text{Int}_n(E, D)$ qui dépend d'un nouveau paramètre M (un idéal) ainsi qu'une nouvelle notion de suite ordonnée associée ([Bha09]) qui permet d'appliquer la même stratégie que dans la partie 2.

On donnera une condition nécessaire et suffisante pour que ce sous-module admette une base régulière, puis un algorithme de construction d'une telle base quand elle existe. On fournira plusieurs exemples concrets en fin de partie.

Dans toute cette partie, h est un entier positif.

4.1 Le sous-module $\text{Int}_n^M(E, D)$

Soit $f \in \text{Int}_n(E, D)$. Même si $f \notin D[X]$, on peut se demander quels sont les $m \in D$ pour lesquels le polynôme composé $f(mX + e) \in D[X]$ pour tout $e \in E$. Si m est tel que $f(mX + e) \in D[X]$, on a $f(m'X + e) \in D[X]$ pour tout m' dans l'idéal mD .

Ceci amène la définition suivante:

Définition 4.1. Soit M un idéal de D . On dit que $f \in \text{Int}_n(E, D)$ est de module M si $f(mX + e) \in D[X]$ pour tout $m \in M$ et $e \in E$.

On note $\text{Int}_n^M(E, D)$ l'ensemble des éléments de $\text{Int}_n(E, D)$ de module M . C'est un sous-module de $\text{Int}_n(E, D)$. On a $\text{Int}_n^{(0)}(E, D) = \text{Int}_n(E, D)$.

4.2 Suite P^h -ordonnée

On définit dans cette section une nouvelle notion de suite ordonnée d'éléments de E qui à vocation à jouer le même rôle pour $\text{Int}_n^M(E, D)$ qu'une suite P -ordonnée pour $\text{Int}_n(E, D)$.

Formellement, se donner un module $M = \prod_i P_i^{h_i}$ revient à associer à chaque P un entier h . La notion de suite P^h -ordonnée que l'on décrit ici est une légère variation de la notion de suite P -ordonnée où l'on souhaite garder un contrôle (dicté par h) sur la décroissance de la P -séquence associée.

Définition 4.2. On appelle suite P^h -ordonnée de E toute suite $(a_n)_{n \geq 0}$ d'éléments de E telle que pour tout $n \geq 1$, a_n vérifie:

$$\min_{x \in E} \left(\sum_{i=0}^{n-1} \min(h, v_P(x - a_i)) \right) = \sum_{i=0}^{n-1} \min(h, v_P(a_n - a_i)) = e_n$$

On appelle P -séquence associée à la suite P^h -ordonnée $(a_n)_{n \geq 0}$ la suite décroissante d'idéaux $(P^{e_0}, P^{e_1}, P^{e_2}, P^{e_3}, \dots)$.

Remarque 4.1. Pour tout $x, y \in D$, $\min(h, v_P(x + \pi^h - y)) = \min(h, v_P(x - y))$.

En conséquence, si $(a_n)_n$ est une suite P^h -ordonnée de E et que l'on remplace a_n par un a_m tel que $a_n \equiv a_m \pmod{P^h}$, la suite obtenue est encore une suite P^h -ordonnée de E .

A partir d'une suite P^h -ordonnée de E , on peut construire une suite P^h -ordonnée de E telle que l'ensemble des termes de la suite qui sont dans la même classe modulo P^h est réduit à un unique élément. Il suffit de remplacer chaque a_n par l'élément a_m de plus petit indice m tel que $a_m \equiv a_n \pmod{P^h}$.

Définition 4.3. Soit $(a_n)_n$ une suite P^h -ordonnée de E . Si pour toute classe C modulo P^h l'ensemble des termes de la suite qui sont dans C est vide ou réduit à un élément, on dit que la suite est restreinte.

Il existe toujours une suite P^h -ordonnée restreinte.

Finalement on a le même théorème d'indépendance que pour les suite P -ordonnée

Théorème 4.1. La P -séquence associée à une suite P^h -ordonnée δ^h de E ne dépend pas de δ^h .

La preuve du Théorème 4.1 sera donnée à la fin de la prochaine section.

4.3 Base régulière dans le cas local

Dans cette section, sauf mention du contraire, D est local. Se donner un module M revient donc à se donner un entier h tel que $M = (\pi^h)$. On montre que dans ce cas $\text{Int}_n^{\pi^h}(E, D)$ admet toujours une base régulière. Ce résultat permet ensuite de démontrer le Théorème 4.1.

Soit $\delta^h = (a_n)_n$ une suite π^h -ordonnée de E . On pose pour tout n

$$n!_{(\delta^h, E)}^h = \pi^{\sum_{i=0}^{n-1} \min(h, v_\pi(a_n - a_i))}$$

Définition 4.4. Pour tout $n \geq 0$, on définit le n -ème polynôme binomial associé à E et δ^h par $\binom{X}{0}_{\delta^h, E}^h = 1$ et pour $n \geq 1$

$$\binom{X}{n}_{\delta^h, E}^h = \frac{(X - a_0)(X - a_1) \dots (X - a_{n-1})}{n!_{(\delta^h, E)}^h}$$

Par construction, $\binom{X}{n}_{\delta^h, E}^h \in \text{Int}_n(E, D)$.

Théorème 4.2. Pour tout $n \geq 0$, $\binom{X}{n}_{\delta^h, E}^h \in \text{Int}_n^{\pi^h}(E, D)$.

Preuve. Soit $e \in E$. Si on développe le polynôme

$$(\pi^h X + (e - a_0))(\pi^h X + (e - a_1)) \dots (\pi^h X + (e - a_{n-1}))$$

les relations coefficients-racines montrent que la π -valuation de chaque coefficient est supérieur à

$$\sum_{i=0}^{n-1} \min(h, v_P(e - a_i))$$

On déduit que la valuation de chaque coefficient de $\binom{\pi^h X + e}{n}_{\delta^h, E}^h$ est supérieur à

$$\sum_{i=0}^{n-1} \min(h, v_\pi(e - a_i)) - \sum_{i=0}^{n-1} \min(h, v_\pi(a_n - a_i))$$

qui est positif car $(a_n)_n$ est une suite π^h -ordonnée de E . Ceci montre que $\binom{\pi^h X + e}{n}_{\delta^h, E}^h \in D[X]$, et donc $\binom{X}{n}_{\delta^h, E}^h \in \text{Int}_n^{\pi^h}(E, D)$. \square

Théorème 4.3. La famille $\left(\binom{X}{k}_{\delta^h, E}\right)_{0 \leq k \leq n}$ est une base régulière de $\text{Int}_n^{\pi^h}(E, D)$.

Preuve. On montre d'abord le théorème lorsque la suite $(a_n)_n$ est restreinte.

Soit $f \in \text{Int}_n^{\pi^h}$ et $f = \sum_{k=0}^n c_k \binom{X}{k}_{\delta^h, E} = \sum_{k=0}^n c_k f_k(X)$ la décomposition de f sur la K -base

$$\left(\binom{X}{k}_{\delta^h, E}\right)_{0 \leq k \leq n}$$

On veut montrer que les c_k sont dans D . Par l'absurde, soit j le plus petit indice tel que $c_j \notin D$ et soit s le nombre d'indices $i \in \{0, \dots, j-1\}$ tels que $a_j = a_i$. L'idée est de regarder le coefficient de X^s dans $c_j f_j(\pi^h X + a_j)$. On regarde pour cela le coefficient de X^s pour chacun des $c_k f_k(\pi^h X + a_j)$, $k \neq j$.

- si $n \geq k > j$, le coefficient de X^s dans $c_k f_k(\pi^h X + a_j)$ est nul par définition de s (on utilise donc ici le fait que la suite est restreinte)
- si $k < j$, le coefficient de X^s dans $c_k f_k(\pi^h X + a_j)$ est dans D puisque $c_k \in D$ (par minimalité de j) et $f_k(\pi^h X + a_j) \in D[X]$.

Puisque le coefficient de X^s dans $f(\pi^h X + a_j)$ est dans D et que le coefficient de X^s dans $c_k f_k(\pi^h X + a_j)$ pour $k \neq j$ est dans D , le coefficient de X^s dans $c_j f_j(\pi^h X + a_j)$ est aussi dans D .

Enfin, $v_\pi(f_j(\pi^h X + a_j)) = 0$ et donc $c_j \in D$, contradiction.

On démontre maintenant le théorème pour une suite π^h -ordonnée quelconque δ^h . On se donne δ_0^h une suite π^h -ordonnée restreinte et

$$(C_k(X))_{0 \leq k \leq n} = \left(\binom{X}{k}_{\delta_0^h, E}\right)_{0 \leq k \leq n}$$

la D -base correspondante. La matrice de la famille

$$(B_k(X))_{0 \leq k \leq n} = \left(\binom{X}{k}_{\delta^h, E}\right)_{0 \leq k \leq n}$$

sur la base $(C_k(X))_{0 \leq k \leq n}$ est triangulaire supérieure avec des 1 sur la diagonale. Elle est donc inversible et la famille $(B_k(X))_{0 \leq k \leq n}$ est une D -base de $\text{Int}_n^{\pi^h}(E, D)$. \square

Corolaire 4.1. La π -séquence associée à une suite π^h -ordonnée δ^h de E ne dépend pas de δ^h .

Preuve. Le Théorème 4.3 implique que l'idéal fractionnaire formé par zéro et l'ensemble des coefficients dominants des éléments de $\text{Int}_n^{\pi^h}(D, E)$ de degré n est

$$(n!_{(\delta^h, E)}^h)^{-1} D$$

et cela pour toute suite π^h -ordonnée δ^h de E . Ainsi l'entier $v_\pi(n!_{\delta^h, E}^h)$ ne dépend pas de δ^h et par conséquent la π -séquence associée à δ^h non plus. \square

Remarque 4.2. On a donc $n!_{(\delta_1^h, E)}^h D = n!_{(\delta_2^h, E)}^h D$ pour tout δ_1^h, δ_2^h . On peut donc noter simplement $n!_E^h D$.

Notation 4.1. On appelle fonction factoriel associée à E et h la fonction

$$n \rightarrow n!_E^h = n!_E^h D$$

Le Théorème 4.1 est conséquence immédiate du Corolaire 4.1:

Preuve du Théorème 4.1. Soit D quelconque, D_P le localisé de D en P , et δ^h une suite P^h -ordonnée de E . La suite δ^h est aussi une suite π^h -ordonnée de $E \subset D_P$ et les exposants dans la π -séquence associée à δ^h sont les même que dans la P -séquence associée à δ^h . On applique alors le Corolaire 4.1. \square

4.4 Base régulière

Dans cette section, D est quelconque (plus nécessairement local) et M est un idéal.

On donne une condition nécessaire et suffisante pour que $\text{Int}_n^M(E, D)$ admette une base régulière et lorsque c'est le cas, on présente un algorithme qui construit une telle base à partir des suites P^h -ordonnée pour P divisant M et du théorème chinois.

Définition 4.5. Pour tout n , on définit $\mathfrak{J}_n^M(E, D)$ comme l'ensemble formé de zéro et des coefficients dominants des éléments de $\text{Int}_n^M(E, D)$ de degré n .

Proposition 4.1. $\mathfrak{J}_n^M(E, D)$ est un idéal fractionnaire.

Preuve. Identique à la preuve de la Proposition 2.1 pour $\mathfrak{J}_n(E, D)$. \square

Théorème 4.4. $\text{Int}_n^M(E, D)$ possède une base régulière si et seulement si les idéaux fractionnaires $\mathfrak{J}_k^M(E, D)_{k \leq n}$ sont principaux.

Preuve. Identique à la preuve du Théorème 2.3 pour $\text{Int}_n(E, D)$. \square

Proposition 4.2.

$$\text{Int}_n^M(E, D_P) = \text{Int}_n^M(E, D)_P$$

Preuve. Soit $f \in \text{Int}_n^M(E, D)_P$. D'après la preuve du Proposition 2.2, $f \in \text{Int}_n(E, D)_P$. De plus $f(mX + e) \in D[X]$ et ses coefficients sont dans D_P , donc $f \in \text{Int}_n^M(E, D_P)$.

Réciproquement, soit $f \in \text{Int}_n^M(E, D_P)$. D'après la Proposition 2.2, $f \in \text{Int}_n(E, D)_P$. Soit I le D -module engendré par les coefficients de f . Les coefficients de $f(mX + e)$ sont dans $I \cap D_P$. Puisque D est Noétherien, il existe $s \in D \setminus P$ tel que $sf(mX + e) \in D[X]$, et donc $f \in \text{Int}_n^M(E, D)_P$. \square

Par définition de $\text{Int}_n^M(E, D)$, les coefficients d'un élément $f \in \text{Int}_n^M(E, D)$ sont dans M^{-1} (puisque $f(mX + e) \in D[X]$).

Notation 4.2. On note $n!_{E_P}^M$ la factoriel $n!_E^h$ associée à $E \subset D_P$ où h est la plus grande puissance de P divisant M .

La Proposition 4.2 permet naturellement d'étendre la fonction factorielle définie dans le cas local à D quelconque:

Définition 4.6. On appelle fonction factorielle associée à E et M la fonction

$$n \rightarrow n!_E^M = \mathfrak{J}_n^M(E, D)^{-1} = \prod_{P|M} P^{v_P(n!_E^M)}$$

On présente maintenant un algorithme pour construire un polynôme $A_n \in D[X]$ de degré n tel que $A_n(D) \subset n!_E^M$.

Soient $n \in \mathbb{N}$ et $\{P_1, P_2, \dots, P_m\}$ les premiers qui divisent M . Pour tout $1 \leq i \leq m$ soit $(u_{i,k})_{0 \leq k < n}$ les n premiers termes d'une suite $P_i^{h_i}$ -ordonnée de E où h_i est la plus grande puissance de P_i divisant M .

Algorithme 4.1.

1. Pour tout $0 \leq k < n$, on construit à l'aide du théorème chinois un élément a_k vérifiant pour tout $1 \leq i \leq m$:

$$a_k \equiv u_{i,k} \pmod{P_i^{h_i}}$$

2. On retourne le polynôme $A_n = (X - a_0)(X - a_1) \dots (X - a_{n-1})$.

Théorème 4.5. On a $A_n(E) \subset n!_E^M$.

Preuve. Soit $x \in E$. Il suffit de montrer que $v_P(A_n(x)) \geq v_P(n!_E^M)$ pour tout P . Si $P \notin \{P_0, P_1, \dots, P_m\}$, $v_P(n!_E^M) = 0$. On peut donc se restreindre aux P qui divisent M . On a pour $P_i^{h_i} | M$:

$$\begin{aligned} v_{P_i}(A_n(x)) &= \sum_{k=0}^{n-1} v_{P_i}(x - a_k) \\ &\geq \sum_{k=0}^{n-1} v_{P_i}(a_n - a_k) \\ &\geq \sum_{k=0}^{n-1} \min(h_i, v_{P_i}(a_n - a_k)) \quad \left(= \sum_{k=0}^{n-1} \min(h_i, v_{P_i}(u_{i,n} - u_{i,k})) \right) \\ &\geq v_P(n!_E^M) \end{aligned}$$

□

Pour que $\text{Int}_n^M(E, D)$ admette une base régulière, il est nécessaire que les idéaux $k!_E^M$ pour $k \leq n$ soient principaux. On suppose donc que c'est le cas et on note β_k un générateur de $k!_E^M$.

Soit $(A_k)_{0 \leq k \leq n}$ des polynômes de $D[X]$ tels que $A_k(D) \subset k!_D^M$. On pose $B_k = \frac{1}{\beta_k} A_k$.

Théorème 4.6. La famille $\{B_0, B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n^M(E, D)$

Preuve. Pour tout k , B_k est un polynôme de $\text{Int}_n^M(E, D)$ de degré k et de coefficient dominant β_k par construction. D'après la preuve du Théorème 4.4, $\{B_1, B_2, \dots, B_n\}$ est une base régulière de $\text{Int}_n^M(E, D)$. □

4.5 Calcul effectif pour $E = D$

Pour construire en utilisant les résultats de la section précédente une base régulière de $\text{Int}_n^M(E, D)$ lorsque les $(k!_E^M)_{k \leq n}$ sont principaux, on a besoin de savoir construire les n premiers termes d'une suite P^h -ordonnée de E .

Cela demande si on applique la définition d'une suite P^h -ordonnée de E de prendre un minimum sur un ensemble infini, ce qui n'est pas réalisable tel quel.

Cependant, dans le cas où $E = D$ et où D/P est de cardinal fini pour tout P , il est possible de construire effectivement les n premiers termes d'une suite P^h -ordonnée de D en utilisant la finitude de D/P et l'homogénéité de D .

On montre en fait que les n termes produits par l'Algorithme 2.2 servant à construire une suite P -ordonnée de D forment aussi les n premiers termes d'une suite P^h -ordonnée de D et cela pour tout h !

Dans cette partie, D/P est de cardinal fini pour tout P .

4.5.1 Construction d'une suite P^h -ordonnée de D

Le cardinal de D/P est noté q . On note $\{r_0, \dots, r_{q-1}\}$ un système de représentants modulo P et $D_{r_i} = \{x \in D : x \equiv r_i \pmod{P}\}$.

Théorème 4.7. *Pour tout r_i, r_j et $n \geq 0$:*

$$v_P(n!_{D_{r_i}}^h) = v_P(n!_{D_{r_j}}^h)$$

Autrement dit les P -séquences associées aux suites P^h -ordonnées des D_{r_i} sont les mêmes.

Preuve. Identique à la preuve de la Proposition 2.3 pour les suites P -ordonnées. \square

Proposition 4.3. *Pour $h \geq 1$, l'application $\theta_i : x \rightarrow x\pi + r_i$ envoie une suite $P^{(h-1)}$ -ordonnée de D sur une suite P^h -ordonnée de D_{r_i} .*

Preuve. Soit $(a_n)_n$ une suite P^{h-1} -ordonnée de D . Pour tout $x, y \in D$:

$$\begin{aligned} \min(h, v_P(\theta_i(x) - \theta_i(y))) &= \min(h-1, v_P(\pi(x-y)) - 1) + 1 \\ &= \min(h-1, v_P((x-y) + 1 - 1) + 1) \\ &= \min(h-1, v_P(x-y)) + 1 \end{aligned}$$

Par récurrence sur $n \geq 1$, le minimum à la n -ème étape de construction d'une suite P^h -ordonnée de D_{r_i} est atteint par $\theta_i(a_n)$ ce qui fait de $(\theta_i(a_n))_n$ une suite P^h -ordonnée de D_{r_i} . \square

Corolaire 4.2. *Pour tout $h \geq 1$ et $n \geq 0$:*

$$v_P(n!_{D_{r_i}}^h) = v_P(n!_D^{(h-1)}) + n$$

Preuve. Soit $(a_n)_n$ une suite $P^{(h-1)}$ -ordonnée de D . Pour tout $n \geq 1$ on a :

$$\begin{aligned} v_P \left(n!_{D_{r_i}}^h \right) &= \sum_{k=0}^{n-1} \min(h, v_P(\theta_i(a_n) - \theta_i(a_k))) \\ &= \sum_{k=0}^{n-1} (\min(h-1, v_P(a_n - a_k)) + 1) \\ &= v_P \left(n!_D^{(h-1)} \right) + n \end{aligned}$$

□

On cherche désormais à construire une suite P^h -ordonnée de D à partir de suites P^h -ordonnée des D_{r_i} . On rappelle que la notion d'entrelacement de suites a été introduite dans la Définition 2.7.

On montre que l'entrelacement q -uniforme de suites P^h -ordonnée des D_{r_i} résulte en une suite P^h -ordonnée de D .

Proposition 4.4. *Pour tout $0 \leq i < q$ et tout $n \in \mathbb{N}$ soit*

$$\phi_i(n) = nq + i$$

La suite obtenue par $(\phi_i)_{0 \leq i < q}$ entrelacement de suites P^h -ordonnée des D_{r_i} est une suite P^h -ordonnée de D .

Preuve. Identique à la preuve de la Proposition 2.5 pour les suites P -ordonnée. □

Corolaire 4.3. *Pour tout $n \geq 0$ et $h \geq 1$, on a*

$$v_P(n!_D^h) = v_P(\lfloor n/q \rfloor!_D^{(h-1)}) + \lfloor n/q \rfloor$$

Preuve. Soit $(a_n)_n$ la suite obtenue par $(\phi_i)_{0 \leq i < q}$ entrelacement des D_{r_i} . Par définition des ϕ_i , a_n est le $\lfloor n/q \rfloor$ -ème terme d'une suite P^h -ordonnée de l'un des $D_{r_i} = D_{r_{i_0}}$. Puisque $v_P(a_n - a_k) = 0$ dès que $a_k \notin D_{r_{i_0}}$, on a

$$v_P(n!_D^h) = v_P \left(\lfloor n/q \rfloor!_{D_{r_{i_0}}}^h \right)$$

On applique alors le Corolaire 4.2. □

Théorème 4.8. *Pour tout $n \geq 0$, on a :*

$$v_P(n!_D^h) = \sum_{k=1}^h \lfloor n/q^k \rfloor$$

Preuve. Par récurrence sur $h \geq 0$. Si $h = 0$, $v_P(n!_D^h) = 0$ pour tout n .

Supposons la formule vrai au rang $h-1$. On a d'après le Corolaire 4.3 et l'hypothèse de récurrence

$$\begin{aligned} v_P(n!_D^h) &= v_P(\lfloor n/q \rfloor!_D^{(h-1)}) + \lfloor n/q \rfloor = \sum_{k=1}^{h-1} \lfloor n/q^{k+1} \rfloor + \lfloor n/q \rfloor \\ &= \sum_{k=2}^h \lfloor n/q^k \rfloor + \lfloor n/q \rfloor = \sum_{k=1}^h \lfloor n/q^k \rfloor \end{aligned}$$

□

Définition 4.7 (La fonction $w_{q,h}$). Pour tout $h, n \geq 0$ et tout $q \geq 2$, on pose:

$$w_{q,h}(n) = \sum_{k=1}^h \lfloor n/q^k \rfloor = w_q(n) - w_q(\lfloor n/q^h \rfloor)$$

Corolaire 4.4. Soit $M = \prod_{j \in J} P_j^{h_j}$ un module. On note q_j le cardinal de D/P_j . On a alors

$$n!_D^M = \prod_{j \in J} P_j^{w_{q_j, h_j}(n)}$$

Remarquons maintenant que si $h \geq \lfloor \log_q(n) \rfloor$, on a $w_q(n) = w_{q,h}(n)$ et donc les n termes produits par l'Algorithme 2.2 servant à construire une suite P -ordonnée de D forment aussi les n premiers termes d'une suite P^h -ordonnée.

Si au contraire $h < \lfloor \log_q(n) \rfloor$, les Proposition 4.3 et Proposition 4.4 impliquent que l'Algorithme 2.2 servant à construire une suite P -ordonnée de D peut être utilisé pour construire les n premiers termes d'une suite P^h -ordonnée de D à condition de prendre pour q premiers termes à l'étape 1) les q premiers termes d'une suite $P^{\lfloor \log_q(n) \rfloor - h}$ -ordonnée de D . Mais il est immédiat que les q premiers termes $(r_0, r_1, \dots, r_{q-1})$ utilisés dans l'algorithme sont aussi les q premiers termes d'une suite P^h -ordonnée de D quelque soit h . En conséquence:

Théorème 4.9. La suite P -ordonnée de D produite par l'Algorithme 2.2 est aussi une suite P^h -ordonnée de D pour tout $h \geq 0$.

4.5.2 Algorithme pour $\text{Int}_n^M(D)$

On résume ici la procédure pour construire lorsque les idéaux $(k!_D^M)_{k \leq n}$ sont principaux une base régulière de $\text{Int}_n^M(D)$.

Soit T l'ensemble des premiers P divisant M .

1. Pour tout P dans T , on utilise l'Algorithme 2.2 pour construire les n premiers termes d'une suite P^h -ordonnée de D où h est la plus grande puissance telle que P^h divise M .
2. Pour tout $0 \leq k \leq n$, on utilise l'Algorithme 4.1 pour construire un polynôme A_k vérifiant $A_k(D) \subset k!_D^M$. On utilisera pour cela les k premiers termes des suites P^h -ordonnée construites à l'étape 1).
3. Pour tout $0 \leq k \leq n$, on calcul l'idéal $k!_D^M$ en utilisant la formule du Corolaire 4.4.
4. Pour tout $0 \leq k \leq n$, on calcul un générateur β_k de $k!_D^M$ par les méthodes standards puis $B_k = \frac{1}{\beta_k} A_k$.

La famille (B_0, B_1, \dots, B_k) ainsi construite est une base régulière de $\text{Int}_n^M(D)$.

4.5.3 Exemples

Exemple 1

Soit $K = \mathbb{Q}(i)$ d'anneau des entiers $\mathbb{Z}[i]$ (principal) et soit le module

$$M = (3 - i) = (1 + i)(2 + i)$$

Voici une base régulière $B = (B_i(X))_{0 \leq i \leq 3}$ de $\text{Int}_3^M(\mathbb{Z}[i])$:

$$B_0(X) = 1, \quad B_1(X) = X, \quad B_2(X) = \frac{1-i}{2}X^2 - \frac{1-i}{2}X$$

$$B_3(X) = \frac{1-i}{2}X^3 - \frac{1+i}{2}X^2 + iX$$

Dans le tableau suivant, on donne dans la première colonne un polynôme $P(X)$ de $\text{Int}_3^M(\mathbb{Z}[i])$ exprimé par ses $\mathbb{Z}[i]$ -coordonnées sur la base régulière B , dans la deuxième des couples (m, e) avec $m \in (M)$ et $e \in \mathbb{Z}[i]$ et dans la troisième les polynôme $P(mX + e) \in \mathbb{Z}[i][X]$ correspondants.

$P(X)$	(m, e)	$P(mX + e)$
$(0, 1, i, 1 - i)_B$	$(3 - i, 1)$	$(-26 - 18i)X^3 - (19 + 17i)X^2 - 5iX + 1$
	$(3 - i, i)$	$(-26 - 18i)X^3 + (23 - 11i)X^2 + (4 + 7i)X + i - 1$
	$((3 - i)2i, i - 1)$	$(-144 + 208i)X^3 - (164 + 52i)X^2 - 30iX + 1$
$(i, 0, i, 1 + i)_B$	$((3 - i)i, 0)$	$(-26 - 18i)X^3 - (1 - 7i)X^2 - (3 + 4i)X + i$
	$((3 - i), (2 - i))$	$(18 - 26i)X^3 + (31 - 67i)X^2 + (11 - 52i)X - 1 - 11i$
	$((3 - i)^2, 1)$	$(-352 - 936i)X^3 + 50 - 350i)X^2 + (17 - 19i)X + i$
$(0, 0, 1, -1)_B$	$((3 - i), 1)$	$(4 + 22i)X^3 + (5 + 15i)X^2 + (1 + 3i)X$
$(0, 1, -1, 0)_B$	$((3 - i)(2 + 2i), 2 - 3i)$	$(-56 - 8i)X^2 + (2 + 46i)X + (10 - 2i)$

Table 3: Polynôme $P(mX + e) \in \mathbb{Z}[i][X]$ pour quelques couples (m, e)

Exemple 2

On note $\alpha = \sqrt[3]{2}$.

Soit $K = \mathbb{Q}[\alpha]$. Une base de l'anneau des entiers $\mathbb{Z}[\alpha]$ est $(1, \alpha, \alpha^2)$.

Soit le module $M = (2\alpha)$. Voici une base régulière de $\text{Int}_4^M(\mathbb{Z}[\alpha])$:

$$B_0(X) = 1, \quad B_1(X) = X, \quad B_2(X) = \frac{-\alpha^2}{2}X^2 + \frac{\alpha^2}{2}X, \quad B_3(X) = \frac{-\alpha^2}{2}X^3 + \frac{\alpha^2 + 2}{2}X^2 - X$$

$$B_4(X) = \frac{1}{2}X^4 + (\alpha - 1)X^3 + \frac{\alpha^2 - 3\alpha + 1}{2}X^2 + \frac{\alpha - \alpha^2}{2}X$$

4.5.4 Fonctions pour $\text{Int}_n^M(D)$

Voici quelques fonctions utiles:

- la fonction `ispolyaupto_mod(K, M, n)` teste si $\text{Int}_n^M(D)$ admet une base régulière
- la fonction `zkmodregbasis(K, M, n, "X")` retourne (si possible) une base régulière (d'indéterminée "X") de $\text{Int}_n^M(D)$.
- la fonction `zkmodregbasis_dec(K, pol, M, "X")` retourne une matrice $(n + 1) \times 2$ (où $n = \deg(\text{pol})$) avec une base régulière de $\text{Int}_n^M(D)$ (d'indéterminée "X") dans la deuxième colonne et les coefficients de la K -décomposition de `pol` sur cette base dans la première.

References

- [Bha97] Manjul Bhargava. “P-orderings and polynomial functions on arbitrary subsets of Dedekind rings.” In: *Journal für die reine und angewandte Mathematik* 490 (1997), pp. 101–128. URL: <http://eudml.org/doc/153942>.
- [Bha09] Manjul Bhargava. “On P -orderings, rings of integer-valued polynomials, and ultrametric analysis”. In: *Journal of The American Mathematical Society - J AMER MATH SOC* 22 (Oct. 2009), pp. 963–993. DOI: [10.1090/S0894-0347-09-00638-9](https://doi.org/10.1090/S0894-0347-09-00638-9).
- [CC16] Paul-Jean Cahen and Jean-Luc Chabert. “What You Should Know About Integer-Valued Polynomials”. In: *The American Mathematical Monthly* 123.4 (2016), pp. 311–337. DOI: [10.4169/amer.math.monthly.123.4.311](https://doi.org/10.4169/amer.math.monthly.123.4.311).
- [Joh10] Keith Johnson. “Computing r -removed P -orderings and P -orderings of order h ”. en. In: *Actes des rencontres du CIRM* 2.2 (2010), pp. 33–40. DOI: [10.5802/acirm.31](https://doi.org/10.5802/acirm.31). URL: acirm.centre-mersenne.org/item/ACIRM_2010__2_2_33_0/.
- [Ler10] Amandine Leriche. “Groupes, corps et extensions de Polya : une question de capitulation”. Theses. Université de Picardie Jules Verne, Dec. 2010. URL: <https://tel.archives-ouvertes.fr/tel-00612597>.