RÉPUBLIQUE DU CAMEROUN
Paix-Travail-patrie
****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
****
UNIVERSITÉ DE BERTOUA
****

ÉCOLE NORMALE SUPÉRIEURE DE BERTOUA
B.P. : 652 Bertoua
****

DÉPARTEMENT DE MATHÉMATIQUES

REPUBLIC OF CAMEROON
Peace-Work-fatherland
****
MINISTRY OF HIGHER EDUCATION

****
THE UNIVERSITY OF BERTOUA
****

HIGHER TEACHER TRAINING COLLEGE BERTOUA
P.O. Box: 652 Bertoua
****

DEPARTMENT OF MATHEMATICS

UNE CARACTÉRISATION DES QUASIGROUPES POLYNOMIAUX MODULO p^w

A CHARACTERIZATION OF POLYNOMIAL QUASIGROUPS MODULO p^w

Mémoire soutenu publiquement le 25 Mai 2023, en vue de l'obtention du Diplôme de Professeur de l'Enseignement Secondaire, Deuxième grade (DIPES II) en Mathématiques /

Dissertation publicly defended on May 25, 2023 in partial fulfillment of the requirements for the degree of secondary school teacher, second grade in Mathematics

Par / By:

NGAPGUE TEGOMO Wilfried Dimitri

Matricule / Registration number: 18A176EB

Licence en Mathématiques / Bachelor in Mathematics

Devant le jury composé de / In front of the jury composed of:

Président:	**ABDOUL NTIECHE Rahman**	**MC.**	Univ. Bertoua/ENSB
Rapporteur:	**MENGUE MENGUE David Joël**	**CC.**	Univ. Yaounde 1/FS
Examinateur:	**FOUETIO DONGMEZA Aurelien**	**CC.**	Univ. Bertoua/ENSB

Mai 2023/May 2023

Avertissement

« L'Université de Bertoua ne donne aucune approbation, ni improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur. »

Dédicace

Á mes parents :

Papa NGAPGUE François et maman JEULEFACK NGUEMO Honorée

Remerciements

➠ Nous remercions tout d'abord l'**Éternel DIEU** qui m'a donné la patience et le courage durant ces années de dur labeur que j'ai passé au sein de cette illustre et jeune institution universitaire qui est l'École Normale Supérieure (ENS) de l'Université de Bertoua.

➠ Nous remercions **Pr. Remy Magloire Dieudonné ETOUA**, Recteur de l'Université de Bertoua, pour avoir mis les moyens et toutes les ressources en jeu pour notre formation.

➠ Nous remercions **Pr. Léontine NKAGUE NKAMBA**, Directeur de l'ENS de Bertoua et Chef de Département de mathématiques de l'ENS de Bertoua, pour avoir mis les moyens et toutes les ressources en jeu pour notre formation.

➠Nous remercions **Dr. David Joël MENGUE MENGUE**, Chef de Département de mathématiques de la Faculté des Sciences de l'Université d'Ebolowa, mon encadreur pour son encadrement lors de la rédaction de ce mémoire.

➠ Nous remercions **Dr. Alexandre FOTUE TABUE**, enseignant au département de mathématiques de l'ENS de Bertoua pour son soutien, ses multiples conseils, son orientation et ses remarques constructives.

➠ Nous remercions **Dr. Aurélien FOUETIO**, enseignant au département de mathématiques de l'ENS de Bertoua pour ses multiples conseils, son orientation et ses remarques constructives.

➠ Nous remercions mes parents **Francois NGAPGUE** et **Honorée JEULEFACK NGUEMO**, pour les valeurs nobles, la bienveillance et le soutien permanent tant moral que financier.

➠ Nous remercions les membres de ma famille (les grandes familles **NGAPGUE** et **JEULEFACK**) et mes amis qui m'ont encouragé et qui m'ont toujours aidé à garder l'équilibre.

➠ Nous remercions **l'ensemble des enseignants de l'ENS de Bertoua**, chacun en ce qui le concerne pour nous avoir apporté un plus dans sa discipline.

➠ Nous remercions **mes camarades de promotion** pour leur soutien moral durant ma formation.

➠ À tous ceux qui, **de près ou de loin m'ont soutenu financièrement ou moralement**, et dont nous n'avons pas pu citer les noms, nous vous disons **merci**.

Déclaration sur l'honneur

Le présent travail est une œuvre originale du candidat et n'a été soumis nulle part ailleurs, en partie ou en totalité, pour une autre évaluation académique. Les contributions externes ont été dûment mentionnées et recensées en bibliographie.

Signature du candidat

NGAPGUE TEGOMO Wilfried Dimitri

Résumé

Pour tout nombre premier p et pour tout entier naturel non nul w, un quasigroupe poynômial modulo p^w est l'ensemble $\{0; \cdots; p^w - 1\}$ muni d'une loi de composition interne $*$ définie par : $a*b := f(a,b)(\mathtt{mod}\ p^w)$, pour tout (a,b) dans $\{0; \cdots; p^w-1\}^2$, où $f : \mathbb{Z}^2 \to \mathbb{Z}$ est une permutation polynomiale à deux variables. D'une part, une caractérisation des quasigroupes polynomiaux modulo p^w est établie et d'autre part une transposition et une situation didactique du concept de "expression polynomiale" en classe de troisième sont examinées.

Mots-clés : Quasigroupe, Anneau des entiers modulo p^w, Polynôme, Fonction polynomiale.

Abstract

For any prime number p and for any positive integer w, a polynomial quasigroup modulo p^w est the set $\{0; \cdots; p^w - 1\}$ provided with an inner composition law $*$ defined as follows : $a * b := f(a, b)(\mathtt{mod}\ p^w)$, for any (a, b) in $\{0; \cdots; p^w - 1\}^2$, where $f : \mathbb{Z}^2 \to \mathbb{Z}$ is a polynomial permutation with two variables. On one hand, an characterization of polynomial quasigroups modulo p^w is established and the other hand a didactic transposition and situation of the concept of "polynomial expression" into form 4 are investigated.

Keywords : Quasigroup, Ring of integers modulo p^w, Polynomial, Polynomial function.

Table des matières

Introduction

Comment paver une surface carrée de côté n unités (n est un entier naturel supérieur à 2) avec n types de dalles carrées de côté **une** unité, de telle sorte que chaque dalle apparaisse exactement une fois dans chaque ligne et dans chaque colonne ? Pour le cas $n = 5$, une observation du tableau ci-dessous permet de se rendre compte que cette surface carrée de taille 5×5 est remplie à l'aide des couleurs 0 ; 1 ; 2 ; 3 et 4 de telle manière que chaque couleur apparaisse exactement une fois dans chaque ligne et dans chaque colonne.

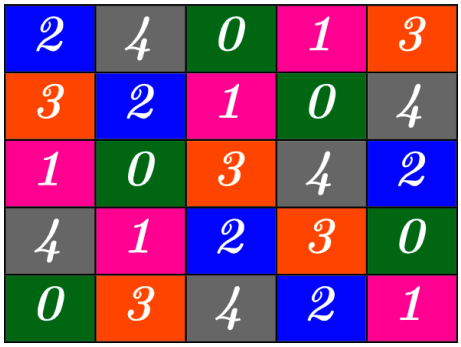


FIGURE 1: Un carré latin d'ordre 5

Ce tableau est appelé **carré latin** d'ordre 5. Un carré latin d'ordre n (n est un entier naturel supérieur à 2) est une matrice carrée de taille $n \times n$ dans laquelle chaque coefficient apparaît exactement une fois dans chaque ligne et dans chaque colonne. Le concept de carré latin a probablement commencé avec des problèmes au sujet du mouvement et la disposition des pièces sur un échiquier. Historiquement, les carrés latins sont des objets mathématiques fascinants, étudiés systématiquement pour la première fois par Leonhard Euler en 1782 (voir [5] et les références à cet égard). Depuis lors, de nombreux mathématiciens ont étudié leurs propriétés, et proposé différentes constructions des carrés latins [9]. La construction d'un carré latin est un problème important et intéressant en combinatoire algébrique.

Question : comment peut-on remplir les cases manquantes dans le tableau ci-dessous, à l'aide des éléments de l'ensemble $\{0; 1; 2; 3; 4\}$ de façon à obtenir un carré latin complet ?

	0	1		2
0		4		3
1			2	
	1			4
3		2	4	

Cette question peut sembler simple, mais elle est en fait assez complexe et fait l'objet de recherches actives en mathématiques. Lorsqu'on ajoute une première ligne et une première colonne au carré latin d'ordre n, on obtient la **table de Cayley** d'une loi composition interne $*$ sur $[|n|] := \{0; 1; \cdots; n-1\}$ ayant la **propriété de régularité** : *chaque élément de* $[|n|]$ *apparaît une et une seule fois dans chaque ligne et chaque colonne du carré latin*. Par exemple,

$*$	0	1	2	3	4
0	2	4	0	1	3
1	3	2	1	0	4
2	1	0	3	4	2
3	4	1	2	3	4
4	0	3	4	2	1

est la table de Cayley de la loi de composition interne $*$ sur $[|5|]$ associée au carré latin (Figure 1). En général, la table de Cayley de la loi $*$ sur $[|n|]$, est la table de valeurs de l'application $* : [|n|] \times [|n|] \to [|n|]$; la loi $*$ n'étant pas associative, non forcément commutative et ne possédant pas toujours un élément neutre.

Ce couple $([|n|]; *)$ dont la loi $*$ est régulière, est appelé **quasigroupe** d'ordre n. S'il existe $f : \mathbb{Z}^2 \to \mathbb{Z}$ une fonction polynomiale à deux variables telle que la loi de composition interne $*$ est définie comme suit : $a * b := f(a, b) (\mathtt{mod}\ p^w)$, l'opération $*$ est qualifié de **polynomial**.

Étant donné $\star : [|p^w|] \times [|p^w|] \to [|p^w|]$ une opération polynomiale modulo p^w, notre problématique est d'établir une **condition nécessaire et suffisante** sur $\star$ pour que $([|p^w|]; \star)$ soit un quasigroupe. De cette problématique ressort une question de recherche celle de savoir étant donné une fonction polynomiale $f : \mathbb{Z}^2 \to \mathbb{Z}$, la condition pour qu'elle définisse un quasigroupe polynomial modulo p^w donné. Dans la littérature, les permutations polynomiales (qui nous permettront de caract) sur $\mathbb{Z}_n$ ont été abondamment étudiées (voir [3, 7, 8]).

Dans la littérature, les permutations polynomiales (qui nous permettront cette caractérisation) sur $\mathbb{Z}_n$ ont été abondamment étudiées (voir [3, 7, 8]).

Pour établir cette caractérisation, ce mémoire s'organise autour de trois chapitres. Notamment, le chapitre 1 aborde quelques matériaux. Ensuite, le chapitre 2 propose une caractérisation des quasigroupes polynomiaux à partir de l'anneau des entiers modulo p^w. Enfin, le chapitre 3 étudie l'enseignement des expressions polynomiales en classe de 3ième de l'enseignement secondaire général au Cameroun.

★ ★ **Chapitre Un** ★ ★

Applications polynomiales à d variable(s) sur l'anneau $\mathbb{Z}_n$

Soient n et s deux entiers naturels non nuls et $[|s|] := \{0; 1; \cdots; s-1\}$. Le poids de tout élément $\underline{\mathbf{j}} := (j_1, \cdots, j_d)$ dans $\mathbb{N}^d$ est $|\underline{\mathbf{j}}| := j_1 + j_2 + \cdots + j_d$. L'ensemble $R[X_1, \cdots, X_d]$ des polynômes sur un anneau R à d indéterminée(s) $X_1, \cdots, X_d$, est :

$$R[X_1, \cdots, X_d] := \left\{ \sum_{\underline{\mathbf{j}}:=(j_1,\cdots,j_d)\in[|k|]^d} a_{\underline{\mathbf{j}}} X_1^{j_1} \cdots X_d^{j_d} \ : \ (\exists k \in \mathbb{N})(\forall |\underline{\mathbf{j}}| < k)(\exists a_{\underline{\mathbf{j}}} \in R) \right\}.$$

Cet ensemble $R[X_1, \cdots, X_d]$ a une structure d'anneau. Étant donné P dans $R[X_1, \cdots, X_d]$, il existe s dans $\mathbb{N}$ tel que

$$P = \sum_{\underline{\mathbf{j}}:=(j_1,\cdots,j_d)\in[|s|]^d} a_{\underline{\mathbf{j}}} X_1^{j_1} \cdots X_d^{j_d}.$$

Le support de P, noté $\mathtt{Supp}(P)$, est défini comme : $\mathtt{Supp}(P) := \{\underline{\mathbf{j}} \in \mathbb{N}^d \ : \ a_{\underline{\mathbf{j}}} \neq 0\}$, et son degré, noté $\mathtt{deg}(P)$, est défini comme : $\mathtt{deg}(P) := \max\{|\underline{\mathbf{j}}| \ : \ \underline{\mathbf{j}} \in \mathtt{Supp}(P)\}$. Dans ce chapitre, $\mathbb{Z}_n$ désigne l'anneau des entiers modulo n, où $n := p^w \geq 2$ avec p un nombre premier et w un entier naturel non nul.

L'ensemble $\mathcal{A}(n; d)$ des applications de $(\mathbb{Z}_n)^d$ dans $\mathbb{Z}_n$, a une structure d'anneau unitaire avec l'addition et de la multiplication point par point. L'application

$$\begin{array}{rccccc} \Phi_{n,d} : & \mathbb{Z}[X_1, \cdots, X_d] & \to & \mathcal{A}(n; d) & & \\ & P & \mapsto & \widetilde{P} : & (\mathbb{Z}_n)^d & \to & \mathbb{Z}_n \\ & & & & (a_1, \cdots, a_d) & \mapsto & \widetilde{P}(a_1, \cdots, a_d) \ (\mathtt{mod}\, n) \end{array} \tag{1.1}$$

est un morphisme d'anneaux. On note $\mathtt{Im}(\Phi_{n,d})$ l'image de $\Phi_{n,d}$ et $\mathtt{Ker}(\Phi_{n,d})$ le Kernel de $\Phi_{n,d}$. L'ensemble des **applications polynomiales à d variable(s) sur** $\mathbb{Z}_n$ est $\mathtt{Im}(\Phi_{n,d})$ et l'ensemble des **polynômes nuls à d variable(s) sur** $\mathbb{Z}_n$ est $\mathtt{Ker}(\Phi_{n,d})$. Bien sûr, $\mathtt{Im}(\Phi_{n,d})$ est un sous-anneau de $\mathcal{A}(n; d)$, et $\mathtt{Ker}(\Phi_{n,d})$ est un idéal de l'anneau $\mathbb{Z}[X_1, \cdots, X_d]$. Cette section étudie $\mathtt{Ker}(\Phi_{n,d})$

et caractérise $\mathtt{Im}(\Phi_{n,d})$.

1.1 Applications à d variables à valeurs entières

Les éléments de $\mathbb{N}^d$ sont appelés d-**indices**. Soit $x_1, x_2, \cdots, x_d$ les d variables correspondants respectivement aux indéterminées $X_1, X_2, \cdots, X_d$. Désignons $\mathcal{A}(\mathbb{Q}^d, \mathbb{Q})$ l'ensemble des applications de $\mathbb{N}^d$ dans $\mathbb{Q}$. Nous aurons besoin de $\leq$, la relation ordre partiel sur $\mathbb{Q}^d$ définie par : $\underline{\mathbf{k}} \leq \underline{\mathbf{r}}$, si pour tout $1 \leq i \leq d$, $k_i \leq r_i$.

Notation **1.** *Soit* $\underline{\boldsymbol{k}} := (k_1, k_2, \cdots, k_d) \in \mathbb{N}^d$ *et* $\vec{\boldsymbol{x}} := (x_1, x_2, \cdots, x_d) \in \mathbb{Q}^d$.

• **Multipuissance :** $\vec{\boldsymbol{x}}^{\underline{\boldsymbol{k}}} := \prod_{i=1}^{d} x_i^{k_i}$.

• **Multifactorielle :** $\underline{\boldsymbol{k}}! := k_1!k_2!\cdots k_d!$ *et* $\mathrm{A}_{\vec{\boldsymbol{x}}}^{\underline{\boldsymbol{k}}} := \prod_{i=1}^{d} \mathrm{A}_{x_i}^{k_i}$, *où* $\mathrm{A}_{x_i}^{k_i} := \begin{cases} \prod_{t=1}^{k_i}(x_i - t + 1), & \text{si } \underline{\boldsymbol{k}} \leq \vec{\boldsymbol{x}} ; \\ 0, & \text{sinon.} \end{cases}$

Exemple **1.** *Prenons* $d = 2$ *et* $\underline{\boldsymbol{k}} := (2, 3)$. *Pour tout* $\vec{\boldsymbol{x}} := (x, y)$ *dans* $\mathbb{N}^2$, *on a :*

$$\frac{\mathrm{A}_{\vec{\boldsymbol{x}}}^{\underline{\boldsymbol{k}}}}{2!3!} = \begin{cases} \frac{\mathrm{A}_x^2}{2!} \cdot \frac{\mathrm{A}_y^3}{3!} = \frac{xy(x-1)(y-1)(y-2)}{12}, & \text{si } (x, y) \geq (2, 3) ; \\ 0, & \text{sinon.} \end{cases}$$

Définition 1.1.1

Une application $f : \mathbb{Q}^d \to \mathbb{Q}$ est **une application à valeurs entières**, si pour tout $(x_1, x_2, \cdots, x_d)$ dans $\mathbb{Z}^d$, on a : $f(x_1, x_2, \cdots, x_d) \in \mathbb{Z}$.

Par exemple, les applications polynomiales à coefficients dans $\mathbb{Z}$ sont à valeurs entières.

Proposition 1.1.1

Soit $\underline{\mathbf{k}}$ dans $\mathbb{N}^d$. Alors la $\underline{\mathbf{k}}$-multicombinaison $\mathrm{C}_{\underline{\mathbf{k}}} : \mathbb{Q}^d \to \mathbb{Q}$ définie par $\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} := \frac{\mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}}}{\underline{\mathbf{k}}!}$, est une application polynomiale à valeurs entières.

Preuve. Prenons $\vec{x} = (x_1, x_2, \cdots, x_d)$ dans $\mathbb{Z}^d$ et $k = (k_1, k_2, \cdots, k_d)$ dans $\mathbb{Z}^d$.
S'il existe un x_i ou un k_i négatif, ou encore si $x_i < k_i$ pour un certain $1 \leq i \leq d$ alors $\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} = 0$. Ce qui entraine la véracité de la proposition.

Supposons maintenant que tous les x_i et k_i appartiennent à $\mathbb{N}$ et que tous les $x_i \geq k_i$ pour tout i allant de 1 à d. Montrons que $\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} \in \mathbb{Z}$. On a :

$$\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} = \frac{\mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}}}{\underline{\mathbf{k}}!} = \frac{\prod_{i=1}^{d} \mathrm{A}_{x_i}^{k_i}}{\prod_{i=1}^{d} k_i!} = \prod_{i=1}^{d} \mathrm{C}_{x_i}^{k_i}.$$

Or, on montre facilement par récurrence sur x que $\mathrm{C}_x^k \in \mathbb{N}$, pour tout $(k; x) \in \mathbb{N}^2$. Ainsi, pour tout $1 \leq i \leq d$; $\mathrm{C}_{x_i}^{k_i} \in \mathbb{N} \subset \mathbb{Z}$. C'est-à-dire pour tout $1 \leq i \leq d$; $\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} = \prod_{i=1}^{d} \mathrm{C}_{x_i}^{k_i} \in \mathbb{Z}$.

D'où la $\underline{\mathbf{k}}$-multicombinaison $\mathrm{C}^{\underline{\mathbf{k}}} : \mathbb{Q}^d \to \mathbb{Q}$ définie par $\mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} := \frac{\mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}}}{\underline{\mathbf{k}}!}$, est une application polynomiale à valeurs entières. ■

Pour tout $1 \leq i \leq d$, posons $\vec{\mathbf{e}}_i := (0, \cdots, 0, 1, 0, \cdots, 0) \in \mathbb{N}^d$, avec le 1 à la i-ème position, et 0 ailleurs. Pour tout $1 \leq i \leq d$, la différentielle partielle Δ_i est définie de la manière suivante :

$$\begin{array}{rccccc} \Delta_i : & \mathcal{A}(\mathbb{Q}^d, \mathbb{Q}) & \to & \mathcal{A}(\mathbb{Q}^d, \mathbb{Q}) & & \\ & g & \mapsto & \Delta_i g : & \mathbb{Q}^d \to & \mathbb{Q} \\ & & & & \vec{\mathbf{x}} \mapsto & g(\vec{\mathbf{x}} + \vec{\mathbf{e}}_i) - g(\vec{\mathbf{x}}) \end{array} \tag{1.2}$$

où Δ_i^0 est l'application identité, et pour tout entier naturel k on a : $\Delta_i^k := \Delta_i \circ \Delta_i^{k-1}$. Pour un d-indice $\underline{\mathbf{k}} := (k_1, \cdots, k_d)$, posons $\Delta^{\underline{\mathbf{k}}} := \Delta_1^{k_1} \circ \cdots \circ \Delta_d^{k_d}$. Ainsi, pour tout $(\underline{\mathbf{r}}, \underline{\mathbf{k}})$ dans $(\mathbb{N}^d)^2$, on vérifie facilement par récurrence que

$$\Delta^{\underline{\mathbf{r}}} \vec{\mathbf{x}}^{\underline{\mathbf{k}}} = \begin{cases} \mathrm{A}_{\underline{\mathbf{k}}}^{\underline{\mathbf{r}}} \cdot \vec{\mathbf{x}}^{\underline{\mathbf{k}}-\underline{\mathbf{r}}} & \text{si } \underline{\mathbf{r}} \leq \underline{\mathbf{k}} ; \\ 0 & \text{sinon,} \end{cases} \quad \text{et} \quad \Delta^{\underline{\mathbf{r}}} \mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} = \begin{cases} \mathrm{C}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}-\underline{\mathbf{r}}} & \text{si } \underline{\mathbf{r}} \leq \underline{\mathbf{k}} ; \\ 0 & \text{sinon.} \end{cases} \tag{1.3}$$

Proposition 1.1.2

Soit g dans $\mathcal{A}(\mathbb{Q}^d, \mathbb{Q})$ et $(\vec{\mathbf{x}}, \underline{\mathbf{k}})$ dans $\mathbb{Z}^d \times \mathbb{N}^d$. Alors $\Delta^{\underline{\mathbf{k}}} g(\vec{\mathbf{x}}) = \sum_{\underline{\mathbf{j}} \leq \underline{\mathbf{k}}} (-1)^{|\underline{\mathbf{j}}|} \left(\frac{g(\vec{\mathbf{x}}+\underline{\mathbf{k}}-\underline{\mathbf{j}})}{\underline{\mathbf{j}}!} \right) \mathrm{A}_{\underline{\mathbf{k}}}^{\underline{\mathbf{j}}}$, et

$$g(\vec{\mathbf{x}}) = \sum_{\underline{\mathbf{j}} \leq \vec{\mathbf{x}}} \left(\frac{\Delta^{\underline{\mathbf{j}}} g(\vec{\mathbf{0}})}{\underline{\mathbf{j}}!} \right) \mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{j}}}. \tag{1.4}$$

Preuve. Pour tout $\underline{\mathbf{k}}$ dans $\mathbb{N}^d$, on a :

$$\begin{aligned}
\Delta_i^{k_i} g(\vec{\mathbf{x}}) &= \Delta_i^{k_i-1} g(\vec{\mathbf{x}} + \vec{\mathbf{e}}_i) - \Delta_i^{k_i-1} g(\vec{\mathbf{x}}); \\
&= \left(\Delta_i^{k_i-2} g(\vec{\mathbf{x}} + 2\vec{\mathbf{e}}_i) - \Delta_i^{k_i-2} g(\vec{\mathbf{x}} + \vec{\mathbf{e}}_i)\right) - \left(\Delta_i^{k_i-2} g(\vec{\mathbf{x}} + \vec{\mathbf{e}}_i) - \Delta_i^{k_i-2} g(\vec{\mathbf{x}})\right); \\
&\vdots \\
&= \sum_{j=0}^{k_i} (-1)^j g(\vec{\mathbf{x}} + (k_i - j)\vec{\mathbf{e}}_i) \complement_{k_i}^{j}.
\end{aligned}$$

Comme l'opérateur Δ est $\mathbb{Q}$-linéaire, et $\Delta^{\underline{\mathbf{i}}} \circ \Delta^{\underline{\mathbf{j}}} = \Delta^{\underline{\mathbf{i}}+\underline{\mathbf{j}}}$, pour tout $(\underline{\mathbf{i}}, \underline{\mathbf{j}})$ dans $\mathbb{N}^d$, il résulte que

$$\begin{aligned}
\Delta^{\underline{\mathbf{k}}} g(\vec{\mathbf{x}}) &= \Delta_1^{k_1} \circ \cdots \circ \Delta_d^{k_d} g(\vec{\mathbf{x}}); \\
&= \sum_{j_1}^{k_1} \cdots \sum_{j_d}^{k_d} (-1)^{j_1+\cdots+j_d} \prod_{i=1}^{d} g(\vec{\mathbf{x}} + \sum_{t=1}^{d} (k_t - j_t)\vec{\mathbf{e}}_t) \complement_{k_i}^{j_i}; \\
&= \sum_{\underline{\mathbf{j}} \leq \underline{\mathbf{k}}} (-1)^{|\underline{\mathbf{j}}|} g(\vec{\mathbf{x}} + \underline{\mathbf{k}} - \underline{\mathbf{j}}) \complement_{\underline{\mathbf{k}}}^{\underline{\mathbf{j}}}.
\end{aligned}$$

Finalement, pour tout $\vec{\mathbf{x}}$ dans $\mathbb{N}^d$, il résulte que $g(\vec{\mathbf{x}}) = \sum_{\underline{\mathbf{j}} \leq \vec{\mathbf{x}}} \Delta^{\underline{\mathbf{j}}} g(\vec{\mathbf{0}}) \complement_{\vec{\mathbf{x}}}^{\underline{\mathbf{j}}}$. ■

Remarque. *Soit $g : \mathbb{Q}^d \to \mathbb{Q}$ une application. Il résulte que*

1. *D'après (1.4), $g : \mathbb{Z}^d \to \mathbb{Q}$ est une application polynomiale à d variable(s) sur $\mathbb{Z}$.*
2. *D'après (1.3), si $\Delta^{\underline{j}} g(\vec{\mathbf{0}}) = 0$ alors $\underline{j} \notin \mathsf{Supp}(P)$, où P est un polynôme sur $\mathbb{Z}$ à d indéterminée(s) de degré k associé à g. De plus,*

$$g(\vec{x}) = \sum_{|\underline{j}| \leq k} \left(\frac{\Delta^{\underline{j}} g(\vec{\mathbf{0}})}{\underline{j}!} \right) \mathrm{A}_{\vec{x}}^{\underline{j}}.$$

Lemme 1.1.1

Soit $g : \mathbb{Q}^d \to \mathbb{Q}$ une application polynomiale associée à un polynôme P sur $\mathbb{Z}$ à d indéterminée(s) de degré k. Les assertions suivantes sont équivalentes.

1. g est à valeurs entières.
2. pour tout $\underline{\mathbf{j}}$ dans $\mathsf{Supp}(P)$, on a : $\underline{\mathbf{j}}!$ divise $\Delta^{\underline{\mathbf{j}}} g(\vec{\mathbf{0}})$.

Preuve. Soit $g(\vec{\mathbf{x}}) = \sum_{|\underline{\mathbf{j}}|\leq k} a_{\underline{\mathbf{j}}}\vec{\mathbf{x}}^{\underline{\mathbf{j}}}$. D'après (1.3), on a :

$$\begin{aligned}\Delta^{\underline{\mathbf{r}}}g(\vec{\mathbf{0}}) &= \left(\sum_{|\underline{\mathbf{j}}|\leq k} a_{\underline{\mathbf{j}}}\Delta^{\underline{\mathbf{r}}}\vec{\mathbf{x}}^{\underline{\mathbf{j}}}\right)_{\vec{\mathbf{x}}=\vec{\mathbf{0}}};\\ &= \left(\sum_{|\underline{\mathbf{j}}|\leq k} a_{\underline{\mathbf{j}}}\mathrm{A}^{\underline{\mathbf{r}}}_{\underline{\mathbf{j}}}\cdot\vec{\mathbf{x}}^{\underline{\mathbf{j}}-\underline{\mathbf{r}}}\right)_{\vec{\mathbf{x}}=\vec{\mathbf{0}}};\\ &= \underline{\mathbf{j}}!a_{\underline{\mathbf{j}}}.\end{aligned}$$

Ainsi, si g est à valeurs entières alors pour tout $\underline{\mathbf{j}}$ dans $\mathtt{Supp}(P)$, on a : $\underline{\mathbf{j}}!$ divise $\Delta^{\underline{\mathbf{j}}}g(\vec{\mathbf{0}})$.
Réciproquement, si pour tout $|\underline{\mathbf{i}}| \leq k$, $a_{\underline{\mathbf{i}}} \in \mathbb{Z}$; d'après la proposition (1.1.1), la $\underline{\mathbf{i}}$-multicombinaison $\mathrm{C}^{\underline{\mathbf{i}}}_{\vec{\mathbf{x}}}$ est à valeurs entières. Par conséquent, g est à valeurs entières. ■

Exemple 2. *Soit $g : \mathbb{Q}^2 \to \mathbb{Q}$ tel que $g(x,y) := 3 + x + 2x^2y + y^2$. Alors $P := 3 + X + 2X^2Y + Y^2$ est un polynôme associé à g. Ainsi $\mathtt{Supp}(P) = \{(0,0),(1,0),(2,1),(0,2)\}$. Pour tout $\underline{\boldsymbol{k}} := (i,j) \leq (2,2)$ et pour tout $\vec{\boldsymbol{x}} := (x,y)$, on dresse le tableau suivant :*

$\underline{\boldsymbol{k}}$:=(i,j)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
$\mathrm{A}^{\underline{\boldsymbol{k}}}_{\vec{\boldsymbol{x}}}$	1	y	$y(y-1)$	x	xy	$xy(y-1)$	$x(x-1)$	$xy(x-1)$	$xy(x-1)(y-1)$
$\frac{\Delta^{\underline{\boldsymbol{k}}}g(\vec{\boldsymbol{0}})}{\underline{\boldsymbol{k}}!}$	3	1	1	1	2	0	0	2	0
$\left(\frac{\Delta^{\underline{\boldsymbol{k}}}g(\vec{\boldsymbol{0}})}{\underline{\boldsymbol{k}}!}\right)\mathrm{A}^{\underline{\boldsymbol{k}}}_{\vec{\boldsymbol{x}}}$	3	y	$y(y-1)$	x	$2xy$	0	0	$2xy(x-1)$	0

Ainsi, on vérifie que : $3+y+y(y-1)+x+2xy+0+0+2xy(x-1)+0 = 3+x+2x^2y+y^2 = g(x,y)$.

1.2 Applications polynomiales modulo n

L'application

$$\begin{array}{rccc}\iota : & [|n|] & \to & \mathbb{Z}_n\\ & x & \mapsto & \bar{x} := x + n\mathbb{Z}\end{array} \tag{1.5}$$

est bijective. Ainsi, les éléments de $\mathbb{Z}_n$ s'identifient à $[|n|]$ via la bijection ι ainsi définie en (1.5). De plus, pour toute application $f : (\mathbb{Z}_n)^d \to \mathbb{Z}_n$, il existe une application polynomiale $g : \mathbb{Z}^d \to \mathbb{Z}$ telle que pour tout $\vec{\mathbf{x}}$ dans $[|n|]^d$,

$$f(\vec{\mathbf{x}}) = g(\vec{\mathbf{x}}) \bmod n. \tag{1.6}$$

Pour tout $1 \leq i \leq d$, posons

$$\Gamma_i := \prod_{k=0}^{n-1}(X_i - k). \tag{1.7}$$

On vérifie que $\deg(\Gamma_i) = n$ et $\Gamma_i \in \mathtt{Ker}(\Phi_{n,d})$. Comme Γ_i sont des polynômes unitaires, en effectuant la division euclidienne de P par Γ_i, on se rend compte qu'il suffit de prendre P tel que $\deg(P) < n$. Pour le reste de ce mémoire, nous supposerons sans nuire à la généralité que $\deg(P) < n$. Ainsi, pour tout $\vec{\mathbf{x}} := (x_1, x_2, \cdots, x_d)$ dans $[|n|]^d$, nous avons :

$$\begin{aligned} f(\vec{\mathbf{x}}) &\overset{\text{by (1.6)}}{=} g(\vec{\mathbf{x}}) \bmod n; \\ &\overset{\text{by (1.4)}}{=} \sum_{|\underline{\mathbf{k}}|<n} \left(\frac{\Delta^{\underline{\mathbf{k}}} g(\vec{\mathbf{0}})}{\underline{\mathbf{k}}!} \right) \mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}} \bmod n; \\ &\overset{\text{by (1.6)}}{=} \underbrace{\sum_{|\underline{\mathbf{k}}|<n} \left(\frac{\Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}})}{\underline{\mathbf{k}}!} \right) \mathrm{A}_{\vec{\mathbf{x}}}^{\underline{\mathbf{k}}}}_{=:h(\vec{\mathbf{x}})}. \end{aligned}$$

On peut se rendre compte que l'application polynomiale h représente f, mais h n'a pas nécessairement des coefficients entiers. Cependant, d'après Lemme 1.1.1 et en exploitant le fait que dans $\mathbb{Z}_n$,

$$\Delta^{\underline{\mathbf{k}}} g(\vec{\mathbf{0}}) \bmod n = \Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}})$$

est vrai pour tout $\underline{\mathbf{k}}$ dans $\mathbb{N}^d$, nous obtenons le lemme suivant :

Lemme 1.1.2

Si $f : (\mathbb{Z}_n)^d \to \mathbb{Z}_n$ est une application polynomiale, alors pour tout $\underline{\mathbf{k}}$ tel que $|\underline{\mathbf{k}}| < n$, il existe $\alpha_{\underline{\mathbf{k}}}$ dans $\mathbb{Z}$ tel que $\underline{\mathbf{k}}!$ divise $\Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}}) + \alpha_{\underline{\mathbf{k}}} n$. De plus,

$$\mathtt{pgcd}(n, \underline{\mathbf{k}}!) \ \text{ divise } \ \Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}}) \tag{1.8}$$

pour tout $\underline{\mathbf{k}}$ avec $|\underline{\mathbf{k}}| < n$.

Si la condition (1.8) est satisfaite pour f, pour tout $\underline{\mathbf{k}}$, nous cherchons l'entier $\beta_{\underline{\mathbf{k}}}$ tel que

$$\beta_{\underline{\mathbf{k}}} - \Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}}) \in n\mathbb{Z},$$

et comme ci-dessus au lemme (1.1.2(i)) $\underline{\mathbf{k}}!$ divise $\beta_{\underline{\mathbf{k}}}$. D'où,

$$f(\vec{\mathbf{x}}) = \sum_{|\underline{\mathbf{k}}|<n} \frac{\beta_{\underline{\mathbf{k}}}}{\underline{\mathbf{k}}!} \cdot \mathrm{A}^{\underline{\mathbf{k}}}_{\vec{\mathbf{x}}} \bmod n,$$

pour tout $\vec{\mathbf{x}} \in [|n|]^d$. En d'autres termes, la condition (1.8) implique que f est une application polynomiale sur $\mathbb{Z}_n$ et nous avons la caractérisation suivante :

Théorème 1.1.1

Une application $f : (\mathbb{Z}_n)^d \to \mathbb{Z}_n$ est polynomiale si et seulement si pour tout $\underline{\mathbf{k}}$ avec $|\underline{\mathbf{k}}| < n$, on a : $\mathtt{pgcd}(n, \underline{\mathbf{k}}!)$ divise $\Delta^{\underline{\mathbf{k}}} f(\vec{\mathbf{0}})$.

Le résultat suivant est immédiat.

Corollaire 1.1.3

L'entier naturel n est premier si et seulement si $\mathtt{Im}(\Phi_{n,d}) \subseteq \mathcal{A}(n; d)$.

Lorque $n = 2$, on montre qu'il y a une bijection entre $\mathcal{A}(2; d)$ et l'ensemble des tables de vérité à d entrées.

Définition 1.1.2

Soit a un élément de $[|n|]$ et $\underline{\mathbf{k}} := (k_1, \cdots, k_d) \in \mathbb{N}^d$. Le monôme $aX_1^{k_1} \cdots X_d^{k_d}$ est **réductible modulo** n, s'il existe un polynôme P dans $\mathbb{Z}[X_1, \cdots, X_d]$ tels que $\mathtt{deg}(P) < |\underline{\mathbf{k}}|$ et $\Phi_{n,d}(aX_1^{k_1} \cdots X_d^{k_d}) = \Phi_{n,d}(P)$.

Exemple 3. *Prenons $d = 1$ et $n = p$ où p est un nombre premier. Le monôme X^p est réduit modulo p au polynôme X. En effet, p étant un nombre premier, d'après le petit théorème de Fermat, pour tout x dans $\mathbb{Z}_p$, on a : $x^p - x \equiv 0 (mod p)$.* ○

Lemme 1.1.3

Soit a un élément de $[|n|]$ et $\underline{\mathbf{k}} := (k_1, \cdots, k_d) \in \mathbb{N}^d$. Alors $aX_1^{k_1} \cdots X_d^{k_d}$ est réductible modulo n, si et seulement si n divise $a \cdot \underline{\mathbf{k}}!$

Preuve. Soit a un élément de $[|n|]$ et $\underline{\mathbf{k}} := (k_1, \cdots, k_d) \in \mathbb{N}^d$.

$\Rightarrow$) Supposons que le polynôme P réduit modulo n le monôme $aX_1^{k_1} \cdots X_d^{k_d}$ dans $\mathbb{Z}[X_1, \cdots, X_d]$. De là, $Q := aX_1^{k_1} \cdots X_d^{k_d} - P \in \mathtt{Ker}(\Phi_{n,d})$. Alors nous écrivons $q := \Phi_{n,d}(Q)$ dans la forme

$$q(\vec{\mathbf{x}}) = \sum_{\substack{\underline{\mathbf{r}} \in \mathbb{N}^d \\ |\underline{\mathbf{r}}| \leq |\underline{\mathbf{k}}|}} q_{\underline{\mathbf{r}}} \vec{\mathbf{x}}^{\underline{\mathbf{r}}}, \tag{1.9}$$

où $q_{\underline{\mathbf{r}}} \in \mathbb{Z}_n$ avec $q_{\underline{\mathbf{k}}} = a$. En utilisant la linéarité de l'opérateur Δ, nous avons obtenu que,

$$0 = \Delta^{\underline{\mathbf{k}}} q(\vec{\mathbf{x}}) \overset{(1.9)}{=} \sum_{\substack{\underline{\mathbf{r}} \in \mathbb{N}^d \\ |\underline{\mathbf{r}}| \leq |\underline{\mathbf{k}}|}} q_{\underline{\mathbf{r}}} \Delta^{\underline{\mathbf{k}}} \vec{\mathbf{x}}^{\underline{\mathbf{r}}} \overset{(1.3)}{=} a \cdot \underline{\mathbf{k}}!.$$

En effet, tous les termes dans la somme ci-dessus avec $\underline{\mathbf{r}} \neq \underline{\mathbf{k}}$ s'annulent d'après (1.3), puisque $|\underline{\mathbf{r}}| \leq |\underline{\mathbf{k}}|$ et $\underline{\mathbf{r}} \neq \underline{\mathbf{k}}$ alors, $\underline{\mathbf{k}} \notin \mathtt{Supp}(\vec{\mathbf{x}}^{\underline{\mathbf{r}}})$. Et l'unique terme restant, $\Delta^{\underline{\mathbf{k}}} \vec{\mathbf{x}}^{\underline{\mathbf{k}}}$, égale $\underline{\mathbf{k}}!$, encore d'après (1.3).

$\Leftarrow$) Supposons que n divise $a \cdot \underline{\mathbf{k}}!$. Alors, le polynôme

$$Q := a \prod_{i=1}^{d} \prod_{l=1}^{k_i} (X_i + l).$$

Alors $\Phi_{n,d}(Q) = q(\vec{\mathbf{x}}) = a\underline{\mathbf{k}}! \mathbb{C}^{\underline{\mathbf{k}}}_{\vec{\mathbf{x}}+\underline{\mathbf{k}}} \in \mathtt{Ker}(\Phi_{n,d})$, puisque n divise $a \cdot \underline{\mathbf{k}}!$. Comme $\mathtt{deg}(Q) = |\underline{\mathbf{k}}| > \mathtt{deg}\left(Q - aX_1^{k_1} \cdots X_d^{k_d}\right)$, donc $Q - aX_1^{k_1} \cdots X_d^{k_d}$ se réduit à $aX_1^{k_1} \cdots X_d^{k_d}$.

■

Lemme 1.1.3 permet de compter le nombre de monômes $X_1^{k_1} \cdots X_d^{k_d}$ irréductibles modulo n, où $\underline{\mathbf{k}} := (k_1, \cdots, k_d) \in \mathbb{N}^d$. Posons

$$S_d(n) := \left\{ \underline{\mathbf{k}} \in \mathbb{N}^d \ : \ n \nmid \underline{\mathbf{k}}! \right\}, \tag{1.10}$$

l'ensemble des d-indices $\underline{\mathbf{k}}$ tels que $\vec{\mathbf{x}}^{\underline{\mathbf{k}}}$ soit irréductible.

Exemple 4. *Déterminons $S_d(2^i)$ pour $d \in \{1; 2\}$ et $i \in \{1; 2; 3\}$.*

- *Pour $d = 1$, on a : $S_1(2) = \{0; 1\}$ et $S_1(4) = S_1(8) = \{0, 1, 2, 3\}$.*
- *Pour $d = 2$, on a : $S_2(2) = \{(0; 0); (0; 1); (1; 0); (1; 1)\}$ et*

$$S_2(4) = \{(0; 0); (0; 1); (0; 2); (0; 3); (1; 0); (1; 1); (1; 2); (1; 3); (2; 0); (2; 1); (3; 0); (3; 1)\}.$$

Le tableau suivant donne $s_d(n)$ pour quelques premières valeurs de d et n, où $s_d(n) := |S_d(n)|$.

n	1	2	3	4	5	6	7	8	9
s_1	0	2	3	4	5	3	7	4	6
s_2	0	4	9	12	25	9	49	16	27
s_3	0	8	27	32	125	27	343	56	108
s_4	0	16	81	80	625	81	2401	176	405

Table 1 : Valeurs de $s_d(n)$.

Théorème 1.1.2

Toute application polynomiale $f : (\mathbb{Z}_{p^w})^d \to \mathbb{Z}_{p^w}$ a une unique représentation de la forme

$$f(\vec{\mathbf{x}}) = \sum_{i=1}^{w} p^{w-i} \left(\sum_{\underline{\mathbf{k}} \in S_d(p^i)} \alpha_{\underline{\mathbf{k}}}(i) \vec{\mathbf{x}}^{\underline{\mathbf{k}}} \right), \tag{1.11}$$

où $0 \leq \alpha_{\underline{\mathbf{k}}}(i) < p$.

Preuve. Il est commun d'écrire $n = \prod p^{\nu_p(n)}$ pour la décomposition en produits de facteurs premiers d'un entier n. Nous adoptons cette notation et on écrit

$$\nu_p(\underline{\mathbf{k}}!) = \max\{x \in \mathbb{N} \ : \ p^x \text{ divise } \underline{\mathbf{k}}!\}$$

pour le nombre de facteur p dans $\underline{\mathbf{k}}!$. Noter que $\nu_p(\underline{\mathbf{k}}!) < i$ si et seulement si $\underline{\mathbf{k}} \in S_d(p^i)$. Ainsi, comme conséquence immédiate du lemme 1.1.3, toute application polynomiale f à d variables sur $\mathbb{Z}_{p^w}$ a une unique représentation sous la forme

$$f(\vec{\mathbf{x}}) = \sum_{\substack{\underline{\mathbf{k}} \in \mathbb{N}^d \\ \nu_p(\underline{\mathbf{k}}!) < w}} \alpha_{\underline{\mathbf{k}}} \vec{\mathbf{x}}^{\underline{\mathbf{k}}}, \tag{1.12}$$

où $0 \leq \alpha_{\underline{\mathbf{k}}} < p^{w-\nu_p(\underline{\mathbf{k}}!)}$. Puisque d'autre part tout nombre $0 \leq \alpha_{\underline{\mathbf{k}}} < p^{w-\nu_p(\underline{\mathbf{k}}!)}$ a une unique représentation sous la forme

$$\alpha_{\underline{\mathbf{k}}} = \sum_{i=1}^{w} p^{w-i} \alpha_{\underline{\mathbf{k}}}(i),$$

pour certains coefficients $0 \leq \alpha_{\underline{\mathbf{k}}}(i) < p$, nous pouvons réécrire (1.12) de telle sorte que l'on obtienne le second membre de l'égalité (1.11). ■

Exemple 5. *Soit $f : (\mathbb{Z}_{p^w})^d \to \mathbb{Z}_{p^w}$ une application polynomiale.*

- *Pour $p = 2$, $w = 3$ et $d = 1$, nous avons $n = 8$. Ainsi, l'application polynomiale d'une variable $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ a une unique représentation de la forme :*

$$\begin{aligned} f(x) &= \sum_{i=1}^{3} 2^{3-i}\left(\sum_{k\in S_1(2^i)} \alpha_k(i)x^k\right); \\ &= 2^2\left(\sum_{k\in S_1(2)} \alpha_k(1)x^k\right) + 2^1\left(\sum_{k\in S_1(4)} \alpha_k(2)x^k\right) + 2^0\left(\sum_{k\in S_1(8)} \alpha_k(3)x^k\right); \\ &= 4\left(\alpha_0(1) + \alpha_1(1)x^1\right) + 2\left(\alpha_0(2) + \alpha_1(2)x^1 + \alpha_2(2)x^2 + \alpha_3(2)x^3\right) \\ &\quad + \left(\alpha_0(3) + \alpha_1(3)x^1 + \alpha_2(3)x^2 + \alpha_3(3)x^3\right); \\ &= [4\alpha_0(1) + 2\alpha_0(2) + \alpha_0(3)] + [4\alpha_1(1) + 2\alpha_1(2) + \alpha_1(3)]\, x + [2\alpha_2(2) + \alpha_2(3)]\, x^2 \\ &\quad + [\alpha_3(2) + \alpha_3(3)]\, x^3, \quad \text{où} \quad \alpha_i(j) \in \{0; 1\}. \end{aligned}$$

- *Pour $p = w = 2$ et $d = 2$, nous avons $n = 4$. Ainsi, l'application polynomiale de deux variables $f : (\mathbb{Z}_4)^2 \to \mathbb{Z}_4$ a une unique représentation de la forme :*

$$\begin{aligned} f(x,y) &= 2^1\left(\sum_{(s,t)\in S_2(2)} \alpha_{\underline{k}}(1)x^s y^t\right) + 2^0\left(\sum_{(s,t)\in S_2(4)} \alpha_{(s,t)}(2)x^s y^t\right); \\ &= 2\left(\alpha_{(0;0)}(1) + \alpha_{(0;1)}(1)y + \alpha_{(1;0)}(1)x + \alpha_{(1;1)}(1)xy\right) + \alpha_{(0;0)}(2) + \alpha_{(1;0)}(2)x \\ &\quad + \alpha_{(0,1)}(2)y + \alpha_{(1,1)}(2)xy + \alpha_{(2,0)}(2)x^2 + \alpha_{(2,1)}(2)x^2y + \alpha_{(1,2)}(2)xy^2; \\ &\quad + \alpha_{(0,2)}(2)y^2 + \alpha_{(3,0)}(2)x^3 + \alpha_{(3,1)}(2)x^3y + \alpha_{(1,3)}(2)xy^3 + \alpha_{(0,3)}(2)y^3, \text{avec } \alpha_i(j) \in \{0; 1\}. \end{aligned}$$

Le résultat suivant est une conséquence immédiate du théorème 1.1.2. Ce résultat donne la formule du nombre d'applications polynomiales modulo p^w. Pour une meilleure lisibilité, nous adopterons la notation $\exp_p a := p^a$.

Corollaire 1.1.4

Le nombre $\Psi_d(p^w)$ d'applications polynomiales à d variable(s) sur $\mathbb{Z}_{p^w}$, est donné par :

$$\Psi_d(p^w) := |\mathrm{Im}(\Phi_{p^w,d})| = \exp_p\Big(\sum_{i=1}^{w} s_d(p^i)\Big).$$

Particulièrement, il y a $\exp_p(p^d)$ applications polynomiales à d variable(s) sur $\mathbb{Z}_p$.

Exemple 6. *Pour calculer le nombre d'applications polynomiales $\Psi_2(8)$ à deux variables sur*

$\mathbb{Z}_8$, nous aurons besoin de :

$$\begin{aligned} S_2(2) &= \{(k_1,k_2) \,:\, 0 \le k_1 \le 1, 0 \le k_2 \le 1\},\ \textit{donc}\ s_2(2) = 4; \\ S_2(4) &= \{(k_1,k_2) \,:\, 0 \le k_1 \le 3, 0 \le k_2 \le 3, k_1k_2 < 4\};\ \textit{donc}\ s_2(4) = 12; \\ S_2(8) &= \{(k_1,k_2) \,:\, 0 \le k_1 \le 3, 0 \le k_2 \le 3\},\ \textit{donc}\ s_2(8) = 16. \end{aligned}$$

Il résulte que $\Psi_2(8) = 2^{4+12+16} = 2^{32}$. ○

Il y a $\exp_p\left(wp^w\right)$ applications de $\left(\mathbb{Z}_{p^w}\right)^d$ dans $\mathbb{Z}_{p^w}$. Donc la probabilité d'obtenir une application polynomiale à d variable(s) sur $\mathbb{Z}_{p^w}$ dans $\mathcal{A}(p^w, d)$ est

$$\exp_p\left(\sum_{i=1}^{w}\left(s_d(p^i) - p^w\right)\right). \tag{1.13}$$

★ ★ **Chapitre Deux** ★ ★

Quasigroupes polynomiaux modulo p^w

Dans ce chapitre, $n := p^w$ avec p un nombre premier et n un entier naturel non nul. On désigne par :

- $\mathrm{M} := p\mathbb{Z}_n$ l'unique idéal maximal de l'anneau $(\mathbb{Z}_n; +, \times)$;
- $\mathbb{Z}_n \backslash \mathrm{M}$ le groupe multiplicatif de l'anneau $(\mathbb{Z}_n; +, \times)$;
- $\mathrm{T} := \{a^{p^{w-1}} \ : \ a \in \mathbb{Z}_n \backslash \mathrm{M}\}$ l'unique sous-groupe cyclique de $\mathbb{Z}_n \backslash \mathrm{M}$ d'ordre $p-1$.

L'objectif est de caractériser les quasigroupes polynomiaux modulo p^w en passant par les permutations polynomiales de $\mathbb{Z}_n$.

2.1 Permutations polynomiales

Une **permutation polynomiale** de $\mathbb{Z}_n$ est une application polynomiale bijective de $\mathbb{Z}_n$ dans $\mathbb{Z}_n$. On désigne par $\mathtt{PP}(n)$, l'ensemble des permutations polynomiales de $\mathbb{Z}_n$ et $\mathcal{S}_n$ l'ensemble des permutations de $\mathbb{Z}_n$. Tout élément σ de $\mathcal{S}_n$ s'écrira :

$$\sigma := \begin{pmatrix} 0 & 1 & \cdots & n-2 & n-1 \\ \sigma(0) & \sigma(1) & \cdots & \sigma(n-2) & \sigma(n-1) \end{pmatrix}.$$

Exemple **7.** *L'application $\sigma : \mathbb{Z}_8 \to \mathbb{Z}_8$ définie par : $\sigma(x) = 2x^2 + x$, est une permutation polynomiale de $\mathbb{Z}_8$, et donc*

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix} = (1, 3, 5, 7).$$

Évidemment, $(\mathtt{PP}(n); \circ)$ est un sous-groupe du groupe $(\mathcal{S}_n; \circ)$. Dans le cas où $w = 1$, le corollaire 1.1.3 permet d'obtenir $\mathtt{Im}(\Phi_{p,1}) = \mathbf{A}(p, 1)$. Donc $\mathcal{S}_p = \mathtt{PP}(p)$.

Proposition 2.2.1

Soit $f \in \mathtt{PP}(n)$. Si $f(\overline{0}) \in \mathrm{M}$, alors $f|_{\mathrm{M}}$ est une permutation de M.

Preuve. Soit f dans PP(n). Alors il existe s un entier naturel non nul, et $(a_0, a_1, \cdots, a_s)$ dans $[|n|]^s$ tel que pour tout x dans $[|n|]$, on a :

$$f(\overline{x}) = \overline{a}_s\overline{x}^s + \cdots + \overline{a_1}\,\overline{x} + \overline{a_0}.$$

Comme $\overline{a_0} = f(\overline{0}) \in \mathrm{M}$, on a : $f(\mathrm{M}) \subseteq \mathrm{M}$. Or f est injective, donc $|f(\mathrm{M})| = |\mathrm{M}|$. D'où la restriction $f|_{\mathrm{M}}$ est une permutation de M. ■

Proposition 2.2.2

L'application

$$\begin{array}{rccl} \mu_{\mathrm{M}} : & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & x & \mapsto & \begin{cases} \overline{1}, & \text{si } x \in \mathrm{M}\,; \\ \overline{0}, & \text{sinon.} \end{cases} \end{array}$$

est polynomiale.

Preuve. Considérons le polynôme P sur $\mathbb{Z}_n$ défini par :

$$P = \Big(\prod_{k\in\mathbb{Z}_n\setminus M}(X-k)\Big)^{\phi(n)}$$

qui est une application polynomiale, où $\phi(n) = p^{w-1}(p-1)$.

- Si $x \notin \mathrm{M}$ alors $x \in \mathbb{Z}_n\setminus M$. Alors

$$\tilde{P}(x) = (x-x)\cdot\Big(\prod_{k\in(\mathbb{Z}_n\setminus M)\setminus\{x\}}(x-k)\Big)^{\phi(n)} = \overline{0}\cdot\Big(\prod_{k\in(\mathbb{Z}_n\setminus M)\setminus\{x\}}(x-k)\Big)^{\phi(n)} = \overline{0}.$$

- Si $x \in \mathrm{M}$, alors pour tout $k \in \mathbb{Z}_n\setminus\mathrm{M}$, on a : $x - k \in \mathbb{Z}_n\setminus\mathrm{M}$. Comme $\mathbb{Z}_n\setminus\mathrm{M}$ est le groupe multiplicatif de $\mathbb{Z}_n$ et $|\mathbb{Z}_n\setminus\mathrm{M}| = \phi(n)$, il resulte que pour tout $k \in \mathbb{Z}_n\setminus\mathrm{M}$, on a : $(x-k)^{\phi(n)} = \overline{1}$. Ainsi,

$$\begin{aligned} \tilde{P}(x) &= \Big(\prod_{k\in\mathbb{Z}_n\setminus M}(x-k)\Big)^{\phi(n)}; \\ &= \prod_{k\in\mathbb{Z}_n\setminus M}(x-k)^{\phi(n)}; \\ &= \prod_{k\in\mathbb{Z}_n\setminus M}\overline{1}; \\ &= \overline{1}. \end{aligned}$$

Finalement,

$$\tilde{P}(x) = \begin{cases} \overline{1}, & \text{si } x \in \mathrm{M}\,; \\ \overline{0}, & \text{sinon.} \end{cases}$$

Ainsi, $\tilde{P} = \mu_{\mathrm{M}}$ et $\widetilde{P}$ est une application polynomiale sur $\mathbb{Z}_n$. On conclut que μ_{M} est une application polynomiale. ■

Dans la suite, $\mathrm{PP}_n(\mathrm{M}) := \left\{f|_{\mathrm{M}} \ : \ f \in \mathrm{PP}(n) \text{ et } f(\overline{0}) \in \mathrm{M}\right\}$. Clairement, $(\mathrm{PP}_n(\mathrm{M}); \circ)$ est un groupe. Pour tout $\alpha \in \mathcal{S}_p$ et pour tout (g, g') dans $\left((\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}\right)^2$, on définit la loi $\diamond_\alpha$ sur $(\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$ l'ensemble des applications de T dans $\mathrm{PP}_n(\mathrm{M})$ de la façon suivante :

$$\begin{array}{rccc} g \diamond_\alpha g' : & \mathbb{Z}_p & \to & \mathrm{PP}_n(\mathrm{M}) \\ & i & \mapsto & g(i) \circ g'(\alpha(i)). \end{array} \tag{2.1}$$

Proposition 2.2.3

L'ensemble $\mathcal{S}_p \times (\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$ muni de l'opération $\diamond$ définie par :

$$(\alpha; g) \diamond (\alpha'; g') \ = \ (\alpha \circ \alpha'; g \diamond_\alpha g') \tag{2.2}$$

est un groupe, noté $\mathcal{S}_p \rtimes (\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$.

Considérons l'application $\mathbb{I}_{\mathrm{M}} : \mathrm{M} \to \mathrm{M}$ telle que $\mathbb{I}_{\mathrm{M}}(i) = \mathrm{Id}_{\mathrm{M}}$.

Preuve. Montrons que l'ensemble $\mathcal{S}_p \times (\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$ muni de l'opération définie en (2.2) a une structure de groupe :

- La loi est interne par définition ;
- Associativité : Soit $x := (\alpha; g)$, $y := (\alpha'; g')$ et $z := (\alpha''; g'')$ dans $\mathcal{S}_p \times (\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$. Alors :

$$\begin{aligned} (x \diamond y) \diamond z &= (\alpha\alpha'; g \diamond_\alpha g') \diamond (\alpha''; g'') ; \\ &= ((\alpha \circ \alpha') \circ \alpha''; (g \diamond_\alpha g') \diamond_{\alpha\circ\alpha'} g'') ; \\ &= (\alpha \circ (\alpha' \circ \alpha''); g_i \diamond_\alpha (g' \diamond_{\alpha\circ\alpha'} g'')) ; \\ &= (\alpha; g) \diamond (\alpha'\alpha''; g' \diamond_{\alpha'} g'') ; \\ &= (\alpha; g_i) \diamond ((\alpha'; g') \diamond (\alpha''; g'')) ; \\ &= x \diamond (y \diamond z). \end{aligned}$$

  Donc la loi $\cdot$ est associative.
- Existence de l'élément neutre : Soit $(\alpha; g) \in \mathcal{S}_p \times (\mathrm{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$. Posons $\mathrm{Id} := (\mathrm{Id}_p; \mathbb{I}_{\mathrm{M}})$.

Ainsi, on a :

$$\begin{aligned}(\alpha; g) \diamond \mathrm{Id} &= \left(\alpha \circ \mathrm{Id}_p; g \diamond_\alpha \mathbb{I}_{\mathrm{M}}\right);\\ &= (\alpha; g);\\ &= \mathrm{Id} \diamond (\alpha; g)\\ &= (\alpha; g).\end{aligned}$$

D'où Id considéré est bel et bien l'élément neutre pour la loi $\cdot$ dans $\mathcal{S}_p \times (\mathtt{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$.

- Existence de l'élément symétrique : Soit $x := (\alpha; g) \in \mathcal{S}_p \times (\mathtt{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$. Posons $x^{-1} := \left(\alpha^{-1}; g^{-1} \circ \alpha^{-1}\right)$ où $g^{-1} : \mathbb{Z}_p \to \mathtt{PP}_n(\mathrm{M})$ telle que $g^{-1}(i) = (g(i))^{-1}$. On a alors :

$$\begin{aligned}x \diamond x^{-1} &= (\alpha; g) \cdot \left(\alpha^{-1}; g \circ \alpha^{-1}\right);\\ &= \left(\alpha \circ \alpha^{-1}, g \diamond_\alpha (g^{-1} \circ \alpha^{-1})\right);\\ &= \left(\mathrm{Id}_p, \mathbb{I}_{\mathrm{M}}\right);\\ &= \mathrm{Id},\end{aligned}$$

et de même,

$$\begin{aligned}x^{-1} \diamond x &= \left(\alpha^{-1}; g^{-1} \circ \alpha^{-1}\right) \diamond (\alpha; g);\\ &= \left(\alpha^{-1} \circ \alpha, (g^{-1} \circ \alpha^{-1}) \diamond_{\alpha^{-1}} g\right);\\ &= (\mathrm{Id}_p; \mathbb{I}_{\mathrm{M}});\\ &= \mathtt{Id}.\end{aligned}$$

Donc chaque élément de l'ensemble admet donc un symétrique par la loi $\diamond$ et ainsi nous avons montré que l'ensemble $\mathcal{S}_p \times (\mathtt{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}$ muni de l'opération définie en (2.2) est un groupe.

■

Un générateur t du groupe cyclique T, permet de définir l'application

$$\begin{aligned}\eta : \mathbb{Z}_p &\to \mathrm{T} \cup \{0\}\\ i &\mapsto \begin{cases} t^i, & \text{si } i \neq 0;\\ \overline{0}, & \text{si } i = 0.\end{cases}\end{aligned} \tag{2.3}$$

On remarque que pour tout (x, y) dans $\mathrm{T} \times \mathbb{Z}_p$, on a : $\eta \circ \pi(x) = x$ et $\pi \circ \eta(y) = y$. [3, Théorème 2.4] permet d'obtenir le résultat suivant.

Lemme 2.2.1

L'application

$$\begin{array}{rccc} \Theta : & \left(\mathcal{S}_p \rtimes (\mathtt{PP}_n(\mathrm{M}))^{\mathbb{Z}_p}; \diamond\right) & \to & (\mathtt{PP}(n); \circ) \\ & (\alpha; g) & \mapsto & \sum\limits_{i\in\mathbb{Z}_p} \Big(g(\mathtt{Id}_p - i) + \eta(\alpha(i))\Big)\mu_{\mathrm{M}}(\eta(\mathtt{Id}_p - i)), \end{array} \tag{2.4}$$

où μ_{M} est définie en (2.2.2) et η est définie en (2.3), est un isomorphisme de groupes.

Proposition 2.2.4

Soit $\sigma \in \mathtt{PP}(n)$. Alors

$$\begin{array}{rccc} \overline{\sigma} : & \mathbb{Z}_p & \to & \mathbb{Z}_p \\ & x \,(\mathtt{mod}\, p) & \mapsto & \sigma(x) \,(\mathtt{mod}\, p) \end{array} \tag{2.5}$$

est une permutation polynomiale de $\mathbb{Z}_p$.

Preuve. L'application $\overline{\sigma}$ est polynomiale, et $\overline{\sigma} \circ \pi = \pi \circ \sigma$. Il suffit de montrer que $\overline{\sigma}$ est surjective. Soit $\overline{y}$ dans $\mathbb{Z}_p$, cherchons $\overline{x}$ dans $\mathbb{Z}_p$ tel que $\overline{\sigma}(\overline{x}) = \overline{y}$. Comme $\pi : \mathbb{Z}_n \to \mathbb{Z}_p$ est surjective, il existe (x, y) dans $(\mathbb{Z}_n)^2$ tels que $\pi(x) = \overline{x}$ et $\pi(y) = \overline{y}$. Ainsi, il existe uniquement (x_0, y_0) dans T^2 tel que $\pi(x) = \pi(x_0)$ et $\pi(y) = \pi(y_0)$. Par conséquent, $\overline{\sigma}(\overline{x}) = \overline{\sigma}(\overline{x_0}) = \overline{y} = \overline{y_0}$. Donc $\pi(y) = \pi(y_0) = \overline{\sigma}(\pi(x_0)) = \pi(\sigma(x_0)) \Leftrightarrow y_0 = \eta(\pi(y_0)) = \eta(\pi(\sigma(x_0))) = \sigma(x_0)$. Comme σ est bijective, on a : $x_0 = \sigma^{-1}(y_0)$. Prendre $\overline{x} = \pi(\sigma^{-1}(y_0))$. ■

Lemme 2.2.2

Soit $f : \mathbb{Z}_n \to \mathbb{Z}_n$ tel que $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ avec $a_k \neq 0$. Alors $f|_{\mathrm{M}} \in \mathtt{PP}_n(\mathrm{M})$ si et seulement si $a_0 \in \mathrm{M}$ et $a_1 \notin \mathrm{M}$.

Preuve. Soit $f : \mathbb{Z}_n \to \mathbb{Z}_n$ tel que $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ avec $a_k \neq 0$.

$\Longrightarrow$) Supposons que $f|_{\mathrm{M}} \in \mathtt{PP}_n(\mathrm{M})$. Cela signifie que pour tout $x \in \mathrm{M}$, $f(x) \in \mathrm{M}$. En particulier, pour $x = 0$, nous avons $f(0) = a_0 \in \mathrm{M}$.

De plus, pour montrer que $a_1 \notin \mathrm{M}$, supposons le contraire, c'est-à-dire que $a_1 \in \mathrm{M}$. Dans ce cas, nous pouvons écrire $a_1 = p \cdot b$ pour un certain $b \in \mathbb{Z}_n$. Ainsi, pour tout $x \in \mathrm{M}$, nous avons $\pi(f(x)) = 0$, puisque pour tout $0 \leq i \leq k$ chaque coefficient $a_i \in \mathrm{M}$. Cela signifie que $f|\mathrm{M}$ est une fonction constante égale à 0 sur M, ce qui implique que $f|\mathrm{M} \notin \mathtt{PP}_n(\mathrm{M})$. Absurde ! Donc $a_1 \notin \mathrm{M}$

$\Longleftarrow$) Supposons que $a_0 \in \mathrm{M}$ et $a_1 \notin \mathrm{M}$. Montrons que $f|_{\mathrm{M}}$ est une bijection de M. Pour cela, il suffit de montrer que f est une bijection de $\mathbb{Z}_n$ sur $\mathbb{Z}_n$.

Puisque $a_k \neq 0$, la fonction polynomiale f est de degré k et s'annule en au plus k élément(s) distinct(s) dans $\mathbb{Z}_n$. Ainsi, pour montrer que f est une bijection, il suffit de montrer que f est injective.

Soit (x, y) dans $(\mathbb{Z}_n)^2$ tel que $f(x) = f(y)$. Alors,

$$a_k(x^k - y^k) + ak - 1(x^{k-1} - y^{k-1}) + \cdots + a_1(x - y) = 0.$$

Puisque $\pi(a_k) \neq 0$, a_k est inversible dans $\mathbb{Z}_n$. Donc

$$x^k - y^k + a_{k-1}a_k^{-1}(x^{k-1} - y^{k-1}) + \cdots + a_1a_k^{-1}(x - y) = 0.$$

Si $x \neq y$, alors nous avons une équation de la forme $a(x - y) = b$, où $(a, b) \in (\mathbb{Z}_n)^2$ avec $\pi(a) \neq 0$. Mais cela impliquerait que a est inversible dans $\mathbb{Z}_n$. Absurde, car p est premier et $a \in \mathrm{M}$. Donc f est injective.

■

Théorème 2.2.1

Soient $f \in \mathcal{A}(n; 1)$ et $\overline{f}$ définie en (2.5). Alors $f \in \mathtt{PP}(n)$ si et seulement si $\overline{f} \in \mathtt{PP}(p)$ et $(\forall x \in \mathbb{Z}_p)(\overline{f'}(x) \neq 0)$.

Preuve. Soit $f : \mathbb{Z}_n \to \mathbb{Z}_n$ tel que $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$ avec $a_k \neq 0$. Alors $f'(x) = ka_kx^{k-1} + (k-1)a_{k-1}x^{k-2} + \cdots + xa_2x + a_1$. D'après Lemme 2.2.1, $f \in \mathtt{PP}(n)$ si et seulement si $\overline{f} \in \mathtt{PP}(p)$ et $f(\mathtt{Id}_n + k) - f(k)_{|\mathrm{M}} \in \mathtt{PP}_n(\mathrm{M})$ pour tout k dans T. Or, Lemme 2.2.2 implique $f(x + k) \notin \mathrm{M}$. De plus, $(f(\mathtt{Id}_n + k))'(0) = \overline{f'}(k)$. Ainsi pour tout k dans T, on a : $f(x + k) \notin \mathrm{M}$ signifie que pour tout k dans T, on a : $\overline{f'}(k) \neq 0$. ■

Mullen et Stevens dans [7], ont établi que

$$|\mathtt{PP}(p^w)| = \frac{p!(p-1)^p}{p^{2p}} \prod_{j=0}^{\eta_p(w)} p^{w-\nu_p(j!)},$$

où $\eta_p(w) := \max\{k \in \mathbb{N} : \nu_p(k!) < w\}$.

Exemple 8. *Pour $p = 2$, $w = 3$ et $d = 1$, nous avons $n = 8$ et on a $|PP(8)| = 2^7 = 128$. Nous avons donné à l'exemple 5 la forme générale des applications polynomiales à une variable $f : \mathbb{Z}_8 \to \mathbb{Z}_8$. Pour certaines valeurs des coefficients $\alpha_i(j)$, nous avons des applications polynomiales bijectives c'est-à-dire quelques exemples de permutations polynomiales modulo 8. Nous pouvons citer entre autres :*

x;	$3x$;	$5x$;	$7x$;
$x + 2x^2$;	$3x + 2x^2$;	$5x + 2x^2$;	$7x + 2x^2$;
$x + 2x^3$;	$3x + 2x^3$;	$5x + 2x^3$;	$7x + 2x^3$;
$x + 2x^2 + 2x^3$;	$3x + 2x^2 + 2x^3$;	$5x + 2x^2 + 2x^3$;	$7 + 7x + 2x^2 + 2x^3$.

2.2 Caractérisation des quasigroupes polynomiaux

Dans cette section, $([|n|]; \star)$ est un magma d'ordre n, où $n := p^w$ avec p un nombre premier et w un entier naturel non nul. Pour chaque a dans $[|n|]$, considérons les translations

$$\mathrm{L}_a : \begin{array}{ccc} [|n|] & \to & [|n|] \\ x & \mapsto & a \star x, \end{array} \quad \text{et} \quad \mathrm{R}_a : \begin{array}{ccc} [|n|] & \to & [|n|] \\ x & \mapsto & x \star a. \end{array} \tag{2.6}$$

à gauche et à droite, respectivement.

Définition 2.2.1

Le magma $([|n|]; \star)$ est **polynomial** modulo n, s'il existe une fonction polynomiale $f : \mathbb{Z}^2 \to \mathbb{Z}$ tel que $a \star b = f(a, b) \pmod n$, pour tout (a, b) dans $[|n|]^2$.

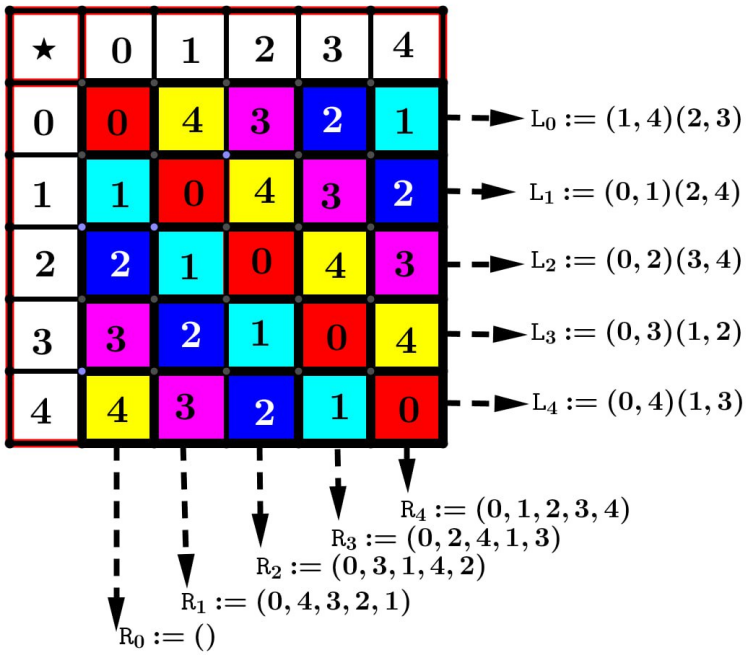
Exemple 9. *Le magma $([|n|]; \star)$ où la loi $\star$ est définie par : pour tout (a, b) dans $[|n|]^2$ on a : $a \star b = a \cdot b \bmod n$, est polynomial modulo n.*

Définition 2.2.2

Le magma $([|n|]; \star)$ est un **quasigroupe polynomial** modulo n, s'il est polynomial modulo n, et pour tout a dans $[|n|]$ les applications L_a et R_a sont bijectives.

Exemple 10. *Considérons l'anneau $(\mathbb{Z}_n; +, \cdot)$ des entiers modulos n.*

► *Définissons le magma $([|5|]; \star)$ d'ordre 5 de manière suivante : $a \star b = \widetilde{P}(a, b) \bmod 5$, avec $P := X - Y \in \mathbb{Z}[X, Y]$. Ce magma est polynomial modulo 5 et possède la table de Cayley suivante :*



où $L_a := \widetilde{P}(a,\_) \in \mathbb{S}_5$ *et* $R_a := \widetilde{P}(\_,a)$ *sont bijectives. Donc ce magma* $([|5|];\star)$ *est un quasigroupe polynomial modulo* 5.

► *Définissons le magma* $([|n|];\star)$ *d'ordre n de manière suivante :*

$$a \star b = \widetilde{P}(a,b) \mod n,$$

où $P := X - Y \in \mathbb{Z}[X,Y]$. *Alors* $L_a := \widetilde{P}(a,\_) \in \mathbb{S}_n$ *et* $R_a := \widetilde{P}(\_,a)$ *sont bijectives. On vérifie que le magma* $([|n|];\star)$ *est un quasigroupe polynomial modulo n.*

Rivest dans [8] a étudié les polynômes sur $\mathbb{Z}_{2^w}$ à deux variables afin de construire certains quasigroupes binaire d'ordre 2^w et a prouvé qu'une application polynomiale $f : \mathbb{Z}^2 \to \mathbb{Z}$ permet de construire un quasigroupe modulo 2^w, si et seulement si pour tout $0 \leq a \leq 1$, les applications polynomiales

$$\begin{array}{rccc} L_a : & [|n|] & \to & [|n|] \\ & y & \mapsto & f(a,y) \bmod n, \end{array} \quad \text{et} \quad \begin{array}{rccc} R_a : & [|n|] & \to & [|n|] \\ & x & \mapsto & f(x,a) \bmod n \end{array}$$

sont bijectives. Dans la suite, nous procédons à un raisonnement heuristique pour généraliser à l'anneau $\mathbb{Z}_{p^w}$, les polynômes qui permettent de construire des quasigroupes d'ordre p^w.

Théorème 2.2.2

Soit $([|n|], \star)$ un magma polynomial modulo n tel que $a \star b = f(a,b) \bmod n$, où $f : \mathbb{Z}^2 \to \mathbb{Z}$ est une fonction polynomiale. Alors $([|n|], \star)$ est un quasigroupe si et seulement si pour tout $0 \leq a < p$, les applications polynomiales

$$\begin{array}{rccc} \mathrm{L}_a : & [|n|] & \to & [|n|] \\ & y & \mapsto & f(a,y) \pmod n, \end{array} \quad \text{et} \quad \begin{array}{rccc} \mathrm{R}_a : & [|n|] & \to & [|n|] \\ & x & \mapsto & f(x,a) \pmod n \end{array}$$

sont bijectives.

Preuve. Soient $f : \mathbb{Z}^2 \to \mathbb{Z}$ et $([|n|], \star)$ un magma polynomial modulo n tel que $a \star b = f(a,b) \bmod n$. Alors pour tout $0 \leq a < p$, on constate que $\mathrm{L}_a : [|n|] \to [|n|]$ et $\mathrm{R}_a : [|n|] \to [|n|]$ sont des applications polynomiales, définies par $\mathrm{L}_a(x) = f(a,y) \pmod n$ et $\mathrm{R}_a(x) = f(x,a) \pmod n$.

$\Rightarrow$) Supposons que f définie un quasigroupe modulo p^w. Alors par définition de quasigroupes, pour tout $0 \leq a < p^w$ (en particulier pour $0 \leq a < p$) les applications L_a et R_a sont bijectives.

$\Leftarrow$) Supposons que pour tout $0 \leq a < p$, les applications polynomiales $\mathrm{L}_a : [|n|] \to [|n|]$ et $\mathrm{R}_a : [|n|] \to [|n|]$ sont bijectives, mais que f ne définit pas un quasigroupe modulo n. Posons

$$f(x,y) := \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_{i,j} x^i \right) y^j.$$

Si f ne definit pas un quasigroupe modulo n, alors il existe c dans $[|n|]$ tel qu'au moins un des polynômes L_c ou R_c ne soit pas bijectif. Sans nuire à la généralité, supposons que ce polynôme soit $\mathrm{R}_c(x) = f(x,c)$. D'après le théorème de la division euclidienne de c par p, il existe un unique couple (c_1, b) dans $\mathbb{N}^2$ tel que $c = b + pc_1$ avec $0 \leq b < p$. Ainsi,

$$\begin{aligned} \mathrm{R}_c(x) \bmod p &= f(x,c) \bmod p = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_{i,j} x^i \right) c^j \bmod p; \\ &= \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_{i,j} x^i \right) b^j \bmod p = f(x,b) \bmod p = \mathrm{R}_b(x) \bmod p, \end{aligned}$$

ainsi, la restriction de R_c à $[|p|]$, est une permutation polynomiale modulo p.

De plus :

$$\begin{aligned} \mathrm{R}'_c(x) \bmod p &= \left(\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{i,j}c^j\right)x^i\right)' \bmod p = \sum_{i=0}^{n-1} i\left(\sum_{j=0}^{n-1} a_{i,j}c^j\right)x^{i-1} \bmod p; \\ &= \sum_{i=0}^{n-1} i\left(\sum_{j=0}^{n-1} a_{i,j}b^j\right)x^{i-1} \bmod p = \left(\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{i,j}b^j\right)x^i\right)' \bmod p; \\ &= \mathrm{R}'_b(x) \bmod p. \end{aligned}$$

Il s'en suit que l'équation $\mathrm{R}'_c(x) \equiv 0 (\bmod n)$ n'a pas de solution dans $[|p|]$. De part le théorème 2.2.1, on conclut que R_c est une permutation polynomiale modulo n. Ainsi donc, notre supposition est fausse et ceci prouve notre second sens.

■

Exemple 11. .

- *Soit $p = 2$, $w = 2$ et $d = 2$; donc $n = 2^2 = 4$. Nous avons donné à l'exemple 5 la forme générale des applications polynomiales à deux variables sur $\mathbb{Z}_4$. Pour certaines valeurs des coefficients $\alpha_i(j)$, nous avons des applications polynomiales qui satisfont le théorème 2.2.2. C'est dans ce sens que nous considérons : $f(x,y) := x + 3y$. Ainsi le couple $([|4|], *)$ où la loi $*$ est définie par : $a * b = f(a,b) (\bmod 4)$ est un quasigroupe polynomial modulo 4 dont la table de Cayley est donnée par :*

$*$	0	1	2	3
0	0	3	2	1
1	3	0	1	2
2	2	1	0	3
3	1	2	3	0

- *De façon analogue, pour $p = d = 2$, $w = 3$; $n = 8$.*

  Considérons l'application polynomiale donné par $q(x,y) := 3x + 5y$. Nous vérifions facilement que q ainsi définie satisfait bien le théorème 2.2.2. Ainsi, en définissant la loi binaire $\star$ par : $a \star b = q(a,b) (\bmod 8)$, nous concluons que le couple $([|8|], \star)$ est un quasigroupe polynomial sur $\mathbb{Z}_8$ dont la table de Cayley est :

$\star$	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	*0*	*3*	*6*	*1*	*4*	*7*	*2*	*5*
1	*3*	*6*	*1*	*4*	*7*	*2*	*5*	*0*
2	*6*	*1*	*4*	*7*	*2*	*5*	*0*	*3*
3	*1*	*4*	*7*	*2*	*5*	*0*	*3*	*6*
4	*4*	*7*	*2*	*5*	*0*	*3*	*6*	*1*
5	*7*	*2*	*5*	*0*	*3*	*6*	*1*	*4*
6	*2*	*5*	*0*	*3*	*6*	*1*	*4*	*7*
7	*5*	*0*	*3*	*6*	*1*	*4*	*7*	*2*

Ce qui représente bel et bien la table de Cayley d'un quasigroupe et comme la loi de ce quasigroupe est définie à l'aide d'un polynôme, nous concluons que c'est une table de Cayley du quasigroupe polynomial ([|8|], $\star$).

★ ★ Chapitre Trois ★ ★

Enseignement des expressions polynomiales en classe de Troisième

3.1 Transposition didactique : expressions polynomiales

La didactique est l'étude des questions posées par l'enseignement et l'acquisition des connaissances dans les différentes disciplines scolaires. La didactique sert alors à transposer des savoirs dits « utiles » en savoirs enseignables, et s'applique à définir avec précision chaque objet (savoir) qu'elle souhaite enseigner, mais également à définir comment on enseigne cet objet aux apprenants.

Parmi les théories didactiques les plus importantes, nous avons la théorie de la transposition didactique :

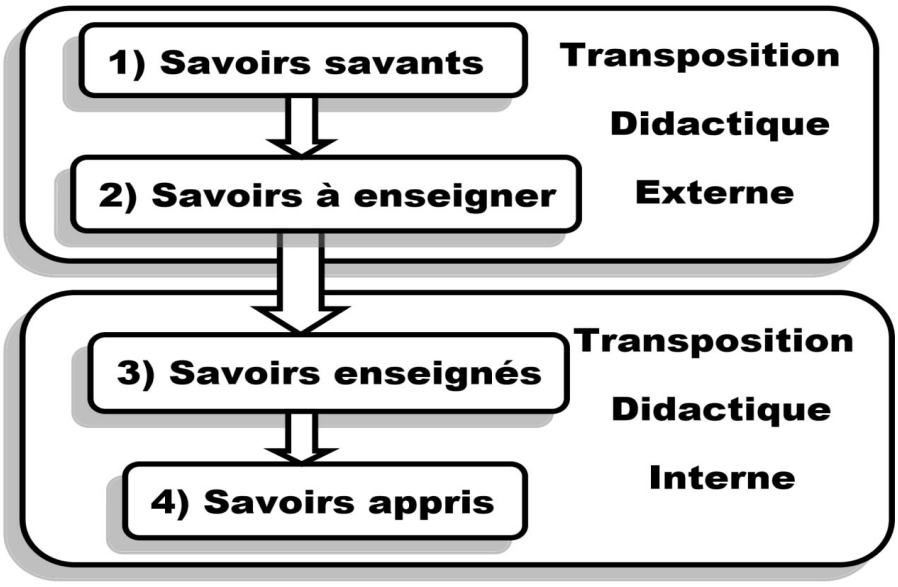


FIGURE 3.1: Étapes de la transposition didactique

La transposition didactique est en effet l'une des théories les plus importantes en didactique des mathématiques et a été développée par le chercheur Yves Chevallard [2].

Selon ce modèle, le savoir savant, qui est le savoir scientifique complet et complexe, doit être adapté par les concepteurs de programmes pour devenir le savoir à enseigner, qui est une version simplifiée et structurée du savoir savant. Le savoir à enseigner est ensuite transposé par l'enseignant en savoir enseigné, qui est la version effective et concrète du savoir à enseigner, présentée aux élèves par l'enseignant. Enfin, le savoir appris est le savoir effectivement acquis par les élèves. Il existe deux étapes de la transposition didactique :

- La transposition didactique externe : elle est appelée ainsi, car elle a lieu hors du système d'enseignement, hors de la classe. Elle est réglée par ce qu'appelle Chevallard (1985) "noosphère", littéralement" la sphère où l'on pense". La noosphère est donc l'ensemble des personnes qui pensent les contenus d'enseignement. Ce sont les universitaires qui s'intéressent aux problèmes d'enseignement, les représentants du système d'enseignement (le président d'une association d'enseignants par ex.), les auteurs de manuels, les inspecteurs scolaires, etc.
- La transposition didactique interne : elle se réfère à la manière dont l'enseignant transforme les connaissances scientifiques ou disciplinaires en connaissances didactiques, c'est-à-dire en savoirs adaptés au contexte de l'enseignement et à la compréhension des élèves.

Dans l'enseignement secondaire au Cameroun, les expressions polynomiales sont enseignées depuis la classe de 3ième [6, classe de troisième, module 13] :

IV. CALCUL LITTÉRAL	
¤ Expressions littérales. ¤ Exemples d'expressions littérales : - Polynôme (monôme, degré, coefficient, variable). - fraction rationnelle (condition d'existence d'une valeur numérique). ¤ Règle de suppression des parenthèses ¤ Règle de priorité. ¤ Égalités remarquables . ¤ Factorisation d'une expression littérale. **Savoirs**	¤ Calculer la valeur numérique d'une expression littérale, des expressions littérales particulières rencontrées jusque là : débit, volumes, aires. ¤ Développer, réduire et ordonner suivant les puissances de la variable, un produit de 2 polynômes de degré 2 au plus. ¤ Écrire en produit de facteurs du premier degré, une expression littérale à l'aide d'un facteur commun, d'une identité remarquable, des deux éléments. ¤ Simplifier une fraction rationnelle. **Savoirs-faire**

FIGURE 3.2: Savoirs à enseigner en classe de troisième extrait du programme officiel en mathématiques des classes de 3^e (voir[6]).

Remarque : Le vocabulaire concernant les polynômes ne cadrent pas avec les savoirs-savants. L'utilisation de polynôme dans les programmes d'études est une métonymie, d'après le savoir-savant ce qui entraîne très souvent la confusion faite par les étudiants de première année universitaire entre "expression polynomiale" et "polynôme".

En ce qui concerne les expressions polynomiales, la transposition didactique implique de les présenter d'une manière qui facilite leur compréhension par les élèves. Cela peut inclure l'**utilisation de représentations graphiques ou visuelles** pour montrer la relation entre les coefficients et les termes, ainsi que l'enseignement de techniques de simplification.
Voici quelques éléments clés à prendre en compte lors de l'enseignement des expressions polynomiales :

1. **Définition** : commencer par expliquer ce qu'est une expression polynomiale et ses différentes composantes telles que les termes, les coefficients et les exposants :
   - Une expression monomiale de la variable x est une expression littérale de la forme ax^n, où a est un nombre coefficient ou constante, x est une inconnue et n est un entier naturel appelé degré de l'expression monomiale. Par exemple, $4x^2$ est une expression monomiale de variable x, de coefficient 4 et de degré 2.
   - Une expression polynomiale est une somme algébrique de plusieurs expressions monomiales. La variable peut être n'importe quelle lettre de l'alphabet. Le degré d'une expression polynomiale est celui de son expression monomiale de plus haut degré :

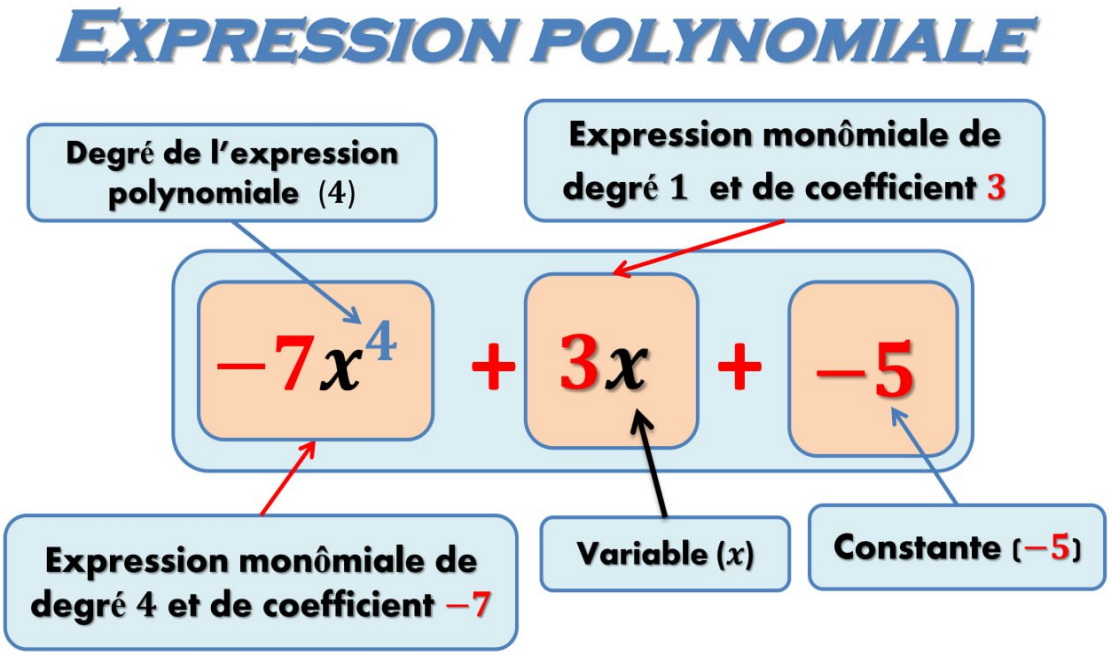


FIGURE 3.3: Exemple d'expression polynomiale.

– La valeur numérique d'une expression polynomiale est la valeur obtenue lorsqu'on remplace toutes ses variables (lettres) par des nombres donnés. Par exemple, la valeur numérique de $A = 2x - 6y + 5$ pour $x = 2$ et $y = 3$ est $A = 2(2) - 6(3) + 5 = -9$.

2 **Vocabulaire** : utiliser des mots simples et précis pour expliquer les concepts mathématiques. Par exemple, expliquez que le coefficient est le nombre qui multiplie la variable et que le terme constant est le nombre qui n'a pas de variable. Par exemple, dans l'expression monomiale $3x^2$, le coefficient est 3 et l'exposant qui est le nombre qui indique la puissance à laquelle la variable est élevée est 2. Le terme constant de cette expression polynômial est -5.

3 **Notation** : enseigner la notation standard pour les expressions polynomiales et aidez les élèves à comprendre comment lire et écrire des expressions polynomiales.
Par exemple, $3x^2 + 2xy - 5$ se lit ***"trois*** x ***au carré plus deux*** x y ***moins*** 5***"***.

4 **Opérations** : enseigner les différentes opérations que l'on peut effectuer avec des expressions polynomiales, telles que le développement et la factorisation. Utilisez des exemples pour montrer comment effectuer ces opérations :

⋆ Développer un produit de 2 polynômes ou expressions polynomiales c'est l'écrire sans parenthèse, c'est-à-dire écrire sous la forme d'une somme algébrique d'expressions monomiales. Développons l'expression polynomiale $(a_0+a_1x+a_2x^2)(b_0+b_1x+b_2x^2)$:

+		0		1		2	
	×	b_0		b_1		b_2	
0	a_0	0	a_0b_0	1	a_0b_1	2	a_0b_2
1	a_1	1	a_1b_0	2	a_1b_1	3	a_1b_2
2	a_2	2	a_2b_0	3	a_2b_1	4	a_2b_2

$$(a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) = (a_0b_0)x^0 + (a_1b_0 + a_0b_1)x^1 + (a_2b_0 + a_1b_1 + a_0b_2)x^2$$
$$+(a_2b_1 + a_1b_2)x^3 + (a_2b_2)x^4$$

FIGURE 3.4: Dispositif permettant de développer le produit de deux(2) expressions polynomiales de degré ≤ 2, suivant les puissances croissantes de la variable x.

Après avoir rangé les coefficients et les degrés dans le dispositif, on fait les produits

des coefficients ensuite, on additionne les degrés et à la fin, on additionne tous les expressions monomiales.

⋆ Factoriser une expression c'est l'écrire sous la forme d'un produit de facteurs.

∗ Utilisation des identités remarquables :

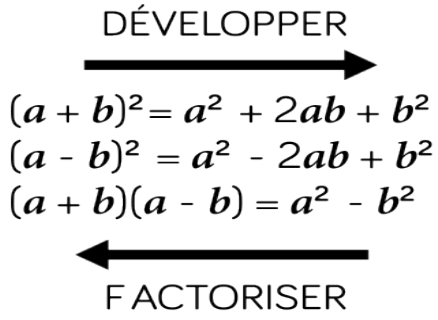


FIGURE 3.5: Identités remarquables

Par exemple, pour factoriser l'expression x^2+4x+4, nous pouvons utiliser l'identité remarquable suivante : $(a+b)^2 = a^2 + 2ab + b^2$ en identifiant $a = x$ et $b = 2$, nous avons : $x^2 + 4x + 4 = x^2 + 2(2)(x) + 2^2 = (x+2)^2$

∗ Utilisation des facteurs communs : factorisons $A = (2x+3)(2x-1)+(2x+3)(3x+2)$.

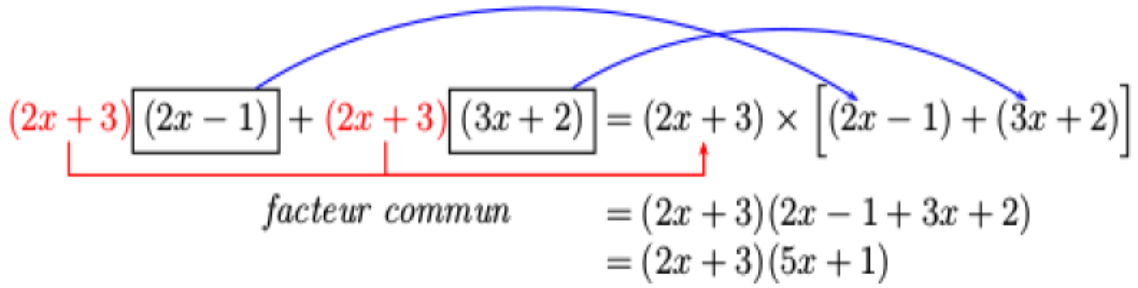


FIGURE 3.6: Factorisation.

∗ Utilisation du facteur commun et des identités remarquables : il suffit juste d'associer les deux méthodes évoquées plus haut.

5 **Utilisation de cas concrets** : Les enseignants peuvent utiliser des exemples concrets pour aider les élèves à comprendre les expressions polynomiales. Par exemple, les élèves peuvent être invités à calculer le coût total d'un certain nombre d'articles en utilisant une expression polynomiale comme fait à la section 3.2.

6 **Application de la théorie à des situations pratiques** : Les enseignants peuvent aider les élèves à comprendre les expressions polynomiales en les appliquant à des situations

pratiques. C'est dans ce sens que nous présentons ci-dessous une situation didactique sur les expressions polynomiales.

3.2 Situation didactique : expressions polynomiales

La théorie des situations didactiques développée par Brousseau (voir [1]) fait référence à un contexte d'apprentissage spécifique qui est créé par l'enseignant pour aider les élèves à acquérir des connaissances et des compétences. Cela peut inclure des activités structurées telles que des leçons, des exercices, des projets et des jeux éducatifs, ainsi que des discussions et des interactions entre l'enseignant et les élèves.
L'objectif d'une situation didactique est de fournir un environnement d'apprentissage stimulant qui permet aux élèves d'explorer, de découvrir et d'apprendre de manière autonome tout en étant encadrés par l'enseignant. Cela implique souvent la manipulation de matériel pédagogique, la réalisation d'expériences ou de simulations, ou la résolution de problèmes pour aider les élèves à comprendre les concepts clés.

Situation didactique : Expressions polynomiales en classe de troisième

Vous êtes professeur de mathématiques en classe de troisième au secondaire. Vous avez remarqué que vos élèves ont des difficultés à comprendre les expressions polynomiales. Pour les aider à mieux comprendre ce concept, vous leur proposez la situation de vie et l'activité d'apprentissage suivantes :

Situation de vie :

Le gérant d'un parc d'attractions a décidé de mettre en place un système de tarification pour les billets d'entrée. Le prix d'un billet dépend du nombre de tours que l'on souhaite faire pour chacune des catégories d'attractions. Les attractions sont regroupées en deux catégories : les attractions simples et les attractions complexes. Les prix sont les suivants pour chaque attraction :

– *Une attraction simple coûte 500Fcfa ;*
– *Une attraction complexe coûte 1000Fcfa.*

Il sollicite ton aide pour établir une expression polynomiale qui permettra de calculer le coût du billet d'un client en fonction du nombre de tour qu'il souhaite effectuer pour chaque catégorie d'attraction.

Activité d'apprentissage + Solution :

1 Combien coûtera le billet d'un client qui veut faire 2 tours d'attractions simples et un tour d'attraction complexe ?

Réponse : Son billet coûtera :

$$(500 \text{ Fcfa} \times 2 \text{ tours a. simples}) + (1000 \text{ Fcfa} \times 1 \text{ tour a. complexe}) = 2000 \text{ Fcfa}$$

Son billet coûtera donc $2000 Fcfa$

2 Proposer les variables représentant le nombre de tours pour chaque catégorie d'attraction.

Réponse : Nous pouvons utiliser les variables suivantes :

- x pour le nombre de tours d'attractions simples ;
- y pour le nombre de tours d'attractions complexes.

3 Donner en fonction de chaque variable choisie le prix total pour chaque attraction.

Réponse : Pour le prix total pour $P(x)$ l'attraction simple et $P(y)$ pour l'attraction complexe, nous avons :

- Le prix total pour l'attraction simple est $P(x) = 500 \times x = 500x$;
- Le prix total pour l'attraction complexe est $P(y) = 1000 \times y = 1000y$.

4 Établir alors une expression polynomiale qui permettra au gérant de calculer le coût du billet d'un client en fonction du nombre de tour qu'il souhaite effectuer pour chaque catégorie d'attraction.

Réponse : Le prix total d'un billet représente la somme des prix pour chaque attraction et donc, peut être calculé à l'aide de l'expression polynomiale suivante :

$$P(x, y) = P(x) + P(y) = 500x + 1000y$$

L'expression polynomiale $p(x, y)$ permettra donc au gérant du parc de calculer le prix du billet d'un client en fonction du nombre de tour d'attraction simple (x) et d'attraction complexe (y) qu'il souhaite effectuer.

En conclusion, cette situation didactique permet d'introduire de manière progressive et concrète les différentes notions liées aux expressions polynomiales. Les élèves peuvent ainsi comprendre comment manipuler ces expressions pour résoudre des problèmes concrets et se familiariser avec les techniques de calcul nécessaires pour les travaux mathématiques futurs.

Conclusion et perspectives

En conclusion, ce mémoire était axé sur un point essentiel, celui de caractériser les quasigroupes polynomiaux modulo p^w, en tenant compte des problèmes tels que la non unicitéde factorisation pour les quasigroupes modulo p^w pour $w \geq 2$, une cause étant la non associativité de la loi. Il etait donc nécessaire de trouver des polynômes appropriés pour construire ces quasigroupes, et d'étudier les propriétés de ces quasigroupes. Pour y parvenir, des outils tels que les applications polynomiales à d variables(s) sur l'anneau $\mathbb{Z}_n$ ont étés utilisés, ce qui a permis d'aborder la notion d'applications polynomiales modulo p^w. Ladite notion quant à elle a permis de définir les concepts de permutations polynomiales et enfin une caractérisation des quasigroupes polynomiaux modulo p^w a été donné.

Le travail présenté ici peut être utile pour les chercheurs et les étudiants qui travaillent sur des sujets liés aux quasigroupes polynomiaux modulo p^w ; il pourra leur servir notamment pour des lectures. En fin de compte, ce mémoire contribue modestement à la littérature sur les quasigroupes polynomiaux modulo p^w.

Cependant, il reste encore de nombreuses perspectives de recherche à explorer dans le domaine des quasigroupes polynomiaux modulo p^w. En particulier, on peut se poser la question de savoir s'il existe une méthode efficace pour construire tous les quasigroupes polynomiaux modulo p^w. En d'autres termes, peut-on trouver un algorithme qui génère tous les quasigroupes polynomiaux modulo p^w ? Cette question est d'une importance fondamentale pour la cryptographie, où la connaissance de tous les quasigroupes polynomiaux modulo p^w peut être utilisée pour la conception de crypto-systèmes efficaces.

Nous pourrons aussi étudier comment le théorème des restes chinois pourrait être utilisé pour généraliser cette étude aux quasigroupes polynomiaux modulo un entier naturel quelconque supérieur à 2. En effet, le théorème des restes chinois pourrait permettre de construire un quasigroupe polynomial modulo un entier naturel composé en utilisant ses représentations modulo des puissances de nombres premiers. Cette approche permettra de généraliser l'étude des quasigroupes polynomiaux à un plus grand ensemble de nombres.

Bibliographie

[1] G. Brousseau, *Theory of Didactical Situations in Mathematics : Didactique des mathématiques*, Kluwer Academic Publishers,19, (1970-1990) : 185-186.

[2] Y. Chevallard, *La transposition didactique : du savoir savant au savoir enseigner*, Revue française de pédagogie, 76, 1986. pp. 89-91.

[3] D. Görcsös, G. Horváth, A. Mészáros, *Permutation polynomials over finite rings*, Finite Fields and Their Applications, 49(2018), 198-211.

[4] N. Hungerbuhler, E. Specker, *A generalization of the Smarandache function to several variables*, Integers, 6(2006). (1-10)

[5] A. D. Keedwell and J. Dénes, *Latin Squares and their Applications*, Second Edition-Elsevier, North Holland (2015)

[6] MINESEC, *Programme officiel de mathémathiques*, note de lecture(2012).

[7] G. Mullen and H. Stevens, *Polynomial functions (mod m)*, Acta Math. Hung. 44 (1984) 237-241.

[8] R.L. Rivest, *Permutation polynomials modulo* 2^w, Finite Fields and Their Applications 7, 287-292(2001).

[9] V. Shcherbacov, *Elements of Quasigroup Theory and Applications*, Chapman and Hall Crc 2017. (437-509)

[10] B. Tchantcho, *Cours de méthodologie de la recherche*, Département de Mathématiques de l'ENS Bertoua, (2022).