Cours du Master 2
Algèbre et théorie des nombres
-
Autour de l'algèbre des polynômes à valeurs entières dans un corps de nombres ou un corps de fonctions

Jean-Luc Chabert

Amiens, printemps 2006
Université de Picardie
LAMFA CNRS UMR 6140

Autour de l'algèbre des polynômes à valeurs entières
dans un corps de nombres ou un corps de fonctions

Au carrefour de l'algèbre et de la théorie des nombres, ce cours met en pratique les outils classiques de la théorie algébrique des nombres et de l'analyse p-adique.

Les deux grands thèmes traités seront

1- Le module des polynômes à valeurs entières : construction de bases de Pólya dans le cas local ; obstruction la globalisation : groupe de Pólya-Ostrowki ; liens avec la ramification ; factorielles généralisées.

2 - Bases normales d'espaces de fonctions p-adiques : théorèmes de Stone-Weierstrass p-adiques ; séries de Mahler ; extensions par les q-digits de Conrad.

Bibliographie.

a- Ouvrages déjà anciens :

- W. Narkiewicz, *Polynomial mappings*, Lecture Notes 1600, Springer, 1995.
- P.-J. Cahen et J.-L. Chabert, *Integer-Valued Polynomials*, Math. Surveys and Monographs, vol. 48, American Mathatical Society, 1997.

b- Articles plus récents (précisés chapitre par chapitre)

Mise en garde : le texte qui suit est rédigé au fil des semaines et n'est pas corrigé de ses coquilles (voire pire).

Chapter 1

Polynômes à valeurs entières et factorielles de Bhargava

1.1 Propriétés arithmétiques des factorielles

Rappelons quelques propriétés bien connues des factorielles classiques $n!$ où n désigne un entier naturel :

Propriété 1.1.1. *Quels que soient $k, l \in \mathbb{N}$,*

$$\frac{(k+l)!}{k!l!} \in \mathbb{N}.$$

Interprétation combinatoire : C_{k+l}^{k}. Une conséquence immédiate :

Propriété 1.1.2. *Le produit de n entiers consécutifs est divisible par $n!$.*

L'énoncé est optimal : le quotient vaut 1 pour la suite $1, \ldots, n$.

Propriété 1.1.3. *Pour toute suite de $n+1$ entiers, $a_0, a_1, \ldots, a_n$, le produit*

$$\prod_{0 \leq i < j \leq n} (a_j - a_i) \ \ est\ divisible\ par\ \ 1!2! \cdots n!$$

L'énoncé est optimal : le quotient vaut 1 pour la suite $0, 1, \ldots, n$.

Interprétation combinatoire : le quotient est la dimension d'un certaine représentation irréductible de $SU(n)$. La propriété 3 sera prouvée dans le cadre général des factorielles de Bhargava dans un anneau de Dedekind.

Propriété 1.1.4. *(Kempner, 1921 [1]) Le nombre de fonctions polynomiales de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est égal à :*

$$\psi(n) = \prod_{k=0}^{n-1} \frac{n}{\mathrm{pgcd}(n, k!)}.$$

Précisons qu'ici une fonction polynomiale désigne ici une fonction qui peut être représentée par un polynôme à coefficients entiers (et non pas à valeurs entières, auquel cas le résultat serait bien différent [*le montrer*]). Le théorème des restes chinois et le fait que la fonction arithmétique ψ est multiplicative montre que, pour la preuve, on peut se limiter à une vérification dans le cas où n est une puissance p^e d'un nombre premier [*le faire*] (cf. aussi [2]). Lorsque $n = p$ est un nombre premier, $\psi(p) = p^p$ redonne le fait que toute fonction de $\mathbb{F}_p$ dans lui-même est polynomiale.

Propriété 1.1.5. *Pour tout polynôme unitaire $f \in \mathbb{Z}[X]$ de degré n,*
$$d(f) = \mathit{pgcd}\{f(k) \mid k \in \mathbb{Z}\} \textit{ divise } n!.$$

L'énoncé est optimal : $d(f) = n!$ pour $f(X) = X(X-1)(X-n+1)$.

Cette propriété est une conséquence immédiate de la suivante.

Propriété 1.1.6. *Pour tout polynôme $g \in \mathbb{Q}[X]$ de degré n à valeurs entières, c.-à-d., tel que $g(\mathbb{Z}) \subset \mathbb{Z}$, on a : $n!g \in \mathbb{Z}[X]$.*

L'énoncé est optimal : le polynôme binomial

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

est un polynôme à valeurs entières de degré n.

La preuve de cette propriété 6 est l'objet de la section suivante. Terminons ce rappel avec *la formule de Legendre* :

Proposition 1.1.7. *Pour tout $n \geq 0$, on a :*

$$n! = \prod_{p \in \mathbb{P}} p^{w_p(n)} \text{ avec } w_p(n) = \sum_{k>0} \left[\frac{n}{p^k}\right]$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers.

En effet, pour $p \in \mathbb{P}$, notant v_p la valuation p-adique de $\mathbb{Q}$, on a :

$$w_p(n) = v_p(n!) = \sum_{k \in \mathbb{N}^*} k \left\{ \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right] \right\} = \sum_{k>0} \left[\frac{n}{p^k}\right].$$

1.2 Polynômes à valeurs entières sur $\mathbb{Z}$

Par analogie avec les coefficients binomiaux, on appelle *polynômes binomiaux* les polynômes suivants :

$$\binom{X}{0} = 1 \quad \text{et, pour } k \geq 1, \quad \binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}.$$

Les polynômes $\binom{X}{k}$ prennent des valeurs entières sur tous les entiers.
[Pour $j \in \mathbb{Z}$, on calcule $\binom{j}{k}$ en distinguant selon que $0 \leq j < k,\ j \geq k$ et $j < 0$.]

Proposition 1.2.1 (Pólya, 1915 [3])**.** *Un polynôme $P(X)$ coefficients rationnels prenant des valeurs entières sur tous les entiers s'écrit d'une façon et d'une seule sous la forme :*

$$P(X) = \sum_{k=0}^{\deg(P)} a_k \binom{X}{k} \quad \text{avec} \quad a_k \in \mathbb{Z}.$$

Plus précisément,

$$a_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(i)$$

Les a_k sont déterminés par un système de Cramer à coefficients entiers et de déterminant 1. [La matrice du système est triangulaire inférieure, c'est le triangle de Pascal et donc la diagonale ne comporte que des 1.]

Exercice 1.2.2. On rappelle que l'opérateur linéaire Δ est défini sur $\mathbb{Q}[X]$ par :

$$\Delta P(X) = P(X+1) - P(X) \quad \text{et} \quad \Delta^k P(X) = \Delta(\Delta^{k-1} P(X)).$$

Vérifier les formules :

$$\Delta^k P(X) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(X+i).$$

$$\text{pour } k \geq 1, \ \binom{X+1}{k} = \binom{X}{k} + \binom{X-1}{k-1} \text{ et } \Delta\binom{X}{k} = \binom{X}{k-1}.$$

$$\text{Si } P = \sum_{k=0}^{n} a_k \binom{X}{k}, \text{ alors } \Delta P = \sum_{k=0}^{n-1} a_{k+1} \binom{X}{k} \text{ et } a_k = \Delta^k P(0).$$

Définition 1.2.3. L'algèbre des *polynômes à valeurs entières* sur $\mathbb{Z}$ est la $\mathbb{Z}$-algèbre

$$\mathrm{Int}(\mathbb{Z}) = \{P(X) \in \mathbb{Q}[X] \mid P(\mathbb{Z}) \subset \mathbb{Z}\}.$$

Ainsi, la proposition 1.2.1 nous dit que $\mathrm{Int}(\mathbb{Z})$ est un $\mathbb{Z}$-module libre de base $\left(\binom{X}{k}\right)_{k\in\mathbb{N}}$ et nous montre qu'un polynôme de degré $\leq n$ qui prend des valeurs entières sur les $n+1$ premiers entiers (plus généralement, sur $n+1$ entiers consécutifs) est à valeurs entières.

Exercice 1.2.4. Retrouver ce dernier résultat à l'aide des polyômes de Lagrange : Soient n et h deux entiers tels que $n > 0$ et $0 \leq h \leq n$. Soit Π_h^n le polynôme de Lagrange de degré n caractérisé par $\Pi_h^n(k) = \delta_{h,k}$ pour $0 \leq k \leq n$. Montrer la formule :

$$\Pi_h^n(X) = \prod_{0\leq k\leq n,\, k\neq h} \frac{X-k}{h-k} = (-1)^{n-h}\binom{X}{h}\binom{X-h-1}{n-h}.$$

Corollaire 1.2.5. *Soit* $P = \sum_{k=0}^{n} a_k\binom{X}{k} \in \mathrm{Int}(\mathbb{Z})$. *Alors*

$$\text{p.g.c.d.}\{P(k) \mid k \in \mathbb{Z}\} = \text{p.g.c.d.}\{P(k) \mid 0 \leq k \leq n\} = \text{p.g.c.d.}\{a_k \mid 0 \leq k \leq n\}.$$

Corollaire 1.2.6. *Soit* $n \in \mathbb{N}$. *Posons*

$$\mathrm{Int}_n(\mathbb{Z}) = \{P \in \mathrm{Int}(\mathbb{Z}) \mid \deg(P) \leq n\}.$$

Le nombre $n!$ *est le plus petit entier* > 0 *tel que*

$$n!\mathrm{Int}_n(\mathbb{Z}) \subset \mathbb{Z}[X].$$

C'est cette proposition que l'on va utiliser pour généraliser la notion de factorielle.

Corollaire 1.2.7. *Pour tout polynôme* $Q \in \mathbb{Z}[X]$ *unitaire et de degré* $\leq n$, *le* p.g.c.d. *des valeurs prises par* Q *sur* $\mathbb{Z}$ *divise* $n!$.

1.3 Polynômes à valeurs entières en général

Suivant Pólya [4] et Ostrowski [5], pour tout corps de nombres K d'anneau d'entiers $\mathcal{O}_K$, on appelle polynôme à valeurs entières dans K tout polynôme $P(X)$ à coefficients dans K tel que $P(\mathcal{O}_K) \subset \mathcal{O}_K$. Plus généralement, suivant [6] :

Définition 1.3.1. Pour tout anneau intègre A de corps des fractions K, on appelle *polynôme à valeurs entières sur* A, tout polynôme $P \in K[X]$ tel que $P(A) \subset A$.

Ces polynômes forment une A-algèbre comprise entre $A[X]$ et $K[X]$ que l'on note $\mathrm{Int}(A)$:

$$\mathrm{Int}(A) = \{P \in K[X] \mid P(A) \subset A\}.$$

Non seulement $\mathrm{Int}(A)$ est stable par addition et multiplication, mais aussi par composition. Plus généralement encore, on introduit :

Définition 1.3.2. Pour tout anneau intègre A de corps des fractions K et pour toute partie E de K, on appelle *polynôme à valeurs entières sur* E *relativement à* A, tout polynôme $P \in K[X]$ tel que $P(E) \subset A$.

Ces polynômes forment une sous-A-algèbre de $K[X]$ que l'on note $\mathrm{Int}(E, A)$:

$$\mathrm{Int}(E, A) = \{P \in K[X] \mid P(E) \subset A\}.$$

Cette fois, l'ensemble $\mathrm{Int}(E, A)$ n'est a priori pas stable par composition. Ce chapitre va pour l'essentiel être consacré à l'étude de la structure additive de $\mathrm{Int}(E, A)$, c'est-à dire, sa structure de A-module. On s'intéressera notamment à l'existence éventuelle de bases.

Remarques 1.3.3. Il est immédiat (ou presque) que :
1- Si $E \subset F$, alors $\mathrm{Int}(F, A) \subset \mathrm{Int}(E, A)$.
2- $\mathrm{Int}(E, A) \cap K = A$, mais $\mathrm{Int}(E, A)$ ne contient pas toujours $A[X]$. En effet, $A[X] \subset \mathrm{Int}(E, A) \Leftrightarrow E \subset A$.
3- Si $E = \emptyset$, alors $\mathrm{Int}(E, D) = K[X]$ et, si $A \neq K$, alors $\mathrm{Int}(K, A) = A$.
4- Si E est une partie cofinie de A, alors $\mathrm{Int}(E, A) = \mathrm{Int}(A)$ (mais la condition n'est pas nécessaire : $\mathrm{Int}(\mathbb{N}, \mathbb{Z}) = \mathrm{Int}(\mathbb{Z})$.)

EXEMPLE 1.3.4. Si $E = \{a_1, \ldots, a_r\}$ est une partie finie, alors

$$\mathrm{Int}(E, A) = fK[X] + \sum_{1 \leq j \leq r} A\varphi_j$$

où

$$f = \prod_{1 \leq i \leq r} (X - a_i) \quad \text{et} \quad \varphi_j = \prod_{i \neq j} \frac{X - a_i}{a_j - a_i}.$$

Proposition 1.3.5. *Si la A-algèbre $\mathrm{Int}(E, A)$ contient des polynômes non constants, alors E est un sous-ensemble fractionnaire de la clôture intégale de A.*

On rappelle qu'une partie E du corps des fractions K de A est dite *fractionnaire* s'il existe un élément non nul $d \in A$ tel que $dE \subset A$.

Corollaire 1.3.6. *Si A est intégralement clos, $\mathrm{Int}(E, A) \neq A$ si et seulement si E est une partie fractionnaire de A.*

Pour écarter le cas trivial où $\mathrm{Int}(E, A) = A$, on supposera le plus souvent que E est une partie fractionnaire de A. Comme, de plus, pour tout élément non nul d, on a un isomorphisme de A-algèbres :

$$P(X) \in \mathrm{Int}(E, A) \mapsto P(X/d) \in \mathrm{Int}(dE, A),$$

on pourra supposer que E est une partie de A.

1.4 Polynômes à valeurs entières et localisation

Notations. *On désigne toujours par A un anneau intègre de corps des fractions K et par E une partie de A.*

On considère maintenant une partie multiplicative S de A. On va s'intéresser aux valeurs prises sur l'anneau de fractions $S^{-1}A$ par un polynôme à valeurs entières sur A.

On rappelle qu'une *partie multiplicative* S de A est une partie de A stable par multiplication, contenant 1 et ne contenant pas 0 et que l'*anneau de fractions* $S^{-1}A$ est l'anneau compris entre A et K défini par :

$$S^{-1}A = \left\{ \frac{A}{s} \mid a \in A, s \in S \right\}.$$

Il est immédiat que l'on a toujours l'inclusion :

$$\mathrm{Int}(E, A) \subset \mathrm{Int}(E, S^{-1}A),$$

et donc aussi :

$$S^{-1}\mathrm{Int}(E, A) \subset \mathrm{Int}(E, S^{-1}A).$$

Il faut noter qu'en général cette dernière inclusion est stricte. Cependant :

Proposition 1.4.1. *Si l'anneau A est noethérien, alors on a l'égalité:*

$$S^{-1}\mathrm{Int}(E,A) = \mathrm{Int}(E, S^{-1}A).$$

En effet, le A-module engendré par les valeurs d'un polynôme étant contenu dans le A-module de type fini engendré par les coefficients de ce polynôme est lui-même de type fini et possède donc un dénominateur commun.

Notation. Pour tout idéal premier $\mathfrak{p}$ de A, on note :

$$A_{\mathfrak{p}} = \left\{ \frac{a}{s} \mid a \in A, s \in A \setminus \mathfrak{p} \right\}, \text{ autrementdit, } A_{\mathfrak{p}} = S^{-1}A \text{ avec } S = A \setminus \mathfrak{p}.$$

Rappelons que pour tout anneau intègre A, on a :

$$A = \cap_{\mathfrak{m} \in \max(A)} A_{\mathfrak{m}}$$

où $\max(A)$ désigne l'ensemble des idéaux maximaux de A. Plus généralement, pour tout idéal fractionnaire $\mathcal{J}$ de A, on a :

$$\mathcal{J} = \cap_{\mathfrak{m} \in \max(A)} \mathcal{J}_{\mathfrak{m}} \text{ avec } \mathcal{J}_{\mathfrak{m}} = \left\{ \frac{j}{s} \mid j \in \mathcal{J}, s \in A \setminus \mathfrak{m} \right\}.$$

Corollaire 1.4.2. *Pour tout anneau intègre A, on a l'égalité :*

$$\mathrm{Int}(E,A) = \cap_{\mathfrak{m} \in \max(A)} \mathrm{Int}(E, A_{\mathfrak{m}}).$$

Mais on souhaite voir ce qui se passe si l'on considère les valeurs d'un polynôme sur un anneau de fractions. Pour cela, il nous faut nous placer dans la cas où E est un anneau :

Proposition 1.4.3. *Soit R un sous anneau de A et soit T une partie multiplicative de R. Alors, pour tout polynôme de $P \in K[X]$,*

$$P(R) \subset A \text{ implique } P(T^{-1}R) \subset T^{-1}A,$$

autrement dit :

$$\mathrm{Int}(R,A) \subset \mathrm{Int}(T^{-1}R, T^{-1}A).$$

La proposition se vérifie facilement par récurrence sur le degré du polynôme. On en déduit l'égalité :

$$\mathrm{Int}(R, T^{-1}A) = \mathrm{Int}(T^{-1}R, T^1A)$$

et, lorsque R est noethérien, on a aussi :

$$T^{-1}\mathrm{Int}(R, A) = \mathrm{Int}(R, T^{-1}A) = \mathrm{Int}(T^{-1}R, T^1A).$$

En particulier, pour $R = A$, on obtient :

Proposition 1.4.4. *Pour toute partie multiplicative S de A, on a :*

$$S^{-1}\mathrm{Int}(A) \subset \mathrm{Int}(S^{-1}A)$$

et donc

$$\mathrm{Int}(A) = \cap_{\mathfrak{m}\in\max(A)} \mathrm{Int}(A_{\mathfrak{m}}).$$

De plus, lorsque A est noethérien, on a l'égalité :

$$S^{-1}\mathrm{Int}(A) = \mathrm{Int}(S^{-1}A).$$

Remarque 1.4.5. Dans le cas particulier où $A = \mathbb{Z}$ et $S = \mathbb{Z} \setminus p\mathbb{Z}$ où p désigne un nombre premier, l'égalité :

$$\mathrm{Int}(\mathbb{Z})_{(p)} = \mathrm{Int}(\mathbb{Z}_{(p)})$$

pourrait se montrer par des arguments de continuité p-adique. Ceci fera l'objet du chapitre suivant.

Encore des anneaux de fractions mais relatifs cette fois aux coefficients et non plus aux valeurs :

Proposition 1.4.6. *Soit $P \in K[X]$ de degré n et soient $a_0, \ldots, a_n \in A$ tels que $P(a_i) \in A$ pour $0 \leq i \leq n$. Alors $dP \in A[X]$ où :*

$$d = V(a_0, a_1, \ldots, a_n) = \prod_{0\leq i<j\leq n} (a_j - a_i).$$

Corollaire 1.4.7. *Si E est une partie de A qui rencontre une infinité de classes modulo $\mathfrak{p}$, alors*

$$\mathrm{Int}(E, A) \subset A_{\mathfrak{p}}[X].$$

Corollaire 1.4.8. *Si $\mathfrak{p}$ est un idéal premier de A tel que $A/\mathfrak{p}$ soit infini, alors*

$$\mathrm{Int}(A) \subset A_{\mathfrak{p}}[X] \quad \text{et} \quad \mathrm{Int}(A_{\mathfrak{p}}) = A_{\mathfrak{p}}[X].$$

Corollaire 1.4.9. *Si les idéaux maximaux de A sont tous de corps résiduel infini, alors* $\mathrm{Int}(A) = A[X]$.

1.5 Factorielles généralisées

Notations. *On désigne toujours par A un anneau intègre de corps des fractions K et on supposera systématiquement que $A \neq K$. On désignera aussi par E une partie du corps des fractions K qui est fractionnaire pour A.*

On va utiliser la définition très générale des polynômes à valeurs entières pour donner une définition très étendue des factorielles. Pour tout entier $n \geq 0$, on introduit la notation :

$$\mathrm{Int}_n(E, A) = \{P \in \mathrm{Int}(E, A) \mid \deg(P) \leq n\}.$$

Idéaux caractéristiques

Définition 1.5.1. On appelle n-ième *idéal caractéristique* de l'algèbre $\mathrm{Int}(E, A)$ et on note $\mathcal{I}_n(E, A)$ le sous-A-module de K engendré par les coefficients des polynômes de $\mathrm{Int}_n(E, A)$.

Il est clair que la suite $(\mathcal{I}_n(E, A))_{n\in\mathbb{N}}$ est une suite croissante et que :

$$A \subset \mathcal{I}_n(E, A) \subset K, \quad \mathcal{I}_0(E, A) = A$$

et

$$\mathcal{I}_n(E, A) = K \Leftrightarrow n \geq card(E).$$

La proposition 1.4.6 montre que :

$$\text{Pour } n < card(E),\ \mathcal{I}_n(E, A) \text{ est un ideal fractionnaire de } A.$$

Ainsi, lorsque E est infini, les $\mathcal{I}_n(E, A)$ sont vraiment tous des idéaux fractionnaires.

Par ailleurs, pour tous $n, m \in \mathbb{N}$, on a évidemment :

$$\mathcal{I}_n(E, A) \times \mathcal{I}_m(E, A) \subset \mathcal{I}_{n+m}(E, A).$$

Les énoncés 1.4.2 and 1.4.1 montrent respectivement que :

Proposition 1.5.2. *En général, on a :*

$$\mathcal{I}_n(E, A) = \cap_{\mathfrak{m}\in\max(A)} \mathcal{I}_n(E, A_{\mathfrak{m}})$$

et, lorsque A est noethérien, pour toute partie multiplicatie S de A, on a :

$$S^{-1}\mathcal{I}_n(E, A) = \mathcal{I}_n(E, S^{-1}A).$$

Rappels. Pour tout idéal fractionnaire $\mathcal{J}$ de A, on note classiquement :

$$\mathcal{J}^{-1} = (A : \mathcal{J}) = \{x \in K \mid xJ \subset A\}$$

bien que, en général, l'inclusion $\mathcal{J} \cdot \mathcal{J}^{-1} \subset A$ soit stricte et que $(\mathcal{J}^{-1})^{-1}$ puisse contenir strictement $\mathcal{J}$. En revanche, de tels 'inverses' $\mathfrak{a} = \mathcal{J}^{-1}$ sont toujours des idéaux (fractionnaires) *divisoriels*, c.-à-d., intersection d'idéaux fractionnaires principaux et ils vérifient $\mathfrak{a} = (\mathfrak{a}^{-1})^{-1}$ car, selon Bourbaki [7, VII, § 1, 1]), on a toujours :

$$((\mathcal{J}^{-1})^{-1})^{-1} = \mathcal{J}^{-1}.$$

Par convention, on posera :

$$K^{-1} = (0) \quad \text{et} \quad (0)^{-1} = K.$$

Idéaux factoriels

Définition 1.5.3. On appelle n-ième *idéal factoriel* de E relativement à A et on note $(n!)_E^A$ le sous-ensemble de A suivant :

$$(n!)_E^A = \{a \in A \mid a \times \mathrm{Int}_n(E, A) \subset A[X]\}.$$

Il est immédiat que

$$(n!)_E^A = \{a \in A \mid a\mathcal{I}_n(E, A)\} = \mathcal{I}_n^{-1}(E, A).$$

Ainsi,

$$(n!)_{\mathbb{Z}}^{\mathbb{Z}} = (n!)_{\mathbb{N}}^{\mathbb{Z}} = n!\mathbb{Z}.$$

On a les propriétés immédiates suivantes :

Proposition 1.5.4. *1-* $(0!)_E^A = A$,
2- $((n!)_E^A)_{n\in\mathbb{N}}$ *est une suite décroissante d'idéaux entiers divisoriels,*
3- $(n!)_E^A = (0)$ *si et seulement si* $n \geq card(E)$,
4- si $F \subset E \subset A$, *alors* $(n!)_F^A \subset (n!)_E^A$.
5- Si $F = aE + b = \{ax + b \mid x \in E\}$ *où* $a, b \in K$, *alors* $(n!)_F^A = a^n(n!)_E^A$.

Proposition 1.5.5. *Lorsque l'anneau A est noethérien, pour toute partie multiplicative S de A, on a :*

$$S^{-1}(n!)_E^A = (n!)_E^{S^{-1}A}$$

et, par suite,

$$(n!)_E^A = \cap_{\mathfrak{m}\in\max(A)} \, (n!)_E^{A\mathfrak{m}}.$$

Cela résulte de ce que, lorsque A est noethérien, le localisé de l'inverse d'un idéal fractionnaire $S^{-1}(A : \mathcal{J})$ est égal à l'inverse du localisé $(S^{-1}A : S^{-1}\mathcal{J})$.

1.6 Factorielles de Bhargava (A de Dedekind)

On va s'intéresser principalement (mais pas toujours) au cas où A est un 'anneau d'entiers' de corps de nombres ou de corps de fonctions et où donc A est un anneau de Dedekind. Or, lorsque A est un anneau de Dedekind, l'inverse (en terme de notation) est vraiment l'inverse (en terme de groupe). En effet :

Proposition 1.6.1. *Si A est un anneau de Dedekind, les idéaux fractionnaires non nuls de A forment un groupe pour la mutiplication. C'est en fait un groupe abélien libre de base l'ensemble des idéaux maximaux de A : tout idéal (resp. fractionnaire) non nul $\mathcal{I}$ de A s'écrit d'une façon et d'une seule sous la forme*

$$\mathcal{I} = \prod_{\mathfrak{m}\in\max(A)} \mathfrak{m}^{v_{\mathfrak{m}}(\mathcal{I})} \text{ avec } v_{\mathfrak{m}}(\mathcal{I}) \in \mathbb{N} \text{ (resp. } \mathbb{Z}).$$

En particulier, dans l'ensemble des idéaux entiers non nuls d'un anneau de Dedekind, l'inclusion correspond à la divisibilité :

$$\mathfrak{a} \subset \mathfrak{b} \quad \Leftrightarrow \quad \exists \mathfrak{c} \text{ tel que } \mathfrak{a} = \mathfrak{b}\cdot\mathfrak{c}.$$

Du coup :

Proposition 1.6.2. *Si A est un anneau de Dedekind, on a la relation de division suivante entre idéaux :*

1- $\forall m, n \in \mathbb{N}, \quad (m!)_E^A \times (n!)_E^A \mid ((m+n)!)_E^A.$

2- $\forall n \in \mathbb{N},\ \forall F \subset E, \quad (m!)_E^A \mid (m!)_F^A.$

Un anneau de Dedekind étant noethérien :

Proposition 1.6.3. *Pour tout anneau de Dedekind A, pour toute partie E de A et pour tout entier naturel n, on a :*

$$(n!)_E^A = \prod_{\mathfrak{m}\in\max(A)} (n!)_E^{A\mathfrak{m}}.$$

C'est dans le cadre des anneaux de Dedekind que Bhargava ([8] et [9]) a introduit la généralisation des factorielles.

Cas où $A = \mathbb{Z}$

On a vu que la généralisation de la notion de factorielles impose de remplacer les nombres par des idéaux. Cependant, dans le cas de $\mathbb{Z}$, on pourra toujours considérer l'entier naturel $n!_E$ engendrant l'idéal $(n!)_E^{\mathbb{Z}}$ comme dans les exemples ci-dessous. Les $n!_E$ étant des entiers naturels on peut, à l'instar de $n!$ et $C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$, se poser la question de la recherche d'une interprétation combinatoire des entiers $n!_E$ ou $\frac{n!_E}{k!_E(n-k)!_E}$ (cf. [10]).

EXEMPLES 1.6.4. 1- Il résulte de la propriété 5 de 1.5.4 que, pour tous $a, b \in \mathbb{Z}$:

$$n!_{A+b\mathbb{Z}} = b^n n!.$$

On prouvera un peu plus loin que (cf. exemples 1.7.4 et proposition 1.8.5) :
2- Si $N^{(2)} = \{n^2 \mid n \in \mathbb{N}\}$, alors

$$n!_{\mathbb{N}^{(2)}} = \frac{1}{2}(2n)!.$$

3- Si q désigne un entier ≥ 2 et si $E(q) = \{q^n \mid n \in \mathbb{N}\}$, les factorielles correspondantes dites *factorielles de Jackson* sont égales à :

$$n!_{E_(q)} = q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1).$$

Interprétation. Dans le cas où q est une puissance d'un nombre premier, l'entier $n!_{E(q)}$ est aussi le nombre d'éléments du groupe $GL(n, \mathbb{F}_q)$ et l'entier $\frac{n!_{E(q)}}{k!_{E(q)}(n-k)!_{E(q)}}$ est aussi le nombre de sous-espaces vectoriels de dimension k d'un espace vectoriel de dimension n sur $\mathbb{F}_q$.

D'après les propriétés 2 et 4 de 1.5.4, quel que soit le sous-ensemble infini E de $\mathbb{Z}$, la suite d'entiers $n!$ est croissante et, pour tout n, $n!$ divise $n!_E$.

Exercice 1.6.5. (ouvert). Caractériser les suites d'entiers naturels $(k_n)_{n\in\mathbb{N}}$ qui correspondent à des idéaux factoriels, c'est-à-dire, pour lesquelles il existe une partie E de $\mathbb{Z}$ telle que

$$\forall n \in \mathbb{N}, \quad n!_E = k_n.$$

On a des conditions nécessaires :
1- $k_0 = 1$,
2- $\forall m, n \in \mathbb{N}, \quad k_n k_m | k_{n+m}$,
3- $\forall n \in \mathbb{N}, \quad n! | k_n$.

1.7 Suites v-ordonnées : cas des valuations discrètes

On vient de voir que pour étudier les idéaux factoriels $(n!)_E^A$ dans le cas d'un anneau de Dedekind A, on peut 'localiser', c'est-à-dire, remplacer A par $A_{\mathfrak{m}}$ où $\mathfrak{m}$ décrit $\max(A)$ et où donc $A_{\mathfrak{m}}$ est un anneau de valuation discrète. La notion de suite v-ordonnée est introduite par Bhargava ([8], [9], [10]) justement dans le cadre des anneaux de valuation discrète en fait pour pouvoir définir les factorielles. Nous avons défini les factorielles directement à l'aide des polynômes à valeurs entières, cependant les suites v-ordonnées vont s'avèrer un outil très utile pour l'étude locale des polynômes à valeurs entières et des factorielles généralisées.

Rappel (cf. Bourbaki [7, VI]). Une *valuation* discrète sur un corps K est une application $v : K^* \to \mathbb{Z}$ telle que, pour tous $x,\ y \in K^*$, on ait :

$v(x+y) \geq \min(v(x), v(y))$,
$v(xy) = v(x) + v(y)$,
$v(1) = 0$.

On prolonge v en posant $v(0) = +\infty$. On vérifie que, pour tous $x,\ y \in K^*$:

$$\text{Si } \ v(x) \neq v(y), \ \text{ alors } \ v(x+y) = \inf(v(x), v(y)).$$

Si v est une valuation discrète sur K, alors $A = \{x \in K \mid v(x) \geq 0\}$ est un anneau appelé *anneau de la valuation* v. Cet anneau est local (possède un seul) d'idéal maximal $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$ et donc l'ensemble des éléments inversibles de A est $A^\times = \{x \in K \mid v(x) = 0\}$.

Remarque 1.7.1. Les exposant $v_{\mathfrak{m}}(I)$ de la proposition 1.6.1 induisent des valuation discrètes sur le corps des fractions K de l'anneau de Dedekind A par :

$$x \in K^* \mapsto v_{\mathfrak{m}}(xA) \in \mathbb{Z}.$$

Hypothèses et notations. *Soit V l'anneau d'une valuation discrète v et soit E une partie de V. On note K le corps des fractions de V, $\mathfrak{m}$ l'idéal maximal de V, t une uniformisante, c.-à-d. un générateur de $\mathfrak{m}$, et q le cardinal (fini ou infini) du corps résiduel $A/\mathfrak{m}$.*

Définition 1.7.2. Une suite v*-ordonnée* de E est une suite (finie or infinie) $(a_n)_{n=0}^N$ d'éléments distincts de E telle que, pour $1 \leq n \leq N$, on ait :

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \min_{x \in E}\ v\left(\prod_{k=0}^{n-1}(x - a_k)\right).$$

Le nombre N est appelé la *longueur* de la suite.

Remarques 1.7.3. 1- Pour tout $N < Card(E)$, il existe toujours des suites v-ordonnées de E de longueur N. De telles suites se construisent de façon inductive : on choisit pour a_0 n'importe quel élément de E, puis $a_0, a_1, \ldots, a_{n-1}$ étant fixés, on choisit a_n parmi les y tels que :

$$v\left(\prod_{k=0}^{n-1}(y-a_k)\right) = \min_{x\in E} v\left(\prod_{k=0}^{n-1}(x-a_k)\right).$$

2- Notons q_1 le nombre de classes de V modulo $\mathfrak{m}$ rencontrées par E. Une suite $(a_n)_{0\leq n<q_1}$ d'éléments de E est une suite v-ordonnée de E si et seulement si les a_n sont dans des classes distinctes modulo $\mathfrak{m}$. En particulier, lorsque q_1 est infini, il existe toujours des suites infinies v-ordonnées de E, mais dans ce cas $\mathrm{Int}(E,V) = V[X]$.
3- Si $(u_n)_{n=0}^N$ est une suite v-ordonnée de E et si $x \in E$ vérifie $v(x-u_N) > \max_{0\leq n<N} v(u_N-u_n)$, alors $(u_0, u_1, \ldots, u_{N-1}, x)$ est une suite v-ordonnée de E.

EXEMPLES 1.7.4. Pour $p \in \mathbb{P}$, notons v_p la valuation p-adique de $\mathbb{Q}$.

1- La suite des entiers naturels (et plus généralement, pour tout $k \in \mathbb{Z}$, la suite $(n)_{n\geq k}$) est une suite v_p-ordonnée de $\mathbb{N}$, et aussi de $\mathbb{Z}$, pour tout $p \in \mathbb{P}$.

2- Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$ tel que p ne divise pas b. Alors la suite $(a+kb)_{k\in\mathbb{N}}$ est une suite v_p-ordonnée de $\mathbb{Z}$.

3- Plus généralement, pour tous $a \in V$ et $b \in V^\times$, si $(u_n)_{n=0}^N$ est une suite v-ordonnée de E, alors $(a+bu_n)_{n=0}^N$ est une suite v-ordonnée de $F = a+bE = \{a+bx \mid x \in E\}$.

4- Soit r un entier ≥ 2 et soit $E(r) = \{r^n \mid n \in \mathbb{N}\}$. Alors la suite $(r^n)_{n\in\mathbb{N}}$ est une suite v_p-ordonnée de $E(r)$ pour tout $p \in \mathbb{P}$.

5- Soit $\mathbb{N}^{(2)} = \{n^2 \mid n \in \mathbb{N}\}$. La suite $(n^2)_{n\in\mathbb{N}}$ est une suite v_p-ordonnée de $\mathbb{N}^{(2)}$ pour tout $p \in \mathbb{P}$ (cf. exercice 1.8.2). L'assertion n'est plus vraie pour la suite $(n^2)_{n\in\mathbb{N}^*}$.

6- Pour tout $p \in \mathbb{P}$, la suite $(a_n)_{n\in\mathbb{N}^*}$ où a_n est défini par $a_n = n + \left[\frac{n-1}{p-1}\right]$ est une suite v_p-ordonnée de $\mathbb{N} \setminus p\mathbb{N}$.

Voici maintenant un exemple fondamental :

Proposition 1.7.5. *Supposons $q = Card(A/\mathfrak{m})$ fini et soit $a_0 = 0, a_1, \ldots, a_{q-1}$ un système de représentants de V modulo $\mathfrak{m}$. Si n s'écrit $n_k n_{k-1} \cdots n_1 n_0$ en base q, c'est-à-dire :*

$$n = n_0 + n_1 q + n_2 q^2 + \cdots + n_k q^k \quad \text{avec} \quad 0 \leq n_j < q,$$

on pose :

$$u_n = u_{n_0} + u_{n_1}t + u_{n_2}t^2 + \ldots + u_{n_k}t^k.$$

Alors,

(1) $\forall m, n \in \mathbb{N},\ v(u_n - u_m) = v_q(m-n)$

où $v_q(x)$ désigne la plus grande puissance de q qui divise $m-n$.

(2) $\forall r, s \in \mathbb{N},\ \{u_{r+1}, u_{r+2}, \ldots, u_{r+q^s}\}$ *est un système complet de représentants de* $V \pmod{\mathfrak{m}^s}$.

(3) $v\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \sum_{k\geq 1}\left[\frac{n}{q^k}\right]$.

(4) *La suite (u_n) est une suite v-ordonnée de V.*

Notation. Pour tout $n \in \mathbb{N}$, on pose :

$$w_q(n) = \sum_{k\geq 1}\left[\frac{n}{q^k}\right].$$

[Lorsque q sera infini, on posera $w_q(n) = 0$ pour tout $n \in \mathbb{N}$.]

Preuve. (1) $v_q(m-n) = s$ signifie que $u_{n_i} = u_{m_i}$ pour $0 \leq i < s$ et $u_{n_s} \neq u_{m_s}$.

(2) : $Card(A/\mathfrak{m}^s) = q^s$ or, d'après (1), les q^s éléments sont non congrus modulo $\mathfrak{m}^s$.

(3) résulte de (2) et de ce que :

$$\sum_{k>0} k\left\{\left[\frac{n}{q^k}\right] - \left[\frac{n}{q^{k+1}}\right]\right\} = \sum_{k>0}\left[\frac{n}{q^k}\right].$$

(4) : posons, pour tout $n \in \mathbb{N}$, $g_n(X) = \prod_{k=0}^{n-1}(X - u_k)$. On a $v(g_n(u_n)) = w_q(n)$. Il s'agit de vérifier que, pour tout $x \in V$, $v(g_n(x)) \geq w_q(n)$. Si $g_n(x) \neq 0$, il existe $m \geq n$ tel que $v(x - u_m) > v(g_n(x))$ et alors $v(g_n(x)) = v(g_n(u_m))$. Or, $v(g_n(u_m)) =$

$$= \sum_{k=0}^{n-1} v(u_m - u_k) = \sum_{k=0}^{n-1} v_q(m-k) = \sum_{k\geq 1}\left[\frac{m}{q^k}\right] - \sum_{k\geq 1}\left[\frac{m-n}{q^k}\right] \geq w_q(n).$$

Remarque 1.7.6. (qui servira plus tard). Selon la preuve effectuée, si une suite (u_n) vérifie l'assertion (1) de la proposition 1.7.5, alors elle vérifie l'assertion (2) et, si elle vérifie l'assertion (2), alors elle vérifie l'assertion (3).

Exercice 1.7.7. Si n s'écrit $n_k \cdots n_1 n_0$ en base q, alors

$$w_q(n) = \frac{n - (n_0 + n_1 + \ldots + n_k)}{q-1}.$$

1.8 Suites v-ordonnées et polynômes

Utilisons maintenant les suites v-ordonnées pour l'étude des polynômes à valeurs entières et des factorielles. Les hypothèses et notations sont toujours celles de la section précédente.

Proposition 1.8.1. *Soit $(a_n)_{n=0}^N$ une suite d'éléments distincts de E. Pour tout $n \in \mathbb{N}$, posons :*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}.$$

Les assertions suivantes sont équivalentes :

1. *La suite $(a_n)_{n=0}^N$ est une suite v-ordonnée de E.*
2. *$f_n(X) \in \mathrm{Int}(E, V)$ pour $0 \leq n \leq N$.*
3. *Les $(f_n(X))_{n=0}^N$ forment une base du V-module $\mathrm{Int}_N(E, V)$.*
4. *Pour tout $f(X) \in K[X]$ de degré $\leq N$,*
   $f \in \mathrm{Int}_N(E, V)$ si et seulement si $f(a_n) \in V$ pour $0 \leq n \leq N$.

On notera que, les f_n formant une base du K-espace vectoriel $K_N[X] = \{g \in K[X] \mid \deg(g) \leq N\}$, ils formeront une base du V-module $\mathrm{Int}_N(E, V)$ dès que les f_n seront dans $\mathrm{Int}(E, V)$ puisque $f_n(a_n) = 1$ pour tout $n \leq N$.

Exercices 1.8.2. 1- Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$ tel que p ne divise pas b. Montrer qu'un polynôme $f \in \mathbb{Q}[X]$ de degré n appartient $\mathrm{Int}(\mathbb{Z})$ si et seulement si les valeurs $f(a + kb) \in \mathbb{Z}$ pour $k = 0, 1, \ldots, n$.
Application : considérer $P(X) = \prod_{k=0}^{n-1} \frac{X^2 - k^2}{n^2 - k^2}$ et déterminer $n!_{\mathbb{N}^{(2)}}$.
2- Soit $r \geq 2$ et soit $E(r) = \{r^n \mid n \in \mathbb{N}\}$. En utilisant le fait $(r^n)_{n \in \mathbb{N}}$ est une suite v-ordonnée de $E(r)$, montrer que les *coefficients binomiaux de Gauss* $\left[\begin{array}{c} n \\ k \end{array} \right]_r$ $(1 \leq k \leq n)$ sont des entiers naturels où

$$\left[\begin{array}{c} n \\ k \end{array} \right]_r = \frac{(r^n - 1)(r^{n-1} - 1) \cdots (r^{n-k+1} - 1)}{(r - 1)(r^2 - 1) \cdots (r^k - 1)}.$$

Ce que l'on pourrait aussi démontrer par récurrence à l'aide de la formule :

$$\left[\begin{array}{c} n+1 \\ k \end{array} \right]_r = \left[\begin{array}{c} n \\ k \end{array} \right]_r + \left[\begin{array}{c} n \\ k-1 \end{array} \right]_r r^{n-k+1}.$$

Bien que l'on puisse avoir une infinité des suites v-ordonnées pour un même ensemble E, la proposition 1.8.1 montre que :

Corollaire 1.8.3. *Si $\{a_n\}_{n=0}^N$ est une suite v-ordonnée de E alors, pour $n \leq N$, on a* :

$$(n!)_E^V = \mathfrak{I}_n(E,V)^{-1} = \prod_{k=0}^{n-1}(a_n - a_k)V,$$

et la somme

$$w_E(n) = \sum_{k=0}^{n-1} v(a_n - a_k)$$

ne dépend pas du choix de la suite v-ordonnée de E.

Définition 1.8.4. Pour toute partie E de V, on appelle *fonction caractéristique* de E et on note w_E la fonction arithmétique suivante :

$$n \in \mathbb{N} \mapsto w_E(n) = v\left((n!)_E^V\right) \in \mathbb{N} \cup \{+\infty\}.$$

De sorte que :

$$(n!)_E^V = \mathfrak{m}^{w_E(n)},$$

et la proposition 1.6.3 se formule de la façon suivante :

Proposition 1.8.5. *Soient A un anneau de Dedekind et F une partie de A. Pour tout idéal maximal $\mathfrak{m}$ de A, notons $v_\mathfrak{m}$ la valuation correspondante et $w_{\mathfrak{m},F}$ la valuation de l'idéal $(n!)_F^A\mathfrak{m}$. On a :*

$$(n!)_E^A = \prod_{\mathfrak{m}\in\max(A)} \mathfrak{m}^{w_{\mathfrak{m},E}(n)}.$$

Il s'agit donc de déterminer ces fonctions arithmétiques $w_{\mathfrak{m},F}$.

Proposition 1.8.6. *Soit $(g_n)_{n=0}^N$ une suite de polynômes de $\mathrm{Int}(E,V)$ tels que $\deg(g_n) = n$. Alors $(g_n)_{n=0}^N$ est une base de $\mathrm{Int}_n(E,V)$ si et seulement si, pour $0 \leq n \leq N$, le coefficient directeur de g_n a pour valuation $-w_E(n)$.*

On montre la suffisance par récurrence sur N. En effet, pour tout $f \in \mathrm{Int}(E,V)$, il existe $a \in V$ tel que $\deg(f - ag) < N$.

Corollaire 1.8.7. *Si $(a_n)_{0\leq n\leq N}$ est une suite v-ordonnée de E, alors les polynômes*

$$f_n^*(X) = t^{w_E(n)} \prod_{k=0}^{n-1} (X - a_k) \quad (0 \leq n \leq N)$$

forment une base de $\mathrm{Int}_N(E, V)$.

Dans la suite du paragraphe, le cardinal q du corps résiduel est supposé fini.

Proposition 1.8.8 (Pólya [4])**.** *Si V est un anneau de valuation discrète cardinal q, alors*

$$w_V(n) = w_q(n) = \sum_{k\geq 1} \left[\frac{n}{q^k} \right].$$

Exercice 1.8.9. (facile) Montrer que si V désigne l'anneau de valuation discrète $\mathbb{F}_2[[T]]$, alors $w_V(n) = v_2(n!)$.

Définition 1.8.10. On appelle *binôme de Fermat* de V le polynôme

$$F_q(X) = \frac{X^q - X}{t}.$$

Pour tout $n = n_0 + n_1 q + \cdots + n_k q^k$, on appelle n-ième *polynôme de Fermat* de V le polynôme

$$F_n = \prod_{j=0}^{k} \left(F_q^{*j}\right)^{n_j}$$

où F_q^{*j} désigne le j-ième itéré de F_q, c'est-à-dire,

$$F_q^{*j}(X) = F_q(F_q^{*(j-1)}(X)).$$

Proposition 1.8.11. *Les polynômes de Fermat F_n forment une base de* $\mathrm{Int}(V)$.

Il suffit de vérifier que $F_n \in \mathrm{Int}(V)$, $\deg(F_n) = n$ et le coefficient directeur de F_n est $t^{-w_q(n)}$.

1.9 Une étude de cas

Hypothèses et notations. *Soient V l'anneau d'une valuation discrète v, K le corps des fractions de V, $\mathfrak{m}$ l'idéal maximal de V et q le cardinal (fini ou infini) du corps résiduel $A/\mathfrak{m}$.*

Nous allons déterminer la fonction $w_E(n)$ pour une partie E de V qui est une réunion finie de classes modulo $\mathfrak{m}^l$, donc de la forme :

$$E = \cup_{i=1}^{r}(b_i + \mathfrak{m}^l) \quad \text{avec } l \in \mathbb{N}^*,\ b_i \not\equiv b_j \pmod{\mathfrak{m}^l} \quad \forall i \neq j.$$

On commence par un lemme qui s'avère souvent utile :

Lemme 1.9.1. *Soient F une partie de V et b un élément de V. Si $(a_n)_{n=0}^{M}$ est une suite v-ordonnée de F, alors la sous-suite extraite formée des a_n qui appartiennent à $b + \mathfrak{m}^l$ est une suite v-ordonnée de $(b + \mathfrak{m}^l) \cap F$.*

Preuve. Remarquons tout d'abord que même si la suite (a_n) est infinie, la sous-suite formée des éléments a_n qui sont dans $F_1 = (b + \mathfrak{m}^l) \cap F$ peut être finie. Si cette sous-suite est vide ou réduite à un élément, il n'y a rien à montrer. On raisonne par récurrence sur n : on suppose que les n premiers éléments $a_{k_0}, a_{k_1}, \ldots, a_{k_{n-1}}$ forment une suite v-ordonnée de F_1. Montrons que, s'il existe un suivant a_{k_n} dans F_1, alors $a_{k_0}, a_{k_1}, \ldots, a_{k_n}$ est une suite v-ordonnée de F_1. Posons $N = k_n$. Pour tout $x \in F_1$, on a :

$$\sum_{k=0}^{N-1} v(x - a_k) = \sum_{k<N,\, a_k \in F_1} v(x - a_k) + \sum_{k<N,\, a_k \notin F_1} v(x - a_k).$$

Pour $a_k \notin F_1$, on a $v(b - a_k) < l$, tandis que $v(x - b) \geq l$, d'où :

$$\sum_{k<N,\, a_k \notin F_1} v(x - a_k) = \sum_{k<N,\, a_k \notin F_1} v(b - a_k)$$

et cette somme ne dépend pas du choix de $x \in F_1$. Or, par hypothèse, la somme $\sum_{k=0}^{N-1} v(x - a_k)$ est minimale, lorsque x décrit F, pour $x = a_{k_n}$. Donc, la somme

$$\sum_{k<N,\, a_k \in F_1} v(x - a_k) = \sum_{i=0}^{N-1} v(b - a_{k_i})$$

est aussi minimale pour ce choix de x dans F_1.

Notations. Pour $1 \leq j \leq r$ et $\delta_1, \ldots, \delta_r \in \mathbb{N}$, soit

$$w_E^j(\delta_1, \ldots, \delta_r) = w_q(\delta_j) + l\delta_j + \sum_{i \neq j} v(b_i - b_j)\delta_i.$$

Lemme 1.9.2. *Pour $1 \leq j \leq r$, soit $\delta_j \in \mathbb{N}$ et soient $a_{j,1}, \ldots, a_{j,\delta_j}$ des éléments de $b_j + \mathfrak{m}^l$ qui forment une suite v-ordonnée de $b_j + \mathfrak{m}^l$. Considérons le polynôme*

$$g(X) = \prod_{j=1}^{r} \left(\prod_{k=1}^{\delta_j} (X - a_{j,k}) \right).$$

Alors, pour tout j, on a :

$$\min \left\{ v(g(x)) \mid x \in b_j + \mathfrak{m}^l \right\} = w_E^j(\delta_1, \ldots, \delta_r).$$

Proposition 1.9.3. *[11] Avec les hypothèses et notations précédentes, on a :*

$$w_E(n) = \max_{\delta_1 + \ldots + \delta_r = n} \left(\min_{1 \leq j \leq r} w_E^j(\delta_1, \ldots, \delta_r) \right).$$

On peut donc calculer la fonction w_E en oubliant les suites v-ordonnées.

Corollaire 1.9.4. *Si $v(b_i - b_j) = h$ pour tous $i \neq j$ où $0 \leq h < l$, alors :*

$$w_E(n) = w_q\left(\left[\frac{n}{r} \right] \right) + (l - h) \left[\frac{n}{r} \right] + hn.$$

EXEMPLE 1.9.5. Si $E = \mathbb{Z} \setminus p\mathbb{Z}$ où p désigne un nombre premier, alors

$$w_E(n) = \sum_{k \geq 0} \left[\frac{n}{(p-1)p^k} \right].$$

Corollaire 1.9.6. *[12] Supposons q infini. Soit $B = (\beta_{i,j}) \in \mathcal{M}_r(\mathbb{N})$ la matrice symétrique définie par*

$$\beta_{i,j} = v(b_i - b_j) \ \ pour \ \ i \neq j \quad et \quad \beta_{i,i} = l.$$

Posons

$$\nu(B) = \sum_{1 \leq i \leq r} \det(B_i)$$

où B_i est la matrice déduite de B en remplaçant la i-ème colonne par une colonne de 1. *Alors, pour*

$$n = m\nu(B) + n_0 \quad \text{avec} \quad m, n_0 \in \mathbb{N},$$

on a

$$w_E(n) = w_E(m\nu(B)) + w_E(n_0) = m\det(B) + w_E(n_0).$$

Corollaire 1.9.7. *Supposons q fini. Soit $B^* = B + \frac{1}{q-1}I_r$. Alors,*

$$\lim_{n\to+\infty} \frac{w_E(n)}{n} = \frac{\det(B^*)}{\nu(B^*)}.$$

EXEMPLE 1.9.8. Si $E = \mathbb{Z} \setminus p^2\mathbb{Z}$ où p désigne un nombre premier, alors

$$\lim_{n\to+\infty} \frac{w_E(n)}{n} = \frac{p(p^2-p+1)}{(p-1)^2(p^2+1)}.$$

1.10 Suites v-ordonnées générales

La notion de suite v-ordonnées peut a priori être considérée dans un anneau de valuation quelconque.

Définition 1.10.1. (cf. Bourbaki [7, VI]) Soient K un corps et Γ un groupe abélien totalement ordonné. Une *valuation* sur K à valeurs dans Γ est une application $v : K^* \to \Gamma$ telle que, pour tous $x,\ y \in K^*$, on ait :

$v(x+y) \geq \min(v(x), v(y))$,
$v(xy) = v(x) + v(y)$,
$v(1) = 0$.

On prolonge v en posant $v(0) = \infty$, on prolonge l'ordre de Γ en un ordre sur $\Gamma \cup \{\infty\}$ en posant $\gamma < \infty$ pour tout $\gamma \in \Gamma$, et on prolonge les relations ci-dessus en posant $\gamma + \infty = \infty$ pour tout $\gamma \in \Gamma \cup \{\infty\}$.

Pour tous $x,\ y \in K^*$, si $v(x) \neq v(y)$, alors $v(x+y) = \inf(v(x), v(y))$.

Si v est une valuation sur K, alors

$$A = \{x \in K \mid v(x) \geq 0\}$$

est un anneau local appelé *anneau de la valuation* v dont l'idéal maximal est $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$ et le groupe des unités $A^\times = \{x \in K \mid v(x) = 0\}$.

EXEMPLE 1.10.2. Soient $a \in \mathbb{Z}$ et $p \in \mathbb{P}$. L'anneau

$$W_{a,p} = \{R(X) \in \mathbb{Q}(X) \mid v_p(R(a)) \geq 0\}$$

est l'anneau d'une valuation de groupe de valeurs $\Gamma = \mathbb{Z} \times \mathbb{Z}$ muni de l'ordre lexicographique.

En fait, *dans un souci de simplification*, on va supposzer d'emblée que la valuation v est de hauteur 1, c'est-à-dire que le groupe de valeurs $\Gamma = v(K^*)$ est isomorphe à un sous-groupe de $\mathbb{R}$ (bien que tous les résultats qui suivent restent valables pour une valuation quelconque et ceci jusqu'au paragraphe § 1.13).

Hypothèses et notations. *Soient V un anneau de valuation de hauteur 1 et E une partie de V. On note K le corps des fractions de V, v la valuation correspondante de K et $\mathfrak{m}$ l'idéal maximal de V.*

On a $\Gamma = v(K^*) \subset \mathbb{R}$. Le corps K est un corps valué non archimédien muni de la valeur absolue $|x| = e^{v(x)}$ pour $x \in K^*$.

La définition des suites v-ordonnées est formellement la même :

Définition 1.10.3. Une suite *v-ordonnée* de E est une suite (finie or infinie) $(a_n)_{n=0}^N$ d'éléments distincts de E tel que, pour $1 \leq n \leq N$, on ait :

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) \leq v\left(\prod_{k=0}^{n-1}(x - a_k)\right) \quad \text{pour tout } x \in E.$$

Le nombre N est appelé la *longueur* de la suite.

Remarques 1.10.4. 1- Si la valuation v n'est pas discrète, on doit supposer, à chaque étape n, l'existence d'un minimum pour $v(\prod_{k=0}^{n-1}(x - a_k))$. Or, ceci n'est pas toujours le cas comme le montre le contre-exemple suivant. Supposons que $E = \mathfrak{m}$ et que l'idéal $\mathfrak{m}$ ne soit pas principal, alors $v(a - a_0) > 0$ pour tous a_0, $a \in \mathfrak{m}$, tandis que $\inf_{x \in \mathfrak{m}} v(x - a_0) = 0$. Par conséquent, il n'existe pas dans ce cas de suite v-ordonné de E.

2- L'existence d'un minimum est évidemment satisfaite lorsque l'ensemble E est fini, ou plus généralement si E est compact relativement à la topologie induite par v. En fait, il suffit que E soit *précompact*, c'est-à-dire, que le complété $\widehat{E}$ of E soit compact. Nous y reviendrons (cf. § 1.12).

L'utilisation des suites v-ordonnées pour l'étude des polynômes à valeurs entières et des factorielles est formellement la même. Rappelons les énoncés.

Proposition 1.10.5. *Soit $(a_n)_{n=0}^N$ une suite d'éléments distincts de E. Alors, $(a_n)_{n=0}^N$ est une suite v-ordonnée de E si et seulement si les polynômes*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}$$

forment une base du V-module $\mathrm{Int}_N(E, V)$.

Corollaire 1.10.6. *Soit $(a_n)_{n=0}^N$est une suite v-ordonnée de E. Un polynôme $f \in K[X]$ de degré $\leq N$ appartient à $\mathrm{Int}(E, V)$ si et seulement si ses valeurs $f(a_0), f(a_1), \ldots, f(a_N)$ sont dans V.*

Corollaire 1.10.7. *Si $(a_n)_{n=0}^N$ est une suite v-ordonnée de E alors, pour $n \leq N$, on a* :

$$(n!)_E^V = \mathfrak{I}_n(E, V)^{-1} = \prod_{k=0}^{n-1} (a_n - a_k)V,$$

et la somme

$$w_E(n) = \sum_{k=0}^{n-1} v(a_n - a_k)$$

ne dépend pas du choix de la suite v-ordonnée de E.

Remarque 1.10.8. Ainsi, s'il existe une suite v-ordonnée $(a_n)_{n=0}^N$ de E alors, pour $0 \leq n < N$, $(n!)_E^V$ est un idéal principal, à savoir l'idéal principal engendré par l'élément $\prod_{k=0}^{n-1}(a_n - a_k)$. En revanche, les $(n!)_E$ peuvent être principaux sans qu'il existe de suites v-ordonnées comme le montre le contre-exemple suivant.

EXEMPLE 1.10.9. Si $E = \mathfrak{m}$ et si $\mathfrak{m}$ n'est pas principal, alors $\mathrm{Int}(\mathfrak{m}, V) = V[X]$. Par suite, $(n!)_{\mathfrak{m}}^V = V$ pour tout n, alors qu'il n'existe pas de suite v-ordonnée de $\mathfrak{m}$. Preuve : si $Q \in \mathrm{Int}(\mathfrak{m}, V)$ et $\deg(Q) = n$ alors, pour tout $a \in \mathfrak{m}$, $a \neq 0$, $dQ \in V[X]$ où $d = V(1, a, \ldots, a^n)$ (cf. proposition 1.4.6). Or, $v(a)$ peut être aussi petit que l'on veut, donc $v(d) = \frac{n(n^2-1)}{6}\, v(a)$ aussi.

Proposition 1.10.10. *Une suite $(b_n)_{n=0}^N$ déléments de E est une suite v-ordonnée de E si et seulement si, pour tout $n \in \{1, \ldots, N\}$, on a :*

$$\prod_{0 \leq i < j \leq n} (b_j - b_i)V = (1!)_E^V (2!)_E^V \cdots (n!)_E^V.$$

Proposition 1.10.11. *Soit $a_0, a_1, \ldots, a_n$ une suite v-ordonnée de E. Quels que soient $x_0, x_1, \ldots, x_n$ dans E, on a :*

$$\prod_{0\leq i<j\leq n} \frac{x_j - x_i}{a_j - a_i} \in V.$$

Preuve. Soit $F = \{x_0, \ldots, x_n\}$. On peut supposer que les x_i sont ordonnés de façon à former une suite v-ordonnée de F. Alors

$$\prod_{0\leq i<j\leq n} (x_j - x_i) = \prod_{j=1}^{n} \left(\prod_{i=0}^{j-1} (x_j - x_i) \right) = \sum_{j=1}^{n} w_F(j) \geq$$

$$\sum_{j=1}^{n} w_E(j) = \prod_{j=1}^{n} \left(\prod_{i=0}^{j-1} (a_j - a_i) \right) = \prod_{0\leq i<j\leq n} (a_j - a_i).$$

D'où :

Corollaire 1.10.12. *Pour tous entiers $x_0, x_1, \ldots, x_n$,*

$$\prod_{0\leq i<j\leq n} (x_j - x_i) \quad \text{est divisible par } 1! \times 2! \times \cdots \times n!$$

Exercice 1.10.13. Montrer que quels que soient les $n+1$ entiers $x_0, x_1, \ldots, x_n$,

$$\prod_{0\leq i<j\leq n} (x_j^2 - x_i^2) \text{ est divisible par } \frac{2! \cdots (2n)!}{2^{n+1}}.$$

1.11 Contenu et diviseur d'un polynôme

On conserve les hypothèses et notations de la section précédente.

Définitions 1.11.1. (**et notations**) Pour tout anneau intègre R de corps des fractions L, pour toute partie F de R et pour tout polynôme

$$g = \sum_j c_j X^j \in L[X],$$

— on appelle *contenu* de g et on note $c(g)$ l'idéal fractionnaire de R engendré par les coefficients de g:

$$c(g) = \sum_j c_j R$$

— on appelle *diviseur* de g sur F et on note $d(g,F)$ l'idéal fractionnaire de R engendré par les valeurs de g sur F:

$$d(g,F)=\sum_{x\in F} g(x)R.$$

Proposition 1.11.2. *Supposons qu'il existe une suite v-ordonnée $(a_k)_{k=0}^n$ de E. Soit $f\in \mathrm{Int}(E,V)$ de degré $\leq n$ que l'on écrit sous la forme :*

$$f(X)=\sum_{k=0}^{n} b_k f_k(X) \quad avec \quad f_k(X)=\prod_{l=0}^{k-1}\frac{X-a_l}{a_k-a_l}.$$

Alors,

1. $c(f)(n!)_E^V$ *est un idéal entier.*
2. $d(f,E)=(f(a_0),f(a_1),\ldots,f(a_n))=(b_0,\ldots,b_n)$.
3. $c(f)(n!)_E^V\subseteq d(f,E)\subseteq c(f)$.

En outre,

$$pour\ \ f=\prod_{k=0}^{n-1}(X-a_k),\ \ on\ a\ \ c(f)=V\ \ et\ \ d(f,E)=(n!)_E.$$

Preuve. 1- résulte de ce que, pour $k\leq n$, $(k!)_E^V|(n!)_E^V$ et de l'égalité :

$$c(f)=\left(b_0,\frac{b_1}{a_1-a_0},\ldots,\frac{b_n}{\prod_{k=0}^{n-1}(a_n-a_k)}\right).$$

2- résulte des inclusions successives :

$$d(f,E)\subseteq(b_0,\ldots,b_n)\subseteq(f(a_0),\ldots,f(a_n))\subseteq d(f,E).$$

3. Il est clair que $d(f,E)\subseteq c(f)$. D'autre part, l'égalité dans la preuve de 1 montre que $c(f)(n!)_E^V$ est contenu dans $(b_0,b_1,\ldots,b_n)$ qui par 2 est égal à $d(f,E)$.

Remarque 1.11.3. Les inclusions précédentes signifient que, pour tout $f\in K[X]$ de degré $\leq n$, on a :

$$v(c(f))\leq v(d(f,E))\leq v(c(f))+w_E(n).$$

Mais ces inégalités ont été obtenues sous réserve de l'existence d'une suite v-ordonnée pour la partie E. Nous allons voir qu'elles ont lieu dans un cadre beaucoup plus général (cf. proposition 1.14.2).

1.12 Parties précompactes et parties pseudo-précompactes

Les hypothèses et notations sont toujours celles de § 1.10 : V est l'anneau d'une valuation de hauteur 1 et E est une partie de V.

Le complété $\widehat{K}$ de K est lui-même un corps muni d'une valuation qui étend v, que l'on notera encore v et qui a même groupe des valeurs Γ. L'anneau de valuation correspondant est le complété $\widehat{V}$ de V et l'idéal maximal de $\widehat{V}$ est le complété $\widehat{\mathfrak{m}}$ de $\mathfrak{m}$.

Parties précompactes

Rappelons qu'une partie E est dite *précompacte* si sa fermeture topologique $\widehat{E}$ dans $\widehat{K}$ est compacte. Comme la topologie est métrisable cela revient à dire que toute suite d'éléments de E possède un point d'accumulation (dans $\widehat{E}$).

Proposition 1.12.1. *Soit E une partie non vide de V. Les assertions suivantes sont équivalentes :*

1. *E est précompacte pour la topologie induite par la valuation v.*
2. *Pour tout idéal non nul $\mathfrak{I}$ de V, E rencontre au plus un nombre fini de classes de V modulo $\mathfrak{I}$.*
3. *Pour tout $n \in \mathbb{N}^*$, E rencontre au plus un nombre fini de classes de V modulo $\mathfrak{I}_n = \{x \in V \mid v(x) \geq n\}$.*

Corollaire 1.12.2. *Les assertions suivantes sont équivalentes :*

1. *L'anneau de valuation V est précompact.*
2. *La valuation est discrète et le corps résiduel est fini.*
3. $\mathrm{Int}(V) \neq V[X]$.

Lemme 1.12.3. *Supposons la partie E précompacte. Alors,*
(i) v atteint un minimum sur E,
(ii) pour tout polynôme $P(X) \in K[X]$, $P(E)$ est précompact et $v(P(x))$ atteint un minimum sur E,
(iii) E possède des suites v-ordonnées.

Proposition 1.12.4. *Si E est précompacte, alors toute suite v-ordonnée de E est dense dans E.*

On trouve une preuve directe de cette proposition lorsque la valuation est discrète dans [14, prop. 5]. Ce sera toutefois une conséquence de la version p-adique du théorème de Stone-Weierstrass que l'on montrera au chapitre 3.

Corollaire 1.12.5. *Lorsque E est précompact, tous les points isolés de E apparaissent dans toutes les suites v-ordonnées infinies de E.*

Parties pseudo-précompactes

On va voir qu'il existe des suites v-ordonnées pour des parties plus générales que les parties précompactes.

Définition 1.12.6. Une partie E de V est dite *pseudo-précompacte* si, pour tout $\gamma \in \Gamma$ de la forme $\gamma = v(x-y)$ où $x, y \in E$ et $x \neq y$, E rencontre au plus un nombre fini de classes de V modulo $\mathfrak{I}_\gamma = \{z \in V \mid v(z) \geq \gamma\}$.

Remarque 1.12.7. La terminologie 'pseudo' mérite un commentaire. Elle ne fait pas référence à la pseudo-compacité d'un espace topologique car, dans le cas d'une topologie métrisable (ce qui est le cas ici), cette notion coïncide avec la compacité. Il s'agit une référence à la pseudo-convergence introduite par Ostrowski [15] et utilisée par Kaplansky [16] :

Une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de K est dite *pseudo-convergente* si
pour tous $i < j < k$, on a $v(x_j - x_i) < v(x_k - x_j)$.

On peut alors montrer que, de toute suite infinie d'éléments de E, on peut extraire une suite pseudo-convergente dès que la partie E vérifie la propriété suivante (un peu plus forte que la pseudo-précompacité) :

$\forall \gamma = v(x-y)$ où $x, y \in E, x \neq y$, E rencontre au plus un nombre fini de classes modulo $\mathfrak{I}_\gamma^+ = \{z \in| \ v(z) > \gamma\}$.

Proposition 1.12.8. *Si E est une partie infinie pseudo-précompacte de l'anneau de valuation V, elle possède des suites v-ordonnées infinies.*

Proof. First step: for each $x_0 \in E$, the map

$$x \in E \mapsto v(x - x_0) \in \Gamma \cup \{+\infty\}$$

reaches a minimum on E.

Let $\gamma = v(y_0 - x_0)$ where $y_0 \in E,\ y_0 \neq x_0$ and let $\mathfrak{I}_\gamma = \{z \in V \mid v(z) \geq \gamma\}$. Then, there are finitely many $x_1, \ldots, x_r \in E$ such that

$$E \subseteq \cup_{k=0}^{r} \{x_k + \mathfrak{I}_\gamma\} \quad \text{and} \quad v(x_j - x_i) < \gamma \text{ for } 0 \leq i \neq j \leq r.$$

If $r = 0$, then $\inf_{x \in E} v(x - x_0) = \gamma$.
If $r \geq 1$ then, for $k \geq 1$ and $x \in x_k + \mathfrak{I}_\gamma,\ v(x - x_0) = v(x_k - x_0)$; consequently,

$$\inf_{x \in E} v(x - x_0) = \min_{k=1}^{r} v(x_k - x_0).$$

Second step: for each $a_1, a_2, \ldots, a_n \in E$, the map

$$x \in E \mapsto v((x - a_1)(x - a_2) \ldots (x - a_n)) \in \Gamma \cup \{+\infty\}$$

reaches a minimum on E.
First note that, from every infinite sequence of elements of Γ, we may extract either an infinite increasing sequence, or an infinite strictly decreasing sequence. Assume that $x \mapsto g(x) = v((x - a_1) \ldots (x - a_n))$ does not reach a minimum. Then, there exists an infinite sequence $\{y_k\}$ of elements of E such that $\{g(y_k)\}$ is strictly decreasing. Since the subset $\{y_k \mid k \in \mathbb{N}\}$ of E has the same property of finiteness, it follows from the first step that, for every $i \in \{1, \ldots, n\}$, we cannot extract from the sequence $\{v(y_k - a_i)\}$ a strictly decreasing sequence. Consequently, we may extract from the sequence $\{y_k\}$ an infinite sequence $\{z_l\}$ such that, for every i, the sequence $\{v(z_l - a_i)\}$ is increasing. This is a contradiction with the fact that $\{g(z_l)\}$ is stricly decreasing.

EXEMPLE 1.12.9. Let k be a field and Γ be a subgroup of $\mathbb{R}$ (for instance $\Gamma = \mathbb{Q}$). Let $\Gamma_+ = \{\gamma \in \Gamma \mid \gamma \geq 0\}$ and

$$A = k[\Gamma_+] = k[\{T^\gamma \mid \gamma \in \gamma_+\}; T^\gamma T^\delta = T^{\gamma+\delta}]$$

endowed with the valuation v defined by

$$v(\sum_{k=0}^{n} a_k T^{r_k}) = \inf\{r_k \mid a_k \neq 0\}.$$

Let K be the quotient field of A and let V be the corresponding valuation domain. For every stricly increasing sequence $\{r_n\}_{n \in \mathbb{N}}$ of elements of Γ_+ and every finite subset F of k containing 0, we consider the following subset of V:

$$E = \{k_0 t^{r_0} + k_1 t^{r_1} + \ldots + k_l t^{r_l} \mid l \in \mathbb{N},\ k_0, k_1, \ldots, k_l \in F\}.$$

This subset E has the property assumed in Proposition 1.12.8, and hence, there are infinite v-orderings of E. Note that the completion $\widehat{E}$ of E cannot be compact if the sequence $\{r_n\}$ is bounded (and $F \neq \{0\}$) and this may happen as soon as Γ is not isomorphic to $\mathbb{Z}$. We may obtain a v-ordering $\{a_n\}_{n\in\mathbb{N}}$ in the following way. Let $a_0 = 0, a_1, \ldots, a_{q-1}$ be the elements of F. Writing, for each $n \in \mathbb{N}$,

$$n = n_0 + n_1 q + n_2 q^2 + \ldots + n_s q^s \quad \text{where} \quad 0 \leq n_i \leq q-1,$$

we let

$$a_n = a_{n_0} T^{r_0} + a_{n_1} T^{r_1} + \ldots + a_{n_s} T^{r_s}.$$

As a consequence,

$$w_E(n) = r_0 n + \sum_{k>0} \left[\frac{n}{q^k}\right] (r_k - r_{k-1}).$$

Proof. Denoting by $v_q(n)$ the greatest integer k such that q^k divides n, for each n and $m \in \mathbb{N}$ we have:

$$v(a_n - a_m) = r_{v_q(n-m)}.$$

We then may check that

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \sum_{l=1}^{n} r_{v_q(l)}$$

$$= \sum_{k\geq 0} r_k \left(\left[\frac{n}{q^k}\right] - \left[\frac{n}{q^{k+1}}\right]\right) = r_0 n + \sum_{k>0} \left[\frac{n}{q^k}\right](r_k - r_{k-1}).$$

Consequently, for $m \geq n$,

$$v\left(\prod_{k=0}^{n-1}(a_m - a_k)\right) = \sum_{k=0}^{n-1} r_{v_q(m-k)} = \sum_{l=1}^{m} r_{v_q(l)} - \sum_{l=1}^{m-n} r_{v_q(l)}$$

$$= r_0 n + \sum_{k>0} \left(\left[\frac{m}{q^k}\right] - \left[\frac{m-n}{q^k}\right]\right)(r_k - r_{k-1}).$$

By induction on n, it follows from the previous equalities that the sequence $\{a_n\}$ is a v-ordering of E since, for every $m \geq n$,

$$\left[\frac{m}{q^k}\right] - \left[\frac{m-n}{q^k}\right] \geq \left[\frac{n}{q^k}\right].$$

Question ouverte. Caractériser les parties infinies de V admettant une suite v-ordonnée infinie.

1.13 Suites v-ordonnées modulo ϵ

Hypothèses. *On rappelle que V est l'anneau d'une valuation de hauteur 1, c'est-à-dire que $v(K^*) = \Gamma \subset \mathbb{R}$.* (Et, à partir d'ici, l'hypothèse est essentielle.)

In order to extend the previous results concerning w_E to the case where there doesn't exist any v-ordering, we generalize once more the notion of v-ordering:

Définition 1.13.1. Let $\varepsilon \geq 0$. A *v-ordering of E modulo ε* is a sequence $\{b_n\}_{n=0}^N$ of distinct elements of E such that, for each $n \leq N$, one has:

$$v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) \leq v\left(\prod_{k=0}^{n-1}(x - b_k)\right) + \varepsilon \quad \text{for every } x \in E.$$

For $\varepsilon = 0$, we have the classical notion of v-ordering. Although v-orderings do not necessarily exist, on the opposite, there exist v-orderings modulo ε for every $\varepsilon > 0$. Such sequences may be constructed inductively on n choosing any element in E for b_0. Then, the link between v-orderings and integer-valued polynomials becomes:

Lemme 1.13.2. *Let $N < card(E)$, let $\varepsilon > 0$, and let $\{b_n\}_{n=0}^N$ be a v-ordering of E modulo ε. Every polynomial $f \in K[X]$ of degree $\leq N$ may be written*:

$$f(X) = \sum_{n=0}^{N} c_n \prod_{k=0}^{n-1} \frac{X - b_k}{b_n - b_k} \quad \text{with } c_n \in K.$$

If $v(c_n) \geq \varepsilon$ for each $n \leq N$, then f belongs to $\mathrm{Int}(E, V)$. Conversely, if f belongs to $\mathrm{Int}(E, V)$, then $v(c_n) \geq -n\varepsilon$ for each $n \leq N$.

Proof. For each $n \leq N$, let

$$h_n(X) = \prod_{k=0}^{n-1} \frac{X - b_k}{b_n - b_k}.$$

Then,

$$f(X) = \sum_{n=0}^{N} c_n h_n(X).$$

By definition of the sequence $\{b_n\}$, for each $n \leq N$ and for each $x \in E$, one has $v(h_n(x)) \geq -\varepsilon$. Obviously, if $v(c_n) \geq \varepsilon$, then $v(c_n h_n(x)) \geq 0$ for each $x \in E$, and hence, f belongs to $\mathrm{Int}(E, V)$.

Conversely, assuming that f belongs to $\mathrm{Int}(E,V)$, let us prove by induction on n, that $v(c_n) \geq -n\varepsilon$. First, $f(b_0) = c_0 \in V$, and hence $v(c_0) \geq 0$. Let $n \in \{1,\ldots,N\}$ and suppose that $v(c_k) \geq -k\varepsilon$ for $0 \leq k \leq n-1$. Then,

$$f(b_n) = c_0 + c_1 h_1(b_n) + \ldots + c_{n-1}h_{n-1}(b_n) + c_n h_n(b_n).$$

We have $h_n(b_n) = 1$, $v(c_k) \geq -k\varepsilon$, and $v(h_k(b_n)) \geq -\varepsilon$ for $1 \leq k \leq n-1$. Consequently,

$$v(c_n) \geq \left(\inf_{0<k<n} v(c_k)\right) - \varepsilon \geq -n\varepsilon.$$

As an immediate consequence we have:

Lemme 1.13.3. *If $b_0, b_1, \ldots, b_N$ is a v-ordering modulo ε, then for $n \leq N$:*

$$v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) - \varepsilon \leq w_E(n) \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) + n\varepsilon.$$

1.14 La fonction caractéristique w_E (lorsque $\Gamma \subset \mathbb{R}$)

Hypothèses et notations. *Le corps K est un corps valué non-archimédien et E est une partie quelconque de V.*

On va, sans l'aide des suites v-ordonnées, étudier la *fonction caractéristique* de E, à savoir :

$$w_E : n \in \mathbb{N} \mapsto w_E(n) = v\left((n!)_E^V\right) \in \mathbb{R} \cup \{+\infty\}.$$

Recall some basic properties of this nondecreasing function w_E:

$w_E(n) < +\infty \;\Leftrightarrow\; n < card(E)$.
$\forall\, k,l \in \mathbb{N},\ w_E(k) + w_E(l) \leq w_E(k+l)$.
$\forall a \in V, b \in V \setminus \{0\}$, $w_{a+bE}(n) = w_E(n) + nv(b)$.

Open question. To what extend does the characteristic function w_E characterize the subset E?

Such a sequence $w_E(n)$ was already considered in the special case where the valuation is discrete (Definition 1.8.4) or, more generally, where there exists a v-ordering (Corollary 1.10.7). We can find some computations of this function w_E in Section 1.9 and also in Example 1.12.9.

For every subset F of E and for every $n \in \mathbb{N}$, we have $w_E(n) \leq w_F(n)$ and, if there is a v-ordering $\{a_k\}_{k=0}^n$ of E, then $w_E(n) = w_F(n)$ where $F = \{a_k \mid 0 \leq k \leq n\}$. More generally:

Proposition 1.14.1. *For each* $n \geq 0$*,*

$$w_E(n) = \inf\{w_F(n) \mid F \subseteq E,\ card(F) = n+1\}.$$

Proof. Fix an $n < card(E)$ and an $\varepsilon > 0$. Let $b_0, b_1, \ldots, b_n$ be a v-ordering of E modulo ε and let $F = \{b_0, \ldots, b_n\}$. Then, $b_0, \ldots, b_n$ is also a v-ordering of F modulo ε, thus

$$w_F(n) - n\varepsilon \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) \leq w_E(n) + \varepsilon.$$

Hence, for every $\varepsilon > 0$, there is a subset F of E such that $card(F) = n+1$ and $w_F(n) \leq w_E(n) + (n+1)\varepsilon$.

Analogously to Property 1.1.5 of the classical factorials we have :

Proposition 1.14.2. *For each* $n \in \mathbb{N}$*, we have*:

$$w_E(n) = \sup\{v(d(g,E)) \mid g \in K[X],\ \deg(g) = n,\ g \,\text{monic}\},$$

$$w_E(n) = \sup\{v(d(g,E)) \mid g \in V[X],\ \deg(g) = n,\ g \,\text{monic}\},$$

$$w_E(n) = \sup\{v(d(g,E)) \mid g = \prod_{k=0}^{n-1}(X - x_k),\ \text{with } x_0, \ldots, x_{n-1} \in E\}.$$

Proof. If E is finite, we may assume that $n < card(E)$.
On the one hand, let $y \in K$ be such that $v(y) \geq -v(g(E))$. Then yg belongs to $\mathrm{Int}(E,V)$; and hence, $y \in \mathfrak{I}_n(E,V)$. Consequently, $v(y) \geq -v(g(E))$ implies $v(y) \geq -w_E(n)$; and hence, $v(g(E)) \leq w_E(n)$.
On the other hand, let $\varepsilon > 0$ and let $\{b_k\}_{k=0}^n$ be a v-ordering of E modulo ε. Consider the polynomial $g = \prod_{k=0}^{n-1}(X - b_k)$. It follows from Lemma 1.13.3 that

$$w_E(n) \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) + n\varepsilon.$$

Consequently, by definition of a v-ordering modulo ε,

$$w_E(n) \leq \inf_{x \in E} v\left(\prod_{k=0}^{n-1}(x - b_k)\right) + (n+1)\varepsilon,$$

that is,

$$w_E(n) \leq v(d(g, E)) + (n+1)\varepsilon.$$

Thus, $w_E(n) \leq v(g(E))$.

From now on, we will omit in the proofs the condition $n < card(E)$ because, if $n \geq card(E)$, then all the equalities correspond to $+\infty = +\infty$ or $0 = 0$.

When there is a v-ordering $\{a_k\}_{k=0}^n$, then we have:

$$w_E(n) = v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \inf_{x\in E} v\left(\prod_{k=0}^{n-1}(x - a_k)\right).$$

More generally, the previous proposition shows that:

Corollaire 1.14.3. *For each $n \geq 0$, we have*:

$$w_E(n) = \sup_{x_0,\ldots,x_{n-1}\in E} \inf_{x\in E} v\left(\prod_{k=0}^{n-1}(x - x_k)\right).$$

With Proposition 1.14.1, the previous corollary leads to the following result:

Corollaire 1.14.4. *For each $n \geq 0$, we have*:

$$w_E(n) = \inf_{x_0,\ldots,x_n\in E} \sup_{0\leq i\leq n} v\left(\prod_{0\leq k\leq n\,,\,k\neq i}(x_i - x_k)\right).$$

Finally, analogously to Property 1.1.3 of the classical factorials, we have:

Théorème 1.14.5. *For each $n \in \mathbb{N}$,*

$$\inf_{x_0,\ldots,x_n\in E} v\left(\prod_{0\leq i<j\leq n}(x_j - x_i)\right) = \sum_{k=1}^{n} w_E(k).$$

Proof. Let $x_0, \ldots, x_n \in E$. We first prove that

$$v\left(\prod_{0\leq i<j\leq n}(x_j - x_i)\right) \geq \sum_{k=1}^{n} w_E(k).$$

Let $F = \{x_0, x_1, \ldots, x_n\}$. Assume that these $n+1$ elements are reordered so that the sequence $x_0, x_1 \ldots, x_n$ is a v-ordering of F. Then,

$$v\left(\prod_{0\le i<j\le n}(x_j - x_i)\right) = \sum_{j=1}^{n} v\left(\prod_{i=0}^{j-1}(x_j - x_i)\right) = \sum_{j=1}^{n} w_F(j) \ge \sum_{j=1}^{n} w_E(j)$$

since $F \subseteq E$. In particular, if $x_0, \ldots, x_n$ is a v-ordering of E, then we have an equality.

Conversely, let $\varepsilon > 0$ and let $\{b_k\}_{k=0}^{n}$ be a v-ordering of E modulo ε. It follows from Lemma 1.13.3 that:

$$v\left(\prod_{0\le i<j\le n}(b_j - b_i)\right) = \sum_{j=1}^{n} v\left(\prod_{i=0}^{j-1}(b_j - b_i)\right) \le \sum_{j=1}^{n} w_E(j) + n\varepsilon.$$

Consequently,

$$\inf_{x_0,\ldots,x_n\in E} v\left(\prod_{0\le i<j\le n}(x_j - x_i)\right) \le \sum_{j=1}^{n} w_E(j) + n\varepsilon,$$

that is,

$$\inf_{x_0,\ldots,x_n\in E} v\left(\prod_{0\le i<j\le n}(x_j - x_i)\right) \le \sum_{j=1}^{n} w_E(j).$$

1.15 Comportement asymptotique et capacité valuative

Hypothesis. *We still denote by V a rank-one valuation and by E any subset of V.*

Here we study the asymptotic behaviour of the arithmetic function w_E. More precisely, we show that $\frac{w_E(n)}{n}$ has a limit and that this limit is also the limit of the sequence $\delta_E(n)$ where, for $n \ge 1$:

$$\delta_E(n) = \frac{2}{n(n+1)} \inf_{x_0,\ldots,x_n\in E} v\left(\prod_{0\le i<j\le n}(x_j - x_i)\right).$$

This limit will be denoted by δ_E and, by analogy with the Archimedean case (see for instance [17]), δ_E is called the *valuative capacity* of E (with respect to v).

Proposition 1.15.1. *The sequence $\{\delta_E(n)\}_{n\in\mathbb{N}^*}$ is an increasing sequence, and hence tends to a (finite or infinite) limit $\delta_E \in \mathbb{R}_+ \cup \{+\infty\}$.*

Proof. Let $x_0, \ldots, x_n$ be elements of E. It follows from the obvious formula

$$\left(\prod_{0\le i<j\le n}(x_j - x_i)\right)^{n-1} = \prod_{k=0}^{n}\left(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j - x_i)\right)$$

and from the inequality

$$v\left(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j - x_i)\right) \ge \frac{(n-1)n}{2} \times \delta_E(n-1)$$

that

$$(n-1)v\left(\prod_{0\le i<j\le n}(x_j - x_i)\right)$$

$$= \sum_{k=0}^{n} v\left(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j - x_i)\right) \ge (n+1) \times \frac{(n-1)n}{2} \times \delta_E(n-1).$$

Consequently,

$$(n-1) \times \frac{n(n+1)}{2}\delta_E(n) \ge (n+1) \times \frac{(n-1)n}{2} \times \delta_E(n-1).$$

The limit δ_E is linked to the function w_E because of the formula given by Theorem 1.14.5:

$$\frac{1}{2}n(n+1)\delta_E(n) = w_E(1) + \ldots + w_E(n).$$

Théorème 1.15.2.

$$\lim_{n\to\infty} \frac{w_E(n)}{n} = \sup_{n\ge 1} \frac{w_E(n)}{n} = \delta_E.$$

Proof. First step: $\frac{w_E(n)}{n}$ tends to $\omega_E = \sup_{n\ge1} \frac{w_E(n)}{n}$.
If ω_E is finite (resp., infinite), let m be such that $\frac{w_E(m)}{m}$ is close to ω_E (resp., is large). For $n \ge m$, write $n = km + r$ with $0 \le r < m$. Then, we have :

$$\omega_E \ge \frac{w_E(n)}{n} = \frac{w_E(km+r)}{km+r} \ge \frac{w_E(km)}{(k+1)m} \ge \frac{k}{k+1}\frac{w_E(m)}{m}.$$

Thus, for n large, k is large, $\frac{k}{k+1}\frac{w_E(m)}{m}$ is close to $\frac{w_E(m)}{m}$, and hence, $\frac{w_E(n)}{n}$ is close to ω_E (resp., is large).

Second step: $\omega_E = \delta_E$.
From the equalities:

$$\frac{1}{2}n(n+1)\delta_E(n) = w_E(1) + \ldots + w_E(n).$$

it follows that:

$$n(n+1)\delta_E(n) - (n-1)n\delta_E(n-1) = 2w_E(n),$$

that is,

$$(n+1)\delta_E(n) - (n-1)\delta_E(n-1) = 2\frac{w_E(n)}{n},$$

$$n\delta_E(n-1) - (n-2)\delta_E(n-2) = 2\frac{w_E(n-1)}{n-1}, \ldots$$

By addition,

$$\delta_E(1) + \delta_E(2) + \delta_E(n-1) + (n+1)\delta_E(n) = 2\sum_{k=1}^{n}\frac{w_E(k)}{k},$$

or,

$$\frac{1}{n}(\delta_E(1) + \delta_E(2) + \ldots + \delta_E(n-1)) + (1+\frac{1}{n})\delta_E(n) = \frac{2}{n}\sum_{k=1}^{n}\frac{w_E(k)}{k}.$$

By Cesàro's theorem, the first term in the left side tends to δ_E, of course the second term also tends to δ_E, while the sum in the right side tends to $2\omega_E$ both by the first step and by Cesàro's theorem.

Of course, in some sense, the more E is large, the more δ_E is small.

EXEMPLES 1.15.3. 1. If V is a discrete valuation domain with a finite residue field of cardinality q, it follows from Pólya's formula [Proposition 1.8.8] that

$$\delta_V = \frac{1}{q-1}.$$

Then, for $a \in V$ and $b \in V^*$, we have:

$$\delta(a + bV) = \frac{1}{q-1} + v(b).$$

More generally, it follows from Corollary 1.9.4 that if E is a finite union of classes modulo a nonzero ideal bV, that is,

$$E = \cup_{i=1}^{r} \{c_i + bV\}$$

and if moreover $v(c_i - c_j) = h < v(b)$ for every (i, j) with $i \neq j$, then

$$\delta_E = \frac{1}{r}\left(\frac{1}{q-1} + v(b) + h(r-1)\right).$$

In particular, let p be a prime number and let $V = \mathbb{Z}_{(p)}$ (and hence, $v = v_p$). It follows from Examples 1.9.5 and 1.9.8 that to the containments :

$$\mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z} \setminus p^2\mathbb{Z} \subset \mathbb{Z}$$

correspond the following inequalities for the valuative capacities :

$$\frac{p}{(p-1)^2} > \frac{p(p^2-p+1)}{(p-1)^2(p^2+1)} > \frac{1}{p-1}.$$

2. On the other hand, δ_E may be infinite. Let V be a rank-one valuation domain and let t be an element of its maximal ideal. Then, $\{t^n \mid n \in \mathbb{N}\}$ is a v-ordering of $E = \{t^n \mid n \in \mathbb{N}\}$. Consequently,

$$w_E(n) = \frac{n(n-1)}{2} v(t) \quad \text{and} \quad \delta_E = +\infty.$$

3. The valuative capacity δ_E in Example 1.12.9 may be finite or infinite, since

$$\delta_E = \left(1 - \frac{1}{q}\right) \sum_{k=0}^{\infty} \frac{r_k}{q^k}$$

and $\{r_k\}$ is any strictly increasing sequence of positive rational numbers.

1.16 Capacité logarithmique d'un compact de $\mathbb{R}$ et polynômes de Chebychev

On connaît bien les polynômes de Chebychev : le n-ième *polynôme de Chebychev* est le polynôme unitaire T_n de degré n qui s'écarte le moins possible de 0 sur l'intervalle $[-1,+1]$ (au sens de la convergence uniforme sur $[-1,+1]$). On sait (cf. par exemple [18, chap. 13, § 3]) que ce polynôme est unique et est égal à :

$$T_n(X) = \frac{1}{2^{n-1}} \cos(n \arccos x)$$

et qu'il vérifie la récurrence :

$$T_n(X) = XT_{n-1}(X) - \frac{1}{4}T_{n-2}(X) \quad \text{avec} \quad T_0(X) = 2 \text{ et } T_1(X) = X.$$

Plus généralement (voir [19, chap. 2]) :

Proposition 1.16.1. *Etant donné un compact E de $\mathbb{R}$, il existe, pour tout $n \in \mathbb{N}^*$, un polynôme unitaire de degré n et un seul $T_n(E)$ qui réalise le minimum suivant :*

$$\inf_{P \in \mathbb{R}_n[X],\, P \text{ unitaire}} \left(\sup_{x \in E} |P(x)| \right).$$

Le polynôme $T_n(E)$ est appelé n-ième polynôme de Chebychev relatif à E.

De façon analogue, lorsqu'il existe une suite v-ordonnée (a_k) de E, notamment lorsque E est compact, la proposition 1.14.2 montre que le polynôme unitaire de degré n suivant :

$$T_n(E) = \prod_{k=0}^{n-1} (X - a_k)$$

réalise le maximum suivant :

$$\sup_{P \in K_n[X],\, P \text{ unitaire}} \left(\inf_{x \in E} v(P(x) \right).$$

C'est l'analogue des polynômes de Chebychev, mais ici il n'y a plus unicité.

Cependant, l'analogie ne s'arrête pas là. La capacité valuative est l'analogue non archimédien de la capacité logarithmique $c(E)$ d'une partie compacte E de $\mathbb{R}$. En effet, si l'on considère la quantité :

$$\delta_n(E) = \sup_{x_0,\ldots,x_n \in E} \prod_{0 \le i < j \le n} |x_j - x_i|^{\frac{2}{n(n+1)}},$$

alors la suite $\delta_n(E)$ est décroissante et tend vers une limite $c(E)$ est appelée *capacité logarithmique* ou *rayon de capacité* ou *diamètre transfini* du compact E.

Par exemple, $c([a,b]) = \frac{b-a}{4}$.

Par ailleurs, pour toute fonction $f : E \to \mathbb{R}$ bornée sur E, posons :

$$||f||_E = \sup_{x \in E} |f(x)|.$$

On sait aussi que la suite $\sqrt[n]{||T_n(E)||_E}$ est convergente et que :

$$\lim_{n \to +\infty} \sqrt[n]{||T_n(E)||_E} = c(E).$$

Exercice ouvert. Soit E une partie infinie de $\mathbb{Z}$ ne contenant pas 0 et soit F la partie précompacte de $\mathbb{R}$ définie par $F = \left\{ \frac{1}{x} \mid x \in E \right\}$. Quel lien y a-t-il entre la capacité logarithmique $c(F)$ et les $\delta_p(E)$ où $\delta_p(E)$ désigne la capacité de E correspondant à la valuation v_p ?

Bibliography

POUR LE PREMIER CHAPITRE

[1] A. J. KEMPNER, Polynomials and their residue systems, *Trans. Amer. Math. Soc.* **22** (1921), 240–288.

[2] G. MULLEN ET H. STEVENS, Polynomial functions $(\mathrm{mod}\ m)$, *Acta Math. Hung.* **44** (1984), 237–241.

[3] G. PÓLYA, Ueber ganzwertige ganze Funktionen, *Rend. Circ. Matem. Palermo* **40** (1915), 1–16.

[4] G. PÓLYA, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.

[5] A. OSTROWSKI, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 117–124.

[6] P.-J. CAHEN & J.-L. CHABERT, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs, n. 48, American Mathematical Society, 1997.

[7] N. BOURBAKI, *Algèbre Commutative*, Hermann, 1965, Paris.

[8] M. BHARGAVA, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.* **490** (1997), 101-127.

[9] M. BHARGAVA, Generalized Factorials and Fixed Divisors over Subsets of a Dedekind Domain, *J. Number Theory* **72** (1998), 67–75.

[10] M. BHARGAVA, The factorial function and generalizations, *Math. Monthly*, **107** (2000), 783-799.

[11] J. BOULANGER, J.-L. CHABERT, S. ERARD, G. GERBOUD, The characteristic sequence of integer-valued polynomials on a subset, in *Advances in Commutative Ring Theory*, Lecture Notes in Pure and Appl. Math., vol. **205**, pp. 161–174, Dekker, New York, 1999.

[12] J. BOULANGER, J.-L. CHABERT, Asymptotic Behavior of Characteristic Sequences of Integer-Valued Polynomials, J. Number Theory **80** (2000), 238–259.

[13] P.-J. CAHEN, J.-L. CHABERT, K. ALAN LOPER, High dimension Prüfer domains of integer-valued polynomials, *J. Korean Math. Soc.* **38** (2001), 915-935.

[14] Y. FARES, Factorial preservation, *Arch. Math.* **83** (2004), 497–506.

[15] A. OSTROWSKI, Untersuchen zur aritmetischen Theorie der Körper, *Math. Zeitschrift* **39** (1935), 269–404.

[16] I. KAPLANSKY, Maximal fields with valuations, *Duke Math.* **9** (1942), 303–321.

[17] M. FEKETE, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Zeitsch.* **17** (1923), 228–249.

[18] J.-L. CHABERT ET AL., *A History of Algorithms, From the Pebble to the Microchip*, trad. C. Weeks, Springer, 524 p., 1999.

[19] LE BARON O. FERGUSON, *Approximation by polynomials with integral coefficients*, Mathematical Surveys and Monographs, n. 17, American Mathematical Society, 1980.

Chapter 2

Polynômes à valeurs entières sur un anneau de Dedekind : les pièges de la globalisation

On étudie dans ce chapitre la structure de A-module de $\mathrm{Int}(E, A)$ lorsque A est l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres (ou d'un corps de fonctions), donc dans le cas où A est un anneau de Dedekind à corps résiduels finis. On va se placer dans une situation un peu plus générale en considérant un anneau de Dedekind A quelconque et on va utiliser les résultats de l'étude locale effectuée au chapitre précédent.

Hypothèses et notations. *Dans tout ce chapitre, A désigne un anneau de Dedekind de corps des fractions K et E une partie infinie de A.*

2.1 Le A-module $\mathrm{Int}(E, A)$ et ses idéaux caractéristiques

On rappelle les notations suivantes :

$$\mathrm{Int}(E, A) = \{P \in K[X] \mid P(E) \subset A\},$$

et, pour tout $n \in \mathbb{N}$,

$$\mathrm{Int}_n(E, A) = \{P \in \mathrm{Int}(E, A) \mid \deg(P) \leq n\}$$

$$(n!)_E^A = \{a \in A \mid a \times \mathrm{Int}_n(E, A) \subset A[X]\} = \mathfrak{I}_n^{-1}(E, A).$$

Commençons par ce qui fonctionne bien au niveau de la globalisation grâce à la proposition 1.6.3 :

$$(n!)_E^A = \prod_{\mathfrak{m}\in\max(A)} (n!)_E^{A\mathfrak{m}}. \tag{2.1}$$

Rappelons tout d'abord les assertions de la proposition 1.6.2 :

$$\forall m, n \in \mathbb{N}, \quad (m!)_E^A \times (n!)_E^A \mid (m+n)_E^A. \tag{2.2}$$

$$\forall n \in \mathbb{N},\ \forall F \subset E, \quad (n!)_E^A \mid (n!)_F^A. \tag{2.3}$$

Quant à la proposition 1.10.11, elle devient :

Proposition 2.1.1. *Soit $n \in \mathbb{N}^*$. Quels que soient $x_0, x_1, \ldots, x_n$, l'idéal engendré par $\prod_{0\le i<j\le n}(x_j - x_i)$ est divisible par l'idéal $(0!)_E^A(1!)_E^A \cdots (n!)_E^A$.*

Exercice 2.1.2. 1- Soit E un partie de A et soient a et $b \in A$. Si $F = a + bE = \{a + bx \mid x \in E\}$ alors, pour tout $n \in \mathbb{N}$, $(n!)_F^A = b^n \times (n!)_E^A$.
2- Soit $\mathfrak{a}$ un idéal de A. Pour tout $n \in \mathbb{N}$, on a :

$$(n!)_{\mathfrak{a}}^A = (n!)_A^A \times \mathfrak{a}^n. \tag{2.4}$$

Pour tout idéal maximal $\mathfrak{m}$ de A, $A_{\mathfrak{m}}$ est l'anneau d'une valuation discrète $v_{\mathfrak{m}}$. Notons alors $w_{\mathfrak{m},E}$ la fonction caractéristique de E relative à $A_{\mathfrak{m}}$, c.-à-d.,

$$w_{\mathfrak{m},E}(n) = v_{\mathfrak{m}}\left((n!)_E^{A\mathfrak{m}}\right) = -v_{\mathfrak{m}}(\mathfrak{I}_n(E, A_{\mathfrak{m}})).$$

On a donc :

$$(n!)_E^A = \mathfrak{I}_n^{-1}(E, A) = \prod_{\mathfrak{m}\in\max(A)} \mathfrak{m}^{w_{\mathfrak{m},E}(n)}. \tag{2.5}$$

La base donnée dans la proposition 1.8.1 montre localement, et donc globalement, que :

$\mathfrak{I}_n(E, A)$ est aussi l'idéal fractionnaire formé des coefficients dominants des polynômes de $\mathrm{Int}(E, A)$ de degré n augmenté de 0.

Exercice 2.1.3. Soient $K/\mathbb{F}_q(T)$ un corps de fonctions et $\mathcal{O}_K$ la clôture intégrale de $\mathbb{F}_q[T]$ dans K. Montrer que si l'écriture de n en base q est $n_s n_{s-1} \ldots n_1 n_0$, alors

$$(n!)_{\mathcal{O}_K} = \prod_{i=0}^{s} \left((q^i!)_{\mathcal{O}_K}\right)^{n_i}. \tag{2.6}$$

EXEMPLE 2.1.4. On verra au chapitre suivant à propos de la clôture polynomiale que, pour tout $p \in \mathbb{P}$,

$$\mathrm{Int}(\mathbb{P}, \mathbb{Z})_{(p)} = \mathrm{Int}(\{p\} \cup \mathbb{Z} \setminus p\mathbb{Z}, \mathbb{Z}_{(p)}). \tag{2.7}$$

Par suite, par globalisation de l'exemple 1.9.5, on a :

$$n!_{\mathbb{P}} = \prod_{p \in \mathbb{P}} p^{\sum_{k \geq 0} \left[\frac{n-1}{(p-1)p^k} \right]}. \tag{2.8}$$

Rappelons que les *nombres de Bernoulli* sont définis par :

$$\frac{z}{e^z - 1} = 1 - \frac{z}{2} + \frac{B_1}{2!} z^2 - \frac{B_2}{4!} z^4 + \frac{B_3}{6!} z^6 - \cdots \tag{2.9}$$

Notons δ_n le dénominateur de la fraction $\frac{B_n}{n}$ dans sa représentation irréductible. Les théorèmes de von Staudt et de Kummer (cf. par exemple [3, pp. 429–435]) montrent que

$$\forall p \in \mathbb{P}, \quad v_p(\delta_n) = 1 + v_p(n) \text{ si } p - 1 | 2n \quad \text{et} \quad v_p(\delta_n) = 0 \text{ sinon.} \tag{2.10}$$

Par suite,

$$(2m+1)!_{\mathbb{P}} = 2^{2m} \prod_{1 \leq k \leq m} \delta_k \quad \text{et} \quad (2m+2)!_{\mathbb{P}} = 2(2m+1)!_{\mathbb{P}}. \tag{2.11}$$

Applications (cf. [1] et [2]).

$$\left(-\frac{\log(1-x)}{x} \right)^m = \left(\sum_{k=1}^{\infty} \frac{x^k}{k+1} \right)^m = \sum_{n \geq 1} \frac{C_n(m)}{(n+1)!_{\mathbb{P}}} x^n \tag{2.12}$$

où le polynôme $C_n(m) \in \mathbb{Z}[m]$ est primitif et de degré n.

Par ailleurs, le n-ième *polynôme de Bernoulli d'ordre* m défini par :

$$\left(\frac{t}{e^t - 1} \right)^m = \sum_{n=0}^{\infty} B_n^{(m)} \frac{t^n}{n!} \tag{2.13}$$

est de la forme :

$$B_n^{(m)} = \frac{n!}{(n+1)!_{\mathbb{P}}} D_n(m) \tag{2.14}$$

où le polynôme $D_n(m) \in \mathbb{Z}[m]$ est primitif.

Interprétation combinatoire (mystérieuse) :
Rappelons un résultat de Minkowski [4] :
Pour tout $p \in \mathbb{P}$, il existe une forme quadratique définie positive sur $\mathbb{Q}^n$ telle que l'ordre ρ_p du groupe formé des $\sigma \in GL(n, \mathbb{Q})$ laissant ρ_p invariante vérifie :

$$v_p(\rho_p) = \sum_{k \geq 0} \left[\frac{n}{(p-1)p^k)} \right].$$

Rappelons aussi un résultat de Schur [5] :
L'ordre ρ de tout sous-groupe fini de $GL(n, \mathbb{Q})$ est un diviseur de

$$\prod_{p \in \mathbb{P}} p^{\sum_{k \geq 0} \left[\frac{n}{(p-1)p^k)} \right]}.$$

Conclusion : $(n+1)_{\mathbb{P}}$ est le p.p.c.m. des ordres des sous-groupes finis de $GL(n, \mathbb{Q})$ (et aussi de $GL(n, \mathbb{Z})$).

Exercice 2.1.5. Déterminer $(n!)_{\mathbb{P}_{\mathbb{Z}_{[i]}}}^{\mathbb{Z}_{[i]}}$ où $\mathbb{P}_{\mathbb{Z}_{[i]}}$ désigne l'ensemble des éléments irréductibles de l'anneau des entiers de Gauss.

Rappelons que, pour tout $f \in K[X]$, $c(f)$ et $d(f, E)$ désignent les idéaux fractionnaires de A engendrés respectivement par les coefficients de f et par les valeurs de f sur E. Par globalisation, la proposition 1.11.2 devient :

Proposition 2.1.6. *Pour tout $f \in K[X]$ de degré n, on a les relations de divisibilité :*

$$c(f) \mid d(f, E) \quad et \quad d(f, E) \mid c(f) \cdot (n!)_E^A.$$

Ou encore en termes de valuation :

$$\forall f \in K[X],\ \forall \mathfrak{m} \in \max(A) \quad \text{si } \deg(f) \leq n, \text{ on a } :$$
$$v_{\mathfrak{m}}(c(f)) \leq v_{\mathfrak{m}}(d(f, E)) \leq v_{\mathfrak{m}}(c(f)) + w_{\mathfrak{m},E}(n). \tag{2.15}$$

En particulier,
— si f est de degré n et à valeurs entières sur E, $c(f)$ est contenu dans $\mathfrak{I}_n(E, A)$,
— si f est de degré n, unitaire et à coefficients dans A, $d(f, E)$ divise $(n!)_E^A$.
Cette dernière relation de divisibilité est optimale :
il existe f de degré n, unitaire et à coefficients dans A, tel que $f(E) = (n!)_E^A$:

Proposition 2.1.7. *(i) Il existe une suite $(g_n)_{n\in\mathbb{N}}$ de polynômes unitaires à coefficients dans A telle que $\deg(g_n) = n$ et $d(g_n, E) = (n!)_E^A$.*
(ii) Considérons une telle suite $(g_n)_{n\in\mathbb{N}}$. Pour $f \in K[X]$, posons

$$f(X) = \lambda_0 g_0(X) + \lambda_1 g_1(X) \ldots + \lambda_d g_d(X).$$

Alors $f \in \mathrm{Int}(E, A)$ si et seulement si $\lambda_k \in \mathfrak{I}_k(E, A)$ pour $0 \leq k \leq d$.

La démonstration de la première assertion utilise le théorème et le lemme suivants.

Théorème 2.1.8 (d'approximation dans les anneaux de Dedekind)**.** *Soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ des idéaux maximaux distincts de l'anneau de Dedekind A, $x_1, \ldots, x_s$ des éléments du corps des fractions K de A et $n_1, \ldots, n_s \in \mathbb{N}$. Alors, il existe $x \in K$ tel que*

$$v_{\mathfrak{m}_i}(x - x_i) \geq n_i \quad \textit{pour } i = 1, \ldots, s$$

et

$$v_{\mathfrak{m}}(x) \geq 0 \quad \textit{pour } \ \mathfrak{m} \neq \mathfrak{m}_1, \ldots, \mathfrak{m}_s.$$

Lemme 2.1.9. *Soit $n \geq 2$. Dans l'anneau de Dedekind A, il y a au plus un nombre fini d'idéaux maximaux de norme $\leq n$.*

On rappelle que pour tout idéal $\mathfrak{a}$ de A, on appelle *norme* de $\mathfrak{a}$ et on note $N(\mathfrak{a})$ le cardinal de l'anneau $A/\mathfrak{a}$.

Proof. Soit q une puissance d'un nombre premier et soit $x \in A$ tel que $x^q - x \neq 0$. Pour tout $\mathfrak{m} \in \max(A)$ tel que $N(\mathfrak{m}) = q$, on a $x^q - x \in \mathfrak{m}$ et il ne peut y avoir qu'un nombre fini de tels $\mathfrak{m}$. □

En fait, cela résulte aussi de ce qu'un idéal $\mathfrak{m}$ est de norme $\leq n$ si et seulement si il divise l'idéal entier $(n!)_E^A$.

Proof. de la première assertion la proposition 2.1.7. Pour $n \in \mathbb{N}$ fixé, soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ les idéaux maximaux de norme $\leq n$. Pour chaque $\mathfrak{m} \in \{\mathfrak{m}_1, \ldots, \mathfrak{m}_s\}$, soit $(a_{k,\mathfrak{m}})_{k=0}^n$ une suite $v_{\mathfrak{m}}$-ordonnée de E. Pour $0 \leq k \leq n$, soit $a_k \in A$ tel que

$$v_{\mathfrak{m}}(a_k - a_{k,\mathfrak{m}}) > w_{E,\mathfrak{m}}(n) \ \ \textit{pour } \mathfrak{m} = \mathfrak{m}_1, \ldots, \mathfrak{m}_s.$$

Posons

$$g_{n,\mathfrak{m}}(X) = \prod_{k=0}^{n-1}(X - a_{k,\mathfrak{m}}) \quad \text{et} \quad g_n(X) = \prod_{k=0}^{n}(X - a_k).$$

Tout d'abord, g_n étant unitaire de degré n, $d(g_n, E)$ divise $(n!)_E^A$. Inversement, pour tout $x \in E$ et tout $\mathfrak{m} \in \{\mathfrak{m}_1, \ldots, \mathfrak{m}_s\}$, on a :

$$v_{\mathfrak{m}}(g_n(x) - g_{n,\mathfrak{m}}(x)) > w_{E,\mathfrak{m}}(n) \text{ et } v_{\mathfrak{m}}(g_{n,\mathfrak{m}}(x) \geq w_{E,\mathfrak{m}}(n),$$

donc,

$$v_{\mathfrak{m}}(g_n(x)) \geq w_{E,\mathfrak{m}}(n).$$

Par suite, $(n!)_E^A$ divise $d(g_n, E)$. Ainsi, g_n convient.
La deuxième assertion se vérifie par récurrence sur le degré de f. □

On notera toutefois que les a_k que l'on vient de construire, d'une part dépendent de l'entier n, d'autre part ne sont pas dans E a priori.

Corollaire 2.1.10. *Pour tout $n \in \mathbb{N}$, on a les isomorphismes de A-modules :*

$$\mathrm{Int}_n(E, A) \simeq \mathfrak{I}_0 \oplus \mathfrak{I}_1 \oplus \cdots \oplus \mathfrak{I}_n \simeq A^n \oplus \prod_{k=0}^{n} \mathfrak{I}_k.$$

On rappelle à ce propos :

Proposition 2.1.11. *[7, VII, § 10] Dans un anneau de Dedekind A, quels que soient les idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$, on a :*

$$\mathfrak{a} \oplus \mathfrak{b} = A \oplus \mathfrak{ab}.$$

2.2 Bases régulières et groupe de Pólya-Ostrowski

Proposition 2.2.1. *Le A-module $\mathrm{Int}_n(E, A)$ est projectif de rang $n+1$ tandis que le A-module $\mathrm{Int}(E, A)$ est libre.*

Cela résulte directement de ce que :

Proposition 2.2.2. *[7, VII, § 10] Sur un anneau de Dedekind A, tout A-module sans torsion de type fini (resp. non de type fini) est projectif (resp. libre).*

Mais, comme on le verra sur des exemples, il est difficile en général d'exhiber une base de $\mathrm{Int}(E, A)$ sans hypothèses supplémentaires. Occupons nous pour commencer des systèmes de générateurs. L'assertion suivante se vérifie immédiatement par récurrence :

Proposition 2.2.3. *Un ensemble G de polynômes de $\mathrm{Int}_N(E,A)$ est un système de générateurs du A-module $\mathrm{Int}_N(E,A)$ dès que, pour tout $n \leq N$, les coefficients dominants des polynômes de degré n dans G engendrent l'idéal fractionnaire $\mathfrak{I}_n(E,A)$.*

Rappelons que tout idéal d'un anneau de Dedekind est engendrable par deux éléments, l'un d'eux pouvant être un élément non nul quelconque de l'idéal. Par suite, on peut toujours obtenir un système de générateurs de $\mathrm{Int}(E,A)$ avec 2 polynômes de chaque degré n, l'un des deux étant un polynôme quelconque de degré n, on choisira par exemple X^n. Le cas où il y a exactement un polynôme de chaque degré correspond à la notion suivante :

Définition 2.2.4. (Pólya [4]) Une base $(f_n)_{n\in\mathbb{N}}$ de $\mathrm{Int}(E,A)$ est dite *base régulière* si, pour tout $n \in \mathbb{N}$, $\deg(f_n) = n$.

Mais, $\mathrm{Int}(E,A)$ ne possède pas toujours une base régulière :

Proposition 2.2.5. *Les assertions suivantes sont équivalentes :*
1– $\mathrm{Int}(E,A)$ possède une base régulière.
2– Pour tout $n \in \mathbb{N}$, le A-module $\mathrm{Int}_n(E,A)$ est libre.
3– Pour tout $n \in \mathbb{N}$, l'idéal fractionnaire $\mathfrak{I}_n(E,A)$ est principal.
4– Pour tout $n \in \mathbb{N}$, l'idéal $(n!)_E^A$ est principal.

Remarque 2.2.6. Si $\mathrm{Int}(E,A)$ possède une base régulière, chaque idéal factoriel $(n!)_E^A$ étant principal, on peut en choisir un générateur μ_n. La proposition 2.1.6 montre que la suite $\left(\frac{1}{\mu_n} g_n(X)\right)_{n\in\mathbb{N}}$ est une base régulière.

EXEMPLE 2.2.7. Si A est principal, alors $\mathrm{Int}(E,A)$ possède toujours une base régulière. Ainsi, $\binom{X}{n}$ est une base régulière de $\mathrm{Int}(\mathbb{Z})$. Mais on va voir que la principalité de A n'est pas du tout nécessaire :

A cet effet, nous introduisons maintenant un groupe qui peut être considéré comme une mesure de l'obstruction à ce que $\mathrm{Int}(E,A)$ ait une base régulière. Rappelons que le *groupe des classes d'idéaux*, ou groupe de Picard, de l'anneau de Dedekind A est le groupe $\mathcal{C}(A)$, ou $Pic(A)$, quotient du groupe $\mathcal{I}(A)$ des idéaux fractionnaires non nuls de A (en fait $\mathcal{J}(A)$ groupe des idéaux inversibles) par le sous-groupe $\mathcal{P}(A)$ des idéaux principaux non nuls :

$$\mathcal{C}(A) = \mathcal{I}(A)/\mathcal{P}(A).$$

Définition 2.2.8. On appelle *groupe de Pólya-Ostrowski* de la A-algèbre $\mathrm{Int}(E, A)$ et on note $\mathcal{P}o(E, A)$ le sous-groupe de $\mathcal{C}(A)$ engendré par les classes des idéaux factoriels $(n!)_E^A$ (ou, de façon équivalente, par les classes des idéaux caractéristiques $\mathfrak{I}_n(E, A)$).

Bien sûr, $\mathrm{Int}(E, A)$ possède une base régulière si et seulement si son groupe de Pólya-Ostrowski $\mathcal{P}o(E, A)$ est trivial.

Proposition 2.2.9. *Soit B un anneau intègre quelconque contenant A. Alors, le B-module engendré par $\mathrm{Int}(E, A)$ est égal à $\mathrm{Int}(E, B)$. En particulier :*

$$(n!)_E^A B = (n!)_E^B \quad \text{pour tout } n \in \mathbb{N}.$$

Proof. On vérifie que, pour tout idéal maximal $\mathfrak{m}$ de A, une base régulière du $A_\mathfrak{m}$-module $\mathrm{Int}(E, A_\mathfrak{m})$ construite à partir d'une suite $v_\mathfrak{m}$-ordonnée de E est automatiquement une base régulière du B-module $\mathrm{Int}(E, B)_\mathfrak{m}$. □

Ainsi, pour étudier les factorielles relatives à un ensemble E, on peut se placer dans le plus petit anneau de Dedekind contenant E.

Corollaire 2.2.10. *Soit B la fermeture intégrale de A dans une extension finie de K. Soit*

$$\epsilon_A^B : \overline{\mathfrak{I}} \in \mathcal{C}(A) \mapsto \overline{\mathfrak{I}B} \in \mathcal{C}(B)$$

le morphisme canonique associé à l'inclusion de A dans B. Alors

$$\epsilon_A^B\left(\mathcal{P}o(E, A)\right) = \mathcal{P}o(E, B).$$

Nous allons étudier plus en détail le groupe de Pólya-Ostrowski lorsque $E = A$.

2.3 Le groupe de Pólya-Ostrowski $\mathcal{P}o(A)$ d'un anneau de Dedekind A

Notations. Plus simplement, on notera $\mathcal{P}o(A)$ le groupe $\mathcal{P}o(A, A)$ et on l'appellera *groupe de Pólya-Ostrowski de l'anneau A*. Pour tout idéal maximal $\mathfrak{m}$ de A, on note $N(\mathfrak{m})$ la norme de $\mathfrak{m}$, c.-à-d., le cardinal du corps $A/\mathfrak{m}$, et $w_\mathfrak{m}$ la fonction caractéristique de l'ensemble A relative à l'anneau $A_\mathfrak{m}$, c.-à-d. :

$$w_\mathfrak{m}(n) = w_{N(\mathfrak{m})}(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{N(\mathfrak{m})^k} \right\rfloor. \tag{2.16}$$

Le groupe factoriel

Définition 2.3.1. On appelle *groupe factoriel de* A et on note $\mathcal{F}act(A)$ le sous-groupe du groupe $\mathcal{I}(A)$ des idéaux fractionnaires non nuls de A engendré par les idéaux factoriels de A.

Bien sûr, $\mathcal{F}act(A)$ est aussi le sous-groupe engendré par les idéaux caractéristiques $\mathfrak{I}_n(A)$.

Notations. Pour tout entier $q \geq 2$, soit $\Pi_q(A)$, ou plus simplement Π_q, le produit de tous les idéaux maximaux de A de norme q, c'est-à-dire :

$$\Pi_q(A) = \prod_{\mathfrak{m}\in\max(A),\, N(\mathfrak{m})=q} \mathfrak{m}. \tag{2.17}$$

Si q n'est la norme d'aucun idéal maximal $\mathfrak{m}$ de A, on posera $\Pi_q(A) = A$.

Proposition 2.3.2. *Le groupe factoriel $\mathcal{F}act(A)$ de A est le sous-groupe abélien libre de $\mathcal{I}(A)$ de base les idéaux Π_q distincts de A (q décrit l'ensemble des puissances des nombres premiers.)*

Proof. Tout d'abord, le sous-groupe $\mathcal{F}act(A)$ est contenu dans le sous-groupe de $\mathcal{I}(A)$ engendré par les $\Pi_q(A)$. En effet,

$$(n!)_A = \prod_{\mathfrak{m}\in\max(A)} \mathfrak{m}^{w_{\mathfrak{m}}(n)} = \prod_{2\leq q\leq n} \left(\prod_{N(\mathfrak{m})=q} \mathfrak{m} \right)^{w_q(n)} = \prod_{2\leq q\leq n} \Pi_q^{w_q(n)}. \tag{2.18}$$

Mais on a l'inclusion inverse car, d'une part, $\Pi_2 = (2!)_A$ et, comme $w_n(n) = 1$, on a

$$(n!)_A = \Pi_n \times \prod_{2\leq q<n} \Pi_q^{w_q(n)},$$

et on peut donc vérifier par récurrence que, si les Π_q sont dans $\mathcal{F}act(A)$ pour $q < n$, alors Π_n aussi. Enfin, il n'y a pas de relations entre les idéaux Π_q si l'on excepte ceux égaux à A, car les idéaux maximaux intervenant dans deux Π_q distincts sont eux-mêmes distincts. □

Corollaire 2.3.3. *Le groupe de Pólya-Ostrowski $\mathcal{P}o(A)$ de A est engendré par les classes des idéaux Π_q.*

Corollaire 2.3.4. *Le A-module $\mathrm{Int}(A)$ possède une base régulière si et seulement si, pour tout $q \geq 2$, le produit Π_q des idéaux premiers de A de même norme q est un idéal principal.*

Le problème des corps de fonctions

La définition du groupe factoriel $\mathcal{F}act(A)$ d'un anneau de Dedekind A conduit à une notion satisfaisante dans le cas de l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres K. Dans le cas d'un corps de fonctions K, pour éviter l'ambiguïté liée à la définition de $\mathcal{O}_K$, on pourrait modifier la définition des factorielles de la façon suivante. La n-ième factorielle du corps de fonctions K serait le diviseur :

$$n!_K = \sum_{\mathcal{P}\in\mathbb{P}_K} w_{q^{\deg(\mathcal{P})}}(n)\ \mathcal{P} \tag{2.19}$$

où $\mathbb{P}_K$ désigne l'ensemble des places de K. Ainsi, en notant $n!_{\mathcal{C}}$ la factorielle de Carlitz relative à l'anneau $\mathbb{F}_q[T]$, on aurait la relation :

$$n!_{\mathbb{F}_q(T)} = \log(n!_{\mathcal{C}}) + w_q(n)\frac{1}{T}. \tag{2.20}$$

Du coup, on modifierait la définition du groupe factoriel d'un corps de fonctions, et aussi la notion de corps de Pólya et la définition du groupe de Pólya-Ostrowski. Ainsi, le groupe factoriel d'un corps de fonctions K serait le sous-groupe du groupe $\mathcal{D}_K$ des diviseurs de K engendré par les diviseurs factoriels $n!_K$ pour $n \in \mathbb{N}$. Ce serait aussi le sous-groupe engendré par les diviseurs

$$\Pi_f = \sum_{\mathcal{P}\in\mathbb{P}_K,\,\deg(\mathcal{P})=f} \mathcal{P}.$$

Ce serait en fait le sous-groupe libre de base les Π_f puisque $\mathcal{D}_K$ est libre de base les $\mathcal{P} \in \mathbb{P}_K$ et qu'il ne peut y avoir de relations entre les Π_f. Le groupe de Pólya-Ostrowski d'un corps de fonctions serait alors le sous-groupe du groupe $\mathcal{C}l_K$ des classes de diviseurs de K engendré par les classes des diviseurs factoriels.
A propos des degrés, on aurait :

$$\deg(n!_K) = \sum_{\mathcal{P}\in\mathbb{P}_K} w_{N(\mathcal{P})}(n) = \sum_{q^f\le n} a_f w_{q^f}(n) \tag{2.21}$$

où a_f désigne le nombre de diviseurs $\mathcal{P}$ de degré f, et donc

$$\deg(\Pi_f) = a_f.$$

En fait, on aurait aimer que les diviseurs factoriels soient de degré 0 de façon que le groupe de Pólya-Ostrowski soit un sous-groupe de $\mathcal{C}l^0_K$. Comme, dans tout

corps de fonctions global, il existe au moins un diviseur D de degré 1, on pourrait s'en servir. Si

$$D = \sum_{\mathcal{P} \in S} a_{\mathcal{P}}\, \mathcal{P} \quad \text{avec} \quad \deg(D) = 1,$$

on pourait poser :

$$n!_K = \sum_{\mathcal{P} \notin S} w_{N(\mathcal{P})}(n)\, \mathcal{P} - \sum_{\mathcal{P} \in S} w_{N(\mathcal{P})}(n)\, \mathcal{P}.$$

Mais, si on change de diviseur D de degré 1, comment varie la classe de $n!_K$? et celle de Π_f ?

L'exemple des corps quadratiques

Pour des rappels concernant les corps quadratiques, voir la section suivante. Dans le cas où A est l'anneau $\mathcal{O}_K$ des entiers d'un corps quadratique K, pour tout $p \in \mathbb{P}$, on a de façon immédiate :

$\Pi_p = p\mathcal{O}_K$ si p est décomposé,
$\Pi_{p^2} = p\mathcal{O}_K$ si p est inerte et
$\Pi_p^2 = p\mathcal{O}_K$ si p est ramifié.

De sorte que les seuls idéaux Π_q éventuellement non principaux sont les idéaux Π_p où p est ramifié et de plus, de toutes façons, leur carré est principal. D'où la proposition :

Proposition 2.3.5. *Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique où d désigne un entier sans facteurs carrés. Si le groupe $\mathcal{P}o(\mathcal{O}_K)$ n'est pas trivial, il a pour exposant 2. Si s désigne le nombre de diviseurs premiers du discriminant D de K, alors $\mathcal{P}o(\mathcal{O}_K)$ a au plus $s-1$ générateurs indépendants et donc au plus 2^{s-1} éléments.*

Proof. On rappelle que $D = d$ si $d \equiv 1 \pmod 4$ et $D = 4d$ si $d \equiv 2, 3 \pmod 4$ et qu'un nombre premier p est ramifié si, et seulement si, il divise D. On a donc vu que le groupe abélien $\mathcal{P}o(\mathcal{O}_K)$ est a priori engendrable par au plus s éléments et que ceux-ci sont d'ordre au plus 2. Mais, si $p_1, \ldots, p_s$ divisent d et si $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ désignent les idéaux premiers de $\mathcal{O}_K$ qui les relèvent, alors $\mathfrak{p}_1 \cdots \mathfrak{p}_s = \sqrt{d}\mathcal{O}_K$. □

Remarque 2.3.6. On peut préciser l'énoncé précédent. En effet, en conservant les notations précédentes, on a (Hilbert [6, prop. 105 et 106]) :

— si K est réel ($d > 0$) et l'unité fondamentale est de norme $+1$, alors $\mathcal{P}o(\mathcal{O}_K)$ a $s-2$ générateurs indépendants et donc 2^{s-2} éléments.
— sinon, $\mathcal{P}o(\mathcal{O}_K)$ a $s-1$ générateurs indépendants et donc 2^{s-1} éléments.
On rappelle que l'*unité fondamentale* d'un corps quadratique réel K est la plus petite unité > 1 de $\mathcal{O}_K$ et toutes les unités positives en sont des puissances.

Remarque 2.3.7. Si A est principal, c.-à-d., $\mathcal{C}(A) = \{1\}$, alors évidemment $\mathcal{P}o(A) = \{1\}$. Mais on peut avoir aussi bien :
1- $\{1\} = \mathcal{P}o(A) \neq \mathcal{C}(A)$ comme le montre l'anneau non principal $A = \mathbb{Z}[\sqrt{6}]$ puisque seuls 2 et 3 y sont ramifiés et que $(2+\sqrt{6})^2 A = 2A$ et $(3+\sqrt{6})^2 A = 3A$.
2- $\{1\} \neq \mathcal{P}o(A) \neq \mathcal{C}(A)$ comme le montre l'anneau des entiers $A = \mathbb{Z}[\sqrt{-29}]$. Seuls 2 et 29 sont ramifiés. Or, $\Pi_{29} = \sqrt{-29}A$ est principal, tandis que Π_2 n'est pas principal puisque $a^2 + 29b^2 = 2$ n'a pas de solutions entières. Ainsi, $\mathcal{P}o(A) = \{0, \overline{\pi_2}\}$. Par ailleurs, 3 est décomposé et si $\mathfrak{p}|3$, alors $\mathfrak{p}^2$ ne peut être principal puisque $a^2 + 29b^2 = 9$ a pour solutions $(\pm 3, 0)$. Donc, $0 \neq \overline{\mathfrak{p}} \in \mathcal{C}(A)$.

2.4 Rappels à propos des corps quadratiques et des corps cyclotomiques

Corps quadratiques

Définition 2.4.1. Un *corps quadratique* est un corps $K \subset \mathbb{C}$ tel que $[K : \mathbb{Q}] = 2$.

Tout corps quadratique est de la forme $\mathbb{Q}[\sqrt{d}]$ où $d \in \mathbb{Z}$ est sans "facteurs carrés" (c'est-à-dire, non divisible par le carré d'un nombre premier) et où, pour $d < 0$, on convient d'écrire $\sqrt{d}$ au lieu de $i\sqrt{-d}$. On notera $\mathcal{O}_K$ la fermeture intégrale de $\mathbb{Z}$ dans K et U_K le groupe des unités de K, c.-à-d., le groupe des éléments inversibles de $\mathcal{O}_K$.

Proposition 2.4.2. *Pour tout corps quadratique $K = \mathbb{Q}[\sqrt{d}]$, le $\mathbb{Z}$-module $\mathcal{O}_K$ est libre de rang 2 :*

$$\text{Si } d \equiv 2 \text{ ou } 3 \pmod 4, \quad \mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z},$$

$$\text{Si } d \equiv 1 \pmod 4, \quad \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}.$$

Proposition 2.4.3. *Soient $A = \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ et p un nombre premier. Alors*

1. $pA = \mathfrak{m}_1\mathfrak{m}_2 \Leftrightarrow p \neq 2$ *et* $\overline{d}$ *carré dans* $\mathbb{Z}/p\mathbb{Z}$ *ou* $p = 2$ *si* $d \equiv 1 \pmod 8$.
2. $pA = \mathfrak{m} \Leftrightarrow p \neq 2$ *et* $\overline{d}$ *non carré dans* $\mathbb{Z}/p\mathbb{Z}$ *ou* $p = 2$ *si* $d \equiv 5 \pmod 8$.
3. $pA = \mathfrak{m}^2 \Leftrightarrow p|d$ *ou* $p = 2$ *si* $d \equiv 2, 3 \pmod 4$.

Proposition 2.4.4. (*Unités des corps quadratiques imaginaires*)
Soit $d \in \mathbb{N}^*$ *sans facteurs carrés et soit* $K = \mathbb{Q}[\sqrt{-d}]$.
Le groupe des unités de K *est* $\{\pm 1\}$ *sauf pour* $d = 1$ *et* $d = 3$.
Si $K = \mathbb{Q}[i]$, *alors*

$$U_K = \{\pm 1, \pm i\}.$$

Si $K = \mathbb{Q}[i\sqrt{3}]$, *alors*

$$U_K = \left\{ \left(\frac{1 + i\sqrt{3}}{2} \right)^k \mid 0 \leq k \leq 5 \right\}.$$

Proposition 2.4.5. *(Unités des corps quadratiques réels)*
Soit d *un entier sans facteurs carrés* ≥ 2 *et soit* $K = \mathbb{Q}[\sqrt{d}]$. *Alors*

$$U_K \simeq \{\pm 1\} \times \mathbb{Z}.$$

Corps cyclotomiques

Définition 2.4.6. Un *corps cyclotomique* est un corps $K \subset \mathbb{C}$ engendré sur $\mathbb{Q}$ par une racine de l'unité.

Proposition 2.4.7. *Soient* p *un nombre premier,* $r \in \mathbb{N}^*$, ζ_{p^r} *une racine primitive* p^r*-ième de l'unité et* $K = \mathbb{Q}[\zeta_{p^r}]$. *Alors,*

1. *l'anneau des entiers de* K *est* $\mathbb{Z}[\zeta_{p^r}]$,
2. $|d_K| = p^s$ *où* $s = p^{r-1}(rp - r - 1)$,
3. $pA_K = (1 - \zeta_{p^r})^{\varphi(p^r)}$ *(*p *est totalement décomposé.)*

Proposition 2.4.8. *Soient* m *un entier* ≥ 3, ζ_m *une racine primitive* m*-ième de l'unité et* $K = \mathbb{Q}[\zeta_m]$. *Alors*
1- $G(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ *et* $K/\mathbb{Q}$ *est une extension abélienne de degré* $\varphi(m)$.
2- $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ *et un nombre premier* p *est ramifié dans l'extension* $K/\mathbb{Q}$ *si et seulement s'il divise* m *(sauf si* $p = 2$ *et* $4 \nmid m$*).*

2.5 Le groupe de Pólya-Ostrowski d'une extension galoisienne

Notations. *Dans cette section K désigne un corps de nombres ou un corps de fonctions*, c'est-à-dire, une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_r(T)$ ($\mathbb{F}_r$ est un corps fini de cardinal $r = p^f$ où p est un nombre premier). *Soit $\mathcal{O}_K$ l'anneau des entiers de K*, c'est-à-dire, la fermeture intégrale dans K de l'anneau $\mathbb{Z}$ ou $\mathbb{F}_r[T]$.

Hypothèses. *On supposera toujours dans cette section que l'extension $K/\mathbb{Q}$ ou $K/\mathbb{F}_r(T)$ est galoisienne.*

Proposition 2.5.1. *(d'après Ostrowski [5]) Si le corps de nombres K est une extension galoisienne de $\mathbb{Q}$ (ou $\mathbb{F}_r(T)$), le produit des idéaux maximaux au-dessus d'un nombre premier (ou d'un polynôme irréductible) p non ramifié dans l'extension est un idéal principal.*

Proof. Les idéaux premiers $\mathfrak{m}_1, \ldots, \mathfrak{m}_g$ de $\mathcal{O}_K$ au-dessus d'un nombre premier (ou polynôme irréductible) p ont même degré résiduel f, par suite même norme $q = p^f$ (ou $q = r^{f \deg(p)}$), et même indice de ramification e (cf. prop. 2.8.5). Donc,

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{m}_i^e = \left(\prod_{i=1}^{g} \mathfrak{m}_i \right)^e .$$

Dans le cas d'une extension galoisienne de $\mathbb{Q}$, l'idéal $\Pi_q(\mathcal{O}_K)$, produit des idéaux maximaux $\mathfrak{m}$ ayant la même norme $q = p^f$, est exactement le produit de tous les idéaux maximaux au-dessus de p. Les choses sont moins simples pour les corps de fonctions : les idéaux maximaux intervenant dans un même idéal $\Pi_q(\mathcal{O}_K)$ peuvent être au-dessus de polynômes irréductibles distincts de $\mathbb{F}_r[T]$. C'est pourquoi, pour simplifier, on va désormais, essentiellement considérer le cas des extensions galoisiennes finies de $\mathbb{Q}$.

Corollaire 2.5.2. *Si l'extension $K/\mathbb{Q}$ est galoisienne, son groupe de Pólya-Ostrowski $\mathcal{P}o(\mathcal{O}_K)$ est engendré par les classes des idéaux $\Pi_q(\mathcal{O}_K)$, produits des idéaux maximaux de $\mathcal{O}_K$ au-dessus des nombres premiers p ramifiés dans l'extension.*

Remarque 2.5.3. Lorsque l'extension $K/\mathbb{Q}$ n'est pas galoisienne, $\mathcal{P}o(\mathcal{O}_K)$ n'est pas nécessairement engendré par les idéaux Π_{p^f} où p est ramifié comme le montre l'exemple du corps $K = \mathbb{Q}[X]/(X^4 + 29)$ (voir [6, Exercice II.32]).

On sait que le *nombre de classes* h_K d'un corps de nombres K, c.-à-d., le cardinal du groupe des classes d'idéaux $\mathcal{C}(\mathcal{O}_K)$, est fini (cf., par exemple, Samuel [7, chap. 4]). A fortiori, l'ordre du groupe $\mathcal{P}o(\mathcal{O}_k)$ est fini.

Notations. Pour tout $p \in \mathbb{P}$, notons $e_p(K/\mathbb{Q})$ et $f_p(K/\mathbb{Q})$ respectivement l'indice de ramification et le degré résiduel de p dans l'extension $K/\mathbb{Q}$.

Corollaire 2.5.4. *Supposons l'extension $K/\mathbb{Q}$ galoisienne. Pour tout $p \in \mathbb{P}$, posons $e_p = e_p(K/\mathbb{Q})$. Le morphisme naturel de $\mathcal{F}act(\mathcal{O}_K)$ sur $\mathcal{P}o(\mathcal{O}_K)$ se factorise à travers $\oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z}$:*

$$\mathcal{F}act(\mathcal{O}_K) \xrightarrow{\psi} \oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z} \xrightarrow{\varphi} \mathcal{P}o(\mathcal{O}_K).$$

En particulier, l'ordre de $\mathcal{P}o(\mathcal{O}_K)$ divise $\prod_{p\in\mathbb{P}} e_p$.

Proof. Comme $\mathcal{F}act(\mathcal{O}_K)$ est le groupe abélien libre engendré par les idéaux $\Pi_q(\mathcal{O}_K)$ pour $p \in \mathbb{P}$ et $q = p^{f_p}$, il est isomorphe à une somme directe de copies de $\mathbb{Z}$, $\oplus_{p\in\mathbb{P}} \mathbb{Z}$: un idéal $\mathfrak{I} = \prod_p (\Pi_q(\mathcal{O}_K))^{k_p}$ de $\mathcal{F}act(\mathcal{O}_K)$ correspond à l'élément dont la composante relative à p est k_p. Comme l'idéal $(\Pi_q(\mathcal{O}_K))^{e_p}$ est principal, le morphisme naturel de $\mathcal{F}act(\mathcal{O}_K)$ sur $\mathcal{P}o(\mathcal{O}_K)$ (donc aussi de $\oplus_{p\in\mathbb{P}} \mathbb{Z}$ sur $\mathcal{P}o(\mathcal{O}_K)$) se factorise à travers $\oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z}$. □

Evidemmment, φ est surjectif. On décrira $Ker(\varphi)$ plus loin, dans la section § 2.6.

Proposition 2.5.5. *La suite de groupes abéliens suivante est exacte* :

$$1 \to \mathbb{Q}^*/\{\pm 1\} \to \mathcal{F}act(\mathcal{O}_K) \xrightarrow{\psi} \oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z} \to 0.$$

Proof. Il est clair que le morphisme $\psi : \mathcal{F}act(\mathcal{O}_K) \to \oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z}$ est surjectif. Par ailleurs, un idéal $\mathfrak{I} = \prod_p (\Pi_q(\mathcal{O}_K))^{k_p}$ de $\mathcal{F}act(\mathcal{O}_K)$ appartient à $Ker(\psi)$ si et seulement si, pour tout p, on a $k_p = e_p m_p$ où $m_p \in \mathbb{Z}$, c'est-à-dire, $\mathfrak{I} = \left(\prod_p p^{m_p}\right) \mathcal{O}_K$. Autrement dit, $\mathfrak{I}$ est engendré par un nombre rationnel et $Ker(\psi)$ correspond au groupe des idéaux de $\mathbb{Z}$. □

Notation. Soit L/K une extension finie. Le morphisme injectif

$$j_K^L = \mathfrak{I} \in \mathcal{I}(\mathcal{O}_K) \mapsto \mathfrak{I}\mathcal{O}_L \in \mathcal{I}(\mathcal{O}_L)$$

induit un morphisme (non nécessairement injectif)

$$\varepsilon_K^L : \overline{\mathfrak{I}} \in \mathcal{C}l(\mathcal{O}_K) \mapsto \overline{\mathfrak{I}\mathcal{O}_L} \in \mathcal{C}l(\mathcal{O}_L).$$

Par ailleurs, le *morphisme norme* (voir Serre [8, I, §5])

$$N_L^K : \mathcal{I}(L) \to \mathcal{I}(\mathcal{O}_K)$$

où $N_L^K(\mathfrak{I})$ est l'idéal de $\mathcal{O}_K$ engendré par les $N_{L/K}(x)$ où x décrit $\mathfrak{I}$ est en fait déterminé par ses valeurs sur les idéaux maximaux $\mathfrak{n}$ of $\mathcal{O}_L$:

$$N_L^K(\mathfrak{n}) = \mathfrak{m}^{f_{\mathfrak{n}}(L/K)}$$

où $\mathfrak{m} = \mathfrak{n} \cap \mathcal{O}_K$ et $f_{\mathfrak{n}}(L/K) = [\mathcal{O}_L/\mathfrak{n} : \mathcal{O}_K/\mathfrak{m}]$. Il induit un morphisme :

$$\nu_L^K : \overline{\mathfrak{J}} \in \mathcal{C}l(\mathcal{O}_L) \mapsto \overline{N_L^K(\mathfrak{J})} \in \mathcal{C}l(\mathcal{O}_K)$$

puisque $N_L^K(x\mathcal{O}_L) = N_{L/K}(x)\mathcal{O}_K$.

Rappelons que, si l'extension L/K est séparable, alors pour tout $\mathfrak{I} \in \mathcal{I}(\mathcal{O}_K)$:

$$N_L^K \circ j_K^L(\mathfrak{I}) = \mathfrak{I}^{[L:K]}.$$

Les groupes factoriels et les groupes de Pólya-Ostrowski se comportent bien vis à vis de ces morphismes dès que K et L sont des extensions galoisiennes de $\mathbb{Q}$:

Proposition 2.5.6. *Si $K \subset L$ sont deux extension galoisiennes de $\mathbb{Q}$, alors :*

$$j_K^L(\mathcal{F}act(\mathcal{O}_K)) \subseteq \mathcal{F}act(\mathcal{O}_L) \quad et \quad \varepsilon_K^L(\mathcal{P}o(\mathcal{O}_K)) \subseteq \mathcal{P}o(\mathcal{O}_L)$$

$$N_L^K(\mathcal{F}act(\mathcal{O}_L)) \subseteq \mathcal{F}act(\mathcal{O}_K) \quad et \quad \nu_L^K(\mathcal{P}o(\mathcal{O}_L)) \subseteq \mathcal{P}o(\mathcal{O}_K).$$

Proof. Pour $p \in \mathbb{P}$ fixé, posons $q_K = p^{f_p(K/\mathbb{Q})}$ et $q_L = p^{f_p(L/\mathbb{Q})}$. On a alors :

$$\Pi_{q_K}(\mathcal{O}_K)\mathcal{O}_L = (\Pi_{q_L}(\mathcal{O}_L))^{e_p(L/K)}$$

et

$$N_L^K(\Pi_{q_L}(\mathcal{O}_L)) = (\Pi_{q_K}(\mathcal{O}_K))^{[L:K]/e_p(L/K)}.$$

□

Noter que la description des morphismes est donnée dans la preuve elle-même. Noter aussi que ε_K^L n'est a priori ni injectif, ni surjectif. On a toutefois les résultats suivants :

Proposition 2.5.7. *Soient $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ deux extensions galoisiennes finies et soit $L = K_1K_2$. Si $[K_1 : \mathbb{Q}]$ et $[K_2 : \mathbb{Q}]$ sont premiers entre eux, alors* :

$$j^L_{K_1}(\mathcal{F}act(\mathcal{O}_{K_1})) \cdot j^L_{K_2}(\mathcal{F}act(\mathcal{O}_{K_2})) = \mathcal{F}act(\mathcal{O}_L)$$

et

$$\nu_{L/K_i}(\mathcal{P}o(\mathcal{O}_L)) = \mathcal{P}o(\mathcal{O}_{K_i}).$$

Proof. Soient $n_1 = [K_1 : \mathbb{Q}]$ et $n_2 = [K_2 : \mathbb{Q}]$. Pour $p \in \mathbb{P}$ fixé, soient $e_i = e_p(K_i/\mathbb{Q})$ et $f_i = f_p(K_i/\mathbb{Q})$ $(i = 1, 2)$. Alors $e_p(L/\mathbb{Q}) = e_1e_2$ et $f_p(L/\mathbb{Q}) = f_1f_2$. Soient $\Pi_i = \Pi_{p^{f_i}}(\mathcal{O}_{K_i})$ $(i = 1, 2)$ et $\Pi = \Pi_{p^{f_1f_2}}(\mathcal{O}_L)$. Alors,

$$p\mathcal{O}_{K_i} = \Pi_i^{e_i},\ p\mathcal{O}_L = \Pi^{e_1e_2},\ \Pi_i\mathcal{O}_L = \Pi^{e_{3-i}}\ (i = 1, 2).$$

Posons $n_i = e_id_i$ $(i = 1, 2)$. Soient aussi u_1 et u_2 tels que $u_1n_1 + u_2n_2 = 1$. On a d'une part :

$$\Pi_1^{u_2d_2}\Pi_2^{u_1d_1}\mathcal{O}_L = \Pi^{e_2u_2d_2+e_1u_1d_1} = \Pi.$$

C'est la première assertion. D'autre part,

$$N_L^{K_1}(\Pi)^{u_2e_2} = N_L^{K_1}(\Pi^{e_2})^{u_2} = N_L^{K_1}(\Pi_1\mathcal{O}_L)^{u_2} = \Pi_1^{n_2u_2} =$$

$$\Pi_1^{1-n_1u_1} = \Pi_1 \times (\Pi_1^{e_1})^{-d_1u_1} = \Pi_1 \times (p\mathcal{O}_{K_1})^{-d_1u_1}.$$

C'est la deuxième assertion. □

Proposition 2.5.8. *Soient $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ deux extensions galoisiennes finies et soit $L = K_1K_2$. Si $[K_1 : \mathbb{Q}]$ et $[K_2 : \mathbb{Q}]$ sont premiers entre aux, alors* :
1- Les morphismes $\varepsilon^L_{K_1}$ et $\varepsilon^L_{K_2}$ sont injectifs.
2- Le groupe de Pólya $\mathcal{P}o(\mathcal{O}_L)$ est le produit direct de ses sous-groupes $\varepsilon^L_{K_i}(\mathcal{P}o(\mathcal{O}_{K_i}))$.
3- Par suite, on a l'isomorphisme :

$$\mathcal{P}o(\mathcal{O}_L) \simeq \mathcal{P}o(\mathcal{O}_{K_1}) \times \mathcal{P}o(\mathcal{O}_{K_2}).$$

Proof. Soient $n_1 = [K_1 : \mathbb{Q}]$ et $n_2 = [K_2 : \mathbb{Q}]$.
1. Comme l'ordre de $\mathcal{P}o(\mathcal{O}_{K_1})$ divise le produit des indices de ramification dans l'extension $K_1/\mathbb{Q}$, l'ordre de chacun de ses éléments est un diviseur d'une puissance de n_1, et donc est premier avec n_2. Par suite, le morphisme

$$\nu^{K_1}_L \circ \varepsilon^L_{K_1} : \overline{\mathfrak{I}} \in \mathcal{P}o(\mathcal{O}_{K_1}) \mapsto \overline{\mathfrak{I}}^{n_2} \in \mathcal{P}o(\mathcal{O}_{K_1})$$

est injectif, et $\varepsilon^L_{K_1}$ aussi.

2. En considérant les ordres des éléments, on voit que :

$$\varepsilon_{K_1}^L(\mathcal{P}o(\mathcal{O}_{K_1})) \cap \varepsilon_{K_2}^L(\mathcal{P}o(\mathcal{O}_{K_2})) = \{1\}.$$

D'autre part, l'assertion 1 de la proposition 2.5.7 implique évidemment :

$$\varepsilon_{K_1}^L(\mathcal{P}o(\mathcal{O}_{K_1})) \cdot \varepsilon_{K_2}^L(\mathcal{P}o(\mathcal{O}_{K_2})) = \mathcal{P}o(\mathcal{O}_L).$$

□

Corollaire 2.5.9. *Supposons l'extension $K/\mathbb{Q}$ abélienne de degré n. Posons $n = \prod_{p|n} p^{v_p(n)}$ et, pour tout premier p divisant n, soit K_p l'unique sous-extension de K telle que $[K_p : \mathbb{Q}] = p^{v_p(n)}$. Alors*

$$\mathcal{P}o(\mathcal{O}_K) \simeq \prod_{p|n} \mathcal{P}o(\mathcal{O}_{K_p}).$$

2.6 Une caractérisation cohomologique

Hypothèses. On suppose toujours que $K/\mathbb{Q}$ *est un extension galoisienne finie et on note G le groupe de Galois $G(K/\mathbb{Q})$.*

On va donner ici une caractérisation cohomologique du noyau du morphisme surjectif

$$\varphi : \oplus_{p\in\mathbb{P}} \mathbb{Z}/e_p\mathbb{Z} \to \mathcal{P}o(\mathcal{O}_K).$$

Le groupe de Galois $G = Gal(K/\mathbb{Q})$ opère sur K, K^*, $\mathcal{O}_K$, mais aussi sur le groupe des unités $\mathcal{O}_K^\times$ de $\mathcal{O}_K$, et aussi sur $\mathcal{P}(\mathcal{O}_K)$ et sur $\mathcal{I}(\mathcal{O}_K)$. On peut donc considérer le sous-groupe $\mathcal{I}(\mathcal{O}_K)^G$ de $\mathcal{I}(\mathcal{O}_K)$ formé des idéaux de $\mathcal{O}_K$ stables sous l'action de G ; ce n'est autre que le sous-groupe engendré par les idéaux $\Pi_q(\mathcal{O}_K)$. Par suite,

$$\mathcal{F}act(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)^G,$$

$$\mathcal{F}act(\mathcal{O}_K) \cap \mathcal{P}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)^G \cap \mathcal{P}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)^G$$

et

$$\mathcal{P}o(\mathcal{O}_K) \simeq \mathcal{I}(\mathcal{O}_K)^G/\mathcal{P}(\mathcal{O}_K)^G.$$

Ainsi, dans le cas d'une extension galoisienne K de $\mathbb{Q}$, le groupe de Pólya-Ostrowski $\mathcal{P}o(\mathcal{O}_K)$ est le sous-groupe de $\mathcal{C}l(\mathcal{O}_K)$ formé des classes des idéaux de $\mathcal{O}_K$ que l'on appelle *idéaux ambiges*.

Rappel (cf. par exemple [9]). Lorsqu'un groupe G opère par automorphismes sur des groupes abéliens, le foncteur :

$$U \mapsto U^G = \{a \in U \mid \sigma a = a \ \forall \sigma \in G\}$$

est exact à gauche ; ses foncteurs dérivés droits sont notés $H^q(G,U)$ ($q \geq 1$). Les groupes $H^q(G,U)$ sont appelés *groupes de cohomologie* de G à coefficients dans U. Ici, nous n'avons besoin que des groupes $H^1(G,U)$. Pour être concret, rappelons que

$$H^1(G,U) = Z^1(G,U)/B^1(G,U),$$

où

$$Z^1(G,U) = \{f : G \to U \mid f(\sigma\tau) = f(\sigma) \times \sigma f(\tau) \ \forall \sigma, \tau \in G\}$$

et

$$B^1(G,U) = \{f_a : G \to U \mid f_a(\sigma) = \sigma(a)/a,\ a \in U,\ \forall \sigma \in G\}\,.$$

Proposition 2.6.1. *La suite de groupes abéliens suivante est exacte :*

$$1 \to \mathbb{Q}^*/\{\pm 1\} \to \mathcal{P}(\mathcal{O}_K)^G \xrightarrow{\delta} H^1(G, \mathcal{O}_K^\times) \to 1.$$

Proof. A la suite exacte

$$1 \to \mathcal{O}_K^\times \to K^* \to \mathcal{P}(\mathcal{O}_K) \to 1,$$

correspond une suite exacte de cohomologie commençant par :

$$1 \to \{\pm 1\} \to \mathbb{Q}^* \to \mathcal{P}(\mathcal{O}_K)^G \xrightarrow{\delta} H^1\left(Gal(K/\mathbb{Q}), \mathcal{O}_K^\times\right) \to 1$$

en vertu du théorème dit "Hilbert 90" [6, Thm 90] selon lequel :

$$H^1(Gal(K/\mathbb{Q}), K^*) = \{1\}.$$

□

Proposition 2.6.2. *Si l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois G, la suite de groupe abéliens suivante est exacte* :

$$1 \to H^1(G, \mathcal{O}_K^\times) \xrightarrow{\theta} \oplus_{p \in \mathbb{P}} \mathbb{Z}/e_p\mathbb{Z} \xrightarrow{\varphi} \mathcal{P}o(\mathcal{O}_K) \to 1.$$

où e_p désigne l'indice de ramification de p dans l'extension $K/\mathbb{Q}$.

Proof. Regroupant les suites exactes données dans les propositions 2.5.5 et 2.6.1, on obtient le diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Q}^*/\{\pm 1\} & \longrightarrow & \mathcal{P}(\mathcal{O}_K)^G & \stackrel{\delta}{\longrightarrow} & H^1(G,\mathcal{O}_K^\times) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow\theta & & \downarrow \\ 1 & \longrightarrow & \mathbb{Q}^*/\{\pm 1\} & \longrightarrow & \mathcal{F}act(\mathcal{O}_K) & \stackrel{\psi}{\longrightarrow} & \oplus_{p\in\mathbb{P}}\,\mathbb{Z}/e_p\mathbb{Z} & \longrightarrow & 0 \end{array}$$

où le morphisme θ est construit de la façon suivante. Soit $f \in Z^1(G,\mathcal{O}_K^\times)$. Notons $\overline{f}$ son image dans $H^1(G,\mathcal{O}_K^\times)$. Il existe $x \in K^*$ tel que $x\mathcal{O}_K \in \mathcal{P}(\mathcal{O}_K)^G$ et $\delta(x\mathcal{O}_K) = \overline{f}$. Comme f et $\sigma \in G \mapsto \sigma(x)/x \in \mathcal{O}_K^\times$ sont congrus modulo $B^1(G,\mathcal{O}_K^\times)$, on peut définir θ par $\theta(\overline{f}) = \psi(x\mathcal{O}_K)$.
Le lemme du serpent appliqué au diagramme commutatif montre que :

$$Ker(\theta) = \{1\} \text{ et } Coker(\theta) = \frac{\mathcal{F}act(\mathcal{O}_K)}{\mathcal{P}(\mathcal{O}_K)^G} = \mathcal{P}o(\mathcal{O}_K).$$

D'où la suite exacte annoncée. □

En particulier,

$$|\mathcal{P}o(K)| \times |H^1(G,\mathcal{O}_K^\times)| = \prod_{p\in\mathbb{P}} e_p.$$

Corollaire 2.6.3. *Supposons l'extension $K/\mathbb{Q}$ cyclique de degré n.*
1– *Si K est réel et $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{1\}$, alors*

$$|\mathcal{P}o(\mathcal{O}_K)| = \frac{1}{2n} \times \prod_p e_p$$

2– *Sinon,*

$$|\mathcal{P}o(\mathcal{O}_K)| = \frac{1}{n} \times \prod_p e_p.$$

Proof. On sait que, lorsque le groupe G est cyclique engendré par un élément σ, on a (cf. par exemple Neukirch [9, IV.3.7]) :

$$H^1(G,\mathcal{O}_K^\times) \simeq H^{-1}(G,\mathcal{O}_K^\times) = \frac{\{a \in \mathcal{O}_K^\times \mid N_{K/\mathbb{Q}}(a) = 1\}}{\{\sigma(a)/a \mid a \in \mathcal{O}_K^\times\}}.$$

Le cardinal de ce dernier groupe est connu (cf. par exemple Lang [10, X, §4]) : c'est $2[K:\mathbb{Q}]$ lorsque K est réel et $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{1\}$, c'est $[K:\mathbb{Q}]$ sinon. □

Notons que ce corollaire redonne pour les corps quadratiques les résultats donnés dans la remarque 2.3.6

2.7 Corps de Pólya

Notations. *Dans cette section K désigne un corps de nombres ou un corps de fonctions*, c'est-à-dire, une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_r(T)$ ($\mathbb{F}_r$ est un corps fini de cardinal $r = p^f$ où p est un nombre premier). *Soit $\mathcal{O}_K$ l'anneau des entiers de K*, c'est-à-dire, la fermeture intégrale dans K de l'anneau $\mathbb{Z}$ ou $\mathbb{F}_r[T]$.

Définition 2.7.1. On dit que le corps de nombres ou le corps de fonctions K est un *corps de Pólya* si le $\mathcal{O}_K$-module $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière.

Dire que le corps K est de Pólya revient à dire que le groupe de Pólya-Ostrowski $\mathcal{P}o(\mathcal{O}_K)$ est trivial, c.-à-d., que tous les idéaux factoriels $(n!)_{\mathcal{O}_K}$ sont principaux, ou encore que les idéaux $\Pi_q(\mathcal{O}_K)$, produits des idéaux premiers $\mathcal{O}_K$ de même norme q sont principaux. Cette dernière formulation permet d'oublier ici la notion de polynôme à valeurs entières. On notera toutefois l'ambiguïté de la notion de corps de Pólya pour les corps de fonctions, notion liée au choix (arbitraire) de l'élément T.

Proposition 2.7.2. *Tout corps cyclotomique est un corps de Pólya.*

Proof. Soit $K = \mathbb{Q}[\mu_n]$ où μ_n est une racine primitive n-ième de l'unité. On sait qu'alors $\mathcal{O}_K = \mathbb{Z}[\mu_n]$ et les nombres premiers ramifiés dans l'extension $K/\mathbb{Q}$ sont les diviseurs de n. Soit donc p un nombre premier divisant n. Notons $r = v_p(n)$, $e = (p-1)p^{r-1}$, ζ une racine primitive p^r-ième de l'unité, $K_1 = \mathbb{Q}[\zeta]$ et $\mathcal{O}_{K_1} = \mathbb{Z}[\zeta]$. Alors p est le seul nombre premier ramifié dans l'extension $K_1/\mathbb{Q}$ et on a :

$$p\mathcal{O}_{K_1} = (\zeta - 1)^e \mathcal{O}_{K_1}.$$

Finalement, comme $(\zeta - 1)\mathcal{O}_{K_1}$ n'est pas ramifié dans l'extension K/K_1, le produit des idéaux premiers de $\mathcal{O}_K$ au-dessus de p est égal au produit des idéaux premiers de $\mathcal{O}_K$ au-dessus de l'idéal $(\zeta - 1)\mathcal{O}_{K_1}$ et c'est donc l'idéal principal $(\zeta - 1)\mathcal{O}_K$. □

Proposition 2.7.3. *(Zantema, [13]) Le sous-corps réel maximal $\mathbb{Q}[\mu_n + \mu_n^{-1}]$ du corps cyclotomique $\mathbb{Q}[\mu_n]$ est un corps de Pólya.*

Remarque 2.7.4. Il existe un analogue des corps cyclotomiques et de leur sous-corps réel maximal dans le cadre des corps de fonctions. Ce sont aussi des corps de Pólya (Adam [11]). D'une manière générale, sur les corps de fonctions qui sont des corps de Pólya, voir Van der Linden [12] et surtout Adam [11, chap. 5]. Par exemple, pour les corps de fonctions qui correspondent à des extensions cycliques de Kummer totalement imaginaires, on a la caractérisation suivante :

Proposition 2.7.5 (Adam). *Soit $D = \alpha P_1^{n_1} \cdots P_s^{n_s} \in \mathbb{F}_q[T]$ où $\alpha \in \mathbb{F}_q^*$ et les P_i sont des polynômes irréductibles et unitaires de $\mathbb{F}_q[T]$. Soit n un entier tel que $n|q-1$ et, pour $i = 1, \ldots, s$, $n_i < n$ et $p.g.c.d.(n_i, n) = 1$. Alors*

$$K = \mathbb{F}_q(T)/(Y^n - D(T)),$$

est ce que l'on appelle une extension de Kummer *de $\mathbb{F}_q(T)$. Lorsque K est totalement imaginaire, alors K est un corps de Pólya si et seulement les P_i ont le même degré et les n_i sont eux aussi égaux.*

Pour la complétude de l'énoncé, précisons ce que sont de telles extensions totalement imaginaires :

Proposition 2.7.6 (Adam). *Soit $D \in \mathbb{F}_q[T]$ un polynôme de degré d et de coefficient dominant α. L'extension pure $\mathbb{F}_q(\sqrt[n]{D})/\mathbb{F}_q(T)$ est totalement imaginaire si et seulement si :*

1. *pour tout diviseur premier l de n, soit l ne divise pas d, soit α n'est pas une puissance l-ième dans $\mathbb{F}_q^*$,*
2. *de plus, si $4|n$, alors soit $4 \not| d$, soit $-\frac{\alpha}{4}$ n'est pas une puissance 4-ième dans $\mathbb{F}_q^*$.*

On en déduit aisément :

Corollaire 2.7.7 (Van der Linden). *Soit $D \in \mathbb{F}_q[T]$ de degré impair et de discriminant non nul. On suppose q impair. Alors, le corps $\mathbb{F}_q(T)[Y]/(Y^2 - D(T))$ est de Pólya si et seulement si tous les facteurs irréductibles de D ont le même degré.*

Proposition 2.7.8. *Soit $K/\mathbb{Q}$ une extension* abélienne *finie. Si un seul nombre premier p y est ramifié, alors K est un corps de Pólya.*

Proof. Les hypothèses impliquent que K est contenu dans un corps cyclotomique $L = \mathbb{Q}[\mu]$ où $\mu^{p^r} = 1$ (cf. par exemple, Neukirch [9, Thm V.1.10]). Posons $\xi = N_{L/K}(\mu - 1)$. En appliquant $N_{L/K}$ aux deux membres de la relation :

$$p\mathcal{O}_L = (\mu - 1)^{[L:\mathbb{Q}]}\mathcal{O}_L,$$

on obtient :

$$p\mathcal{O}_K = (\xi\mathcal{O}_K)^{[K:\mathbb{Q}]}.$$

Ainsi, $\mathcal{O}_K$ a un seul idéal maximal au-dessus de p et c'est $\xi\mathcal{O}_K$. □

Il découle immédiatement de la proposition 2.6.2 :

Proposition 2.7.9. *(Zantema [13]). Le corps K, extension galoisienne de $\mathbb{Q}$ de groupe de Galois G, est un corps de Pólya si et seulement si le morphisme naturel de $H^1(G, \mathcal{O}_K^\times)$ dans $\oplus_{p\in\mathbb{P}}\mathbb{Z}/e_p\mathbb{Z}$ est surjectif.*

De façon équivalente si et seulement si :

$$|H^1(G, \mathcal{O}_K^\times)| = \prod_{p\in\mathbb{P}} e_p.$$

Les assertions 2.5.8, 2.5.9 et 2.6.3 ont pour conséquences les résultats respectifs suivants :

Proposition 2.7.10. *Soient $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ deux extensions galoisiennes finies dont les degrés sont premiers entre eux. Alors K_1K_2 est un corps de Pólya si et seulement si K_1 et K_2 sont des corps de Pólya.*

En particulier :

Proposition 2.7.11. *Supposons $K/\mathbb{Q}$ abélienne de degré $n = \prod_{i=1}^s p_i^{r_i}$. Pour tout $i = 1, \ldots, s$, soit K_i l'unique sous-extension telle que $[K_i : \mathbb{Q}] = p_i^{r_i}$. Alors K est de Pólya si et seulement si K_i est de Pólya pour $i = 1, \ldots, s$.*

On peut donc pour les extensions abéliennes se limiter au cas des extensions dont le degré est une puissance d'un nombre premier. Dans le cas d'une extension cyclique, on a alors la caractérisation suivante :

Proposition 2.7.12. *Soit $K/\mathbb{Q}$ une extension* cyclique *de degré p^r où $p \in \mathbb{P}$ et $r \in \mathbb{N}^*$. Le corps K est de Pólya si et seulement si* :
— ou bien un seul nombre premier est ramifié,
— ou bien deux nombres premiers sont ramifiés dont l'un a pour indice de ramification 2, $p = 2$, K est réel et $N(\mathcal{O}_K^\times) = \{1\}$.

Proof. Soit K_1 un sous-corps de K tel que $[K_1 : \mathbb{Q}] = p$ et soit l un nombre premier ramifié dans l'extension $K_1/\mathbb{Q}$. L'inégalité $e_l(K_1/\mathbb{Q}) \neq 1$ implique bien sûr $e_l(K_1/\mathbb{Q}) = p$. Le corollaire 2.8.10 ci-après montre alors que l est totalement ramifié dans $K/\mathbb{Q}$ et $e_l(K/\mathbb{Q}) = p^r$.
On sait que, $K/\mathbb{Q}$ étant cyclique, $|H^1(G, \mathcal{O}_K^*)| = [K : \mathbb{Q}]$ ou $2[K : \mathbb{Q}]$. D'où, si $|H^1(G, \mathcal{O}_K^\times)| = p^r$, alors l'injection θ définie dans la proposition 2.6.2 est une surjection si et seulement si l est le seul nombre premier ramifié.

Si $|H^1(G, \mathcal{O}_K^\times)| = 2p^r$, alors l'injection θ montre qu'il y a un deuxième nombre premier ramifié l' et c'est une surjection si et seulement, d'une part il n'y a pas d'autres nombres premiers ramifiés, d'autre part $e_{l'}(K/\mathbb{Q}) = 2$. Comme 2 divise p^r, nécessairement $p = 2$. □

En particulier, pour les corps quadratiques, on obtient la description suivante de tous les corps de Pólya (description que l'on pouvait déjà obtenir précédemment grâce au résultat de Hilbert rappelé dans la remarque 2.3.6).

Proposition 2.7.13. *Un corps quadratique $K = \mathbb{Q}[\sqrt{d}]$ est un corps de Pólya si et seulement si :*
— si $d > 0$ et $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{+1\}$, deux nombres premiers au plus sont ramifiés
— sinon, un nombre premier exactement est ramifié.
Autrement dit, $K = \mathbb{Q}[\sqrt{d}]$ est un corps de Pólya si et seulement si d vérifie l'une des conditions suivantes :
Corps quadratiques imaginaires
(i) $d = -1,\ d = -2$,
(ii) $d = -p$ *où* $p \in \mathbb{P}$ *et* $p \equiv 3 \pmod 4$,
Corps quadratiques réels
(iii) $d = p$ *où* $p \in \mathbb{P}$,
(iv) $d = 2p$ *où* $p \in \mathbb{P}$ *et*
— *ou bien* $p \equiv 3 \pmod 4$,
— *ou bien* $p \equiv 1 \pmod 4$ *et l'unité fondamentale est de norme* $+1$,
(v) $d = pq$ *où* $p, q \in \mathbb{P}$ *et*
— *ou bien* $p, q \equiv 3 \pmod 4$,
— *ou bien* $p, q \equiv 1 \pmod 4$ *et l'unité fondamentale est de norme* $+1$.

EXEMPLE 2.7.14. *les q-polynômes de Fermat.*
On suppose a priori que $\mathrm{Int}(A)$ possède une base régulière. Alors, l'idéal Π_q étant principal pour tout $q \geq 2$, on peut en choisir un générateur $\pi_q \in A$ (si q n'est la norme d'aucun idéal, on pose $\pi_q = 1$). On va construire une base régulière analogue à celle formée des polynômes de Fermat dans le cas d'un anneau de valuation discrète (cf. Définition 1.8.10). On vérifie d'abord que, pour $q \geq 2$, le q-binôme de Fermat

$$F_q = \frac{X^q - X}{\pi_q}$$

est à valeurs entières. Puis, on définit une suite $(F_{q,n})_{n\in\mathbb{N}}$ de q-polynômes de Fermat de la façon suivante : pour

$$n = n_0 + n_1 q + \cdots + n_k q^k,$$

on pose :

$$F_{q,n} = \prod_{j=0}^{k} \left(F_q^{*j}\right)^{n_j} .$$

Ces polynômes $F_{q,n}$ appartiennent à $\mathrm{Int}(A)$. De plus, $\deg(F_{q,n}) = n$ et le coefficient dominant de $F_{q,n}$ est $\pi_q^{-w_q(n)}$. Le théorème de Bezout appliqué aux éléments π_q pour $2 \leq q \leq n$ permet alors de construire un polynôme G_n combinaison linaire à coefficients dans A des $F_{q,n}$ $(0 \leq q \leq n)$ de sorte que $(G_n)_{n\in\mathbb{N}}$ soit une base régulière de $\mathrm{Int}(A)$.

Par exemple, pour $A = \mathbb{Z}[i]$, les q-binômes de Fermat non triviaux sont :

$$F_2 = \frac{X^2 - 1}{1 + i} \ , \ F_p = \frac{X^p - X}{p} \text{ si } p \equiv 1 \pmod 4 \ ,$$

$$F_{p^2} = \frac{X^{p^2} - X}{p} \text{ si } p \equiv 3 \pmod 4.$$

Par suite, $F_{2,0} = 1,\ F_{2,1} = X,\ F_{2,2} = F_2,\ F_{2,3} = XF_2$,

$$F_{2,4} = \frac{X^4 - 2X^3 - iX^2 + (1 + i)X}{(1 + i)^3},\ F_{2,5} = XF_{2,4},\ \cdots .$$

D'où, le début d'une base régulière :

$$1,\ X,\ F_2,\ XF_2,\ F_{2,4},\ XF_{2,4} + (1 + i)F_5,\ \cdots .$$

2.8 Rappels sur les groupes de décomposition et d'inertie

On trouve les énoncés de cette section par exemple dans Serre [8, Chap. 1, §7].

Ici A désigne un anneau de Dedekind de corps des fractions K, L est une extension finie de K et B est la fermeture intégrale de A dans K.

On sait qu'alors B est lui aussi un anneau de Dedekind et, pour tout idéal premier non nul $\mathfrak{P}$ de B, on notera $v_{\mathfrak{P}}$ la valuation correspondante de L.

Ramification

Soit $\mathfrak{p}$ un idéal premier non nul de A. Les idéaux premiers $\mathfrak{P}$ de B contenant $\mathfrak{p}$, ou encore intervenant dans la décomposition de l'idéal $\mathfrak{p}B$ de B (on note $\mathfrak{P}|\mathfrak{p}$), sont exactement ceux qui sont au-dessus de $\mathfrak{p}$ (c.-à-d., tels que $\mathfrak{P} \cap A = \mathfrak{p}$).
Pour tout idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, on note

$$e_{\mathfrak{P}} = v_{\mathfrak{P}}(pB) = \inf\{v_{\mathfrak{P}}(x) \mid x \in pB,\, x \neq 0\}.$$

On a :

$$pB = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}.$$

Le corps $B/\mathfrak{P}$ étant une extension finie de $A/\mathfrak{p}$, on pose

$$f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}].$$

L'entier $e_{\mathfrak{P}}$ (resp. $f_{\mathfrak{P}}$) est appelé l'*indice de ramification* (resp. le *degré résiduel*) de $\mathfrak{P}$ dans l'extension L/K.

Définition 2.8.1. On dit que L/K est *non ramifiée en* $\mathfrak{P}$ ou que $\mathfrak{P}$ est *non ramifié dans l'extension* L/K si $e_{\mathfrak{P}} = 1$ et si $B/\mathfrak{P}$ est une extension séparable de $A/\mathfrak{p}$. On dit que l'idéal premier non nul $\mathfrak{p}$ de A est *ramifié dans l'extension* L/K s'il existe un idéal premier $\mathfrak{P}$ de B au-dessus de $\mathfrak{p}$ qui est ramifié.

Proposition 2.8.2. *Supposons l'extension L/K séparable de degré n. Soit $\mathfrak{p}$ un idéal premier non nul de A. Alors $B/\mathfrak{p}B$ est une $A/\mathfrak{p}$-algèbre de dimension n et on a* :

$$B/\mathfrak{p}B \simeq \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}} \quad \text{et} \quad n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Proposition 2.8.3. *Soit K un corps de nombres. Supposons qu'il existe un élément $\alpha \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et soit $f(X)$ le polynôme minimal de α sur $\mathbb{Q}$. Fixons un nombre premier p. Considérons l'image canonique $\overline{f}$ de f dans $\mathbb{F}_p[X]$ et sa décomposition*

$$\overline{f}(X) = \prod_{i=1}^{g} g_i(X)^{e_i}$$

où les g_i sont des polynômes unitaires et irréductibles. Notons $f_i(X)$ des polynômes unitaires relevant les $g_i(X)$ dans $\mathbb{Z}[X]$. Alors, les $\mathfrak{m}_i = (p, f_i(\alpha))$ sont les idéaux maximaux de $\mathcal{O}_K$ au-dessus de p,

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{m}_i^{e_i}$$

est la factorisation de $p\mathcal{O}_K$ en produit de puissances d'idéaux maximaux et

$$[\mathcal{O}_K/\mathfrak{m}_i : \mathbb{F}_p] = \deg(f_i).$$

Remarque 2.8.4. Avec les hypothèses précédentes, si p ne divise pas le discriminant de d_K, alors les exposants e_i sont tous égaux à 1 (p est non ramifié dans l'extension).

Proposition 2.8.5. *Supposons l'extension L/K galoisienne de degré n. Pour tout idéal premier $\mathfrak{p}$ de A,*
— le groupe $Gal(L/K)$ opère transitivement sur l'ensemble des idéaux premiers $\mathfrak{P}$ de B au-dessus de $\mathfrak{p}$,
— pour tout idéal premier $\mathfrak{P}$ de B au-dessus de $\mathfrak{p}$, les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de $\mathfrak{p}$ (on les notera $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$),
— si $g_{\mathfrak{p}}$ désigne le nombre d'idéaux premiers $\mathfrak{P}$ de B au-dessus de $\mathfrak{p}$, on a :

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}.$$

Décomposition et inertie

Définition 2.8.6. Supposons l'extension L/K galoisienne de groupe de Galois G. Soient $\mathfrak{p}$ un idéal premier de A et $\mathfrak{P}$ un idéal premier de B au-dessus de $\mathfrak{p}$. Le sous-groupe

$$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

est appelé *groupe de décomposition* de $\mathfrak{P}$ dans l'extension L/K. Le sous-corps $L_{D_{\mathfrak{P}}}$ fixe sous $D_{\mathfrak{P}}$ est appelé *corps de décomposition* de $\mathfrak{P}$ sur K.

Proposition 2.8.7. *Supposons l'extension L/K galoisienne de groupe de Galois G. Soit $\mathfrak{p}$ un idéal premier de A. Notons $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ et $g_{\mathfrak{p}}$ ce que l'on pense. Soit $\mathfrak{P}$ un idéal premier de B au-dessus de $\mathfrak{p}$. Considérons les inclusions $K \subset L_{D_{\mathfrak{P}}} \subset L$. On a*

$$[L : L_{D_{\mathfrak{P}}}] = e_{\mathfrak{p}} f_{\mathfrak{p}} \quad \text{et} \quad [L_{D_{\mathfrak{P}}} : K] = g_{\mathfrak{p}}.$$

Lorsque $\mathfrak{P}$ décrit l'ensemble des idéaux premiers au-dessus de $\mathfrak{p}$, les groupes $D_{\mathfrak{P}}$ sont conjugués entre eux.

Définition 2.8.8. Supposons l'extension L/K galoisienne de groupe de Galois G. Soient $\mathfrak{p}$ un idéal premier de A et $\mathfrak{P}$ un idéal premier de B au-dessus de $\mathfrak{p}$. Le sous-groupe

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \mid \sigma(x) - x \in \mathfrak{P}\ \forall x \in B\}$$

est appelé *groupe d'inertie* de $\mathfrak{P}$. Le sous-corps $L_{I_\mathfrak{P}}$ fixe sous $I_\mathfrak{P}$ est appelé *corps d'inertie* de $\mathfrak{P}$.

Pour tout $\sigma \in D_\mathfrak{P}$, $\sigma(B_\mathfrak{P}) = B_\mathfrak{P}$ et $\sigma(\mathfrak{P}) = \mathfrak{P}$, donc σ induit par passage au quotient un $(A/\mathfrak{p})$-automorphisme du corps $B/\mathfrak{P}$.

Proposition 2.8.9. *Supposons l'extension L/K galoisienne de groupe de Galois G. Soient $\mathfrak{p}$ un idéal premier de A et $\mathfrak{P}$ un idéal premier de B au-dessus de $\mathfrak{p}$. Supposons l'extension $B/\mathfrak{P}/A/\mathfrak{p}$ séparable. Alors, l'extension $B/\mathfrak{P}/A/\mathfrak{p}$ est galoisienne et le morphisme naturel :*

$$\sigma \in D_\mathfrak{P} \mapsto \overline{\sigma} \in G(B/\mathfrak{P}, A/\mathfrak{p})$$

est surjectif de noyau $I_\mathfrak{P}$. Ainsi, $I_\mathfrak{P} \lhd D_\mathfrak{P}$. De plus, $|I_\mathfrak{P}| = e_\mathfrak{p}$. Enfin, lorsque $\mathfrak{P}$ décrit l'ensemble des idéaux premiers au-dessus de $\mathfrak{p}$, les groupes $I_\mathfrak{P}$ sont conjugués entre eux.

Corollaire 2.8.10. *Soit K un corps de nombres tel que $G = Gal(K/\mathbb{Q})$ soit abélien. A tout nombre premier p correspondent dans l'extension $K/\mathbb{Q}$ des entiers e_p, f_p et g_p, et des sous-groupes de G, D_p et I_p. Notons K_{D_p} et K_{I_p} les corps fixes correspondants. On a un suite d'extensions galoisiennes $\mathbb{Q} \subset K_{D_p} \subset K_{I_p} \subset K$ de degrés $[K_{D_p} : \mathbb{Q}] = g_p$, $[K_{I_p} : K_{D_p}] = f_p$ et $[K : K_{I_p}] = e_p$. Le nombre premier p est totalement décomposé dans l'extension $K_{D_p}/\mathbb{Q}$, les idéaux premiers de K_{D_p} au-dessus de p sont inertes dans l'extension K_{I_p}/K_{D_p} et les idéaux premiers de K_{I_p} au-dessus de p sont totalement ramifiés dans l'extension K/K_{I_p}.*

L'automorphisme de Frobenius

Hypothèses. On note K une extension galoisienne finie de $\mathbb{Q}$, G son groupe de Galois, p un nombre premier et $\mathfrak{P}$ un idéal maximal de $\mathcal{O}_K$ au-dessus de p. **On suppose p non ramifié**.

Rappel. Soit $\sigma : x \in \mathbb{F}_{p^f} \mapsto x^p \in \mathbb{F}_{p^f}$. Alors $k \mapsto \sigma^k$ induit un isomorphisme de groupes :

$$\mathbb{Z}/f\mathbb{Z} \simeq G(\mathbb{F}_{p^f}/\mathbb{F}_p).$$

Définition 2.8.11. Notons $\sigma_\mathfrak{P}$ l'unique élément de $D_\mathfrak{P}$ dont l'image dans $G(\mathbb{F}_{p^f}/\mathbb{F}_p)$ est $\sigma : x \mapsto x^p$. Il est caractérisé par :

$$\sigma_\mathfrak{P}(b) - b^p \in \mathfrak{P} \ \text{ pour tout } b \in \mathcal{O}_K.$$

On l'appelle *l'automorphisme de Frobenius* de $\mathfrak{P}$, c'est un générateur de $D_\mathfrak{P}$, son ordre est f. On le note aussi parfois $(\mathfrak{P}, K/\mathbb{Q})$.

Proposition 2.8.12. *1- Pour tout $\tau \in G$, on a :*

$$(\tau(\mathfrak{P}), K/\mathbb{Q}) = \tau(\mathfrak{P}, K/\mathbb{Q})\tau^{-1}.$$

Si l'extension $K/\mathbb{Q}$ est abélienne, $(\mathfrak{P}, K/\mathbb{Q})$ ne dépend que de p, on le note alors parfois $\left(\frac{K/\mathbb{Q}}{p}\right)$ et on l'appelle le symbole d'Artin *de p.*
2- Pour tout corps intermédiaire K' ($\mathbb{Q} \subset K' \subset K$), on a :

$$(\mathfrak{P}, K/K') = (\mathfrak{P}, K/\mathbb{Q})^f \quad \text{avec} \quad f = f(\mathfrak{P} \cap K'/p).$$

Si $K'/\mathbb{Q}$ est galoisienne, alors :

$$(\mathfrak{P}, K/\mathbb{Q})_{|K'} = (\mathfrak{P} \cap K', K'/\mathbb{Q}).$$

Application aux corps cyclotomiques

Soient m un entier ≥ 3, ζ_m une racine primitive m-ième de l'unité et $K = \mathbb{Q}[\zeta_m]$. On a :

Si $p \not| m$, alors $\left(\frac{L/K}{p}\right) = \sigma_p$ où $\sigma_p(\zeta) = \zeta^p$.

$$p \text{ totalement decompose dans } L/K \;\Leftrightarrow\; D_{\mathfrak{P}} = \{1\} \Leftrightarrow\; p \equiv 1 \pmod{m}.$$

Plus généralement :

Proposition 2.8.13. *Si $v_p(m) = r$ et si f_p est le plus petit entier > 0 tel que*

$$p^{f_p} \equiv 1 \pmod{\frac{m}{p^r}},$$

alors

$$p\mathcal{O}_K = \left(\mathfrak{p}_1 \cdots \mathfrak{p}_g\right)^{\varphi(p^r)} \quad \text{avec} \quad [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = f_p \quad \text{pour } i = 1, \ldots, g.$$

2.9 Extensions de Pólya : un problème ouvert

Question 2.9.1. *Tout corps de nombres est-il contenu dans un corps de Pólya ?*

Rappelons le problème du plongement en théorie du corps de classes : étant donné un corps de nombres K, en existe-t-il une extension algébrique finie L dont le nombre de classes est 1, c.-à-d., tel que l'anneau $\mathcal{O}_L$ soit principal ? [Cette question remonte Kronecker, Weber et Hilbert.]

On sait que, pour tout corps de nombres K, il existe une extension abélienne K_1 de K dont le groupe de Galois $Gal(K_1/K)$ est isomorphe au groupe des classes $\mathcal{C}(\mathcal{O}_K)$. Cette extension est donc de degré fini égal au nombre de classes $h_K = |\mathcal{C}(\mathcal{O}_K)|$. On sait de plus (théorème de l'idéal principal) que les extensions à $\mathcal{O}_{K_1}$ des idéaux de $\mathcal{O}_K$ deviennent des idéaux principaux. Cette extension K_1 est appelée le *corps de classes de Hilbert* de K.

Il se peut cependant que l'anneau $\mathcal{O}_{K_1}$ ne soit pas principal lui-même. On associe alors à K_1 son corps de classes de Hilbert K_2. A nouveau $\mathcal{O}_{K_2}$ peut ne pas être principal. On associe alors à K_2 son corps de classes de Hilbert, etc ... On construit ainsi la *tour* des corps de classes de Hilbert :

$$K \subset K_1 \subset K_2 \subset K_3 \subset \cdots$$

Soit $K_\infty = \cup_n K_n$. Le problème du plongement de K admet une solution si et seulement si cette tour d'extension est finie. Dans ce cas, K_∞ est la plus petite solution du problème de plongement. Le problème du plongement s'appelle donc aussi problème de la tour du corps de classes. Précisons enfin que, depuis 1964, on sait avec Golod et Shafarevitch que le problème du plongement n'admet pas toujours une solution.

Revenons à nos bases régulières.

Définition 2.9.2. Une extension de corps de nombres L/K est appelée *extension de Pólya* si tous les idéaux étendus $\Pi_q(\mathcal{O}_K)\mathcal{O}_L$ sont principaux, c'est-à-dire, si l'image naturelle de $\mathcal{P}o(\mathcal{O}_K)$ dans $\mathcal{P}o(\mathcal{O}_L)$ est triviale.

La proposition 2.2.9 montre qu'en d'autres termes :

Proposition 2.9.3. *L'extension de corps de nombres L/K est de Pólya si et seulement si le $\mathcal{O}_L$-module $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ admet une base régulière.*

Bien sûr, si le corps K est de Pólya, alors toute extension L/K est de Pólya. Bien sûr aussi, quel que soit le corps de nombres K, il existe toujours une extension de Pólya de K, à savoir, le corps de classes de Hilbert $H(K)$ de K. D'où, les questions :

Question 2.9.4. Etant donné un corps de nombres K,
1- existe-t-il toujours une plus petite extension de Pólya $P(K)$ de K contenue dans le corps de classes de Hilbert $H(K)$ de K ?
2- sinon, est-ce que deux extensions de Pólya de K contenue dans $H(K)$ et de degré minimum sont toujours isomorphes ?

Et d'où aussi la construction suivante (plus ou moins canonique selon les réponses aux questions précédentes) : étant donné un corps de nombres K et son corps de classes de Hilbert K_1, il existe des corps L compris entre K et K_1 tels que l'extension L/K soit de Pólya. Désignons par K_1^* un tel corps de degré minimum sur K. De façon analogue au problème du plongement, on construit une tour d'extensions :

$$K \subset K_1^* \subset K_2^* \subset K_3^* \subset ...$$

et on peut se demander si cette construction s'arrête toujours à un rang fini. Si oui, on pourra affirmer que tout corps de nombres est contenu dans un corps de Pólya.

EXEMPLE 2.9.5. Toute extension abélienne finie K de $\mathbb{Q}$ est contenue dans un corps de Pólya. En effet, d'après le théorème de Kummer, une telle extension est contenue dans un corps cyclotomique et, on sait, qu'un tel corps est de Pólya.

2.10 Suites de Newton

Polynômes d'interpolation de Newton

Lorsqu'on considère l'interpolation d'une fonction f en $n+1$ points distincts $a_0, a_1, \ldots, a_n$, on sait qu'il existe un polynôme P de degré $\leq n$ et un seul tel que :

$$P(a_k) = f(a_k) \quad \text{pour} \quad k = 0, 1, \ldots, n.$$

Ce polynôme s'écrit de différentes façons et, selon, porte un nom différent.
Le *polynôme d'interpolation de Lagrange* de f en $a_0, a_1, \ldots, a_n$ s'écrit :

$$L_n(X) = \sum_{k=0}^{n} f(a_k) \; \frac{(X-a_0)\cdots\widehat{(X-a_k)}\cdots(X-a_n)}{(a_k-a_0)\cdots\widehat{(a_k-a_k)}\cdots(a_k-a_n)}$$

où $\widehat{(\cdots)}$ signifie que le terme $(\cdots)$ est supprimé. C'est un somme de polynômes de degré n.

Quant au *polynôme d'interpolation de Newton* de f relatif à la suite $a_0, a_1, \ldots, a_n$ (l'ordre a son importance), il s'écrit :

$$N_n(X) = \sum_{k=0}^{n} \Delta^k f(a_0) \ \frac{(X-a_0)(X-a_1)\cdots(X-a_{k-1})}{(a_k-a_0)(a_k-a_1)\cdots(a_k-a_{k-1})}$$

où $\Delta^k f(a_0)$ désigne la k-ième différence finie de f relativement à la suite des éléments $a_0, a_1, \ldots, a_n$. C'est une somme de polynômes de degrés distincts de 0 à n.

Dans le cas particulier où $a_0, a_1, \ldots, a_n$ est la suite $0, 1, \ldots, n$, on reconnaît :

$$N_n(X) = \sum_{k=0}^{n} \Delta^k f(0) \binom{X}{k} \quad \text{avec} \quad \binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}.$$

Remarquons que :
— d'une part les polynômes binomiaux $\binom{X}{k}$ sont des polynômes de Lagrange,
— d'autre part, pour $k \in \mathbb{N}$, les $\binom{X}{n}$ engendrent le $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$.
Nous allons ici étudier cette dernière situation dans un cadre plus général. Nous allons voir que cela correspond à une propriété forte et donc rare.

Suites de Newton

Hypothèses et notations. Momentanément, on va considérer *un anneau intègre D de corps des fractions K et E une partie de D*. A toute suite finie ou infinie $(a_n)_{n=0}^N$ d'éléments distincts de E, on associe une suite $(f_n)_{n=0}^N$ de polynômes de Lagrange :

$$f_0(X) = 1\ ,\ f_1(X) = \frac{X-a_0}{a_1-a_0}\ ,\ldots,\ f_n(X) = \prod_{k=0}^{n-1} \frac{X-a_k}{a_n-a_k}\ ,\ldots$$

Bien sûr, la famille $(f_n)_{n=0}^N$ est une base du K-espace vectoriel $K_N[X]$. On peut se demander si c'est aussi une base du D-module

$$\mathrm{Int}_N(E,D) = \{f \in K_N[X] \mid f(E) \subseteq D\}.$$

Définition 2.10.1. Soit $N \in \mathbb{N} \cup \{\infty\}$. Une suite (finie or infinie) $(a_n)_{0\le k\le N}$ d'éléments distincts de E est appelée *suite de Newton de E dans D* ou, plus simplement, une *suite D-ordonnée de E* si les polynômes

$$f_n(X) = \prod_{k=0}^{n} \frac{X-a_k}{a_n-a_k} \qquad (0 \le n \le N)$$

forment une base du D-module $\mathrm{Int}_N(E, D)$.

Une telle suite sera dite de *longueur* N.

Définition 2.10.2. La longueur maximale (finie ou infinie) d'une suite de Newton de E dans D est appelée *constante de Newton* de E dans D et est notée $\nu_D(E)$.

Ainsi, la constante de Newton de l'anneau D est le degré maximal d'un polynôme à valeurs entières sur D pouvant s'exprimer comme polynôme d'interpolation de Newton en des éléments de D.

EXEMPLES 2.10.3. 1- La suite $0, 1, 2, \ldots$ est une suite $\mathbb{Z}$-ordonnée de $\mathbb{N}$. En fait, pour tout $m \in \mathbb{N}$, la suite $m, m+1, m+2, \ldots$ est une suite $\mathbb{Z}$-ordonnée de $\mathbb{N}$. Il n'y a donc pas unicité en général des suites de Newton. ($\nu_{\mathbb{Z}}(\mathbb{N}) = +\infty$).

2- Pour l'ensemble $E = \mathbb{P} \cup \{\pm 1\}$, voici les seules suites de Newton de longeur 1 : $1, 2$ et $2, 3$, de longueur 2 : $1, 2, 3$, de longueur 3 : $1, 2, 3, 5$ et $1, 2, 3, -1$. Il n'y a pas de suite de Newton de longueur 4. A fortiori, il n'existe pas toujours des suites de Newton de longueur infinie. ($\nu_{\mathbb{Z}}(\mathbb{P}) = 3$)

Proposition 2.10.4. *Les assertions suivantes sont équivalentes :*
(i) la suite $\{a_n\}_{0 \le n \le N}$ est une suite D-ordonnée de E,
(ii) les polynômes f_n $(0 \le n \le N)$ sont dans $\mathrm{Int}(E, D)$,
(iii) pour tout $n \in \{1, \ldots, N\}$ et tout $x \in S$,

$$\prod_{k=0}^{n-1}(a_n - a_k) \ \ divise \ \ \prod_{k=0}^{n-1}(x - a_k).$$

Remarques 2.10.5. 1- Lorsque D est un anneau de Dedekind, la notion de suite de Newton correspond à celle de 'simultaneous ordering' de Bhargava [10].

2- Si $\{a_k\}_{0 \le k \le n}$ est une suite D-ordonnée de E, alors $n!_E^D$ est un idéal principal, à savoir l'idéal engendré par $\prod_{k=0}^{n}(a_n - a_k)$. [C'est une sorte de globalisation de la remarque 1.10.8.]

Proposition 2.10.6. *Lorsque D un anneau de Dedekind, les assertions de la proposition 2.10.4 sont aussi équivalentes à* :
(iv) pour tout $n \in \{1, \ldots, N\}$ et tous $x_0, \ldots, x_n \in E$,

$$\prod_{0 \le i < j \le n}(a_i - a_j) \ \ divise \ \ \prod_{0 \le i < j \le n}(x_i - x_j).$$

Question 2.10.7. Si $\nu_D(E) = N$, est-ce que toute suite de Newton de longueur $n < N$ peut être prolongée en une suite de Newton de longueur $n+1$?

Proposition 2.10.8. *Soit $\mathcal{P}$ un ensemble d'idéaux premiers de D tels que l'on ait $D = \cap_{\mathfrak{p}\in\mathcal{P}} D_{\mathfrak{p}}$. Alors, une suite $\{a_n\}_{0\leq n\leq N}$ d'éléments de E est une suite D-ordonnée de E si et seulement si c'est une suite $D_{\mathfrak{p}}$-ordonnée de E quel que soit $\mathfrak{p} \in \mathcal{P}$.*

EXEMPLE 2.10.9. La suite $0, 1^2, 2^2, 3^2, \ldots, n^2, \ldots$ est une suite de Newton de $\mathbb{N}^{(2)} = \{n^2 \mid n \in \mathbb{N}\}$ dans $\mathbb{Z}$.

Proposition 2.10.10. *Soient D un anneau de Dedekind domain, N un entier positif fixé et $(a_n)_{0\leq n\leq N}$ une suite d'éléments de E. Si $\{a_{n,\mathfrak{m}}\}_{0\leq n\leq N}$ est une suite $D_{\mathfrak{m}}$-ordonnée de E quel que soit $\mathfrak{m} \in \max(D)$, alors une suite $\{a_n\}_{0\leq n\leq N}$ d'éléments de E est une suite D-ordonnée de E dès que, pour tout $\mathfrak{m} \in \max(D)$ et tout $n \in \{0, \ldots, n, \ldots, N\}$, on a :*

$$v_{\mathfrak{m}}(a_n - a_{n,\mathfrak{m}}) > \sup_{0\leq k\leq n} v_{\mathfrak{m}}(a_{n,\mathfrak{m}} - a_{k,\mathfrak{m}}).$$

Cette proposition peut nous aider à construire des suites de Newton lorsque notamment $E = D$ est un anneau de Dedekind. Mais cette construction est loin d'être toujours assurée car on peut avoir une infinité d'inégalités à satisfaire dès lors que l'anneau D n'est pas semi-local (semi-local = nombre fini d'idéaux maximaux).

2.11 Parties de Newton

Définition 2.11.1. Une partie non vide E de D est appelée *partie de Newton* de D s'il existe une suite de Newton de E dans D de longueur $Card(E) - 1$ lorsque E est finie et de longueur infinie lorsque E est infinie. [Autrement dit, $\nu_D(E) + 1 = Card(E)$.]

EXEMPLES 2.11.2. Cas où l'anneau D est local.

1- Soit D un anneau local d'idéal maximal $\mathfrak{m}$. Si E rencontre une infinité de classes de D modulo $\mathfrak{m}$, alors E est une partie de Newton de D. En effet, dans ce cas $\mathrm{Int}(E, D) = D[X]$ et une suite d'élements de E est une suite de Newton si et seulement si ses éléments sont dans des classes distinctes modulo $\mathfrak{m}$.

2- Toute partie de l'anneau V d'une valuation discrète v à corps résiduel fini est une partie de Newton de V. En effet, une suite de Newton dans V n'est pas autre chose qu'une suite v-ordonnée de E.

EXEMPLES 2.11.3. Cas où D n'est pas semi-local.

1- Soit q un entier ≥ 2. Alors $E_{(q)} = \{q^n \mid n \in \mathbb{N}\}$ est une partie de Newton de $\mathbb{Z}$. En outre, la suite $(q^n)_{n\in\mathbb{N}}$ est une suite de Newton de $E_{(q)}$ dans $\mathbb{Z}$ et il n'y en a pas d'autres.

2- De façon analogue, l'ensemble $E_{(T)} = \{T^n \mid n \in \mathbb{N}\}$ est une partie de Newton de $\mathbb{F}_q[T]$ et la suite $(T^n)_{n\in\mathbb{N}}$ est la seule suite de Newton de E dans $\mathbb{F}_q[T]$.

3- Soit $k \in \mathbb{N}^*$. La partie $\mathbb{N}^{(k)} = \{n^k \mid n \in \mathbb{N}\}$ est une partie de Newton de $\mathbb{Z}$ si et seulement si $k = 1$ ou 2.

Exercice 2.11.4. Montrer que $\nu_{\mathbb{Z}}(\mathbb{N}^{(k)}) = 1$ pour $k \geq 3$ et que $\nu_{\mathbb{Z}}(\mathbb{Z}^{(k)}) = 2$ pour k impair ≥ 3.

Exercice 2.11.5. Appliquer la proposition 2.10.6 à la construction de parties de Newton de $\mathbb{Z}$ ou de $\mathbb{P}$. Montrer qu'il y a des parties infinies de $\mathbb{P}$ qui sont de Newton, alors que $\nu_{\mathbb{Z}}(\mathbb{P}) \leq 3$.

Exercice 2.11.6. On s'intéresse aux parties de la forme $\{P(n) \mid n \in \mathbb{N}\}$ où $P \in \mathbb{Z}[X]$.

1- Montrer que les seules parties de ce type qui sont de Newton dans $\mathbb{N}$ sont les suivantes :

$$(\lambda n + \mu)_{n\in\mathbb{N}}\ ,\ (\lambda n^2 + \mu)_{n\in\mathbb{N}}\ ,\ (\lambda\frac{n(n+1)}{2} + \mu)_{n\in\mathbb{N}} \quad \text{avec} \quad \lambda, \mu \in \mathbb{N}.$$

2- Quelles sont les parties de ce type qui sont de Newton dans $\mathbb{Z}$?

Remarque 2.11.7. Soit E une partie de Newton de D et soit $(a_n)_{n=0}^N$ une suite de Newton de E dans D. Posons $E_0 = \{a_n \mid 0 \leq n \leq N\}$. Alors il est immédiat par définition des suites de Newton que $\mathrm{Int}(E, D) = \mathrm{Int}(E_0, D)$. On dit que les parties E et E_0 sont des *parties polynomialement équivalentes* dans D. De sorte que pour tester si une partie E est de Newton, on a souvent intérêt à considérer d'emblée sa *clôture polynomiale* dans D, à savoir, la plus grande partie F de D polynomialement équivalente à E, c'est-à-dire, telle que $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$. Par exemple, on montre que la clôture polynomiale de $\mathbb{P}$ dans $\mathbb{Z}$ est $\mathbb{P} \cup \{\pm 1\}$.

Un exemple

Proposition 2.11.8. *La partie $E_{(T)} = \{T^n \mid n \in \mathbb{N}\}$ est une partie de Newton de $\mathbb{Z}[T]$.*

Proof. Selon la proposition 2.10.8, il s'agit de montrer :
Pour tout élément irréductible π de $\mathbb{Z}[T]$, $(T^n)_{n\in\mathbb{N}}$ est une suite v_π-ordonnée de $E_{(T)}$ où v_π désigne la valuation de $\mathbb{Q}(T)$ associée à π.

L'élément π est soit un nombre premier, soit un polynôme irréductible de $\mathbb{Q}[T]$ que l'on peut supposer unitaire. Evidemment, si $v_\pi(T^n - T^m) \neq 0$ pour un certain couple $n \neq m$, alors $\pi = T$ ou $\Phi_d(T)$ où Φ_d désigne le d-ième polynôme cyclotomique et d divise $n - m$. Pour $\pi = T$, on a déjà vu que la suite $(T^n)_{n\in\mathbb{N}}$ est v_π-ordonnée. Soit donc $d > 0$ et montrons par récurrence sur n que $(T^k)_{k=0}^n$ est v_{Φ_d}-ordonnée. Pour $m > n$, on a :

$$v_{\Phi_d}\left(\prod_{k=0}^{n-1}(T^m - T^k)\right) = v_{\Phi_d}\left(\prod_{k=m-n+1}^{m}(T^k - 1)\right),$$

tandis que

$$v_{\Phi_d}\left(\prod_{k=0}^{n-1}(T^n - T^k)\right) = v_{\Phi_d}\left(\prod_{k=1}^{n}(T^k - 1)\right).$$

Ces quantités sont respectivement égale à :

$$card\{k \mid d|k,\, m-n+1 \leq k \leq m\} \text{ et } card\{k \mid d|k,\, 1 \leq k \leq n\},$$

c'est-à-dire,

$$\left[\frac{m}{d}\right] - \left[\frac{m-n}{d}\right] \quad \text{et} \quad \left[\frac{n}{d}\right].$$

Clairement, cette dernière quantité est inférieure ou égale à la première. □

Proposition 2.11.9 (Sury [14])**.** *Pour tout suite d'entiers $a_0 < a_1 < \ldots < a_n$,*

$$P(T) = \prod_{0\leq i<j\leq n} \frac{T^{a_j - a_i} - 1}{T^{j-i} - 1} \in \mathbb{Z}[T].$$

Proof. D'après la proposition 1.10.11, pour tout élément irréductible π de $\mathbb{Z}[X]$, on a

$$\prod_{0\leq i<j\leq n} \frac{T^{a_j} - T^{a_i}}{T^j - T^i} \in \mathbb{Z}[T]_\pi.$$

Par suite,

$$\prod_{0\leq i<j\leq n} \frac{T^{a_j} - T^{a_i}}{T^j - T^i} \in \mathbb{Z}[T].$$

Finalement, $P(T) \in \mathbb{Z}[T]$ puisque $a_0 + a_1 + \ldots + a_n \geq 0 + 1 + \ldots + n$. □

Application. On retrouve le résultat désormais classique :
Quels que soient les $n+1$ entiers $a_0,\ a_1, \ldots,\ a_n$, le produit

$$\prod_{0\leq i<j\leq n}(a_j - a_i) \quad \text{est divisible par} \quad 1!\ldots n!.$$

Proof. La règle de l'Hôpital appliquée aux facteurs de la fonction

$$P(t) = \prod_{0\leq i<j\leq n} \frac{t^{a_j-a_i}-1}{t^{j-i}-1},$$

montre que :

$$\lim_{t\to 1} P(t) = \prod_{0\leq i<j\leq n} \lim_{t\to 1} \frac{(a_j-a_i)t^{a_j-a_i-1}}{(j-i)t^{j-i-1}} = \prod_{0\leq i<j\leq n} \frac{a_j-a_i}{j-i}.$$

La proposition précédente montre que ce nombre rationnel est en fait un entier. □

Exercice 2.11.10. Peut-on remplacer T par un polynôme $g(T)$ irréductible de $\mathbb{F}_q[T]$ dans l'énoncé de la proposition 2.11.9 ?

La conjecture de Thakur

Dinesh Thakur [15] a remarqué qu'il existe parfois des interpolations complexes ou bien p-adiques naturelles de la fonction $n \mapsto n!_E^D$ sous forme de fonctions Γ généralisées et que tous les cas classiquement connus correspondent à des parties E qui sont de Newton. Par exemple :

1- La fonction $n \in \mathbb{N} \mapsto (n-1)! \in \mathbb{Z}$ possède un prolongement analytique naturel Γ, mais aussi un prolongement p-adique pour tout $p \in \mathbb{P}$ défini par Morita [16] de la façon suivante :

$$\Gamma_p : n \in \mathbb{N} \mapsto \Gamma_p(n) = (-1)^n \prod_{1\leq j<n,\, p\not| j} j \in \mathbb{Z}$$

peut être étendu par continuité à $\mathbb{Z}_p$. Cette extension Γ_p vérifie

$$\Gamma_p(z+1) = -\Gamma_p(z) \text{ si } z \in p\mathbb{Z}_p \text{ et } -z\Gamma_p(z) \text{ si } z \in \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

En outre, Γ_p est analytique sur $p\mathbb{Z}_p$.

2- Ou encore, considérons la fonction :

$$\Pi : n \in \mathbb{N} \mapsto n!_{\mathbb{F}_q[T]} \in \mathbb{F}_q[T].$$

De façon analogue à ce qu'a fait Morita pour la fonction Γ_p, Goss [17] définit la fonction :

$$\Pi_\infty : n \in \mathbb{N} \mapsto \frac{\Pi(n)}{T^{\deg(\Pi(n))}} \in \mathbb{F}_q(T) \subset \mathbb{F}_q((1/T)).$$

Cette fonction peut être prolongée en une fonction continue

$$\Pi_\infty : \mathbb{Z}_p \to \mathbb{F}_q((1/T))$$

de la façon suivante : utilisant l'écriture q-adique de n,

$$n = n_0 + n_1 q + \ldots + n_s q^s,$$

on sait que l'on a :

$$\Pi(n) = \prod_{i=0}^{s} D_i^{n_i},$$

et donc, pour $y = \sum y_i q^i \in \mathbb{Z}_p$, on pose :

$$\Pi_\infty(y) = \prod_i \left(\frac{D_i}{T^{\deg(D_i)}} \right)^{n_i}.$$

3- Pour les q-factorielles, Jackson [18] a lui aussi considéré une interpolation analytique naturelle.

Question 2.11.11. Est-ce un phénomène général ? Est-ce que les extensions naturelles des factorielles généralisées n'existent que pour les parties de Newton ?

2.12 Anneaux de Newton

Définition 2.12.1. Un anneau intègre D est appelé *anneau de Newton* s'il possède une suite de Newton infinie, autrement dit, s'il est une partie de Newton en tant que partie de lui-même ($\nu(D) = +\infty$).

On a vu qu'en général, quand elles existent, les suites de Newton ne sont pas uniques. En particulier, on a le résultat immédiat suivant :

Proposition 2.12.2. *If $(a_n)_{0\leq n\leq N}$ est une suite D-ordonnée alors, quels que soient $u \in U(D)$ et $b \in D$, $(ua_n + b)_{0\leq n\leq N}$ est aussi une suite D-ordonnée (où $U(D)$ désigne le groupe des unités de D).*

On peut donc toujours transformer une suite de Newton de longueur N en une suite de même longueur commençant par 0 et 1, une telle suite sera appelée *suite de Newton normalisée*.

Mais, il peut exister des suites de Newton d'un autre type :

EXEMPLE 2.12.3. La suite

$$\left((-1)^n \left[\frac{n+1}{2}\right]\right)_{n\in\mathbb{N}}$$

est une suite de Newton normalisée de $\mathbb{Z}$.

On sait que $\mathbb{Z}$ est un anneau de Newton. Existe-t-il d'autre anneaux de Newton ? Oui, et on va donner des exemples très simples, mais on va voir que la question est plus difficile pour les anneaux d'entiers. Les exemples 2.11.2 montrent que :

EXEMPLES 2.12.4. 1- Tout anneau de valuation discrète est un anneau de Newton.
2- Un anneau local de corps résiduel infini est un anneau de Newton.

La proposition 2.10.8 donne en particulier :

Proposition 2.12.5. *Une suite $(a_n)_{0\leq n\leq N}$ d'éléments de D est D-ordonnée si et seulement si elle est $D_{\mathfrak{m}}$-ordonnée pour tout idéal maximal $\mathfrak{m}$ de D.*

Avec le théorème d'approximation dans les anneaux de Dedekind et la proposition 2.10.10, on obtient :

Proposition 2.12.6. *Tout anneau principal semi-local est de Newton.*

Remarque 2.12.7. En fait, (cf. Yeramian [19]) dans le cas semi-local principal précédent, on peut montrer l'existence d'une suite de Newton $(a_n)_{n\in\mathbb{N}}$ telle que, de plus, pour tout idéal maximal $\mathfrak{m}$, on ait :

$$v_{\mathfrak{m}}(a_n - a_m) = v_{N(\mathfrak{m})}(n - m).$$

Anneaux d'entiers de corps de nombres

Considérons donc le cas d'anneaux non semi-locaux. La première question naturelle est la suivante :

Question 2.12.8. (Bhargava [10, Question 30]) Existe-t-il un corps de nombres $K \neq \mathbb{Q}$ tel que l'anneau $\mathcal{O}_K$ des entiers de K soit un anneau de Newton ?

On sait [remarque 2.10.5.2] que, s'il existe une suite de Newton, alors les idéaux factoriels sont principaux. Par conséquent, si $\mathcal{O}_K$ est un anneau de Newton, K est un corps de Pólya. On a vu par exemple qu'un corps quadratique imaginaire $\mathbb{Q}[\sqrt{d}]$ est de Pólya si et seulement si $d = -1, -2$ ou $-p$ où $p \in \mathbb{P}$ vérifie $p \equiv 3 \pmod 4$. Mais, être un corps de Pólya est une condition nécessaire qui est loin d'être suffisante. D'ailleurs, à propos des anneaux de Newton, on a essentiellement des résultats négatifs.

Exercices 2.12.9. 1- L'anneau principal $A = \mathbb{Z}[i]$ n'est pas de Newton.
a- Vérifier que

$$(0!)_A = (1!)_A = (1), (2!)_A = (3!)_A = (1+i) \text{ et } (4!)_A = (1+i)^3.$$

Supposons que $(a_n)_{n\in\mathbb{N}}$ soit une suite v_π-ordonnée pour tout π qui commence par $a_0 = 0$ et $a_1 = 1$.
b- Montrer que, nécessairement, à des unités de A près, on a : $\{a_2, a_3\} = \{i, 1+i\}$.
c- Montrer que, quels que soient les choix de a_2, a_3, a_4, on a :

$$N_{\mathbb{Q}[i]/\mathbb{Q}}\left(\prod_{k=0}^{3}(a_4 - a_k)\right) > 8 = N_{\mathbb{Q}[i]/\mathbb{Q}}\left((1+i)^3\right).$$

d- En déduire que $\nu(\mathbb{Z}[i]) = 3$.

2- L'anneau $A = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ n'est pas de Newton.
a- Vérifier que

$$(0!)_A = (1!)_A = (2!)_A = A,\ (3!)_A = \sqrt{-3}A,\ (4!)_A = 2\sqrt{-3}A.$$

b- Vérifier que $0, 1, \frac{1+\sqrt{-3}}{2}, \frac{3+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}$ est une suite de Newton de A.
c- Montrer que $\nu(\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]) = 4$.

Proposition 2.12.10. *(Wood [20]) Si K est un corps quadratique imaginaire, alors l'anneau $\mathcal{O}_K$ n'est jamais de Newton.*

La raison pour laquelle il est sans doute plus facile de donner une réponse négative dans le cas des corps quadratiques imaginaires est vraisemblablement due au fait qu'il n'y a qu'un nombre fini d'unités.

Proposition 2.12.11. *Soient K un corps de nombres et D un localisé de l'anneau des entiers $\mathcal{O}_K$. Notons l_D le plus petit nombre premier non totalement décomposé dans D. Alors la suite $0, 1, 2, \ldots, m$ est une suite de Newton de D si et seulement si $m < l_D$.*

C'est une conséquence immédiate du lemme suivant :

Lemme 2.12.12. *Soient K un corps de nombres de degré d sur $\mathbb{Q}$ et D un localisé de l'anneau des entiers de K. Notons $l = l_D$ le plus petit nombre premier non totalement décomposé dans D. Alors,*

$$\forall n < l, \quad (n!)_D = n!D$$

$$(l!)_D = (l-1)! \prod_{\mathfrak{p} \in \max(D),\, \mathfrak{p}|l,\, f(\mathfrak{p}/l)=1} \mathfrak{p}$$

Pars suite, l'idéal $(l!)_D$ divise strictement $l!D$.

Cas particulier. Soit K un extension galoisienne finie de $\mathbb{Q}$ et soit l le plus petit nombre premier non totalement décomposé dans l'extension. Alors,

$$l!_{\mathcal{O}_K} = \begin{cases} (l-1)!\mathcal{O}_K & \text{si} \quad f_l \neq 1 \\ (l-1)! \prod_{\mathfrak{p}|l} \mathfrak{p} & \text{si} \quad f_l = 1 \end{cases}$$

On en déduit le résultat positif suivant :

Proposition 2.12.13 ([21])**.** *Soient K un corps de nombres et D un localisé de l'anneau des entiers $\mathcal{O}_K$. Alors, la suite $(n)_{n\in\mathbb{N}}$ est une suite D-ordonnée si et seulement si tout nombre premier est totalement décomposé dans D.*

Par suite, on peut toujours construire des anneaux de Newton (non semi-locaux) en localisant l'anneau $\mathcal{O}_K$ par la partie multiplicative S de $\mathbb{Z}$ engendrée par les nombres premiers qui ne sont pas totalement décomposés dans $\mathcal{O}_K$. Par exemple, si S désigne la partie multiplicative de $\mathbb{Z}$ engendrée par les nombres premiers p tels que $p \equiv 1 \pmod 4$, alors $S^{-1}\mathbb{Z}[i]$ est un anneau de Newton. Plus généralement,

Proposition 2.12.14. *[6, §IV.3] Soient D un anneau de Dedekind qui est de Newton, $(a_n)_{n\in\mathbb{N}}$ une suite D-ordonnée et R un anneau intègre contenant D. Les assertions suivantes sont équivalentes :*

1. $(a_n)_{n\in\mathbb{N}}$ *est une suite* R*-ordonnée,*
2. D *est polynomialement dense dans* R*, c'est-à-dire,* $\mathrm{Int}(R, D) = \mathrm{Int}(D)$*,*
3. *quel que soit* $\mathfrak{p} \in \max(D)$ *à corps résiduel fini, quel que soit* $\mathfrak{m} \in \max(R)$ *contenant* $\mathfrak{p}$*, on a :*

$$R/\mathfrak{m} \simeq D/\mathfrak{p} \quad \text{et} \quad \mathfrak{m}R_{\mathfrak{m}} = \mathfrak{p}R_{\mathfrak{m}}.$$

Lorsque R *est noethérien, c'est encore équivalent à :*

4. *tout* $\mathfrak{p} \in \max(D)$ *à corps résiduel fini tel que* $\mathfrak{p}R \neq R$ *est complètement décomposé dans* R *(c'est-à-dire,* $\mathfrak{p}R = \prod_{i=1}^{r} \mathfrak{m}_i$ *où les* $\mathfrak{m}_i$ *sont les idéaux maximaux distincts de* R *de norme égle à la norme de* $\mathfrak{p}$*).*

Cas des corps de fonctions

Si l'on considère la question des anneaux de Newton dans le contexte des corps de fonctions, on a des résultats analogues. Tout d'abord, l'analogue de $\mathbb{Z}$:

Proposition 2.12.15. *Pour tout corps fini* $\mathbb{F}_q$*, l'anneau de polynômes* $\mathbb{F}_q[T]$ *est un anneau de Newton.*

Proof. On construit une suite de Newton pour $\mathbb{F}_q[T]$ de façon analogue à celles construites pour les anneaux de valuation discrète mais ici relativement à la valuation T-adique de $\mathbb{F}_q(T)$. Soit $a_0 = 0, a_1, \ldots, a_{q-1}$ la suite des éléments $\mathbb{F}_q$ et posons :

$$a_n = \sum_{j=0}^{k} a_{n_j} T^j \quad \text{pour} \quad n = \sum_{j=0}^{k} n_j q^j.$$

Par construction, la suite est v_T-ordonnée ; en fait, elle est V_Q-ordonnée pour tout élément irréductible Q de $\mathbb{F}_q[T]$. C'est ce que montre l'assertion suivante. □

Proposition 2.12.16. *Soit* D *un anneau factoriel et, pour tout* $a \in D$ *non nul et non inversible, posons* $N(a) = Card(D/aD)$*. Supposons que la suite* $(a_n)_{n\in\mathbb{N}}$ *d'éléments de* D *vérifie :*

$$\forall a \in D,\ \forall k \in \mathbb{N},\ u_{kN(a)}, u_{kN(a)+1}, \ldots, u_{(k+1)N(a)-1}$$

sont dans des classes distinctes modulo a*. Alors, la suite* $(a_n)_{n\in\mathbb{N}}$ *est une suite* D*-ordonnée.*

Lorsque $N(a)$ est fini, la condition signifie que les éléments forment un système complet de représentants de D modulo a. En fait, la condition n'est utile que pour les a qui sont des puissances d'irréductibles comme le montre l'assertion suivante qui aurait dû figurer dans le chapitre précédent.

Proposition 2.12.17. *(cf. Amice [22] et Yeramian [23]) Soit V l'anneau d'une valuation discrète v d'idéal maximal $\mathfrak{m}$ et de corps résiduel fini de cardinal q. Une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de V est une suite v-ordonnée de V si et seulement si :*

$$\forall s \in \mathbb{N},\ \forall k \in \mathbb{N}^*,\ a_{sq^k}, a_{sq^k+1}, \ldots, \ldots, a_{(s+1)q^k-1}$$

est un système complet de représentants de V modulo $\mathfrak{m}$.

Exercice 2.12.18. Déduire de la suite de Newton construite pour l'anneau $\mathbb{F}_q[T]$ que les *factorielles de Carlitz* $(n!)_{\mathbb{F}_q[T]}$ sont égales à

$$(n!)_{\mathbb{F}_q[T]} = \left(T^{q^k} - T\right)^{n_k} \left(T^{q^{k-1}} - T\right)^{n_{k-1}+n_k q} \cdots (T^q - T)^{n_1+\cdots+n_k q^{k-1}}.$$

Si l'on considère des extensions algébriques K de $\mathbb{F}_q(T)$ et la clôture intégrale $\mathcal{O}_K$ de $\mathbb{F}_q[T]$ dans K, on peut se demander si l'anneau $\mathcal{O}_K$ est de Newton. Voici un résultat très semblable à celui sur les corps quadratiques imaginaires.

Rappelons pour commencer que l'extension quadratique K de $\mathbb{F}_q(T)$ est dite *imaginaire* si la place à l'infini de $\mathbb{F}_q(T)$, c'est-à-dire, la valuation associée à la fraction $\frac{1}{T}$, a deux extensions à K (comme la valeur absolue usuelle sur $\mathbb{Q}$ a deux extensions à tout corps quadratique imaginaire.) Dans ce cas, les unités de K sont uniquement les éléments de $\mathbb{F}_q^*$. Supposons q impair. Une extension quadratique $K = \mathbb{F}_q(T)[Y]/(Y^2 - D(T))$ de $\mathbb{F}_q(T)$ est imaginaire si et seulement si ou bien $\deg(D)$ est impair, ou bien le coefficient dominant de D n'est pas un carré dans $\mathbb{F}_q$.

Proposition 2.12.19. *(Adam [24]) Soit $\mathbb{F}_q$ un corps fini de cardinal q impair. Soit $D \in \mathbb{F}_q[T]$ dont le degré est impair ou bien dont le coefficient dominant n'est pas un carré. Alors, la clôture intégrale de $\mathbb{F}_q[T]$ dans $K = \mathbb{F}_q(T)[Y]/(Y^2 - D(T))$ n'est pas un anneau de Newton sauf si* $\deg(D) = 1$.

En fait, lorsque $\deg(D) = 1$, l'extension quadratique K est isomorphe à $\mathbb{F}_q(T)$.

2.13 Suites de Schinzel

La proposition 2.12.16 rappelle un problème déjà ancien proposé par Browkin en 1965 pour $\mathbb{Z}[i]$ et connu sous le nom de problème de Schinzel dans sa version généralisée.

Le problème de Schinzel [25, Problem 8]
Existe-t-il un corps de nombres $K \neq \mathbb{Q}$ et une suite $\{a_n\}_{n\in\mathbb{N}}$ d'éléments de $\mathcal{O}_K$ tels que, pour tout idéal $\mathfrak{I}$ de $\mathcal{O}_K$ de norme $N = N(\mathfrak{I}) = Card(\mathcal{O}_K/\mathfrak{I})$, la suite $a_0, a_1, \ldots, a_{N-1}$ soit un système complet de représentants de $\mathcal{O}_K$ modulo $\mathfrak{I}$?

On connaît certains résultats :
— K ne peut être un corps quadratique (Wantula [26]).
— $\mathcal{O}_K$ doit être principal (Wasen [27]).
Posons le problème plus généralement :

Définition 2.13.1. Soient D un anneau intègre et $N \in \mathbb{N}\cup\{+\infty\}$. Une suite (finie ou infinie) $(a_n)_{0\leq n\leq N}$ est appelée *suite de Schinzel* de D si, pour tout idéal $\mathfrak{I}$ de D de norme $N(\mathfrak{I})$, la suite $a_0, a_1, \ldots, a_k$, où $k = \min(N, N(\mathfrak{I}) - 1)$, sont dans des classes distinctes modulo $\mathfrak{I}$.

Une telle suite est dite de longueur N.

Définition 2.13.2. La longueur maximale (finie ou infinie) d'une suite de Schinzel de D est appelée *constante de Schinzel* de D est notée $\sigma(D)$.

Notons que, si $N > N(\mathfrak{I})$, alors $\{a_0, \ldots, a_{N(\mathfrak{I})-1}\}$ est un système complet de representants de $D/\mathfrak{I}$.

La proposition 2.12.2 relative aux suites de Newton est valable pour les suites de Schinzel. On peut donc toujours transformer une suite de Schinzel de longueur N en une suite de même longueur commençant par 0 et 1, une telle suite sera appelée *suite de Schinzel normalisée*.

Définition 2.13.3. Un anneau intègre D est appelé *anneau de Schinzel* s'il possède une suite de Schinzel infinie ($\sigma(D) = +\infty$).

EXEMPLES 2.13.4. 1- L'anneau d'une valuation discrète v de corps résiduel fini est un anneau de Schinzel : la proposition 2.12.17 montre que toute suite v-ordonnée est a fortiori une suite de schinzel.

2- Tout anneau intègre local de corps résiduel infini est un anneau de Schinzel : une suite est de Schinzel si et seulement si ses éléments sont dans des classes distinctes modulo l'idéal maximal.

3- $\mathbb{Z}$ est un anneau de Schinzel possédant la suite de Schinzel $\{k\}_{k\in\mathbb{N}}$.

Proposition 2.13.5. *Tout anneau principal semi-local est de Schinzel.*

En effet, la suite évoquée dans la remarque 2.12.7 est de Schinzel.

Proposition 2.13.6. *Pour tout corps fini $\mathbb{F}_q$, l'anneau $\mathbb{F}_q[T]$ est de Schinzel.*

En effet, la suite de Newton construite pour la preuve de la proposition 2.12.15 est aussi une suite de Schinzel.

Il est clair que si D est un anneau de Schinzel, alors tout localisé de D est encore une anneau de Schinzel (considérer la même suite).

Proposition 2.13.7 (S. Frisch)**.** *Soit D un anneau intègre à quotients finis (c'est-à-dire, un anneau noethérien de dimension 1 à corps résiduels finis). Si D est un anneau de Schinzel, alors il est euclidien pour la norme.*

Proof. Supposons D de Schinzel et soit $(a_n)_{n\in\mathbb{N}}$ une suite de Schinzel normalisée. Pour tout $a \in D$, $a \neq 0$, notons $N(a)$ le cardinal de D/aD (fini par hypothèse). Alors, pour tout $n > 0$, on a $N(a_n) \leq n$: sinon $a_0, \ldots, a_{N(a_n)-1}$ ne seraient pas dans des classes distinctes modulo a_n puisque $a_0 = 0$ and a_n sont dans la même classe. Soient maintenant $x, y \in D$ avec $y \neq 0$. Dans la suite $a_0, \ldots, a_{N(y)-1}$ il y a un représentant de la classe de x modulo y, c.-à-d., $x = by + a_r$ pour un certain $r < N(y)$. Par suite, $N(a_r) \leq r < N(y)$. □

En général (et peut-être même toujours), l'anneau des entiers d'un corps de nombres n'est pas un anneau de Schinzel. D'ailleurs, le nombre de Schinzel de certains d'entre eux a été calculé. Ainsi,

Proposition 2.13.8 ([28])**.** *Soit $d \geq 3$ un entier sans facteurs cubiques. Alors, pour le corps cubique pur $K = \mathbb{Q}[\sqrt[3]{d}]$, on a $\sigma(\mathcal{O}_K) = 1$.*

Exercice 2.13.9. Calculer $\sigma(\mathbb{Q}[\sqrt[3]{2}])$.

2.14 Newton $\neq$ Schinzel ?

Il peut être intéressant de comparer les suites de Newton et les suites de Schinzel. En particulier se pose la question suivante :

Question 2.14.1. Est-ce que la classe des anneaux de Newton et la classe des anneaux de Schinzel sont distinctes ?

Tous nos exemples d'anneaux de Newton sont des anneaux de Schinzel et réciproquement. Toutes nos suites infinies normalisées de Newton sont des suites infinies normalisées de Schinzel et réciproquement. Ainsi : $\mathbb{Z}$, $\mathbb{F}_q[T]$, tout anneau local à corps résiduel fini, tout anneau de valuation discrète, tout anneau principal semi-local.

Exercice 2.14.2. Dans le cas où $(k)_{k\in\mathbb{N}}$ est une suite de Newton pour D, est-ce automatiquement une suite de Schinzel pour D.

Remarquons que chacune de ces deux propriétés pour D implique la propriété suivante :

Il existe une suite $(a_n)_{n\in\mathbb{N}}$ telle que, pour tout idéal maximal $\mathfrak{m}$ de D de norme q et pour tout $k \in \mathbb{N}^*$, la suite $a_0, a_1, \ldots, a_{q^k-1}$ soit un système complet de représentants de D modulo $\mathfrak{m}^k$.

En fait, pour un anneau de Dedekind D à corps résiduels finis, on peut considérer 6 propriétés naturelles pour une suite $(a_n)_{n\in\mathbb{N}}$ comme indiqué dans le tableau suivant où ν désigne la norme de tout idéal $\mathfrak{I}$ de D, q la norme de tout idéal maximal $\mathfrak{p}$ de D and, 's. c.r.' signifie 'est un système complet de repréesentants de ...'

propriété	quels que soient	la suite	s.c.r.
I	$\nu = N(\mathfrak{I}), r \in \mathbb{N}$	$a_r, \ldots, a_{r+\nu-1}$	$D/\mathfrak{I}$
I'	$q = N(\mathfrak{p}), s \in \mathbb{N}^*, r \in \mathbb{N}$	$a_r, \ldots, a_{r+q^s-1}$	$D/\mathfrak{p}^s$
II	$\nu = N(\mathfrak{I}), k \in \mathbb{N}$	$a_{k\nu}, \ldots, a_{(k+1)\nu-1}$	$D/\mathfrak{I}$
II' Newton	$q = N(\mathfrak{p}), s \in \mathbb{N}^*, k \in \mathbb{N}$	$a_{kq^s}, \ldots, a_{(k+1)q^s-1}$	$D/\mathfrak{p}^s$
III Schinzel	$\nu = N(\mathfrak{I})$	$a_0, \ldots, a_{\nu-1}$	$D/\mathfrak{I}$
III'	$q = N(\mathfrak{p}), s \in \mathbb{N}^*$	$a_0, \ldots, a_{q^s-1}$	$D/\mathfrak{p}^s$

On dira qu'un anneau de Dedekind D satisfait l'une de ces propriétés s'il existe une suite dans D qui satisfait cette propriété. On a les implications évidentes suivantes :

$$\begin{array}{ccccc} I & \longrightarrow & II & \longrightarrow & III \\ \downarrow & & \downarrow & & \downarrow \\ I' & \longrightarrow & II' & \longrightarrow & III' \end{array}$$

Question 2.14.3. Que peut-on dire des implications inverses ?

Voici quelques exemples d'anneaux satisfaisant les propriétés les plus fortes, à savoir I, I' et II.

EXEMPLES 2.14.4.
Propriété I : a) L'anneau $\mathbb{Z}$. Evidemmment, la suite des entiers naturels satisfait I.

b) Un anneau de valuation discrète à corps résiduel fini. Une suite $(a_n)_{n\in\mathbb{N}}$ satisfait I si et seulement si elle est *très bien répartie et bien ordonnée* [6, §II.2], c'est-à-dire si, pour tous n et m,

$$v(a_n - a_m) = v_q(n - m)$$

où v désigne la valuation, q le cardinal du corps résiduel et $v_q(n-m)$ le plus grand entier k tel que q^k divise $n - m$. La suite décrite dans la proposition 1.7.5 satisfait cette proprirété.

c) Un anneau principal semi-local. En effet, la propriété peut être globalisée pour un nombre fini d'idéaux maximaux (cf. remarque 2.12.7).

Propriété I' : Un anneau de Dedekind D de caractéristique 0 tel que tout nombre premier soit totalement décomposé dans D. En effet, il suffit de considérer la suite des entiers naturels.

Propriété II: L'anneau $\mathbb{F}_q[T]$. La suite décrite dans la proposition 2.12.15 convient comme le montre la proposition 2.12.16.

Voici une réponse partielle à la question ci-dessus. L'anneau $\mathbb{F}_q[T]$ vérifie II, mais ne vérifie pas I' [11, Adam, Prop. 2.8]). Par suite, II$\not\rightarrow$I'.

On peut aussi remarquer que les résultats négatifs concernantla propriété de Newton sont en général obtenus en utilisant seulement les tout premiers termes des suites de Newton et donc finalement la propriété III'. D'où l'intérêt de répondre à la question suivante :

Question 2.14.5. Quels sont les corps de nombres K pour lesquels l'anneau $\mathcal{O}_K$ satisfait III' ?

Voici, pour terminer, quelques comparaisons élémentaires entre certaines des constantes introduites et d'autres constantes classiques. Rappelons tout d'abord la notion de constante de Lenstra [29].

Définition 2.14.6. Etant donné un anneau intègre D, on appelle *suite de Lenstra* de D toute suite $v_0, v_1, \ldots, v_l$ d'éléments de D telle que, pour $0 \leq i < j \leq l$, $v_i - v_j \in U(D)$.

Une telle suite est dite de *longueur* l. On peut toujours transformer une suite de Lenstra de longueur l en une suite de Lenstra de longueur l *normalisée*, c'est-à-dire, commençant par 0 et 1.

Définition 2.14.7. On appelle alors *constante de Lenstra* de D et on note $\lambda(D)$ le sup des longueurs de ces suites augmentées de 1.

On a donc toujours, $\lambda(D) \geq 2$ et, si $\lambda(D) \geq 3$, alors il existe au moins une unité ε de D telle que $1 - \varepsilon$ soit encore une unité de D. Il est imédiat que :

$$D = (0!)_D = (1!)_D = \ldots = (\lambda(D) - 1)!_D.$$

EXEMPLE 2.14.8. Si $K = \mathbb{Q}[\zeta_{p^r}]$, alors $\lambda(\mathcal{O}_K) = p$.

On notera aussi $n_{\min}(D)$ la plus petite des normes des idéaux de D. Si $n_{\min}$ est fini, c'est nécessairement une puissance d'un nombre premier.

Si $v_0, v_1, \ldots, v_l$ est une suite de Lenstra, alors ces $l+1$ termes sont dans des classes distinctes modulo tous les idéaux et donc :

$$\lambda(D) \leq n_{\min}(D).$$

Mais c'est aussi une suite de Newton et de Schinzel de longueur l, donc :

$$\lambda(D) - 1 \leq \min(\nu(D), \sigma(D))$$

où $\nu(D)$ et $\sigma(D)$ désignent respectivement la constante de Newton et la constante de Schinzel de D.

Bibliography

POUR LE DEUXIEME CHAPITRE

[1] J.-L. CHABERT, Integer-valued polynomials on prime numbers and logarithm power expansion, *European Journal of Combinatorics*, à paraître.

[2] J.-L. CHABERT ET P.-J. CAHEN, Old Problems and New Questions around Integer-Valued Polynomials and Factorial Sequences, in *Multiplicative Ideal Theory in Commutative Algebra*, Springer Science, à paraître.

[3] Z. BOREVITCH ET I. CHAFAREVITCH, *Théorie des nombres*, Gauthier-Villars, Paris, 1967.

[4] H. MINKOWSKI, Zur Theorie der quadratischen Formen, *J. Reine Angew. Math.* **101** (1887), 196–202.

[5] I. SCHUR, Ueber eine Klasse von endlichen Gruppen linearer Substitutionen, *Sitzungsber. Preuss. Akad. Wiss.* (1905), 77–91.

[6] D. HILBERT, *Die Theorie der algebaischen Zahlkörper* (1897), in Jahresbericht der Deutschen Mathematiker-Vereinigung **4** (1894–95), 175–546. Trad. fr., A. Lévy et Th. Got, *Théorie des corps de nombres algébriques*, Annales de la Faculté des Sciences de l'Université de Toulouse, t. **1–3** (1909–1911), rééd. Gabay, Paris, 1991.

[7] P. SAMUEL, *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[8] J.-P. SERRE, *Corps Locaux*, Hermann, Paris, 1962.

[9] J. NEUKIRCH, em Algebraic Number Theory, Springer, Berlin, 1999.

[10] S. LANG, *Algebraic Number Theory*, Springer.

[11] D. ADAM, *Fonctions et polynômes à valeurs entières en caractéristique finie*, Thèse Amiens, Juin 2004.

[12] F. J. VAN DER LINDEN, Integer valued polynomials over function fields, *Nederl. Akad. Wetensch. Indag. Math.* **50** (1988), 293–308.

[13] H. ZANTEMA, Integer valued polynomials over a number field, *Manuscr. Math.* **40** (1982), 155–203.

[14] B. SURY, An integral polynomial, *Math. Mag.* **68** (1995), 134–135.

[15] D. THAKUR, Gamma functions for function fields and Drinfeld modules, *Ann. Math.* t. **134** (1991), 25–64.

[16] Y. MORITA, A p-adic analogue of the Γ-function, *J. Fac. Sc. University Tokyo*, t. **22** (1975), 255–266.

[17] D. GOSS, *Basic Structures of Function Field Arithmetic*, Springer, 1998.

[18] F. JACKSON, On q-definite integrals, *Quart. J. Pure and Appl. Math.*, t.**41** (1910), 193–203.

[19] J. YERAMIAN, *Anneaux de Bhargava*, Thèse, Marseille, juillet 2004.

[20] M. WOOD, P-orderings: a metric viewpoint and the non-existence of simultaneous orderings, *J. Number Theory*, **99** (2003), 36-56.

[21] J.-L. CHABERT, G. GERBOUD, Polynômes à valeurs entières et binômes de Fermat, *Canad. J. Math.* **45** (1993), 6–21.

[22] Y. AMICE, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964), 117–180.

[23] J. YERAMIAN, Anneaux de Bhargava, *Comm. Algebra* **32** (2004), 3043–3069.

[24] D. ADAM, Simultaneous orderings in function fields, *J. Number Theory* **112** (2005), 287–297.

[25] W. NARKIEWICZ, Some unsolved problems, *Bull. Soc. Math France, Mémoire* **25** (1971), 159–164.

[26] B. WANTULA, Browkin's problem for quadratic fields (en russe), *Zeszyty Nauk. Politech. Slask. Mat.-Fiz* **24** (1974), 173–178.

[27] R. WASÉN, Remark on a problem of Schinzel, *Acta Arith.* **29** (1976), 425–426.

[28] J. LATHAM, On sequences of algebraic integers, *Journ. London Math. Soc.* **6** (1973), 555–560.

[29] H.W. LENSTRA, Euclidean number fields of large degree, *Invent. Math.* **38** (1977), 237–254.

Chapter 3

Autour du théorème de Stone-Weierstrass p-adique

3.1 Introduction

Rappelons l'énoncé bien connu :

Proposition 3.1.1 (K. Weierstrass, 1885)**.**
L'anneau $\mathbb{R}[x]$ est dense dans l'anneau $\mathcal{C}([0,1],\mathbb{R})$ muni de la topologie de la convergence uniforme.

Dans cet énoncé, on peut évidemment remplacer :
— l'intervalle $[0,1]$ par un compact quelconque de $\mathbb{R}$,
— le sous-anneau $\mathbb{R}[x]$ par l'anneau $\mathbb{Q}[x]$.

Par ailleurs, les *polynômes de Bernstein* fournissent explicitement une telle approximation.

Proposition 3.1.2. *Pour tout $f \in \mathcal{C}([0,1],\mathbb{R})$, le n-ième polynôme de Bernstein de f est défini par :*

$$B_n(f)(x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k}x^k(1-x)^{n-k}.$$

La suite $B_n(f)$ converge vers f uniformément sur $[0,1]$.

Voici quelques compléments plus subtils relatifs à l'approximation par des polynômes à coefficients entiers :

Proposition 3.1.3. *[1, Chlodovsky, 1925] L'anneau $\mathbb{Z}[x]$ est dense dans $\mathcal{C}([a,b],\mathbb{R})$ si et seulement si $[a,b]\cap\mathbb{Z}=\emptyset$.*

Proof. La condition nécessaire est immédiate. Pour la condition suffisante, d'après le théorème de Stone-Weierstrass, il suffit de montrer que tout élément de $\mathbb{R}$ est limite d'éléments de $\mathbb{Z}[x]$. Mais, la considération du développement diadique des réels montre qu'il suffit de pouvoir approcher $\frac{1}{2}$. Or, avec convergence uniforme sur tout intervalle $[a,b]\subset]0,1[$, on a :

$$\frac{1}{2}=(1-x)\sum_{k\geq 0}(1-2(1-x))^k.$$

□

Dans cet ordre d'idées, on a aussi :

Proposition 3.1.4. *[2, Pál, 1914] Soient $0<a<1$ et $f\in\mathcal{C}([-a,+a],\mathbb{R})$. Alors, f est uniformément approximable par des éléments de $\mathbb{Z}[X]$ si et seulement si $f(0)\in\mathbb{Z}$.*

Proposition 3.1.5. *[3, Kakeya, 1914] Soit $f\in\mathcal{C}([-1,+1],\mathbb{R})$. Alors, f est uniformément approximable par des éléments de $\mathbb{Z}[X]$ si et seulement si $f(0)$, $f(1)$ et $f(-1)\in\mathbb{Z}$ et $f(1)+f(-1)$ est pair.*

A l'opposé :

Proposition 3.1.6. *[3, Kakeya, 1914] Si $b-a\geq 4$, alors $\mathbb{Z}[x]$ est discret dans $\mathcal{C}([a,b],\mathbb{R})$.*

Proof. On sait (cf. chapitre 1, §16) que le polynôme de degré n qui s'écarte le moins de 0 sur l'intervalle $[-1,+1]$ est le polynôme de Chebychev $T_n(X)=\frac{1}{2^{n-1}}\cos(n\ \arccos x)$. Par suite, le polynôme de degré n qui s'écarte le moins de 0 sur $[-2,+2]$ est $2\cos(n\ \arccos\frac{x}{2})$ et il a pour norme 2. Par suite, dès que $b-a\geq 4$, pour tout polynôme non constant $Q\in\mathbb{Z}[X]$:

$$\max\{|Q(x)|\mid a\leq x\leq b\}\geq 2.$$

□

Remarque 3.1.7. Si l'on s'intéresse à une version complexe du théorème de Weierstrass, il est immédiat que $\mathbb{C}[x]$ est dense dans $\mathcal{C}([0,1],\mathbb{C})$. En revanche, on ne peut remplacer l'intervalle $[0,1]$ par n'importe quel compact de $\mathbb{C}$. En effet :

Proposition 3.1.8. *La $\mathbb{C}$-algèbre $\mathbb{C}[z]$ n'est pas dense dans $\mathcal{C}(\Gamma, \mathbb{C})$ où Γ désigne le cercle unité, mais est dense dans $\mathcal{C}(\gamma, \mathbb{C})$ si γ désigne un arc de Γ de longueur $< 2\pi$.*

Enfin, rappelons la version de Stone du théorème de Weierstrass :

Proposition 3.1.9. *Soient X un espace compact et $\mathcal{A}$ une sous-algèbre de $\mathcal{C}(X, \mathbb{R})$. Si $\mathcal{A}$ contient les fonctions constantes et sépare les points de X, alors $\mathcal{A}$ est dense dans $\mathcal{C}(X, \mathbb{R})$ pour la topologie de la convergence uniforme.*

En 1944, Dieudonné a le premier donné une version p-adique du théorème de Stone-Weierstrass en remplaçant $\mathbb{R}$, complété de $\mathbb{Q}$ pour la topologie usuelle par $\mathbb{Q}_p$, complété de $\mathbb{Q}$ pour la topologie p-adique.

Proposition 3.1.10 (J. Dieudonné [4])**.** .
$\mathbb{Q}_p[X]$ est dense dans $\mathcal{C}(F, \mathbb{Q}_p)$ où F désigne un compact quelconque de $\mathbb{Q}_p$.

Comme l'anneau $\mathbb{Z}_p$ des entiers p-adiques est lui-même une partie compacte de $\mathbb{Q}_p$, toute fonction $\phi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ peut être approchée uniformément par des polynômes de $\mathbb{Q}[X]$ et, en particulier, par des polynômes de l'anneau $\mathrm{Int}(\mathbb{Z})$.

En fait, Mahler [5, 1958] a donné une description explicite de cette approximation sous la forme de ce que l'on appelle maintenant *les séries de Mahler* :

$$\phi(x) = \sum_{n \geq 0} a_n \binom{x}{n} \quad \text{avec} \quad a_n \in \mathbb{Z}_p \text{ et } \lim_{n \to \infty} v_p(a_n) = +\infty.$$

Mais l'énoncé de Dieudonné a été étendu par Kaplansky [7, 1950] en remplaçant $\mathbb{Q}_p$ par un corps valué quelconque K.

Nous allons démontrer ici cette version du théorème de Weierstrass due à Kaplansky. Puis, dans cette situation générale, à partir des travaux de Bhargava et Kedleya [8, 1999], nous obtiendrons un développement des fonctions continues en séries de Mahler, non plus à l'aide des polynômes binomiaux, mais à l'aide d'une base du V-module $\mathrm{Int}(E, V)$ où V désigne l'anneau de la valuation de K.

Commençons par donner quelques résultats très généraux sur la continuité des polynômes dans le cas de topologies $\mathfrak{a}$-adiques elles-mêmes très générales.

3.2 Continuité $\mathfrak{a}$-adique

Notations. *Dans cette section D désigne un anneau intègre quelconque de corps des fractions K et E une partie infinie de D. On considère un idéal non nul $\mathfrak{a}$ de D et on munit D et K de la topologie $\mathfrak{a}$-adique.*

Les polynômes $f \in K[X]$ seront considérés ici comme des applications de K, D ou E dans K dont on étudie la continuité.

Tout $f \in D[X]$ définit une application uniformément continue de D dans D. En effet, pour tout $r \in \mathbb{N}$:

$$((x-y) \in \mathfrak{a}^r) \Rightarrow ((f(x)-f(y)) \in \mathfrak{a}^r).$$

En revanche, l'application définie par $f \in K[X] \setminus D[X]$ peut ne pas être continue sur D :

Proposition 3.2.1. *Supposons D noethérien. Les assertions suivantes sont équivalentes :*
(1) *Tout polynôme $f \in K[X]$ est continu sur K.*
(2) *Tout polynôme $f \in K[X]$ est uniformément continu sur D.*
(3) *D est semi-local de dimension 1 et $\mathfrak{a}$ est contenu dans le radical de Jacobson de D.*

La preuve est basée sur la remarque suivante : l'assertion 3 équivaut au fait que, pour tout élément non nul d de D, il existe un entier k tel que $\mathfrak{a}^k \subset dD$.

Mais, si l'on se limite aux polynômes valeurs entières sur D, on a des résultats beaucoup plus forts :

Proposition 3.2.2. *[9] Sans hypothèses particulières sur D, tout $f \in \mathrm{Int}(D)$ définit une application uniformément continue de D dans D. Plus précisément, si $n = \deg(f)$:*

$$\forall\, a, b \in D \quad [\,(a-b) \in \mathfrak{a}^n\,] \Rightarrow \quad [\,(f(a)-f(b) \in \mathfrak{a}\,].$$

Proof. On raisonne par récurrence sur n. On remarque qu'il suffit de prouver l'assertion pour $a-b$ de la forme cd où $c \in \mathfrak{a}$ et $d \in \mathfrak{a}^{n-1}$ et pour les f vérifiant $f(0)=0$. La considération du polynôme $g(X) = f(cX) - c^n f(X)$ permet alors d'effectuer la récurrence. □

La proposition 3.2.2 ne se généralise pas aux polynômes $f \in \mathrm{Int}(E, D)$ sauf lorsque E est un sous-anneau de D.

Proposition 3.2.3. *Soit E un sous-anneau de D et soit $\mathfrak{b} = \mathfrak{a} \cap E$. Alors tout $f \in \mathrm{Int}(E, D)$ définit une application uniformément continue de E muni de la topologie $\mathfrak{b}$-adique dans D muni de la topologie $\mathfrak{a}$-adique.*

Si l'on veut pouvoir considérer des polynômes à valeurs entières sur une partie quelconque E de D, on doit (en l'absence d'autres preuves) supposer D noethérien.

Proposition 3.2.4. *Supposons D noethérien. Tout polynôme $f \in \mathrm{Int}(E, D)$ définit une application uniformément continue de E dans D. Plus précisément, pour tout $f \in \mathrm{Int}(E, D)$ et tout $h \in \mathbb{N}$, il existe $k = k(f, h) \in \mathbb{N}$ tel que*

$$\forall a, b \in E \ (a - b \in \mathfrak{a}^k \Rightarrow f(a) - f(b) \in \mathfrak{a}^h).$$

Si l'on suppose D noethérien, pourquoi –du coup– ne pas le supposer local ?

Corollaire 3.2.5. *Supposons D noethérien local d'idéal maximal $\mathfrak{m}$. Alors*

$$\mathrm{Int}(E, D) \subset \mathcal{C}(\widehat{E}, \widehat{D}),$$

où $\widehat{E}$ et $\widehat{D}$ désignent les complétés de E et D pour la topologie $\mathfrak{m}$-adique et $\mathcal{C}(\widehat{E}, \widehat{D})$ l'anneau des fonctions continues de $\widehat{E}$ dans $\widehat{D}$ pour la topologie $\mathfrak{m}$-adique.

Puisque $\mathrm{Int}(E, D) \subset \mathcal{C}(\widehat{E}, \widehat{D})$, on peut essayer d'obtenir un théorème de Stone-Weierstrass dans ce cadre général, c'est-à-dire, à quelles conditions $\mathrm{Int}(E, D)$ est dense dans $\mathcal{C}(\widehat{E}, \widehat{D})$ pour la topologie de la convergence uniforme, autrement dit, quand :

$$\forall \varphi \in \mathcal{C}(\widehat{E}, \widehat{D})\, \forall n \in \mathbb{N}\ \exists f \in \mathrm{Int}(E, D) \text{ tel que } \forall x \in \widehat{E}\ (f(x) - \varphi(x) \in \mathfrak{m}^n) \ ?$$

On peut démontrer :

Proposition 3.2.6. *Supposons D noethérien, local et de dimension 1. Si $\widehat{D}$ est intègre et si $\widehat{E}$ est compact, alors $\mathrm{Int}(E, D)$ est dense dans $\mathcal{C}(\widehat{E}, \widehat{D})$ pour la topologie de la convergence uniforme.*

En fait, nous allons nous limiter au cas des anneaux de valuation sans toutefois se restreindre à ceux qui sont noethériens, c'est-à-dire, les anneaux de valuation discrète. On va considérer n'importe quel anneau de valuation de hauteur 1.

3.3 Cas des anneaux de valuation de hauteur 1 : continuité et compacité

Hypothèses et notations. *Dans toute la suite du chapitre, K désigne un corps valué non archimédien, c'est-à-dire, un corps muni d'une valuation v de hauteur 1, V est l'anneau de la valuation v, $\mathfrak{m}$ est l'idéal maximal de V, $k = V/\mathfrak{m}$ est le corps résiduel (a priori quelconque), enfin $\widehat{K}$, $\widehat{V}$ et $\widehat{\mathfrak{m}}$ désignent les complétés correspondants. On notera encore v la valuation de $\widehat{K}$. On considèrera aussi une partie E de V et on notera $\widehat{E}$ son complété.*

Ainsi, K est un corps muni d'une valeur absolue ultramétrique :

$$|x| = e^{-v(x)}.$$

Pour $x \in K$ et $\delta \in \mathbb{R}_+$, on notera $B(x, \delta)$ la boule fermée de centre x et de rayon $e^{-\delta}$:

$$B(x, \delta) = \{y \in K \mid v(x - y) \geq \delta\}.$$

On note aussi :

$$\mathcal{C}(\widehat{E}, \widehat{K}),\ \mathcal{C}(\widehat{E}, \widehat{V}),\ \mathcal{C}(\widehat{E}, \widehat{\mathfrak{m}})\ \text{ et }\ \mathcal{C}(\widehat{E}, k)$$

les anneaux de fonctions continues de $\widehat{E}$ dans $\widehat{K}, \widehat{V}, \widehat{\mathfrak{m}}$ et k respectivement où k est muni de la topologie discrète. Tous ces anneaux de fonctions sont munis de la topologie de la convergence uniforme.

Lemme 3.3.1. *Tout polynôme $f(X) \in K[X]$ peut être considéré comme une fonction uniformément continue sur V.*

Proof. En effet, si d désigne un dénominateur commun des coefficients de f alors, pour $x, y \in V$, on a :

$$v\left(f(y) - f(x)\right) \geq v(y - x) - v(d).$$

□

Ainsi, $K[X]$ peut-être considéré comme un sous-anneau de $\mathcal{C}(\widehat{E}, \widehat{K})$ et $\mathrm{Int}(E, V)$ comme un sous-anneau de $\mathcal{C}(\widehat{E}, \widehat{V})$.

Précisons cette uniforme continuité des polynômes dans le cas où la valuation v est discrète et le corps résiduel fini.

Proposition 3.3.2. *Soit V l'anneau d'une valuation discrète de corps résiduel fini de cardinal q. Soient $f \in \mathrm{Int}(V)$ et $h \in \mathbb{N}$ tels que $\deg(f) < q^h$. Alors,*

$$\forall r \in \mathbb{N}\ \forall a, b \in V \quad [v(a-b) \geq r+h \Rightarrow v(f(a)-f(b)) \geq r+1.]$$

Proof. Il suffit de prouver : si $f(0) = 0$ et $v(a) \geq r+h$, alors $v(f(a) \geq r+1$. Si les f_n forment une base de $\mathrm{Int}(V)$, il suffit de le prouver pour les f_n où $1 \leq n \leq q^h$. Or, l'assertion est vérifié pour les f_n construits à partir d'une suite TBRBO de V commençant par 0. □

Remarque 3.3.3. Dans la proposition précédente , on ne peut améliorer l'inégalité de droite : pour a et b donnés, il existe f pour lequel on a l'égalité.

Rappelons la caractérisation des précompacts d'un corps valué :

Lemme 3.3.4. *Les assertions suivantes sont équivalentes* :
(1) *E est précompact.*
(2) *Pour tout $\delta \in \mathbb{R}_+$, E rencontre au plus un nombre fini de boules de rayon $e^{-\delta}$.*
(3) *Pour tout $n \in \mathbb{N}$, E rencontre au plus un nombre fini de classes de V modulo l'idéal $\mathfrak{I}_n = \{x \in V \mid v(x) \geq n\}$.*

En particulier, si v est discrète et si $V/\mathfrak{m}$ est fini, alors $\widehat{V}$ est compact et donc, pour toute partie E de V, $\widehat{E}$ est compact.

Exercice 3.3.5. (ouvert) A-t-on un analogue de la proposition 3.3.2 lorsque l'on remplace l'hypothèse $\widehat{V}$ compact par $\widehat{E}$ compact et la condition $\deg(f) < q^h$ par $\deg(f) < q_h$ où $q_h = Card(E/\mathfrak{m}^h)$?

Rappelons aussi la définition que nous avons donnée des parties pseudo-précompactes.

Définition 3.3.6. L'ensemble E est dit *pseudo-précompact* si, pour tout $\gamma \in \mathbb{R}_+$ de la forme $\gamma = v(x-y)$ où $x, y \in E$, $x \neq y$, E rencontre au plus un nombre fini de boules de rayon $e^{-\gamma}$.

Bien sûr, une partie précompacte est pseudo-précompacte. La réciproque n'est pas vraie comme on l'a déjà vu.

3.4 Pseudo-précompacité et interpolation

On a une propriété de séparation des points d'un pseudo-précompact par les polynmes :

Proposition 3.4.1. *Si E est pseudo-précompact alors, quels que soient a et b dans E distincts, il existe $f \in \mathrm{Int}(E, V)$ tel que $f(a) = 1$ et $f(b) = 0$.*

Proof. Fixons a et b dans E et posons $\gamma = v(a - b)$. Comme E est pseudo-compact, il existe $r \in \mathbb{N}$ et $b_0, b_1, \ldots, b_r \in E$ tels que :

$$E \subset \cup_{k=0}^{r} B(b_k, \gamma)$$

où la réunion est disjointe. L'une de ces boules $B(b_k, \gamma)$ contient a et b. On peut supposer que $b_0 = b$ et que la numérotation est telle que :

$$\gamma = v(b - a) = v(b_0 - a) > v(b_1 - a) \geq v(b_2 - a) \geq ... \geq v(b_r - a).$$

Considérons le polynôme :

$$f(x) = \frac{b - x}{b - a} \times \left(\frac{b_1 - x}{b_1 - a}\right)^{m_1} \times ... \times \left(\frac{b_r - x}{b_r - a}\right)^{m_r}$$

où $m_1, \ldots, m_r \in \mathbb{N}$ (et $m_0 = 1$). Evidemment, $f(a) = 1$ and $f(b) = 0$. Il s'agit de montrer que l'on peut choisir les m_i de façon que $f(E) \subset V$.

— Si $x \in B(b, \gamma)$, alors

$$v(b - x) \geq \gamma = v(b - a)$$

et

$$v\left(\frac{b - x}{b - a}\right) \geq 0.$$

— Si $x \in B(b_i, \gamma)$ et $j > i$, alors

$$v\left(\frac{b_j - x}{b_j - a}\right) \geq 0$$

puisque

$$v(b_j - x) = v(b_j - b_i) \geq v(b_j - a).$$

— Si $x \in B(b_i, \gamma)$ avec $i \geq 1$, alors

$$v(b_i - x) \geq \gamma > v(b_i - a)$$

et donc

$$v\left(\frac{b_i - x}{b_i - a}\right) \geq \varepsilon_i \quad \text{avec} \quad \varepsilon_i = \gamma - v(b_i - a) > 0.$$

Ainsi, d'une part, si $x \in B(b, \gamma)$, $f(x) \in V$. D'autre part, si $x \in B(b_i, \gamma)$ où $i \geq 1$, alors

$$v(f(x)) = \sum_{k=0}^{r} m_k v\left(\frac{b_k - x}{b_k - a}\right)$$

$$\geq m_i \varepsilon_i + \sum_{k=0}^{i-1} m_k v\left(\frac{b_k - x}{b_k - a}\right) \geq m_i \varepsilon_i - \sum_{k=0}^{i-1} m_k v(b_k - a).$$

Si $m_1, \ldots, m_{i-1}$ sont choisis, on peut trouver m_i tel que le dernier terme soit ≥ 0 puisque $\varepsilon_i > 0$ [Archimède dixit]. □

D'où une propriété d'interpolation :

Corollaire 3.4.2. *Supposons E pseudo-précompact. Alors, quels que soient le n-uple $(a_1 \ldots, a_n)$ d'éléments distincts de E et le n-uple $(b_1, \ldots, b_n)$ d'éléments quelconques de V, il existe un polynôme $f \in \mathrm{Int}(E, V)$ tel que $f(a_i) = b_i$ pour $1 \leq i \leq n$.*

Cf. [9] sur la question de l'interpolation polynomiale.

3.5 Stone-Weierstrass dans les corps valués

Proposition 3.5.1. *Supposons E compact. Alors $\mathrm{Int}(E, V)$ est dense dans $\mathcal{C}(E, V)$.*

Proof. Soit $\varphi \in \mathcal{C}(E, V)$. Comme E est compact, φ est uniformément continue. Pour tout $\alpha \in \mathbb{R}_+$, il existe $\beta \in \mathbb{R}_+$ tel que,

$$\text{pour } x, y \in E, \;\; v(x - y) \geq \beta \;\; \Rightarrow \;\; v\left(\varphi(x) - \varphi(y)\right) \geq \alpha.$$

Soient $x_1, \ldots, x_s \in E$ un système de représentants des classes de E modulo $B(0, \beta)$ et soient ψ_i les fonctions caractéristiques des ouverts-fermés $B(x_i, \beta) \cap E$ de E. Alors

$$v\left(\varphi(x) - \sum_{i=1}^{s} \varphi(x_i)\psi_i(x)\right) \geq \alpha \;\; \forall x \in E.$$

Ainsi, pour approcher φ à $e^{-\alpha}$ près, il suffit d'approcher les fonctions caractéristiques ψ_i à $e^{-\alpha}$ près.
Soient donc $\alpha \in \mathbb{R}_+$, U un ouvert-fermé de E et ψ sa fonction caractéristique. Fixons $a \in U$. Pour tout $b \in E \setminus U$, il existe $f_b \in \mathrm{Int}(E, V)$ tel que

$$f_b(a) = 1 \ \text{ et } \ f_b(b) = 0.$$

Par continuité de f_b il existe un voisinage de b dans $E \setminus U$ dans lequel $v(f_b(x)) \geq \alpha$. D'où, par compacité de $E \setminus U$, un polynôme g_a produit d'un nombre fini de tels polynômes f_b telle que

$$g_a(a) = 1 \ \text{ et } \ v(g_a(x)) \geq \alpha \ \ \forall x \in E \setminus U.$$

Par continuité de g_a, il existe un voisinage de a dans lequel $v(1 - g_a(x)) \geq \alpha$. Par compacité de U, il existe un nombre fini de tels polynômes g_a tels que le polynôme $g = 1 - \prod(1 - g_a)$ vérifie

$$v(g(x) - 1) \geq \alpha \ \ \forall x \in U \ \text{ et } \ v(g(x)) \geq \alpha \ \ \forall x \in E \setminus U.$$

□

Théorème 3.5.2 (Kaplansky)**.** *Supposons E précompact. Alors, pour la topologie de la convergence uniforme* :

(*i*) $\mathrm{Int}(E, V)$ *est dense dans* $\mathcal{C}(\widehat{E}, \widehat{V})$,

(*ii*) $K[X]$ *est dense dans* $\mathcal{C}(\widehat{E}, \widehat{K})$.

Proof. (i) D'après la proposition précédente, $\mathrm{Int}(\widehat{E}, V)$ est dense dans $\mathcal{C}(\widehat{E}, V)$. Mais $\mathrm{Int}(E, V) = \mathrm{Int}(\widehat{E}, V)$.
(ii) Si $\varphi \in \mathcal{C}(\widehat{E}, \widehat{K})$, alors φ est uniformément continue et on se ramène au cas précédent en multipliant φ par une constante. □

Corollaire 3.5.3. *Soient A l'anneau des entiers d'un corps de nombres et $\mathfrak{m}$ un idéal maximal de A. Alors* $\mathrm{Int}(A)$ *est dense dans* $\mathcal{C}(\widehat{A_{\mathfrak{m}}}, \widehat{A_{\mathfrak{m}}})$.

En particulier, pour tout $p \in \mathbb{P}$, $\mathbb{Q}[X]$ est dense dans $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ et $\mathrm{Int}(\mathbb{Z})$ est dense dans $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$.

Exercice 3.5.4. L'anneau $V[X]$ n'est jamais dense dans $\mathcal{C}(\widehat{V}, \widehat{V})$.

3.6 La compacité est nécessaire

On a vu que la pseudo-précompacité est suffisante pour avoir une interpolation polynomiale. Serait-elle suffisante pour avoir une approximation polynomiale ? En fait, la compacité est nécessaire.

Théorème 3.6.1. *Les assertions suivantes sont équivalentes* :

1. E *est précompact.*
2. *Toute fonction continue* $\phi \in \mathcal{C}(\widehat{E}, \widehat{K})$ *est bornée.*
3. $K[X]$ *est dense dans* $\mathcal{C}(\widehat{E}, \widehat{K})$.
4. $\mathrm{Int}(E, V)$ *est dense dans* $\mathcal{C}(\widehat{E}, \widehat{V})$.

Proof. Le théorème 3.5.2 de Kaplansky montre que $1 \to 3$ et $1 \to 4$. Par ailleurs, $3 \to 2$ car toute fonction polynomiale est bornée sur E. Enfin, $2 \to 1$, ou plutôt non $1 \to$ non 2, car si $\widehat{E}$ n'est pas compact, $\widehat{E}$ est réunion disjointe d'une infinité d'ouvert-fermés disjoints et l'on peut alors contruire une fonction continue, en fait localement constante, qui n'est pas bornée. Il reste à montrer que $4 \to 1$. C'est l'objet du lemme suivant. □

Lemme 3.6.2. *Si* $\mathrm{Int}(E, V)$ *est dense dans* $\mathcal{C}(\widehat{E}, \widehat{V})$*, alors* $\widehat{E}$ *est compact.*

Proof. For every ideal I of V, we shall write that E/I is infinite (resp. finite) if E meets infinitely many (resp. only finitely many) cosets modulo I. For every $\alpha \in \mathbb{R}_+$, let us denote

$$I_\alpha = \{x \in V \mid v(x) \geq \alpha\} \quad \text{and} \quad I'_\alpha = \{x \in V \mid v(x) > \alpha\}.$$

Assume, by way of contradiction, that $\widehat{E}$ is not compact, that is, E/I_α is infinite, for some $\alpha > 0$. The principle of the proof is the following:

We consider a sequence $\{x_n\}$ of elements of E in distinct classes modulo some I_α (or some I'_α). It is thus possible to define a function $\phi \in \mathcal{C}(\widehat{E}, \widehat{V})$ such that, alternatively, for n even and n odd, we have $\phi(x_n) = 0$ and $\phi(x_n) = 1$. Suppose that $\mathrm{Int}(E, V)$ is dense in $\mathcal{C}(\widehat{E}, \widehat{V})$: in particular, there exists $f \in K[X]$ such that, alternatively, $v\big(f(x_n)\big) > 1$ and $v\big(f(x_n)\big) = 0$. We reach a contradiction by choosing the sequence $\{x_n\}$ in a such a way that, for each $f \in K[X]$, the sequence $\big\{v\big(f(x_n)\big)\big\}$ converges. In fact, as we can write $f = a\prod_{1\leq k\leq d}(X - \xi_k)$ in an algebraic extension L of K, it is enough to make sure that, for $\xi \in L$, the

sequence $\{v(x_n - \xi)\}$ converges (in $\mathbb{R}$, extending the valuation v to a rank-one valuation of L).

If E/I_α is infinite, then, a fortiori, E/I_β and E/I'_β are infinite for $\beta \geq \alpha$. We set

$$\gamma = \inf\{\alpha \mid E/I'_\alpha \text{ is infinite}\}.$$

If the valuation is discrete (with value group $\mathbb{Z}$), then γ is an integer and necessarily E/I_γ is finite while E/I'_γ is infinite. We then consider three cases:

1) E/I_γ is finite, and E/I'_γ is infinite: there is a sequence $\{x_n\}$ in E such that all the x_n's are in the same class modulo I_γ, but in distinct classes modulo I'_γ. For $n \neq m$, we then have $v(x_n - x_m) = \gamma$. Let ξ be an element of an algebraic extension L of K. Therefore
— either $v(x_{n_0} - \xi) < \gamma$ for some n_0, then $v(x_n - \xi) = v(x_{n_0} - \xi)$ for all n;
— or $v(x_{n_0} - \xi) > \gamma$ for some n_0, then $v(x_n - \xi) = \gamma$ for $n \neq n_0$;
— or $v(x_n - \xi) = \gamma$ for all n.

At any rate, the sequence $\{v(x_n - \xi)\}$ is eventually constant.

2) E/I'_γ is finite. In this case, the valuation is not discrete and E/I_β is infinite for each $\beta > \gamma$. Let $\{\beta_n\}$ be a strictly decreasing sequence in $\mathbb{R}$ converging to γ. Among the (finitely many) classes that E meets modulo I'_γ, there is one which, for each n, meets infinitely many classes modulo I_{β_n}. By induction, we can thus build a sequence $\{x_n\}$ such that all its terms are in the same class modulo I'_γ but x_n is not in the class of $x_1, x_2, \ldots$ nor x_{n-1} modulo I_{β_n}. For $m > n$, we thus have $\gamma < v(x_m - x_n) < \beta_m$. In particular, all the x_n's are in distinct classes modulo I_{β_1}. Moreover
— either $v(x_{n_0} - \xi) < \gamma$ for some n_0, then $v(x_n - \xi) = v(x_{n_0} - \xi)$ for all n;
— or $v(x_n - \xi) \geq \gamma$ for all n and $v(x_{n_0} - \xi) > \beta_{n_0}$ for some n_0; for $n > n_0$ we then have $v(x_n - \xi) = v(x_n - x_{n_0})$, and hence $\gamma \leq v(x_n - \xi) < \beta_n$;
— or $\gamma \leq v(x_n - \xi) \leq \beta_n$ for all n.

Hence, the sequence $\{v(x_n - \xi)\}$ converges to γ or is eventually constant.

3) E/I_γ is infinite. In this case again the valuation is not discrete and E/I_β is finite for $\beta < \gamma$. Here, we let $\{\beta_n\}$ be a strictly increasing sequence in $\mathbb{R}$ converging to γ. Let X be an infinite subset of E, the elements of which are in distinct classes modulo I_γ. Infinitely many elements of X, forming a subset X_1 of X are in the same class modulo I_{β_1}. Infinitely many elements of X_1, forming a subset X_2 of X_1, are in the same class modulo I_{β_2}. And so on: we define a decreasing sequence $\{X_n\}$ of subsets, the elements of X_n being in the same class modulo I_{β_n}. For each n, choosing x_n in X_n, we thus build a sequence $\{x_n\}$ such that, for $m > n$, we have $\beta_n \leq v(x_m - x_n) < \gamma$. Therefore

— either $v(x_{n_0} - \xi) < \beta_{n_0}$ for some n_0, then $v(x_n - \xi) = v(x_{n_0} - \xi)$ for $n > n_0$;
— or $v(x_n - \xi) \geq \beta_n$ for all n and $v(x_{n_0} - \xi) \geq \gamma$ for some n_0; for $n \neq n_0$ we then have $v(x_n - \xi) = v(x_n - x_{n_0})$, thus $\beta_n \leq v(x_n - \xi) < \gamma$;
— or $\beta_n \leq v(x_n - \xi) < \gamma$ for all n.

Hence, the sequence $\{v(x_n - \xi)\}$ converges to γ or is eventually constant. □

3.7 Application à la clôture polynomiale

Rappelons la notion de clôture polynomiale déjà évoquée à l'occasion.

Définition 3.7.1. Pour toute partie F d'un anneau intègre A, on appelle *clôture polynomiale* de F relativement à l'anneau A la plus grande partie $\overline{F}$ de A telle que $\mathrm{Int}(F, A) = \mathrm{Int}(\overline{F}, A)$, autrement dit :

$$\overline{F} = \{x \in A \mid f(x) \in A \ \ \forall f \in \mathrm{Int}(F, A)\}.$$

Proposition 3.7.2. *Notons $\overline{E}$ la clôture polynomiale de E relativement à l'anneau V et $\widetilde{E}$ la fermeture topologique de E dans V relativement à la topologie de K. Alors :*

1. $\widetilde{E} \subset \overline{E}$.
2. *Si $\widehat{E}$ est compact, alors $\widetilde{E} = \overline{E}$.*

Proof. La première assertion résulte de la continuité des polynômes. La deuxième résulte du théorème de Weierstrass. Soit $x \in V$ n'appartenant pas à $\widetilde{E}$. Soit U un voisinage ouvert-fermé de x ne rencontrant pas E et soit $F = E \cup \{x\}$. Alors $\widehat{F}$ est compact et donc, d'après la proposition suivante (corollaire du théorème de Weierstrass), il existe $h \in K[X]$ tel que $h(E) \subset V$ et $v(h(x)) < 0$. □

Proposition 3.7.3. *Soient $U_1, \ldots, U_r$ des ouverts disjoints formant un recouvrement de $\widehat{E}$ et soient $\gamma_1, \ldots, \gamma_r$ des éléments de $\Gamma = v(K^*)$. Alors, il existe un polynôme $h \in K[X]$ tel que, pour $1 \leq i \leq r$, on ait $v(h(x)) = \gamma_i$ pour tout $x \in U_i \cap E$.*

Proof. Soient $t_1, \ldots, t_r \in V$ tels que $v(t_i) = \gamma_i$. Il existe une fonction $\varphi \in \mathcal{C}(\widehat{E}, \widehat{K})$ localement constante telle que $\varphi(x) = t_i$ pour $x \in U_i$. Soit $\gamma \in \Gamma$ tel que $\gamma > \sup_i \gamma_i$. D'après le théorème de Weierstrass, il existe un polynôme $h \in K[X]$ approchant φ modulo I_γ. Un tel polynôme répond à la question. □

Corollaire 3.7.4. *Soit A un anneau de Dedekind à corps résiduels finis. Pour toute partie E de A, la clôture polynomiale de E relativement à l'anneau A est égale à l'intersection des fermetures topologiques $\widetilde{E}^{A\mathfrak{m}}$ de E dans les anneaux de valuation $A_{\mathfrak{m}}$ où $\mathfrak{m}$ décrit l'ensemble des idéaux maximaux de A, autrement dit :*

$$\overline{E} = \cap_{\mathfrak{m}\in\max(A)}\widetilde{E}^{A\mathfrak{m}}.$$

Exercice 3.7.5. Vérifier à l'aide du théorème de Dirichlet que la clôture topologique de $\mathbb{P}$ dans $\mathbb{Z}_{(p)}$ est égale à $\{p\} \cup \left(\mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}\right)$. En déduire que la clôture polynomiale de $\mathbb{P}$ dans $\mathbb{Z}$ est $\mathbb{P} \cup \{\pm 1\}$.

Corollaire 3.7.6. *Soit E une partie de $\mathbb{Z}$. Les assertions suivantes sont équivalentes :*

1. *La clôture polynomiale de E est égale $\mathbb{Z}$.*
2. *Pour tout $p \in \mathbb{P}$, E est dense dans $\mathbb{Z}$ pour la topologie p-adique.*
3. *Pour tout $p \in \mathbb{P}$ et tout $r \in \mathbb{N}$, E contient un système complet de représentants de $\mathbb{Z}$ modulo p^r.*

Remarque 3.7.7. Un sous-ensemble de $\mathbb{Z}$ est dit *arithmétiquement dense* s'il contient au moins un élément de toute suite arithmétique. Un tel sous-ensemble est dense pour la topologie de $\mathbb{Z}$ dans laquelle les idéaux non nuls de $\mathbb{Z}$ constituent une base de voisinages de 0. Un ensemble arithmétiquement dense est polynomialement dense. La réciproque est fausse : l'ensemble $E = 2\mathbb{Z} \cup 3\mathbb{Z}$ est polynomialement dense dans $\mathbb{Z}$ mais ne rencontre pas la suite $(1 + 6k)_{k\in\mathbb{N}}$.

Exercice 3.7.8. A- Soit K/K_0 une extension algébrique. Supposons K muni d'une valuation discrète v d'anneau V et d'idéal maximal $\mathfrak{m}$. Notons v_0 la restriction de v à K_0, V_0 et $\mathfrak{m}_0$ l'anneau et l'idéal maximal correspondants.
Montrer que la clôture polynomiale de V_0 dans V est égale à V si et seulement si v est une *extension immédiate* de v_0, c.-à-d.,

$$\mathfrak{m}_0 V = \mathfrak{m} \quad \text{et} \quad V_0/\mathfrak{m}_0 \simeq V/\mathfrak{m}.$$

B- Soit K un corps de nombres d'anneau d'entiers $\mathcal{O}_K$. Montrer que la clôture polynomiale de $\mathbb{Z}$ dans $\mathcal{O}_K$ n'est jamais égale à $\mathcal{O}_K$.
[Indication : il y a toujours des nombres premiers qui ne sont pas totalement décomposés dans $\mathcal{O}_K$ dès que $K \neq \mathbb{Q}$.]

3.8 Rappels sur la complétion d'un corps valué

On regroupe ici des résultats bien connus ou déjà utilisés de façon à pouvoir s'en servir dans la suite.

Le corps K étant muni d'une valuation v de hauteur 1, son groupe de valeurs $\Gamma = v(K^*)$ est isomorphe à un sous-groupe de $\mathbb{R}$. Ou bien ce sous-groupe est discret, donc isomorphe à $\mathbb{Z}$ et la valuation est discrète, ou bien il est dense dans $\mathbb{R}$.

Les idéaux de l'anneau V de la valuation. Soit $\mathfrak{m}$ l'idéal maximal de V (les seuls idéaux premiers de V sont (0) et $\mathfrak{m}$). Si la valuation est discrète, $\mathfrak{m}$ est principal et tous les idéaux non nuls de V sont de la forme $\mathfrak{m}^n$ pour $n \in \mathbb{N}$. Si la valuation n'est pas discrète, les idéaux non nuls de V sont de la forme $\mathfrak{I}_\gamma$ ou $\mathfrak{I}_\gamma^+$ ($\gamma \in \mathbb{R}_+$) où $\mathfrak{I}_\gamma = \{x \in K \mid v(x) \geq \gamma\}$ et $\mathfrak{I}_\gamma^+ = \{x \in K \mid v(x) > \gamma\}$. Les idéaux $\mathfrak{I}_\gamma$ sont principaux, les idéaux $\mathfrak{I}_\gamma^+$ ne sont pas de type fini.

La métrique. On sait que

$$x \mapsto |x| = e^{-v(x)}$$

est une valeur absolue sur K. En fait, c'est une *valeur absolue ultramétrique* :

$$|x - y| \leq \max(|x|, |y|).$$

Et on a une distance sur K en posant :

$$d(x, y) = |x - y| = e^{-v(x-y)}.$$

Muni de cette métrique, K est un *corps topologique* : l'addition, la multiplication et le passage à l'inverse sont des opérations continues. Pour $x \in K$ et $\gamma \in \mathbb{R}_+$, les boules fermées $B(x, \gamma) = \{y \in K \mid v(x - y) \geq \gamma\}$ et les boules ouvertes $B^+(x, \gamma) = \{y \in K \mid v(x - y) > \gamma\}$ sont à la fois ouvertes et fermées. En particulier, les idéaux $\mathfrak{I}_\gamma$ et $\mathfrak{I}_\gamma^+$ sont ouverts et fermés. L'espace topologique K est *totalement discontinu* : tout point admet un système fondamental de voisinages à la fois ouverts et fermés, ou encore, la composante connexe de tout point est réduite à ce point.

La complétion. Une suite (x_n) d'éléments de K est de Cauchy si et seulement si $\lim_{n\to+\infty} v(x_n - x_{n+1}) = +\infty$.

Par définition, un *complété* d'un corps valué K est un corps valué $\widehat{K}$ contenant K, dont la valuation $\widehat{v}$ prolonge la valuation v de K et tel que d'une part K soit dense dans $\widehat{K}$, d'autre part $\widehat{K}$ soit complet.

Proposition 3.8.1. *Un corps valué K possède une complétion et cette complétion est unique à isomorphisme isométrique près.*

Une telle complétion peut se construire à l'aide des suites de Cauchy de façon tout à fait analogue à la complétion $\mathbb{R}$ de $\mathbb{Q}$ relativement à la valeur absolue usuelle.

— Si la suite (x_n) converge vers x, il existe n_0 tel que $v(x_n) = \widehat{v}(x)$ pour $n \geq n_0$.
— $v(K^*) = \widehat{v}(\widehat{K}^*)$
— Une série $\sum_{n=0}^{\infty} u_n$ converge dans $\widehat{K}$ si et seulement si $\widehat{v}(u_n) \to +\infty$.
— L'anneau de $\widehat{v}$ est le complété $\widehat{V}$ de V.
— L'idéal maximal de $\widehat{V}$ est le complété $\widehat{\mathfrak{m}}$ de $\mathfrak{m}$.

Proposition 3.8.2. *Les assertions suivantes sont équivalentes :*
1) K est localement compact,
2) V est compact,
3) v est discrète, K est complet, $V/\mathfrak{m}$ est fini.

Proposition 3.8.3 (Développement de Hensel)**.** *Supposons v discrète et K complet. Soit t une uniformisante ($\mathfrak{m} = tV$). Soit S un système de représentants de V modulo $\mathfrak{m}$.*
1) Tout élément a de V s'écrit d'une façon et d'une seule sous la forme

$$a = \sum_{n \geq 0} a_n t^n \quad \text{avec} \quad a_n \in S.$$

2) Tout élément x de K s'écrit d'une façon et d'une seule sous la forme

$$x = \sum_{n \geq n_0} x_n t^n \quad \text{avec} \quad n_0 = v(x) \text{ et } x_n \in S.$$

Le cas de $\mathbb{Q}$.
A tout $p \in \mathbb{P}$ correspond la valuation p-adique de $\mathbb{Q}$ et donc un complété $\mathbb{Q}_p$ et un anneau de valuation $\mathbb{Z}_p$, complété de $\mathbb{Z}$ ou de $\mathbb{Z}_{(p)}$, appelé *anneau des entiers p-adiques*. On peut prendre $S = \{0, 1, \ldots, p-1\}$ et $t = p$. Tout élément a de $\mathbb{Z}_p$ s'écrit d'une façon et d'une seule sous la forme

$$a = \sum_{n \geq 0} a_k p^k \quad \text{avec} \quad 0 \leq a_k < p.$$

Par exemple,

$$-1 = \sum_{n \geq 0} (p-1) p^n.$$

On pourrait aussi prendre

$$S = \{0\} \cup \{\zeta_{p-1}^k \mid 1 \leq k < p-1\}$$

où ζ_{p-1} est une racine primitive $(p-1)$-ième de l'unité (dans $\mathbb{Z}_p$).

3.9 Séries de Mahler

Ainsi, lorsque E est précompact, $\mathrm{Int}(E, V)$ est dense dans $\mathcal{C}(\widehat{E}, \widehat{V})$. En particulier, $\mathrm{Int}(\mathbb{Z}_p)$ est dense dans $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$. Mais, de même que l'on peut remplacer $\mathbb{R}[X]$ par $\mathbb{Q}[X]$, on peut ici remplacer $\mathrm{Int}(\mathbb{Z}_p)$ par $\mathrm{Int}(\mathbb{Z})$. Dans ce cas, on a un résultat plus précis : le développement en série de Malher.

Proposition 3.9.1 (K. Mahler [5])**.**
Toute fonction continue $\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ s'écrit d'une façon et d'une seule sous la forme :

$$\varphi(x) = \sum_{n=0}^{\infty} a_n \, \frac{x(x-1)\cdots(x-n+1)}{n!}$$

où

$$a_n \in \mathbb{Z}_p \quad \text{et} \quad v_p(a_n) \to +\infty.$$

On a de plus :

$$\inf_{x \in \mathbb{Z}_p} v_p(\varphi(x)) = \inf_{n \in \mathbb{N}} v_p(a_n).$$

C'est ce dernier énoncé que l'on souhaite étendre : fournir de façon explicite ce que l'on appelle des bases orthonormales de l'espace des fonctions continues, bases polynomiales pour commencer, bases plus générales ensuite.

Avant de commencer, rappelons qu'il existe un analogue 'corps de fonctions' de l'énoncé de Mahler donné par Wagner [6] :

Proposition 3.9.2. *Soit π un polynôme irréductible de $\mathbb{F}_q[T]$. Notons $\widehat{K}$ et $\widehat{V}$ les complétés respectifs de K et V pour la topologie π-adique. Alors il existe une famille de polynômes $(Q_n(T))_{n\in\mathbb{N}}$ (en fait, une base de $\mathrm{Int}(\widehat{V})$) telle que tout fonction $\varphi \in \mathcal{C}(\widehat{V}, \widehat{V})$ s'écrive d'une façon et d'une seule sous la forme*

$$\varphi(x) = \sum_{n=0}^{\infty} a_n Q_n(x) \quad avec\ a_n \in \widehat{V} \ \ et \ \ v_\pi(a_n) \to +\infty.$$

De plus,

$$\inf_{x\in\widehat{V}} v_\pi(\varphi(x)) = \inf_{n\in\mathbb{N}} v_\pi(a_n).$$

Revenons à une situation générale. La version p-adique du théorème de Weierstrass conduit à :

Lemme 3.9.3. *Soit t un élément non nul quelconque de $\mathfrak{m}$. Si $\widehat{E}$ est compact, alors toute fonction $\varphi \in \mathcal{C}(\widehat{E},\widehat{V})$ peut s'écrire sous la forme*

$$\varphi = \sum_{n\geq 0} t^n g_n \quad \text{avec} \quad g_n \in \mathrm{Int}(E,V).$$

Proof. Il suffit d'utiliser le théorème d'approximation de façon itérative. □

Voyons maintenant comment passer d'une série à une autre :

Lemme 3.9.4. *Soit*

$$\varphi = \sum_{n\geq 0} c_n g_n \in \mathcal{C}(\widehat{E},\widehat{V})$$

où

$$g_n \in \mathrm{Int}(E,V)\ ,\ c_n \in \widehat{V} \text{ et } \lim_{n\to+\infty} v(c_n) = +\infty.$$

Soit $\{h_n \mid n \in \mathbb{N}\}$ un système de générateurs du V-module $\mathrm{Int}(E,V)$. Décomposons les g_n selon les h_n :

$$g_n = \sum_{k=0}^{i_n} b_{k,n} h_k \text{ avec } b_{k,n} \in \widehat{V}.$$

Alors, pour tout $k \in \mathbb{N}$, la série $b_k = \sum_{n=0}^{+\infty} c_n b_{k,n}$ converge dans $\widehat{V}$,

$$\lim_{k\to+\infty} v(b_k) = +\infty \text{ et } \varphi = \sum_{n\geq 0} b_n h_n.$$

Proof. Pour tout $k \in \mathbb{N}$, la série $\sum_{n=0}^{+\infty} c_n b_{k,n}$ converge puisque $v(c_n) \to +\infty$. Notons b_k sa somme. Fixons $N \in \mathbb{N}$. Soit $n_0 \in \mathbb{N}$ tel que $n > n_0$ implique $v(c_n) > N$ et soit $m(n_0) = \sup\{i_0,\ldots,i_{n_0}\}$. Alors, pour $k > m(n_0)$, on a $b_k = \sum_{n>n_0} c_n b_{k,n}$ et donc, $v(b_k) \geq N$. Ainsi, $v(b_k) \to +\infty$.
Considérons maintenant la différence

$$\psi_{n_0} = \varphi - \sum_{k=0}^{m(n_0)} b_k h_k = \sum_{n=0}^{+\infty} c_n g_n - \sum_{k=0}^{m(n_0)} b_k h_k.$$

On déduit de la définition des b_k que :

$$\psi_{n_0} = \sum_{n=n_0+1}^{+\infty} c_n \left\{ g_n - \sum_{k=0}^{m(n_0)} b_{k,n} h_k \right\}.$$

D'où, $\inf_{x\in\widehat{E}} v(\psi_{n_0}(x)) \geq N$, c.-à-d., $\lim_{n\to+\infty} \psi_n = 0$. Autrement dit,

$$\varphi = \sum_{n=0}^{+\infty} c_n g_n = \sum_{k=0}^{+\infty} b_k h_k.$$

□

Les deux lemmes précédents montrent en particulier :

Proposition 3.9.5. *Supposons E précompact et soit $(h_n)_{n\in\mathbb{N}}$ un système de générateurs du V-module $\mathrm{Int}(E,V)$. Alors toute fonction $\varphi \in \mathcal{C}(\widehat{E},\widehat{K})$ s'écrit sous la forme*

$$\varphi = \sum_{n=0}^{+\infty} b_n h_n \quad \text{avec} \quad \lim_{n\to+\infty} v(b_n) = +\infty.$$

Voyons ce que l'on peut dire lorsque l'on considère non plus un système de générateurs, mais une base du V-module $\mathrm{Int}(E,V)$. Commenons par utiliser une base très particulière, à savoir une base régulière obtenue à l'aide d'une suite v-ordonnée.

L'énoncé suivant généralise au cas de tout précompact infini E de V un résultat d'Y. Amice (1964) [22] obtenu seulement pour des compacts très particuliers, à savoir les *compacts valués réguliers*, les compacts vérifiant l'analogue de la formule de Legendre (cf. [11, Evrard and Fares]).

Théorème 3.9.6. *([8] et [10]) Supposons E infini et $\widehat{E}$ compact. Soit $(a_n)_{n\in\mathbb{N}}$ une suite v-ordonnée de E et soient $f_n(X) = \prod_{k=0}^{n} \frac{X-a_k}{a_n-a_k}$ $(n \in \mathbb{N})$. Alors toute fonction $\varphi \in \mathcal{C}(\widehat{E},\widehat{K})$ s'écrit sous la forme*

$$\varphi = \sum_{n=0}^{+\infty} b_n f_n \quad \text{avec} \quad \lim_{n\to+\infty} v(b_n) = +\infty.$$

Les coefficients b_n sont déterminés de façon unique par la récurrence :

$$b_n = \varphi(a_n) - \sum_{k=0}^{n-1} b_k f_k(a_n).$$

De plus,

$$\inf_{x\in\widehat{E}} v(\varphi(x)) = \inf_{n\in\mathbb{N}} v(\varphi(a_n)) = \inf_{n\in\mathbb{N}} v(b_n).$$

Proof. Les deux lemmes précédents montrent que tout $\varphi \in \mathcal{C}(\widehat{E},\widehat{V})$ peut s'écrire $\varphi = \sum_{n=0}^{+\infty} b_n f_n$ avec $\lim_{n\to+\infty} v(b_n) = +\infty$. En fait, cela s'étend aux fonctions $\varphi \in \mathcal{C}(\widehat{E},\widehat{K})$ puisque $\widehat{E}$ étant compact les fonctions φ sont bornées.
La formule de récurrence résulte de ce que $f_n(a_n) = 1$ et $f_k(a_n) = 0$ pour $k > n$. Et donc les b_n sont uniques.
Enfin, soit $\alpha = \inf_{n\in\mathbb{N}} v(b_n)$ et soit $n_0 = \inf_{v(b_n)=\alpha} n \in \mathbb{N}$. On a

$$\varphi(a_{n_0}) = b_{n_0} + \sum_{0\le k<n_0} b_k f_k(a_{n_0}),$$

d'où $v(\varphi(a_{n_0})) = v(b_{n_0}) = \alpha$. Ainsi,

$$\inf_{x\in\widehat{E}} v(\varphi(x)) \le \inf_{n\in\mathbb{N}} v(\varphi(a_n)) \le \inf_{n\in\mathbb{N}} v(b_n).$$

L'inégalité manquante est immédiate. □

Le théorème précédent est bien la généralisation des séries de Mahler. En fait, cette description, explicite dès que l'on dispose d'une suite v-ordonnée, s'inscrit dans le cadre plus général suivant.

3.10 Bases orthonormales du Banach $\mathcal{C}(\widehat{E},\widehat{K})$

Définition 3.10.1. Suposons $\widehat{E}$ compact. Une *base orthonormale* de l'espace de Banach $\mathcal{C}(\widehat{E},\widehat{K})$ est une suite $(f_n)_{n\in\mathbb{N}}$ d'éléments de $\mathcal{C}(\widehat{E},\widehat{V})$ telle que tout élément ϕ de $\mathcal{C}(\widehat{E},\widehat{K})$ s'écrive d'une façon et d'une seule sous la forme :

$$\phi(x) = \sum_{n=0}^{+\infty} a_n\ f_n(x) \quad \text{pour tout } x \in \widehat{E}$$

où

$$a_n \in K\ , \quad \lim_{n\to+\infty} v(a_n) = +\infty$$

et

$$\inf_{x\in\widehat{E}} v(\phi(x)) = \inf_{n\in\mathbb{N}} v(a_n).$$

Le théorème 3.9.6 conduit à l'énoncé suivant moins précis mais un peu plus général :

Proposition 3.10.2. *Supposons E infini et $\widehat{E}$ compact. Soit $(h_n)_{n\in\mathbb{N}}$ une base du V-module $\mathrm{Int}(E,V)$. Alors toute fonction $\varphi\in\mathcal{C}(\widehat{E},K)$ s'écrit sous la forme*

$$\varphi=\sum_{n=0}^{+\infty}b_nh_n\quad\text{avec}\quad b_n\in\widehat{K}\ \text{ et }\ \lim_{n\to+\infty}v(b_n)=+\infty.$$

Les coefficients b_n sont déterminés de façon unique et on a :

$$\inf_{x\in\widehat{E}}v(\varphi(x))=\inf_{n\in\mathbb{N}}v(b_n).$$

Autrement dit, toute base du V-module $\mathrm{Int}(E,V)$ est une base orthonormale de l'espace de Banach ultramétrique $\mathcal{C}(\widehat{E},\widehat{K})$.

Proof. Montrons l'unicité des b_n. Supposons que

$$\varphi=\sum_{n\geq0}b_nh_n=\sum_{n\geq0}b'_nh_n$$

et qu'il existe k_0 tel que $b_{k_0}\neq b'_{k_0}$. Soit $t\in V$ tel que $v(t)>v(b'_{k_0}-b_{k_0})$. Soit n tel que $v(b'_k-b_k)\geq t$ pour tout $k>n$. Considérons le polynôme

$$\psi=\sum_{k=0}^{n}(b_k-b'_k)h_k.$$

On a aussi :

$$\psi=\sum_{k=n+1}^{\infty}(b'_k-b_k)h_k$$

et donc ψ appartient à $t\mathrm{Int}(E,V)$. Comme la décomposition de ψ selon la base des h_n est unique, on a en particulier $v(b_{k_0}-b'_{k_0})\geq v(t)$. C'est une contradiction.

Montrons l'égalité des inf. Soit $\varphi\in\mathcal{C}(\widehat{E},\widehat{K})$. Alors

$$\varphi=\sum_{n\geq0}b_nh_n=\sum_{n\geq0}c_nf_n.$$

D'après le lemme 2, on a $b_k=\sum_{n\geq0}c_nb_{k,n}$ où $b_{k,n}\in V$ et donc

$$\inf_{n\geq0}v(b_n)\geq\inf_{n\geq0}v(c_n),$$

et réciproquement. D'où :

$$\inf_{n\geq 0} v(b_n) = \inf_{n\geq 0} v(c_n) = \inf_{x\in\widehat{E}} v(\varphi(x))$$

d'après le théorème précédent. □

Remarques 3.10.3. 1- L'existence de bases orthonormales de $\mathcal{C}(\widehat{E},\widehat{K})$ formées d'un polynôme de chaque degré était connue de façon théorique (cf. Van der Put [12], 1968), mais on ne savait pas décrire explicitement ces polynômes.

2- L'unicité de l'écriture n'existe plus lorsque le compact E est fini. En effet, si $E = \{a_1,\ldots,a_r\}$, alors toute fonction $\phi \in \mathcal{C}(\widehat{E},\widehat{K})$ s'écrit $\phi = \sum_{i=1}^{n} \phi(a_i)\phi_i$ où $\phi_i = \prod_{j\neq i} \frac{X-a_j}{a_i-a_j}$. Et il n'y a pas unicité puisque la fonction 0 peut aussi être représentée par $f\prod_{i=1}^{r}(X-a_i)$ pour tout $f \in K[X]$.

Exercice 3.10.4. Supposons $\widehat{E}$ compact et soit $(h_n)_{n\in\mathbb{N}}$ une base de $\mathrm{Int}(E,V)$. Une mesure μ sur $\widehat{E}$ valeurs dans $\widehat{K}$ est une application $\widehat{K}$-linéaire continue $\mu : \mathcal{C}(\widehat{E},\widehat{K}) \to \widehat{K}$. Montrer que :
a) Une mesure μ est caractérisée par la suite $(\mu_n)_{n\in\mathbb{N}}$ où $\mu_n = \mu(h_n)$.
b) A une suite $(\mu_n)_{n\in\mathbb{N}}$ dans $\widehat{K}$ correspond une mesure μ telle que $\mu(h_n) = \mu_n$ si et seulement si la suite (μ_n) est bornée.

3.11 A propos des bases orthonormales sur un espace de Banach non archimédien

Hypothèses. *Désormais, le corps valué non archimédien K est supposé complet.*

Soit $\mathcal{E}$ une espace de Banach non archimédien sur K, c'est-à-dire, un espace vectoriel sur K complet pour une norme ultramétrique $||\ ||$, c'est-à-dire vérifiant :

$$||x+y|| \leq max(||x||,||y||) \quad \forall x,y \in \mathcal{E}.$$

On notera $\mathcal{E}_0$ la boule unité de $\mathcal{E}$:

$$\mathcal{E}_0 = \{x \in \mathcal{E} \mid ||x|| \leq 1\}.$$

Alors $\mathcal{E}_0$ est un V-module et la topologie de $\mathcal{E}$ est définie par les sous-V-modules $c_n\mathcal{E}_0$ où $c_n \in K$ et $v(c_n) \to +\infty$.

On peut supposer que $||\mathcal{E}|| = \{\ ||x||\ |\ x \in \mathcal{E}\ \}$ est contenu dans l'adhérence de $|K| = \{|c|\ |\ c \in K\}$ dans $\mathbb{R}$. Ceci est toujours vérifié si la valuation v n'est pas discrète et, lorsque v est discrète, on peut toujours s'y ramener (cf. Serre [13], 1962) en remplaçant la norme initiale par la norme équivalente :

$$||x||' = \inf\{r \in |K|\ |\ r \geq |x|\}$$

auquel cas on a l'égalité : $||\mathcal{E}|| = |K|$.

Définition 3.11.1. Une *base orthonormale* du K-espace de Banach $\mathcal{E}$ est une famille $(e_i)_{i\in I}$ déléments de $\mathcal{E}$ telle que tout élément x de $\mathcal{E}$ s'écrive d'une façon et d'une seule sous la forme :

$$x = \sum_{i\in I} x_i e_i \quad \text{avec } x_i \in K,\ x_i \to 0 \text{ et } ||x|| = \sup_{i\in I} |x_i|.$$

Les limites sont bien sûr prises selon le filtre des parties cofinies de I.

EXEMPLE 3.11.2. La complétion de $K^{(I)}$ est le sous-espace vectoriel $c_0(I;K)$ de K^I formé des suites $(x_i)_{i\in I}$ d'éléments de K tendant vers 0. C'est un espace de Banach admettant la base orthonormale $(e_i)_{i\in I}$ où $e_i = (\delta_{i,j})_{j\in J}$.

La proposition suivante est immédiate :

Proposition 3.11.3. *Si l'espace de Banach ultramétrique $\mathcal{E}$ possède une base orthonormale $(e_i)_{i\in I}$, alors l'application*

$$(x_i)_{i\in I} \in c_0(I;K) \mapsto \sum_{i\in I} x_i e_i \in \mathcal{E}$$

est une isométrie linéaire bijective. Réciproquement, toute isométrie linéaire bijective de $c_0(I;K)$ sur $\mathcal{E}$ définit une base orthonormale de $\mathcal{E}$, à savoir l'image de la base canonique de $c_0(I;K)$.

Comme, dans $c_0(I;K)$, $||x|| = \sup|x_i| = \max|x_i| \in |K|$, si $\mathcal{E}$ possède une base orthonormale, alors nécessairement $||\mathcal{E}|| = |K|$.

Proposition 3.11.4 (Serre [13], 1962 ; Coleman [14], 1997)**.** *Supposons $||\mathcal{E}|| = |K|$. Une famille $(e_i)_{i\in I}$ d'éléments de $\mathcal{E}$ est une base orthonormale de $\mathcal{E}$ si et seulement si les e_i sont dans $\mathcal{E}_0$ et s'il existe un élément $t \in \mathfrak{m}$ (resp. si pour tout $t \in \mathfrak{m}$) les classes $\overline{e_i}$ des e_i modulo $t\mathcal{E}_0$ forment une base du V/tV-module $\overline{\mathcal{E}} = \mathcal{E}_0/t\mathcal{E}_0$.*

Proof. Supposons que $(e_i)_{i\in I}$ soit une base orthonormale de $\mathcal{E}$. S'il existe $j \in I$ tel que $e_j \notin \mathcal{E}_0$, alors $e_j = 1.e_j$ induirait $||e_j|| = \sup |x_i| = 1$ alors que $||e_j|| > 1$. Donc, tous les e_i sont dans $\mathcal{E}_0$.

Fixons maintenant $t \in \mathfrak{m}$. Il est clair que les $\overline{e_i}$ engendrent le V/tV-module $\overline{\mathcal{E}}$. Supposons les $\overline{e_i}$ non linéairement indépendants et considérons une combinaison linéaire non triviale avec le plus petit nombre possible de coefficients non nuls :

$$\sum_{i\in I_0} \overline{\lambda_i}\overline{e_i} = 0 \ \text{ avec } \ \lambda_i \in V \setminus tV, \ I_0 \text{ fini.}$$

Alors, $x = \sum_{i\in I_0} \lambda_i e_i \in t\mathcal{E}_0$, $||x|| = \max_{i\in I_0} |\lambda_i| \leq |t|$. Ainsi, il existe i_0 tel que $v(\lambda_{i_0}) \geq v(t)$, c'est une contradiction.

Réciproquement, supposons les e_i dans $\mathcal{E}_0$ et supposons qu'il existe $t \in \mathfrak{m}$ tel que les classes $\overline{e_i}$ des e_i modulo $t\mathcal{E}_0$ forment une base du V/tV-module $\mathcal{E}_0/t\mathcal{E}_0$.

Soit $x \in \mathcal{E}_0$. Posons $\overline{x} = \sum \xi_i \overline{e_i}$ où $\xi_i \in V/tV$ (la somme est finie). Soient $x_i \in V$ tels que $\overline{x_i} = \xi_i$. Alors $x = \sum x_i e_i + ty$ où $y \in \mathcal{E}_0$ (la somme est toujours finie). De même, $y = \sum y_i e_i + tz$ où $z \in tV$. Ainsi de suite :

$$x = \sum (x_i + ty_i + t^2 z_i + \ldots + t^n w_i)e_i.$$

Posons $x_i(n) = x_i + ty_i + t^2 z_i + \ldots + t^n w_i$. Pour un n fixé, il n'y a qu'un nombre fini de $x_i(n)$ non nuls et on a $x - \sum_{i\in I} x_i(n)e_i \in t^{n+1}\mathcal{E}_0$. Soit $X_i = \lim_{n\in\mathbb{N}} x_i(n)$. Alors $x = \sum_{i\in I} X_i e_i$ (on a bien $\lim_I X_i = 0$).

Si $||x|| = 1$, alors il existe i_0 tel que $\xi_{i_0} \neq 0$ (sinon $x \in t\mathcal{E}_0$). Ainsi, $v(x_{i_0}) = 0$ et $\inf v(x_i) = 0$. Pour x quelconque dans $\mathcal{E}$, par hypothèse, il existe $\lambda \in K$ tel que $|\lambda| = ||x||$. Alors $\frac{1}{\lambda}x = y$ est de norme 1 et l'on n'a pas de mal à conclure.

Enfin, vérifions l'unicité. Supposons

$$\sum_i x_i e_i = \sum_i x'_i e_i \text{ avec } x_i \to 0, x'_i \to 0$$

et qu'il existe i_0 tel que $x_{i_0} \neq x'_{i_0}$. Soit i_1 tel que $v(x_{i_1} - x'_{i_1}) = \min_i v(x_i - x'_i)$. Alors, posant

$$y_i = \frac{x_i - x'_i}{x_{i_1} - x'_{i_1}},$$

on a

$$\sum_i y_i e_i = 0 \text{ avec } y_{i_1} = 1.$$

Par suite, $\sum_i \overline{y}_i \overline{e}_i = 0$ serait une relation linéaire non triviale entre les $\overline{e}_i$. □

Remarque 3.11.5. La proposition précédente appliquée pour $\mathcal{E} = \mathcal{C}(\widehat{E}, \widehat{K})$ et $\mathcal{E}_0 = \mathcal{C}(\widehat{E}, \widehat{V})$ permet de retrouver le théorème 3.9.6. En effet, d'après la proposition 3.5.2, pour tout $t \in \mathfrak{m}$, $\mathcal{C}(\widehat{E}, \widehat{V}) = \mathrm{Int}(E, V) + t\mathcal{C}(\widehat{E}, \widehat{V})$ et donc les classes des f_n engendrent $\mathcal{C}(\widehat{E}, \widehat{V})/t\mathcal{C}(\widehat{E}, \widehat{V})$. Par ailleurs, les égalités $f_n(u_k) = \delta_{k,n}$ pour $0 \leq k \leq n$ montrent que ces classes sont linéairement indépendantes.

Corollaire 3.11.6. *Lorsque v est discrète, $\mathcal{E}$ admet une base orthonormale si et seulement si $||\mathcal{E}|| = |K|$.*

Proof. Lorsque v est discrète, la proposition précédente peut se reformuler : une famille (e_i) d'éléments de $\mathcal{E}_0$ est une base orthonormale de $\mathcal{E}$ si et seulement si les classes des e_i modulo $\mathfrak{m}\mathcal{E}_0$ forment une base du $V/\mathfrak{m}$-espace vectoriel $\mathcal{E}_0/\mathfrak{m}\mathcal{E}_0$. □

Remarque 3.11.7. Dans le cas où v n'est pas discrète, si (c_i) est une base orthonormale de $\mathcal{E}$, alors $(\overline{c_i})$ est une base de $\mathcal{E}_0/\mathfrak{m}\mathcal{E}_0$. Mais, la réciproque n'est pas toujours vraie comme le montre l'exemple suivant.

EXEMPLE 3.11.8. Si v n'est pas discrète, on peut trouver une suite $(b_n)_{n\in\mathbb{N}}$ d'éléments de $\mathfrak{m}$ tels que $b_1 b_2 \cdots b_n \not\to 0$. En effet, on choisit $b_0 \in \mathfrak{m} \setminus \{0\}$, puis les b_i $(i \geq 1)$ tels que $0 < v(b_{i+1}) \leq \frac{1}{2} v(b_i)$, d'où : $v(b_1 \cdots b_n) \leq v(b_0)$. Supposons que (c_n) soit une base orthonormale de $\mathcal{E}$. Posons $d_n = c_n - b_{n+1}c_{n+1}$, alors $\overline{d_i} = \overline{c_i}$. Puisque (c_i) est une base orthonormale de $\mathcal{E}$, $(\overline{d_i}) = (\overline{c_i})$ est une base de $\mathcal{E}_0/\mathfrak{m}\mathcal{E}_0$. Mais (d_i) ne peut être une base orthonormale de $\mathcal{E}$, car sinon on pourrait écrire :

$$c_0 = \sum_{i=0}^{\infty} x_i d_i = \sum_{i=0}^{\infty} x_i (c_i - b_{i+1}c_{i+1}) = x_0 c_0 + \sum_{i=1}^{\infty} (x_i - x_{i-1}b_i)c_i,$$

or, l'unicité impose $x_0 = 1$ et $x_i - x_{i-1}b_i = 0$ pour tout $i \geq 1$, et par suite, $x_i = b_1 \cdots b_i \not\to 0$.

3.12 Extensions de bases orthonormales selon le 'digit principle'

On va maintenant donner une méthode de construction de bases orthonormales de l'algèbre de Banach $\mathcal{C}(V, K)$ éventuellement autres que les bases de polynômes à valeurs entières associées à des suites v-ordonnées.

Définition 3.12.1 (La digit-extension). Soit $(a_n)_{n\in\mathbb{N}}$ une suite déléments d'un monoïde commutatif noté ici multiplicativement. On lui associe une suite $(b_n)_{n\in\mathbb{N}}$ dite obtenue par *digit-extension* de la façon suivante :
Si n s'écrit en base q

$$n = n_0 + n_1 q + \cdots + n_k q^k,$$

alors on pose

$$b_n = a_0^{n_0} a_1^{n_1} \cdots a_k^{n_k}.$$

Noter que, si $n_j = 0$, alors $a_j^{n_j} = 1$ (où 1 désigne l'élément neutre du monoïde) et que

$$a_k = b_{q^k}.$$

EXEMPLE 3.12.2. Si $a_n = a^{q^n}$, alors $b_n = a^n$.

Tous les énoncés de cette section sont dus à Conrad [15, J. Number Theory, 2000].

Hypothèses : désormais, K désigne un corps local (*corps complet pour une valuation discrète v de corps résiduel $\mathbb{F}$ de cardinal fini q*).

Pour simplifier, on se restreint au cas où $E = V$. Pour des parties E plus générales, voir S. Evrard [16, 2006]. On sait, qu'avec les hypothèses précédentes, V est compact. En particulier :

Une suite $(e_n)_{n\in\mathbb{N}}$ d'éléments de $\mathcal{C}(V,V)$ est une base orthonormale de $\mathcal{C}(V,K)$ si et seulement si la suite $(\overline{e}_n)$ des classes modulo $\mathcal{C}(V,\mathfrak{m})$ est une base du $\mathbb{F}$-espace vectoriel $\mathcal{C}(V,\mathbb{F})$.

Or, compte tenu des hypothèses, on a :

$$\mathcal{C}(V,\mathbb{F}) \simeq \varprojlim \mathcal{F}(V/\mathfrak{m}^n,\mathbb{F}),$$

où $\mathcal{F}(V/\mathfrak{m}^n,\mathbb{F})$ désigne l'ensemble des applications de $V/\mathfrak{m}^n$ dans $\mathbb{F}$. En effet, la compacité de V implique l'existence pour tout $\varphi \in \mathcal{C}(V,\mathbb{F})$ d'un entier n tel que φ soit constante modulo $\mathfrak{m}^n$.

Remarque 3.12.3. Dans le cas particulier où, pour tout $n \geq 0$ (ou au moins pour une infinité de n), $\overline{e}_0, \overline{e}_1, \ldots, \overline{e}_{q^n-1}$ définissent des fonctions modulo $\mathfrak{m}^n$, il suffit de vérifier qu'elles définissent une $\mathbb{F}$-base de $\mathcal{F}(V/\mathfrak{m}^n,\mathbb{F})$ pour une infinité de n pour être asssuré que la suite (e_n) est une base orthonormale de $\mathcal{C}(V,K)$.

Faisons maintenant l'hypothèse que la caractéristique de K est > 0. Alors, K contient un sous-corps isomorphe à $\mathbb{F}$ (cf lemme de Hensel) et, par suite, le K-espace de Banach $\mathcal{C}(V, K)$ contient le sous-K-espace vectoriel $\mathcal{L}_{\mathbb{F}}(V, K)$ formé des applications $\mathbb{F}$-linéaires continues de V dans K.

Théorème 3.12.4 (Digit principle en car > 0)**.** *Soit K un corps local de caractéristique p, d'anneau V et de corps résiduel $\mathbb{F}$ de cardinal q. La digit-extension d'une base orthonormale de $\mathcal{L}_{\mathbb{F}}(V, K)$ est une base orthonormale de $\mathcal{C}(V, K)$.*

Proof. Soit donc (e_i) une base orthonormale de $\mathcal{L}_{\mathbb{F}}(V, K)$. Alors $(\overline{e}_i)$ est une base du $\mathbb{F}$-espace vectoriel

$$\mathcal{L}_{\mathbb{F}}(V, \mathbb{F}) = \oplus_{i\geq 0}\mathbb{F}\overline{e}_i.$$

Posons

$$H_n = \cap_{i=0}^{n-1}\ Ker(\overline{e}_i).$$

Alors H_n est un sous-$\mathbb{F}$-espace vectoriel fermé de codimension n dans V. De plus, $H_{n+1} \subset H_n$ et $\cap_n\ H_n = \{0\}$. Par suite,

$$V \simeq \lim_{\rightarrow}\ V/H_n,$$

d'où :

$$\mathcal{C}(V, \mathbb{F}) = \lim_{\leftarrow}\ \mathcal{F}(V/H_n, \mathbb{F}).$$

On remarque que les fonctions $\overline{e}_0, \ldots, \overline{e}_{n-1}$ sont des fonctions sur V/H_n, elles forment même une base de $(V/H_n)^*$ dual de V/H_n. Or, compte tenu de la remarque 3.12.3, il suffirait de montrer que les fonctions $(f_i)_{0\leq i<q^n}$ construites par digit-extension à partir des e_i vérifient : les $(\overline{f_i})_{0\leq i<q^n}$ forment une base de $\mathcal{F}(V/H_n, \mathbb{F})$. Or, cela résulte de la proposition suivante (avec $W = V/H_n$) où l'on oublie l'origine du problème. □

Proposition 3.12.5. *Soit W un $\mathbb{F}_q$-espace vectoriel de dimension n. Considérons une base $(\varphi_0, \ldots, \varphi_{n-1})$ de W^*. Si on étend les φ_i en des Φ_i selon la digit-extension, alors les Φ_i $(0 \leq i < q^n - 1)$ forment une base du $\mathbb{F}_q$-espace vectoriel $\mathcal{F}(W, \mathbb{F}_q)$.*

Proof. Le $\mathbb{F}_q$-espace vectoriel $\mathcal{F}(W, \mathbb{F}_q)$ est de dimension q^n et contient W^*. Il s'agit de montrer que les Φ_i engendrent $\mathcal{F}(W, \mathbb{F}_q)$. Soit $w_0, \ldots, w_{n-1}$ la base de W duale de la base des φ_i de W^*. Pour $w \in W$, écrivons

$$w = a_0w_0 + \cdots + a_{n-1}w_{n-1} \quad \text{avec } a_i \in \mathbb{F}_q.$$

Définissons $h_w : W \to \mathbb{F}_q$ par :

$$h_w(u) = \prod_{i=0}^{n-1}(1 - (\varphi_i(u) - a_i)^{q-1}) = \prod_{i=0}^{n-1}(1 - (\varphi_i(u) - \varphi_i(w))^{q-1}).$$

Alors $h_w(u) = 0$ si $u \neq w$ et $h_w(w) = 1$. Par suite, les h_w pour $w \in W$ engendrent W. Or, le développement des h_w montre qu'ils sont engendrés par les Φ_i puisque l'exposant des φ_i ne dépasse pas $q - 1$. □

Voici maintenant une extension de ce théorème en caractéristique nulle.

Théorème 3.12.6 (digit principle en car qcq)**.** *Soit K un corps local, d'anneau V et de corps résiduel $\mathbb{F}$ de cardinal q. Soit H_n une suite de sous-groupes ouverts de V tels que $card(V/H_n) = q^n$, $H_{n+1} \subset H_n$ et $\cap_n H_n = \{0\}$. Supposons qu'il existe une suite d'éléments e_i de $\mathcal{C}(V, V)$ telle que, pour tout n, les classes $\overline{e}_0, \ldots, \overline{e}_{n-1} \in \mathcal{C}(V, \mathbb{F})$ soient constantes sur les classes de V modulo H_n et l'application*

$$x \in V/H_n \mapsto (\overline{e}_0(x), \ldots, \overline{e}_{n-1}(x)) \in \mathbb{F}^n$$

soit bijective. Alors la suite (f_i) obtenue par digit-extension à partir de la suite (e_i) est une base orthonormale de $\mathcal{C}(V, K)$.

Bien sûr, le plus souvent, on prendra $H_n = \mathfrak{m}^n$.

Proof. Par hypothèse,

$$V \simeq \lim_{\rightarrow} V/H_n,$$

d'où :

$$\mathcal{C}(V, \mathbb{F}) \simeq \lim_{\leftarrow} \mathcal{F}(V/H_n, \mathbb{F})$$

et il suffit de montrer que, pour tout n, les $(\overline{f}_i)_{0 \leq i < q^n}$ forment une base de $\mathcal{F}(V/H_n, \mathbb{F})$. La proposition 3.12.5 ne peut plus se formuler, mais en définissant de façon analogue, pour $w \in V/H_n$, des fonctions $h_w : V/H_n \to \mathbb{F}$ par

$$h_w(u) = \prod_{i=0}^{n-1} (1 - (\overline{e}_i(u) - \overline{e}_i(w))^{q-1}),$$

on montre encore que les $\overline{f}_i$ sont générateurs. □

3.13 Exemples de bases orthonormales obtenue par digit-extension

Premier exemple

On connaît bien la base orthonormale de $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ formée des polynômes $\binom{x}{n}$. En voici une autre :

Proposition 3.13.1. *La suite de polynômes* $\left\{ \begin{array}{c} x \\ n \end{array} \right\}$ *définis ci-dessous est une base orthonormale de* $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. *Pour*

$$n = n_0 + n_1 p + \cdots + n_k p^k \text{ avec } 0 \leq n_i < p,$$

on pose :

$$\left\{ \begin{array}{c} x \\ n \end{array} \right\} = \binom{x}{1}^{n_0} \binom{x}{p}^{n_1} \cdots \binom{x}{p^k}^{n_k}.$$

Proof. Il suffit de vérifier que les fonctions $e_i = \binom{x}{p^i} \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ vérifient les conditions du théorème 3.12.6.
Si $0 \leq j < p^n$, alors

$$j = j_0 + j_1 p + \cdots + j_{n-1} p^{n-1} \text{ avec } 0 \leq j_i < p$$

et si

$$x \equiv x_0 + x_1 p + \cdots + x_{n-1} p^{n-1} \pmod{p^n},$$

alors le théorème de Lucas nous dit :

$$\binom{x}{j} \equiv \binom{x_0}{j_0} \binom{x_1}{j_1} \cdots \binom{x_{n-1}}{j_{n-1}} \pmod{p}.$$

Ainsi, pour $0 \leq j < p^n$, $\binom{x}{j}$ induit une fonction de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{F}_p$. En particulier, pour $0 \leq i \leq n-1$, $\overline{e}_i = \binom{x}{p^i} \pmod{p}$ induit une application de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{F}_p$. Comme, pour $x = \sum x_k p^k$, $\overline{e}_i(x) = x_i$, l'application :

$$x = x_0 + x_1 p + \cdots + x_{n-1} p^{n-1} \in \mathbb{Z}/p^n\mathbb{Z} \mapsto$$

$$(\overline{e}_0(x), \ldots, \overline{e_{n-1}}(x)) = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_q^n$$

est bijective. □

Deuxième exemple

Proposition 3.13.2 (Tateyama [17], 1999)**.** *Soit K un corps local. Notons q le cardinal de son corps résiduel et fixons une uniformisante π. La suite de polynômes F_n définis ci-dessous est une base orthonormale de $\mathcal{C}(\mathcal{O}_K, K)$. Pour*

$$n = n_0 + n_1 q + \cdots + n_k q^k \text{ avec } 0 \leq n_i < q,$$

on pose :

$$F_n = F_0^{n_0} F_q^{n_1} \cdots F_{q^k}^{n^k}$$

où F_{q^r} est défini par récurrence par :

$$F_0(x) = 1,\ F_q(x) = \frac{x^q - x}{\pi} \text{ et } F_{q^{r+1}}(x) = F_{q^r}(F_q(x)).$$

On voit que $F_q \in \mathrm{Int}(\mathcal{O}_K, \mathcal{O}_K)$ et par suite, pour tout n, $F_n \in \mathrm{Int}(\mathcal{O}_K, \mathcal{O}_K)$. Il suffit alors de vérifier que, pour tout n, les polynômes $F_0, F_q, \ldots, F_{q^{n-1}}$ vérifient les assertions du théorème 3.12.6. On a reconnu les polynômes de Fermat introduits antérieurement.

Voici maintenant deux exemples de bases qui ne sont pas formées de polynômes.

Troisième exemple

Soit K un corps local. Notons q le cardinal de son corps résiduel. Hensel nous dit que le groupe U_K des unités de K contient un sous-groupe V formé des racines de l'unité d'ordre premier à p, isomorphe à $\mathbb{F}_q^*$, donc cyclique d'ordre $q-1$. Posons $tV = V \cup \{0\}$ [$u \in tV$ équivaut à $u^q = u$].

Pour tout $x \in \mathcal{O}_K$, il existe un élément et un seul dans tV que l'on notera $\omega(x)$ tel que $\omega(x) - x \in \mathfrak{m}_K$. La fonction $\omega : \mathcal{O}_K \to \mathcal{O}_K$ ainsi définie est localement constante, on l'appelle *caractère de Teichmüller* de $\mathcal{O}_K$. Fixons maintenant une uniformisante π de K. On appelle alors *représentation de Teichmüller* de $x \in \mathcal{O}_K$ son écriture sous la forme :

$$x = \sum_{k \geq 0} \omega_k(x) \pi^k$$

où $\omega_k(x) \in tV$ pourrait être défini par récurrence par

$$\omega_k(x) = \omega\left(\frac{1}{\pi^k} \sum_{i=0}^{k-1} \omega_i(x) \pi^i\right).$$

Proposition 3.13.3 (Baker [18], 1986)**.** *Soit K un corps local de corps résiduel de cardinal q. La suite de fonctions $\mathcal{B}_n$ définies ci-dessous est une base orthonormale de $\mathcal{C}(\mathcal{O}_K, K)$. Pour*

$$n = n_0 + n_1 q + \cdots + n_k q^k \ \text{ avec } \ 0 \leq n_i < q,$$

on pose :

$$\mathcal{B}_n(x) = \omega_0^{n_0} \omega_1^{n_1} \cdots \omega_k^{n_k}$$

où $\omega_i(x)$ désigne le i-ème représentant de Teichmüller de x (relatif au choix de l'uniformisante π).

Cet énoncé démontré par Baker en caractéristique 0 est vrai en toute caractéristique comme le montre le théorème 3.12.6 puisque les fonctions $\omega_0, \ldots, \omega_{n-1}$ séparent les points de $\mathcal{O}_K/\mathfrak{m}_K$.

Le quatrième et dernier exemple est traité dans la section suivante.

3.14 Base d'opérateurs hyperdifférentiels

Dans cette section, on va considèrer le corps local $K = \mathbb{F}_q((T))$. C'est cet exemple qui a motivé l'étude de Conrad.

Définition 3.14.1. Soit $\mathbb{F}$ un corps. On appelle j-ème *opérateur hyperdifférentiel* sur $\mathbb{F}[T]$ l'endomorphisme $\mathbb{F}$-linéaire $\mathcal{D}_j$ de $\mathbb{F}[T]$ caractérisé par :

$$\mathcal{D}_j(T^m) = \binom{m}{j} T^{m-j} \quad \text{pour tout } \ m \geq 0.$$

En caractéristique 0, on a :

$$\mathcal{D}_j = \frac{1}{j!} \frac{d^j}{dT^j}.$$

En caractéristique $p > 0$, cette formule n'a de sens que pour $0 \leq j \leq p-1$ car, pour $j \geq p$, $\mathcal{D}_J \neq 0$ alors que $\frac{d^j}{dT^j} = 0$.

Pour

$$f(T) = \sum_{m \geq 0} a_m T^m,$$

on a

$$\mathcal{D}_j(f(T)) = \sum_{m \geq j} a_m \binom{m}{j} T^{m-j} \quad \text{et} \quad \mathcal{D}_j(f(0)) = a_j.$$

Les formules suivantes avec la formule de Leibniz caractérisent les opérateurs différentiels parmi les applications $\mathbb{F}$-linéaires.

$$\mathcal{D}_0(T) = T \ , \ \mathcal{D}_1(T) = 1 \ \text{ et } \ \mathcal{D}_j(T) = 0 \text{ pour } j \geq 2.$$

Formule de Leibniz :

$$\mathcal{D}_j(fg) = \sum_{k=0}^{j} \mathcal{D}_k(f)\mathcal{D}_{j-k}(g) \ \ \forall f, g \in \mathbb{F}[T].$$

Par linéarité, cette dernière formule se vérifie sur $f = T^r$ et $g = T^s$ et on est ramené à la formule de Vandermonde.

Remarquons la formule de Taylor en caractéristique quelconque :

$$f(T + X) = \sum_{j \geq 0} \mathcal{D}_j(f(T))X^j.$$

Les $\mathcal{D}_j$ sont uniformément continues pour la topologie T-adique.

En effet, pour $m \geq j$, on a :

$$\mathcal{D}_j(T^n \sum_{m \geq 0} a_m T^m) = \sum_{m \geq 0} a_m \binom{m+n}{j} T^{m+n-j} = T^{n-j} \sum_{m \geq 0} a_m \binom{m+n}{j} T^m.$$

D'où :

$$g \equiv h \pmod{t^n} \Rightarrow \mathcal{D}_j(g) \equiv \mathcal{D}_j(h) \pmod{T^{n-j}}.$$

Ainsi, $\mathcal{D}_j$ s'étend par continuité à $\mathbb{F}[[T]]$.

Soit maintenant $K = \mathbb{F}_q((T))$ et $V = \mathbb{F}_q[[T]]$. Alors $\mathcal{D}_j \in \mathcal{L}_{\mathbb{F}_q}(\mathbb{F}_q[[T]])$ et $\overline{\mathcal{D}}_j \in \mathcal{L}_{\mathbb{F}_q}(\mathbb{F}_q[[T]], \mathbb{F}_q)$. Comme, pour $0 \leq j \leq n-1$,

$$\mathcal{D}_j(T^n \alpha) \in T\mathbb{F}_q[[T]] \ \ \forall \alpha \in \mathbb{F}_q[[T]],$$

on a :

$$\overline{\mathcal{D}}_0, \ldots, \overline{\mathcal{D}}_{n-1} \in \mathcal{L}_{\mathbb{F}_q}(\mathbb{F}_q[T]/(T^n), \mathbb{F}_q).$$

En fait,

$$\overline{\mathcal{D}}_j(T)) \equiv \delta_{i,j} \pmod{T},$$

et donc $\overline{\mathcal{D}}_0, \ldots, \overline{\mathcal{D}}_{n-1}$ est la base duale de $1, T, \ldots, T^{n-1}$.

Proposition 3.14.2. *La suite des fonctions $\mathbb{D}_n$ définies ci-dessous est une base orthonormale de $\mathcal{C}(\mathbb{F}_q[[T]], \mathbb{F}_q((T)))$. Pour*

$$n = n_0 + n_1 q + \cdots + n_k q^k \text{ avec } 0 \leq n_i < q,$$

on pose :

$$\mathbb{D}_n = \mathcal{D}_0^{n_0} \mathcal{D}_1^{n_1} \cdots \mathcal{D}_k^{n_k}.$$

Remarquer que dans l'énoncé précédent, les $\mathbb{D}_n$ sont définis comme produits des $\mathcal{D}_j$ considérés comme fonctions (les $\mathbb{D}_n$ ne sont pas obtenus par composition d'opérateurs).

Bibliography

POUR LE TROISIEME CHAPITRE

[1] M. CHLODOVSKY, Une remarque sur la représentation des fonctions continues par des polynômes à coefficients entiers, *Mat. Sb.* **32** (1925), 472–474.

[2] J. PÁ L, Zwei kleine Bemerkungen, *Tôhoku Math. J.* **6** (1914/1915), 42–43.

[3] S. KAKEYA, On approximate polynomials, *Tôhoku Math. J.* **61** (1914), 182–186.

[4] J. DIEUDONNÉ, Sur les fonctions continues p-adiques, *Bull. Sci. Math.*, 2ème série. **68** (1944), 79–95.

[5] K. MAHLER, An Interpolation Series for Continuous Functions of a p-adic Variable, *J. reine angew. Math.* **199** (1958), 23–34 and **208** (1961), 70–72.

[6] C.G. WAGNER, Interpolation series for continuous functions on π-adic completions of $\mathrm{GF}(q, x)$, *Acta Arith.* **17** (1971), 389–406.

[7] I. KAPLANSKY, Weierstrass theorem in fields with valuations, *Proc. Amer. Math. Soc.* **1** (1950), 356–357.

[8] M. BHARGAVA AND K.S. KEDLAYA, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999), 191–198.

[9] P.-J. CAHEN, J.-L. CHABERT, AND S. FRISCH, Interpolation domains, *J. of Algebra* **125** (2000), 794–803.

[10] P.-J. CAHEN AND J.-L. CHABERT, On the ultrametric Stone-Weierstrass theorem and Mahler's expansion, *Journal de Théorie des Nombres de Bordeaux* **14** (2002), 43-57.

[11] S. EVRARD ET Y. FARES, Compacts valués réguliers, suites très bien réparties et formule de Legendre, to appear.

[12] M. VAN DER PUT, Algèbres de fonctions continues p-adiques, *Indag. Math.* **30** (1968), 401–411.

[13] J.-P. SERRE, Endomorphismes complètement continus des espaces de Banach p-adiques, *Inst. Hautes Etudes Sci. Publ. Math.* **12** (1962), 69–85.

[14] R.F. COLEMAN, p-adic Banach spaces and families of modular forms, *Invent. Math.* **127** (1997), 417–479.

[15] K. CONRAD, The Digit Principle, *J. Number Theory* **84** (2000), 230–257.

[16] S. EVRARD, Normal bases in rings of continuous functions, based on the q_n-digits principle, *Workshop on Commutative Rings*, Cortona, June 2006 (preprint).

[17] K. TATEYAMA, Continuous Functions on Discrete Valuations Rings, *J. Number Theory* **75** (1999), 23–33.

[18] A. BAKER, p-adic continuous functions on rings of integers and a theorem of K. Mahler, *J. London Math. Soc.* **33** (1986), 414–420.

Contents