Automorphismes projectifs et polynômes binaires irréductibles

Philippe Ravache

Thèse de doctorat de l'université de Rouen

Discipline : Informatique

École doctorale : Sciences Physiques, Mathématiques et de l'Information pour l'Ingénieur

présentée le 19 octobre 2010 par

Philippe RAVACHE

pour obtenir le grade de

Docteur de l'université de Rouen

Automorphismes projectifs et polynômes binaires irréductibles

Jury

Rapporteurs	
M. Philippe Langevin	Université du Sud Toulon-Var
M. Patrick Solé	Telecom ParisTech
Éxaminateurs	
M. Claude Carlet	Université Paris VIII
Mme Brigitte Vallée	Université de Caen
Directeur	
M. Jean-Francis Michon	Université de Rouen

Automorphismes projectifs et polynômes binaires irréductibles

Philippe Ravache

LITIS - Équipe Combinatoire et Algorithmes
Université de Rouen
Avenue de l'Université
76800 Saint-Étienne-du-Rouvray

Table des matières

Remerciements

Ça y est, j'arrive au terme de ma thèse, il est temps pour moi de remercier tous ceux qui m'ont entouré durant ces quatre années.

Bien évidemment, mes premiers remerciements s'adressent à mon directeur de thèse, Jean-Francis Michon, sans qui cette aventure n'aurait pas été possible. Qu'il sache que je lui suis extrêmement reconnaissant, tout d'abord, d'avoir accepté de me prendre sous sa direction, puis, de m'avoir éclairé de ses lumières tout au long de mon parcours, d'avoir été toujours disponible et enfin, parce c'est une personne avec qui j'aime discuter, qu'il soit question de recherche ou non. Travailler avec lui a été très plaisant et j'espère que cela continuera à l'avenir.

Ensuite, je tiens à remercier Philippe Langevin et Patrick Solé d'avoir accepté d'être les rapporteurs de cette thèse. Cela demande beaucoup d'investissement et pour cela, je leur en suis très reconnaissant. De plus, leurs remarques ont à la fois été instructives, pour les références et les idées qu'ils m'ont données en rapport avec mes travaux, et encourageantes. Je remercie également Claude Carlet et Brigitte Vallée de s'être intéressés à mes travaux et d'avoir accepté de faire partie de mon jury. De manière générale, merci aux membres de mon jury de m'avoir consacré une partie de leur temps, qu'ils sachent que leur présence est pour moi un réel honneur.

Un grand merci au département informatique de l'Université de Rouen de m'avoir accueilli durant toute cette période. Je remercie tous ses membres (ou anciens membres) pour leur gentillesse et leur bonne humeur. Je remercie tous ceux avec qui j'ai partagé des enseignements de m'avoir facilité la tâche : Arnaud, Christophe C., Christophe H., Florent H., Jean-Gabriel, Jean-Philippe, Laurent, Magali, Martine, Olivier, Pascal et Saïd. Mention spéciale à Jean-Philippe et Martine qui m'ont pris sous leurs ailes la première année et à Eric pour avoir été mon tuteur. Je remercie également Pavel de m'avoir encadré lors du stage de Master et donné goût à la cryptologie. Merci à Maryse et Bruno M. pour toutes les petites choses que j'ai pu leur demander. Et merci à Carla pour les bons moments passés à table ou autour d'un café.

Je remercie l'ensemble du LITIS de m'avoir offert une bourse de thèse et ainsi permis d'en arriver là. J'en profite d'ailleurs pour remercier Brigitte, Fabienne et Dominique pour tous les services qu'elles ont pu me rendre.

Je passe maintenant à mes “semblables”, les doctorants. En premier lieu, je pense bien sûr à mon cher Bedine, qui a été mon co-bureau tout au long de la thèse, je le remercie pour sa gentillesse et pour tous les moments que l'on a passé à discuter de tout et de rien. Je remercie également tous les autres doctorants passés par le département : Benoist, Élise, Faissal, Hadrien, Houda, Janvier, Ludovic, Mikaël et Molka. J'ai passé de bons moments avec eux et je suis heureux de les avoir rencontrés. Merci aussi à John, Simon et Yoann, mes collègues représentants. Je remercie Nadia, avec qui ce fut un plaisir de travailler, et même simplement, de discuter. Et merci à Karina, qui fut une bonne amie durant cette période.

Enfin, je conclus avec mes proches, je serai bref pour ne pas en faire trop, mais qu'ils sachent que le cœur y est. J'adresse un très grand merci à ma famille pour le soutien qu'ils m'ont apporté, c'est réconfortant de savoir qu'ils sont derrière moi, quoi qu'il arrive. Merci aussi à tous mes amis, j'ai toujours autant de plaisir à les voir, ils me permettent de déconnecter et ça fait du bien.

Et je tiens à remercier tout particulièrement Eleonora. Elle a été présente durant toute cette période et m'a supporté (dans tous les sens du terme) dans les moments difficiles. Je la remercie pour sa patience et sa joie de vivre, c'est une chance de l'avoir à mes côtés.

Ce n'est pas évident de se remémorer toutes les personnes rencontrées ces dernières années, donc je remercie tous ceux que j'ai pu oublier et j'espère qu'ils ne m'en tiendront pas trop rigueur.

Notations

$\mathfrak{S}_3$	groupe symétrique d'indice 3
$\mathfrak{A}_3$	sous-groupe alterné de $\mathfrak{S}_3$
$\mathbb{F}_q$	corps fini à q éléments
$\overline{\mathbb{F}_q}$	clôture algébrique de $\mathbb{F}_q$
$\mathbb{F}_q^*$	groupe multiplicatif de $\mathbb{F}_q$
$\mathbb{F}_q[X]$	anneau des polynômes à une indéterminée X à coefficients dans $\mathbb{F}_q$
$[K_1 : K_2]$	degré d'extension du corps K_1 sur le corps K_2
$< K_1 \cup K_2 >$	plus petit corps contenant les corps K_1 et K_2
$\log_g(x)$	logarithme discret de x en base g
deg	degré (d'un polynôme, d'un hexagone, d'un élément ou d'un point)
Card(E)	cardinal de l'ensemble E
ord	ordre (d'un élément ou d'un polynôme)
$\mathbb{P}^1(\mathbb{F}_q)$	droite projective de $\mathbb{F}_q$
$\mathrm{PGL}_2(\mathbb{F}_q)$	groupe projectif linéaire de $\mathbb{F}_q$
$\mathrm{GL}_2(\mathbb{F}_q)$	groupe linéaire de $\mathbb{F}_q$
$\mathcal{I}$	ensemble des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré ≥ 2
$\mathcal{I}(n)$	ensemble des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré n
$I(n)$	nombre de polynômes irréductibles de $\mathbb{F}_2[X]$ de degré n
Hex(P)	orbite du polynôme P sous l'action de $\mathfrak{S}_3$
$hex(n)$	nombre d'hexagones de degré n
$h_i(n)$	nombre d'hexagones à i éléments de degré n
μ	fonction de Möbius
χ_n	caractère de Dirichlet modulo n
Tr(P)	coefficient de X^{n-1}, pour P un polynôme de degré n
$\mathrm{Tr}_n(a)$	trace $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}$ de a, notée Tr(a) lorsqu'il n'y a pas d'ambiguïté
P_a	polynôme minimal de l'élément a
rg	rang (d'un élément ou d'un polynôme)
$\otimes$	produit symbolique (composition)

Introduction

Les polynômes irréductibles de $\mathbb{F}_2[X]$ servent essentiellement, en Informatique, au codage de l'information : codage auto-correcteur et codage cryptographique. Ils jouent un rôle analogue aux nombres premiers en arithmétique.

En effet, si nous prenons d'un côté l'anneau des entiers $\mathbb{Z}$ et ses nombres premiers et de l'autre, l'anneau des polynômes binaires $\mathbb{F}_2[X]$ et ses polynômes irréductibles, les analogies sont nombreuses. Il est tout aussi intéressant d'examiner les différences entre ces objets. Pour ne citer que deux exemples :

- la factorisation d'un polynôme de $\mathbb{F}_2[X]$ est algorithmiquement bien plus facile (on pense qu'elle peut être réalisée en temps polynomial) que la factorisation d'un entier,
- l'hypothèse de Riemann pour $\mathbb{Z}$ est toujours un mystère alors que le problème analogue pour $\mathbb{F}_2[X]$ est simple.

Ces deux exemples classiques (et de nombreux autres) portent à croire que l'arithmétique de $\mathbb{F}_2[X]$ est plus simple que celle de $\mathbb{Z}$. Néanmoins, il reste beaucoup de problèmes ouverts concernant $\mathbb{F}_2[X]$, à l'image de l'existence d'une infinité de trinômes irréductibles.

Dans cette thèse nous nous intéressons à l'une de ces différences et à ses conséquences : il existe des transformations algébriques simples qui préservent l'irréductibilité. La plus connue est celle qui renvoie le polynôme "réciproque" d'un irréductible de degré > 1. Cette transformation est "visible" sur l'écriture même du polynôme et a évidemment attiré l'attention de plusieurs chercheurs, tels que Carlitz [Car67], Varshamov [Var84], Wiedemann [Wie88], Meyn [Mey90], Niederreiter [Nie90] ou encore Cohen [Coh92]. Leurs travaux ont notamment permis :

- le dénombrement des polynômes réciproques irréductibles de degré donné,
- la construction de familles explicites infinies de polynômes réciproques irréductibles.

On peut d'ailleurs remarquer que ces résultats n'ont pas d'équivalents pour les nombres premiers.

Notre travail généralise leurs résultats. Il est basé sur l'action naturelle du groupe $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ sur la droite projective $\mathbb{P}^1(\mathbb{F}_2)$. Chacun des sous-groupes $G \subset \mathfrak{S}_3$ engendre une famille différente de polynômes G-invariants. Les polynômes réciproques constituent l'une de ces familles.

La troisième partie est consacrée à l'interprétation des constructions des polynômes

irréductibles G-invariants. En particulier, des résultats complets sont donnés pour le cas des polynômes réciproques. Nous illustrons le résultat de Niederreiter (basé sur l'évaluation de certaines sommes de Kloosterman) en utilisant une courbe elliptique sur $\mathbb{F}_2$ particulière : la construction des polynômes réciproques irréductibles reflète alors, dans notre interprétation, la division par deux des points rationnels de cette courbe.

Nous donnons aussi des interprétations originales pour les autres constructions de familles G-invariantes infinies, mais nous ne pouvons donner un tableau vraiment complet (pour chaque G) pour l'instant. En tout cas, les courbes elliptiques semblent jouer un rôle majeur.

Enfin nous nous sommes limités volontairement aux polynômes de $\mathbb{F}_2[X]$ et on ne trouvera ici aucun résultat concernant le cas "général" des polynômes irréductibles de $\mathbb{F}_q[X]$. Le lecteur qui veut se lancer dans cette entreprise devra utiliser le groupe $\mathrm{PGL}_2(\mathbb{F}_q)$, mais le travail nécessaire pour établir les résultats analogues semble non négligeable. Un premier pas pourrait consister à se limiter à la caractéristique 2.

Première partie

Les familles de polynômes invariants

Dans cette première partie, nous commencerons par une introduction sur les corps finis et les polynômes irréductibles : nous rappellerons brièvement les définitions et propriétés nécessaires à une bonne compréhension de ce qui va suivre, en supposant néanmoins que le lecteur possède certaines bases en algèbre.

Ensuite, dans le Chapitre 2, nous allons expliquer comment le groupe des permutations de trois éléments, ou groupe symétrique $\mathfrak{S}_3$, agit sur les polynômes binaires irréductibles. Pour cela, nous décrirons dans un premier temps l'action de $\mathfrak{S}_3$ sur la droite projective de $\mathbb{F}_2$, puis, nous verrons que cette action peut s'étendre aux polynômes irréductibles de $\mathbb{F}_2[X]$.

Enfin, dans le Chapitre 3, nous décrirons cette action en détails. Le groupe symétrique $\mathfrak{S}_3$ est constitué de six éléments (l'identité, trois transpositions et deux cycles) et possède quatre sous-groupes non-triviaux (trois sous-groupes à deux éléments contenant chacun une transposition et un sous-groupe à trois éléments contenant les cycles). Nous allons alors définir des familles de polynômes irréductibles invariants sous l'action de ces sous-groupes : les sous-groupes à deux éléments vont engendrer trois familles d'invariants distinctes mais complètement analogues (parmi lesquelles on trouve la famille des polynômes irréductibles réciproques) et le sous-groupe à trois éléments va en engendrer une quatrième. Nous allons étudier ces familles par l'intermédiaire de l'étude des différents types d'hexagones qui existent, un hexagone étant l'orbite d'un polynôme irréductible sous l'action de $\mathfrak{S}_3$. En particulier, nous allons donner quelques propriétés des polynômes invariants qui composent les hexagones ainsi que les formules permettant de calculer le nombre d'hexagones de chaque type, pour un degré donné.

L'essentiel des résultats présentés dans cette première partie se trouve dans l'article [MR10a]. De plus, si le lecteur souhaite utiliser ces travaux, nous proposons dans l'Annexe B plusieurs fonctions mises en œuvre à l'aide du logiciel SAGE [Sag], illustrées de quelques exemples.

Chapitre 1

Notions de base

Dans ce premier chapitre, nous allons donner les définitions et les propriétés, concernant les corps finis et les polynômes irréductibles, nécessaires à la bonne compréhension de ce manuscrit. Nous considérons que le lecteur possède certaines bases en algèbre, notamment les notions de groupe, d'anneau ou de corps. Pour les notions de bases ou pour plus de détails sur ce qui va suivre, le lecteur pourra consulter, par exemple, les livres de Lang [Lan02], de Cohn [Coh03] et de Lidl et Niederreiter [LN94] (les deux premiers étant des classiques d'algèbre et le dernier étant spécialisé sur les corps finis).

On considère que K est un **corps** et que $+$ et $\cdot$ sont les lois, respectivement additive et multiplicative, de K. On dit que K est un **corps fini** s'il possède un nombre fini d'éléments. Le **cardinal** q d'un corps fini est toujours une puissance n d'un nombre premier p et on écrit alors $\mathrm{Card}(K) = q = p^n$. On dit que p est la **caractéristique** de K. Il y a unicité du corps à q éléments, nous le noterons $\mathbb{F}_q$.

Si $n = 1$, alors $\mathbb{F}_q = \mathbb{F}_p$ et on dit que le corps est **premier**, il est alors isomorphe à $\mathbb{Z}/(p)$, l'anneau des entiers modulo p. D'autre part, si $n > 1$, $\mathbb{F}_q$ est une **extension** de degré n du corps premier $\mathbb{F}_p$, n est appelé **degré d'extension** de $\mathbb{F}_q$ sur $\mathbb{F}_p$ et on écrit $[\mathbb{F}_q : \mathbb{F}_p] = n$. Dans ce cas, on peut considérer $\mathbb{F}_q$ comme étant un espace vectoriel de dimension n sur $\mathbb{F}_p$. Ainsi, si $\alpha_1, \alpha_2, ..., \alpha_n$ est une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$, tout élément $\beta \in \mathbb{F}_q$ pourra s'écrire $\beta = a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n$, où $a_i \in \mathbb{F}_p$, $i \in \{1, ..., n\}$.

Soient $K_1 = \mathbb{F}_{p^{k_1}}$ et $K_2 = \mathbb{F}_{p^{k_2}}$ deux corps finis de caractéristique p, avec k_1 et k_2 deux entiers strictement positifs. Alors, premièrement, K_1 est un sous-corps de K_2 si et seulement si $k_1 | k_2$. Et dans ce cas, K_2 est une extension de K_1 de degré k_2/k_1. Deuxièmement, l'intersection des deux corps $K_1 \cap K_2$ est $\mathbb{F}_{p^d}$, où d est le plus grand commun diviseur de k_1 et k_2. Et troisièmement, le plus petit corps contenant K_1 et K_2, noté $< K_1 \cup K_2 >$, est le corps $\mathbb{F}_{p^m}$, où m est le plus petit commun multiple de k_1 et k_2.

Le **groupe multiplicatif** de $\mathbb{F}_q$, noté $\mathbb{F}_q^*$, est l'ensemble des éléments inversibles pour la loi multiplicative, on a donc $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ et $\mathrm{Card}(\mathbb{F}_q^*) = q - 1$. Une propriété importante est que tout groupe multiplicatif d'un corps fini est **cyclique**. Il existe donc

un élément $g \in \mathbb{F}_q^*$, appelé **générateur**, tel que tout élément x de $\mathbb{F}_q^*$ peut s'écrire comme une puissance l de g, $1 \leq l \leq q-1$. Dans ce cas, on dit que l est le **logarithme discret** de x en base g et on écrit $\log_g(x) = l$.

Maintenant, soit $x \in \mathbb{F}_q^*$, on appelle **ordre** de x le plus petit entier $k > 0$ tel que $x^k = 1$, on note alors $\text{ord}(x) = k$. Le **Petit Théorème de Fermat** nous dit que, $\forall x \in \mathbb{F}_q^*$, $x^{q-1} = 1$ et que par extension, $\forall x \in \mathbb{F}_q$, $x^q = x$. Ainsi, d'une part, on sait que l'ordre d'un élément de $\mathbb{F}_q^*$ est un diviseur de $q-1$. Si l'ordre est $q-1$, alors l'élément est un générateur de $\mathbb{F}_q^*$, on dit aussi que c'est un élément **primitif** de $\mathbb{F}_q$. D'autre part, on sait que tous les éléments de $\mathbb{F}_q$ sont racines du polynôme $f(X) = X^q - X$. Par conséquent, $f(X)$ se décompose en facteurs de degré 1 dans $\mathbb{F}_q$. On dit que $\mathbb{F}_q$ est le **corps de décomposition** de f car c'est le plus petit corps vérifiant cela.

On note $\mathbb{F}_p[X]$ l'anneau des polynômes à une inconnue X, à coefficients dans $\mathbb{F}_p$. Soient $P \in \mathbb{F}_p[X]$ et n le degré de P, noté $\deg(P)$. On suppose que P est **irréductible**, c'est à dire qu'il ne possède aucun facteur non-trivial. D'une part, $\mathbb{F}_q$ est le corps de décomposition de P. D'autre part, tout élément de $\mathbb{F}_q$ est racine d'un polynôme irréductible de $\mathbb{F}_p[X]$ de degré un diviseur de n. De plus, $\mathbb{F}_q$ est isomorphe à $\mathbb{F}_p[X]/(P(X))$, l'ensemble des polynômes de $\mathbb{F}_p[X]$ modulo P. Ce dernier point est très important car c'est de cette manière que l'on fait les opérations sur les corps finis : les éléments de $\mathbb{F}_q$ sont considérés comme des polynômes de $\mathbb{F}_p[X]$ de degré strictement inférieur à n et les opérations entre les éléments sont les opérations habituelles entre polynômes, modulo $P(X)$ (pour reprendre ce que l'on a vu plus tôt, si α est une racine de P, alors $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ est une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$).

Maintenant, soit α une racine de P, l'automorphisme de **Frobenius** σ se définit de la manière suivante : $\sigma(\alpha) = \alpha^p$. Toutes les racines de P peuvent s'écrire sous la forme $\sigma^i(\alpha) = \alpha^{p^i}$, $0 \leq i \leq n-1$. On dit que les racines de P sont **conjuguées** par l'automorphisme de Frobenius. Toutes les racines d'un polynôme irréductible ont le même ordre donc par extension, on dira que c'est également l'ordre du polynôme. Et si les racines sont des éléments primitifs de $\mathbb{F}_q$, on dira que le polynôme est primitif.

Tous les travaux qui seront présentés dans cette thèse seront faits en caractéristique 2. En particulier, nous allons étudier les polynômes de $\mathbb{F}_2[X]$ ainsi que les racines de ces polynômes, appartenant aux extensions de $\mathbb{F}_2$.

Chapitre 2

Action de $\mathfrak{S}_3$

Dans ce qui suit, nous allons expliquer comment le groupe symétrique $\mathfrak{S}_3$ agit sur l'ensemble des polynômes irréductibles à coefficients dans $\mathbb{F}_2$. Pour cela, nous décrivons dans un premier temps l'action de $\mathfrak{S}_3$ sur la droite projective de $\mathbb{F}_2$ et nous transposons ensuite cette action aux polynômes, de manière naturelle.

2.1 Sur $\mathbb{P}^1(\mathbb{F}_2)$

Le groupe symétrique d'indice 3 ($\mathfrak{S}_3$), ou groupe des permutations de trois éléments (que nous appellerons 1, 2 et 3), est un groupe non-commutatif composé de six éléments : l'identité Id, les trois transpositions (12), (23) et (13) et les deux cycles (123) et (132). $\mathfrak{S}_3$ possède six sous-groupes qui sont :

- Le sous-groupe trivial : $\{Id\}$.
- Les trois sous-groupes cycliques d'ordre 2 générés par les trois transpositions : $\{Id, (12)\}$, $\{Id, (23)\}$ et $\{Id, (13)\}$. Ces sous-groupes sont conjugués.
- Le sous-groupe cyclique d'ordre 3 contenant les deux cycles : $\{Id, (123), (132)\}$. Ce sous-groupe est distingué, on l'appelle le groupe alterné $\mathfrak{A}_3$.
- Le groupe tout entier.

On sait que $\mathfrak{S}_3$ peut être généré par un ensemble de 2 transpositions. Par exemple, prenons $u = (12)$ et $v = (23)$, alors on a $uv = (123)$, $vu = (132)$ et $uvu = vuv = (13)$. Ces relations forment une présentation de $\mathfrak{S}_3$. Cette présentation n'est pas unique, on retrouve souvent dans la littérature :

$$U^2 = 1,\ V^3 = 1,\ UVU = V^2$$

($u = U$ et $uv = V$).

La droite projective sur un corps K, notée $\mathbb{P}^1(K)$, est l'ensemble des droites vectorielles du plan vectoriel K^2. Si $K = \mathbb{F}_2$, cela représente trois droites que l'on peut

identifier par les trois points $\mathbb{F}_2$-rationnels suivants : $(0,1)$, $(1,1)$ et $(1,0)$. On a donc :

$$\mathbb{P}^1(\mathbb{F}_2) = \{(0,1),(1,1),(1,0)\}.$$

Nous appellerons ces points respectivement 0, 1 et ∞.

Le groupe d'automorphismes de la droite projective est le groupe $\mathrm{PGL}_2(\overline{\mathbb{F}_2})$, c'est le groupe projectif linéaire de $\overline{\mathbb{F}_2}$. Son sous-ensemble formé des éléments $\mathbb{F}_2$-rationnels est $\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2)$, le groupe des matrices 2×2 inversibles à coefficients dans $\mathbb{F}_2$. $\mathrm{GL}_2(\mathbb{F}_2)$ agit sur l'espace vectoriel $\mathbb{F}_2 \times \mathbb{F}_2$ par la transformation habituelle suivante, appelée transformation de Möbius :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix},$$

avec $ad - bc = 1$. En utilisant les coordonnées projectives, on obtient l'homographie classique :

$$(x:1) \to \begin{cases} (\frac{ax+b}{cx+d} : 1) & \text{si } cx+d \neq 0 \\ \infty & \text{sinon,} \end{cases}$$

et

$$\infty \to \begin{cases} (\frac{a}{c} : 1) & \text{si } c \neq 0 \\ \infty & \text{sinon.} \end{cases}$$

Maintenant, du fait de l'isomorphisme

$$\mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3,$$

on a une correspondance entre les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$, les homographies et les éléments de $\mathfrak{S}_3$. Nous présentons explicitement cette correspondance en commençant par les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Les homographies correspondantes sont :

$$x \to x,\ x+1,\ \frac{x}{x+1},\ \frac{1}{x},\ \frac{1}{x+1},\ \frac{x+1}{x}.$$

Et enfin, les permutations des trois points de la droite projective correspondantes sont :

$$Id,\ (0\ 1),\ (1\ \infty),\ (0\ \infty),\ (0\ 1\ \infty),\ (0\ \infty\ 1).$$

2.2 Sur les polynômes irréductibles de $\mathbb{F}_2[X]$

Nous avons vu précédemment que $\mathfrak{S}_3$ peut être généré à l'aide de deux transpositions, ainsi, pour définir une action gauche de $\mathfrak{S}_3$ sur l'ensemble

$$\mathcal{I} = \{P \in \mathbb{F}_2[X],\ P \text{ irréductible}\} \setminus \{X, X+1\}$$

(0 et 1 ne sont pas racines de P), nous la définissons pour les transpositions (01) et (0∞) de la manière suivante :

$$P^{(01)} = P(X+1)$$
$$P^{(0\infty)} = X^{\deg(P)} P(\frac{1}{X}).$$

Pour une écriture simplifiée, nous utiliserons les notations

$$P^{+}(X) = P(X+1)$$
$$P^{*}(X) = X^{\deg(P)} P(\frac{1}{X}).$$

Le polynôme P^* est appelé **réciproque** de P.

Les actions des autres éléments de $\mathfrak{S}_3$ sont alors définies par composition. En utilisant le fait que, étant données deux transpositions σ et τ, on a $P^{\sigma\circ\tau} = (P^{\tau})^{\sigma}$, cela donne :

$$P^{(01\infty)} = P^{(0\infty)\circ(01)} = (P^{+})^{*},$$

$$P^{(0\infty 1)} = P^{(01)\circ(0\infty)} = (P^{*})^{+},$$

$$P^{(1\infty)} = P^{(01)\circ(0\infty)\circ(01)} = P^{(0\infty)\circ(01)\circ(0\infty)} = ((P^{+})^{*})^{+} = ((P^{*})^{+})^{*}.$$

Pour ne pas surcharger les notations, nous ne mettrons pas les parenthèses dans la suite, ainsi, par exemple, $((P^{+})^{*})^{+}$ sera noté P^{+*+}. Aussi, nous utiliserons la notation suivante :

$$\mathcal{I}(n) = \{P \in \mathcal{I} \mid \deg(P) = n\}.$$

Chapitre 3

Hexagones

Dans ce chapitre, nous allons nous intéresser à la notion d'hexagone. Dans un premier temps, nous allons donner sa définition. Nous allons voir qu'il existe 4 types d'hexagones à savoir les hexagones à 1 élément, 2 éléments, 3 éléments et 6 éléments. Ensuite, nous étudierons plus en détails chaque type d'hexagones, en particulier, ceux à 2 et 3 éléments, pour lesquels nous introduirons et donnerons quelques propriétés sur les polynômes invariants qui les composent. Et nous donnerons les formules d'énumération des hexagones de chaque type pour un degré donné ce qui nous permettra de connaître la répartition en hexagones des polynômes irréductible de $\mathbb{F}_2[X]$ pour chaque degré.

3.1 Introduction aux hexagones

Soit $P \in \mathcal{I}$.

Définition 1. *L'**hexagone** de P, noté* $\mathrm{Hex}(P)$*, est l'orbite de P sous l'action de $\mathfrak{S}_3$:*

$$\begin{aligned}\mathrm{Hex}(P) &= \{P^\sigma | \sigma \in \mathfrak{S}_3\} \\ &= \{P, P^*, P^+, P^{*+}, P^{+*}, P^{*+*} = P^{+*+}\}.\end{aligned}$$

Ainsi, un hexagone est inclus dans $\mathcal{I}$. Le nom hexagone vient du fait que si P n'est invariant par l'action d'aucun des éléments non-triviaux de $\mathfrak{S}_3$, alors tous les polynômes de son orbite sont distincts les uns des autres, donc l'orbite contient 6 polynômes et peut être représentée de la manière suivante :

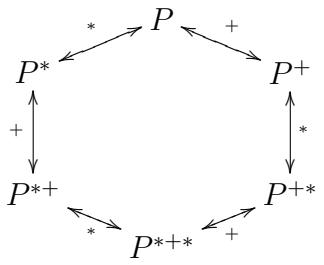


FIG. 3.1 – Hexagone non-dégénéré

Par contre, si P est invariant, alors $\mathrm{Card}(\mathrm{Hex}(P)) < 6$ et on dit que $\mathrm{Hex}(P)$ est un hexagone **dégénéré**. Plus précisément, si P est invariant par l'action de l'un des sous-groupes de $\mathfrak{S}_3$ d'ordre 2, son hexagone contient 3 polynômes, s'il est invariant par l'action du sous-groupe d'ordre 3, le groupe alterné $\mathfrak{A}_3$, son hexagone contient 2 polynômes et enfin, s'il est invariant par l'action de $\mathfrak{S}_3$ tout entier, son hexagone ne contient qu'un seul polynôme.

Du fait de l'irréductibilité de P, tous les polynômes de $\mathrm{Hex}(P)$ sont de même degré. Ainsi, d'une part nous définissons le degré d'un hexagone comme suit :

$$\deg(\mathrm{Hex}(P)) = \deg(P),$$

d'autre part, nous pouvons définir la fonction $hex(n)$ (resp. $h_1(n), h_2(n), h_3(n), h_6(n)$) sur les entiers ≥ 2 comme étant le nombre de tous les hexagones (resp. des hexagones à $1, 2, 3, 6$ élément(s)) de degré n et on a :

$$hex(n) = h_1(n) + h_2(n) + h_3(n) + h_6(n).$$

Nous pouvons maintenant passer à la description de chaque type d'hexagone.

3.2 Hexagone à 1 élément

Un hexagone ne contient qu'un seul polynôme si et seulement si ce polynôme est invariant par l'action de $\mathfrak{S}_3$ tout entier. Ce cas est très simple car en fait, un seul polynôme irréductible vérifie cette propriété :

Proposition 1. *Soit $P \in \mathcal{I}$ tel que $\mathrm{Hex}(P) = \{P\}$, alors $P = X^2 + X + 1$.*

Démonstration. Supposons que P soit invariant par l'action de $\mathfrak{S}_3$, autrement dit $P = P^* = P^+$. Cela implique que, si g est une racine de P, alors g^{-1} et $g + 1$ le sont aussi. De ce fait

$$g + 1 = g^{2^k} \text{ et } g^{-1} = g^{2^l},$$

pour 2 entiers $k, l < n$, ce qui donne :

$$g = g^{2^{2k}} = g^{2^{2l}}.$$

Les racines de P sont distinctes et conjuguées donc

$$g = g^{2^{2k}} \Rightarrow 2k = 0 \mod n$$

et pour la même raison

$$2l = 0 \mod n.$$

Ainsi

$$k = l = 0 \mod n/2.$$

Du fait que ni k, ni l ne peuvent être égaux à 0, l'unique possibilité est $k = l = n/2$. Par conséquent

$$g + 1 = g^{-1}$$

et $P = X^2 + X + 1$. □

On en déduit donc trivialement la valeur de la fonction h_1 :

$$h_1(n) = \begin{cases} 1 & \text{si } n = 2. \\ 0 & \text{sinon.} \end{cases}$$

3.3 Hexagones à 2 éléments

3.3.1 Présentation

Soit $P \in \mathcal{I}$. Nous commençons par donner la définition suivante :

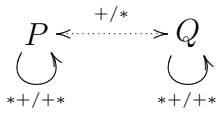
Définition 2. *Si $P^{+*} = P^{*+} = P$, on dit que P est **alternatif**.*

Comme énoncé plus tôt, l'hexagone de P, $P \neq X^2 + X + 1$, comporte 2 éléments si P est invariant par l'action du groupe alterné $\mathfrak{A}_3$, c'est à dire, invariant par l'action des permutations $(0\ 1\ \infty)$ et $(0\ \infty\ 1)$. Cela se traduit plus explicitement par

$$P^{*+} = P^{+*} = P \text{ et } P \neq P^*.$$

On en déduit la définition suivante :

Définition 3. *Un **hexagone dégénéré à 2 éléments** est composé de 2 polynômes irréductibles alternatifs distincts P et Q tels que :*



Exemple 1. *Voici, par exemple, les 2 hexagones dégénérés à 2 éléments de plus petit degré : pour former le premier, on retrouve les 2 polynômes irréductibles de degré 3, le deuxième hexagone est de degré 9 et c'est le seul.*

$$\underset{*+/+*}{X^3+X+1} \xleftrightarrow{+/*} \underset{*+/+*}{X^3+X^2+1}$$

FIG. 3.2 – Hexagone dégénéré à 2 éléments de degré 3

$$\underset{*+/+*}{X^9+X+1} \xleftrightarrow{+/*} \underset{*+/+*}{X^9+X^8+1}$$

FIG. 3.3 – Hexagone dégénéré à 2 éléments de degré 9

3.3.2 Propriétés des alternatifs et formules d'énumération

Nous allons maintenant donner quelques propriétés sur les polynômes irréductibles alternatifs :

Théorème 1. *Les polynômes irréductibles alternatifs sont exactement les facteurs irréductibles des polynômes*

$$B_k(X) = X^{2^k+1} + X + 1,$$

pour $k \in \mathbb{N}$.
Si P *est alternatif, alors* $\deg(P) \equiv 0 \mod 3$ *ou* $P = X^2 + X + 1$. *Si* $\deg(P) = 3m$, *alors* $P|B_m$ *ou* $P|B_{2m}$.

Démonstration. Soit g une racine d'un polynôme irréductible P, alors $1 + 1/g$ est une racine de P^{*+}. On suppose que P est un facteur irréductible de B_k, cela implique que $\deg(P) \geq 2$, car 0 et 1 ne sont pas racine de B_k. Toute racine g de P est une racine de B_k donc

$$g^{2^k} = 1 + \frac{1}{g}.$$

Par conséquent, l'ensemble des racines de P est invariant par la transformation

$$T : g \to 1 + \frac{1}{g}$$

(définie sur $\overline{\mathbb{F}_{2^n}} \setminus \{0, 1\}$), ainsi, $P^* = P^+$ et P est alternatif.

Réciproquement, si P est alternatif et g une de ses racines, alors

$$g^{2^k} = 1 + \frac{1}{g},$$

pour un entier $0 \leq k < n = \deg(P)$ et donc $P|B_k$.

La transformation T est d'ordre 3 et permute les racines de P, car P est alternatif. Si $\deg(P) > 2$, aucune racine de P ne peut être invariante par cette transformation, car dans ce cas, on aurait

$$g = 1 + \frac{1}{g}$$

et g serait une racine de $X^2 + X + 1$, ce qui est une contradiction. On en déduit que le nombre de racines de P est divisible par 3 et donc :

$$\deg(P) = n \equiv 0 \mod 3.$$

Étant donné que $T^3 = I$, on a

$$g^{2^{3k}} = g.$$

Cela implique que g est un élément du corps $\mathbb{F}_{2^{3k}}$, donc, si $\deg(P) = n$,

$$\mathbb{F}_{2^n} \subseteq \mathbb{F}_{2^{3k}}.$$

Alors

$$3k \equiv 0 \mod n$$

et la limite sur k imposée plus haut implique que $k = n/3$ ou $k = 2n/3$. □

Dans le théorème précédent, on voit qu'un polynôme irréductible alternatif de degré $3m$ divise B_m ou B_{2m}. On introduit alors la notion de type pour différencier ces 2 cas :

Définition 4. *Soit P un polynôme irréductible alternatif de degré $3m$. Si $P|B_m$, on dit que le **type** de P est 1. Si $P|B_{2m}$, on dit que son type est 2.*

Nous n'avons pas besoin de définir le type de $P = B_0$.

Proposition 2. *P et P^* sont de types différents.*

Démonstration. Soit P un polynôme irréductible alternatif de type 1. Le réciproque P^* est lui aussi alternatif, de même degré. Supposons que $\deg(P) = 3m$ (étant de type 1, cela implique que $P|B_m$) et soit g une racine de P. On a :

$$g^{2^m} = 1 + \frac{1}{g}.$$

Maintenant, prenons $h = g^{-1}$, c'est une racine de P^* et

$$\begin{aligned} h^{-2^m} &= 1 + h \\ h^{2^m} &= \frac{1}{1+h} \\ h^{2^{2m}} &= \left(\frac{1}{1+h}\right)^{2^m} = \frac{1}{1+h^{2^m}} = 1 + \frac{1}{h}, \end{aligned}$$

ainsi $B_{2m}(h) = 0$ et donc $P^* | B_{2m}$.

La démonstration pour un polynôme de type 2 est similaire. □

Pour résumer, nous énonçons le corollaire suivant :

Corollaire 1. *Soit $P \in \mathcal{I}$ de degré $3m$. Si P est de type 1, alors, P divise B_m et B^*_{2m} et P^* est de type 2 et divise B^*_m et B_{2m}.*

Exemple 2. *Le polynôme $P = B_1 = X^3 + X + 1$, comme nous l'avons déjà vu, est alternatif et on remarque que $P^* = X^3 + X^2 + 1$ est un facteur de*

$$B_2 = (X^2 + X + 1)(X^3 + X^2 + 1).$$

On peut également déduire du Théorème 1 un résultat sur l'ordre des polynômes alternatifs :

Corollaire 2. *L'ordre d'un polynôme irréductible alternatif de degré $3m$, divise $2^{2m} + 2^m + 1$.*

Démonstration. Soit $P \in \mathcal{I}(3m)$, P alternatif. On suppose que P est de type 1. Soit a une racine de P, d'après le Corollaire 1, $a^{2^n+1} + a + 1 = 0$. En mettant cette équation à la puissance 2^n, on obtient $a^{2^n(2^n+1)} + a^{2^n} + 1 = 0$. Maintenant, en multipliant par a, on a $a^{2^n(2^n+1)+1} + a^{2^n+1} + a = 0$. Enfin, on remplace le terme du milieu en utilisant la première équation, on obtient $a^{2^n(2^n+1)+1} + 1 = 0$.

Si P est de type 2, alors P^* est de type 1 et puisque P et P^* sont de même ordre, cela conclut la démonstration. □

Par la suite, nous utiliserons le corollaire suivant, conséquence triviale de la Proposition 2 :

Corollaire 3. *La moitié des polynômes irréductibles alternatifs de degré $3m$ divise B_m, l'autre moitié divise B_{2m}.*

Dans les propositions et théorèmes suivants, nous allons donner plusieurs caractéristiques concernant les polynômes B_k.

Proposition 3. *B_k n'a pas de racine multiple.*

Démonstration. On a $B_k(X) = X^{2^k+1}+X+1$ et sa dérivée $B'_k(X) = X^{2^k}+1 = (X+1)^{2^k}$. Étant donné que $B_k(1) \neq 0$, alors $B_k(X)$ et $B'_k(X)$ n'ont pas de racine commune et donc B_k n'a pas de racine multiple. □

Proposition 4. *$(X^2+X+1)|B_k$ si et seulement si k est pair.*

Démonstration. Soit α une racine de X^2+X+1, on sait que $\alpha^3 = 1$. De plus, $2^k+1 \equiv (-1)^k+1 \mod 3$. Donc si k est pair, $B_k(\alpha) = \alpha^2+\alpha+1 = 0$ et si k est impair, $B_k(\alpha) = \alpha$. □

Théorème 2. *Soit P un polynôme irréductible de degré $3m$, alors, $P|B_k$ si et seulement si les 3 conditions suivantes sont vérifiées :*

- *P est alternatif*
- *$m|k$*
- *$\frac{k}{m} \mod 3$ est égal au type de P.*

Démonstration. Dans un premier temps, nous prouvons que les conditions sont nécessaires.

Nous savons d'après le Théorème 1 que P est alternatif. En utilisant les mêmes arguments que plus tôt, on peut dire que toutes les racines de B_k sont dans $\mathbb{F}_{2^{3k}}$ et le plus petit corps contenant les racines de P est $\mathbb{F}_{2^{3m}}$. Si $P|B_k$, cela implique que $\mathbb{F}_{2^{3m}} \subseteq \mathbb{F}_{2^{3k}}$ et $m|k$.

Prenons $k = ml$, pour un certain entier l, et soit g une racine de P, alors, si P est de type 1 :

$$g^{2^m} = 1 + \frac{1}{g} = g^{2^k} = g^{2^{ml}}.$$

Puisque les $3m$ racines de P sont distinctes et d'après les propriétés de l'opérateur de Frobenius, on a

$$m = ml \mod 3m$$

et donc

$$l = 1 \mod 3.$$

Si P est de type 2, alors :

$$g^{2^{2m}} = 1 + \frac{1}{g} = g^{2^k} = g^{2^{ml}}$$

et $l = 2 \mod 3$ pour les mêmes raisons.

Nous prouvons maintenant que ces propriétés sont suffisantes.

Soit $P \in \mathcal{I}$ un polynôme alternatif de degré $3m$. Supposons que P soit de type t et $k = lm$, avec $l = t \mod 3$, alors pour toute racine g de P :

$$g^{2^k} = g^{2^{lm}} = g^{2^{tm}} = 1 + \frac{1}{g}.$$

La dernière égalité est une conséquence de la définition du type. Ainsi, g est toujours une racine de B_k et $P|B_k$. □

Nous donnons 2 exemples pour illustrer cela :

Exemple 3. *Pour $k = 2$: $B_2 = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$. Le facteur irréductible alternatif $X^3 + X^2 + 1$ correspond à $m = 1$ et son type est 2. On vérifie simplement que son type est 2 car si g est une racine de ce facteur, alors*

$$g^{2^2} = 1 + \frac{1}{g}.$$

Pour $k = 3$: $B_3 = X^9 + X + 1$. D'après le Théorème 2, $m = 3$ est l'unique cas dans lequel B_3 peut avoir des facteurs irréductibles (de type 1), de plus, on sait que ces facteurs sont de degré $3 \cdot 3 = 9$. On en déduit que B_3 est alternatif, irréductible et de type 1.

Nous pouvons maintenant établir notre principal résultat, qui est une simple conséquence du Théorème 2 :

Théorème 3. *Prenons $h_2(3m)$, avec $m \geq 1$, c'est à dire, la moitié des polynômes irréductibles alternatifs de degré $3m$. Alors, pour tout $k \geq 1$:*

$$2^k - (-1)^k = \sum_{\substack{d|k \\ \frac{k}{d} \not\equiv 0 \mod 3}} 3d\ h_2(3d). \tag{3.1}$$

Démonstration. Soit EB_k l'ensemble de tous les polynômes de degré ≥ 3 divisant B_k, d'après la Proposition 2 :

$$EB_k = \bigcup_{\substack{d|k \\ \frac{k}{d} \equiv 1 \mod 3}} E_1(3d) \ \cup \bigcup_{\substack{d|k \\ \frac{k}{d} \equiv 2 \mod 3}} E_2(3d),$$

avec $E_1(3d)$ (resp. $E_2(3d)$) l'ensemble des polynômes irréductibles alternatifs de degré $3d$ et de type 1 (resp. de type 2) divisant B_k. Alors, en regardant les degrés, on a :

$$\sum_{Q \in EB_k} \deg(Q) = \sum_{\substack{d|k \\ \frac{k}{d} \equiv 1 \mod 3}} 3d\ \mathrm{Card}(E_1(3d)) \ + \sum_{\substack{d|k \\ \frac{k}{d} \equiv 2 \mod 3}} 3d\ \mathrm{Card}(E_2(3d)).$$

Le Corollaire 3 implique :

$$\begin{aligned} \sum_{Q \in EB_k} \deg(Q) &= \sum_{\substack{d|k \\ \frac{k}{d} \equiv 1 \mod 3}} 3d\ h_2(3d) \ + \sum_{\substack{d|k \\ \frac{k}{d} \equiv 2 \mod 3}} 3d\ h_2(3d) \\ &= \sum_{\substack{d|k \\ \frac{k}{d} \not\equiv 0 \mod 3}} 3d\ h_2(3d). \end{aligned}$$

De plus, d'après la Proposition 4 on sait que :

$$\sum_{Q\in EB_k} \deg(Q) = \begin{cases} 2^k - 1 & \text{si } k \text{ est pair} \\ 2^k + 1 & \text{si } k \text{ est impair} \end{cases}$$
$$= 2^k - (-1)^k,$$

ce qui conclut notre démonstration. □

Comme nous avons vu précédemment, un hexagone dégénéré à 2 éléments est constitué de 2 polynômes irréductibles alternatifs, ainsi, le nombre de ces hexagones est en fait $h_2(3m)$.

En utilisant l'inversion de Möbius et les caractères de Dirichlet (voir Annexe A) sur (3.1), nous pouvons donner la formule permettant de calculer $h_2(3m)$:

Théorème 4. *Le nombre $h_2(n)$ des hexagones à 2 éléments de degré $n \geq 2$ est 0 si $n \not\equiv 0 \mod 3$, sinon, pour $n = 3m$:*

$$h_2(3m) = \frac{1}{3m} \sum_{\substack{d\neq 0 \\ d|m, \\ \mod 3}} \mu(d)(2^{m/d} - (-1)^{m/d}), \tag{3.2}$$

où μ est la fonction de Möbius.

Démonstration. Pour obtenir h_2 à partir du théorème précédent, nous utilisons des résultats élémentaires sur les caractères de Dirichlet et la convolution. De brèves explications sont données en annexe.

Nous définissons les fonctions arithmétiques :

$$f(m) = 2^m - (-1)^m$$
$$g(m) = 3m\, h_2(3m),$$

pour tout $m \geq 1$. Soit χ_3 le caractère principal de Dirichlet modulo 3 (voir Annexe A), la formule (3.1) peut s'écrire :

$$f(m) = \sum_{\substack{d\neq 0 \\ d|m, \\ \mod 3}} g(\frac{m}{d}) = \sum_{d|m} \chi_3(d) g(\frac{m}{d}),$$

or, en utilisant la convolution de Dirichlet, on obtient :

$$f = \chi_3 * g.$$

Par conséquent,

$$\mu\chi_3 * f = g.$$

Cette dernière égalité nous donne la formule (3.2). □

Nous donnons également la formule permettant de calculer $h_2(3m)$ récursivement.

Théorème 5. *Le nombre d'hexagones dégénérés à 2 éléments de degré* $3m$, $m \geq 1$, *est donné par la formule :*

$$h_2(3m) = \frac{I(m) + h_2(m)}{3}.$$

Nous donnerons une démonstration simple et dans l'esprit des résultats de cette thèse en deuxième partie.

Les premières valeurs de h_2 sont :

$3m$	3	6	9	12	15	18	21	24	27	30
$h_2(3m)$	1	0	1	1	2	3	6	10	19	33

Nous avons ajouté la suite des valeurs de h_2 au site de Sloane : The On-Line Encyclopedia of Integer Sequences [Slo]. C'est la suite A165920.

Enfin, nous donnons une borne pour $h_2(3m)$, afin d'avoir une estimation de la densité du nombre d'hexagones à 2 éléments :

Corollaire 4. *Pour un entier* $m \geq 1$ *:*

$$|3m\ h_2(3m) - 2^m| \leq 2^{\lfloor m/2 \rfloor + 1} + \lfloor m/2 \rfloor - 1.$$

Démonstration. D'après la formule (3.1), on a :

$$3m\ h_2(3m) = 2^m - (-1)^m + \sum_{\substack{d|m,\ d\geq 2 \\ d\not\equiv 0 \mod 3}} \mu(d)(2^{m/d} - (-1)^{m/d}).$$

Ainsi,

$$\begin{aligned} |3m\ h_2(3m) - 2^m| &\leq 1 + \sum_{1\leq i\leq \lfloor m/2 \rfloor} (2^i + 1) \\ &\leq 1 + 2(2^{\lfloor m/2 \rfloor} - 1) + \lfloor m/2 \rfloor = 2^{\lfloor m/2 \rfloor + 1} + \lfloor m/2 \rfloor - 1. \end{aligned}$$

□

On constate que le nombre d'hexagones à 2 éléments est strictement positif et croit de manière exponentielle à partir de $m = 3$.

3.4 Hexagones à 3 éléments

3.4.1 Présentation

Soit $P \in \mathcal{I}$, nous rappelons que $X+1 \notin \mathcal{I}$ et nous considérons que $P \neq X^2+X+1$. Là encore, nous commençons par donner la définition des polynômes invariants qui constituent les hexagones dégénérés à 3 éléments :

Définition 5. *On dit que P est **réciproque** (resp. **périodique**, **médian**) si $P^* = P$ (resp. $P^+ = P$, $P^{*+*} = P^{+*+} = P$).*

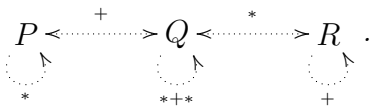
Les résultats présentés dans cette section sont bien connus, car comme nous venons de le voir, les hexagones dégénérés à 3 éléments sont liés aux polynômes irréductibles réciproques. Ces derniers ont été étudiés de nombreuses fois, pour plus de détails, notamment sur ce qui va suivre, nous nous référons aux articles de Carlitz [Car67], Cohen [Coh92], Meyn [Mey90] ou de Meyn et Götz [MG90]. Nous souhaitons cependant souligner le fait que, bien que les réciproques aient été plus étudiés que les médians ou les périodiques, ces 3 familles de polynômes jouent exactement le même rôle sur $\mathbb{F}_2$. L'intérêt suscité par les réciproques est en grande partie dû au fait que l'on peut les reconnaître visuellement, leurs coefficients étant symétriques.

Chacun des polynômes qui composent un hexagone à 3 éléments est invariant par l'action de l'un des trois sous-groupes à 2 éléments de $\mathfrak{S}_3$. Ainsi, si $P \in \mathcal{I}$ est tel que son orbite est de taille 3, cela signifie que P est invariant par l'action de l'une des trois transpositions. Supposons que ce soit par $(0\ \infty)$ (il est réciproque). Dans ce cas, P^+ est invariant par l'action de $(1\ \infty)$ (c'est un polynôme médian) et P^{+*} est invariant par l'action de $(0\ 1)$ (c'est un polynôme périodique) et ainsi :

$$\mathrm{Hex}(P) = \{P, P^+, P^{+*}\}.$$

Nous résumons cela dans la définition suivante :

Définition 6. *Un **hexagone dégénéré à 3 éléments** est constitué d'un polynôme irréductible réciproque P, d'un médian Q et d'un périodique R tels que :*



Étant donné que les inverses des racines de P sont aussi racines de P, le degré d'un polynôme irréductible réciproque est pair. Par conséquent, le degré d'un hexagone à 3 éléments est lui aussi pair.

Exemple 4. *Pour illustrer cela, nous donnons les 2 hexagones dégénérés à 3 éléments de plus petit degré : le premier est formé de l'ensemble des irréductibles de degré 4, le suivant intervient dès le degré 6.*

$$\underset{*}{X^4+X^3+X^2}+X+1 \overset{+}{\longleftrightarrow} \underset{*+*}{X^4+X^3}+1 \overset{*}{\longleftrightarrow} \underset{+}{X^4+X}+1$$

FIG. 3.4 – Hexagone dégénéré à 3 éléments de degré 4

$$\underset{*}{X^6+X^3}+1 \overset{+}{\longleftrightarrow} X^6+\underset{*+*}{X^4+X^3}+X+1 \overset{*}{\longleftrightarrow} X^6+X^5+\underset{+}{X^3}+X^2+1$$

FIG. 3.5 – Hexagone dégénéré à 3 éléments de degré 6

3.4.2 Propriétés des réciproques, médians et périodiques et formules d'énumération

Nous donnons maintenant quelques principaux résultats sur les polynômes composant les hexagones à 3 éléments. Le théorème suivant étend celui de Meyn (voir [Mey90], Théorème 1) aux médians et aux périodiques :

Théorème 6. *i) Tout polynôme irréductible réciproque (resp. médian, périodique) de degré $2n$ ($n \geq 1$) sur $\mathbb{F}_2$ est un facteur du polynôme*

$$H_{r,n}(X) = X^{2^n+1}+1$$

$$\textit{(resp. } H_{m,n}(X) = X^{2^n}+X^{2^n-1}+1, \quad H_{p,n}(X) = X^{2^n}+X+1\textit{).}$$

ii) Tout facteur irréductible de degré ≥ 2 de $H_{r,n}$ (resp. $H_{m,n}$, $H_{p,n}$) est un polynôme réciproque (resp. médian, périodique) de degré $2d$, où d divise n tel que n/d est impair.

Démonstration. Dans [Mey90], Meyn prouve le théorème pour les polynômes réciproques. Nous l'étendons simplement aux médians (resp. périodiques) en notant, d'une part, que $H_{m,n} = H^{+}_{r,n}$ (resp. $H_{p,n} = H^{+*}_{r,n}$) et d'autre part, qu'un polynôme irréductible médian (resp. périodique) est obtenu à partir d'un irréductible réciproque en lui appliquant la transformation $+$ (resp. $+^*$). □

En 1967, Carlitz a donné la formule calculant le nombre de réciproques irréductible pour un degré donné :

Théorème 7 (Carlitz, [Car67])**.** *Le nombre de polynômes irréductibles réciproques de degré $2m$ ($m \geq 1$) dans $\mathbb{F}_2[X]$ est*

$$S(2m) = \frac{1}{2m} \sum_{d|m,\ d\ odd} \mu(d) 2^{\frac{m}{d}},$$

où μ est la fonction de Möbius.

Dans [Car67], Carlitz prouve ce résultat par de longs calculs utilisant les séries L. Pour une démonstration utilisant l'inversion de Möbius, comparable à celle de la formule (3.2), nous renvoyons au papier de Meyn et Götz ([MG90]).

D'après nos définitions,

$$h_3(n) = S(n) \text{ pour } n \text{ pair}, n > 2$$

et $h_3(n) = 0$ pour toutes les autres valeurs de n. Le cas $n = 2$ correspond au polynôme $X^2 + X + 1$ qui donne un hexagone dégénéré à 1 élément, comme nous l'avons vu précédemment.

De même que pour h_2, nous donnons la formule permettant de calculer $h_3(2m)$ récursivement. Le lecteur pourra remarquer la symétrie entre les 2 formules.

Théorème 8. *Le nombre d'hexagones dégénérés à 3 éléments de degré $2m$, $m \geq 1$, est donné par la formule :*

$$h_3(2m) = \frac{I(m) + h_3(m)}{2}.$$

Là encore, nous donnerons une démonstration simple dans la deuxième partie de ce manuscrit.

Les premières valeurs de h_3 et S sont :

$2m$	2	4	6	8	10	12	14	16	18	20
$h_3(2m)$	0	1	1	2	3	5	9	16	28	51
$S(2m)$	1	1	1	2	3	5	9	16	28	51

Nous aurions pu ajouter la valeur $S(1) = 1$: elle correspond au polynôme $X+1$ (qui n'est pas dans notre ensemble $\mathcal{I}$). La suite $S(n)$, $n \geq 1$, est la suite A48 dans [Slo].

3.5 Hexagones à 6 éléments

Comme nous l'avons vu précédemment, les hexagones à 6 éléments sont composés de polynômes qui ne sont invariants par aucune des permutations non-triviales de $\mathfrak{S}_3$.

Exemple 5. *Voici par exemple l'hexagone à 6 éléments de plus petit degré, il regroupe tous les irréductibles de degré 5 :*

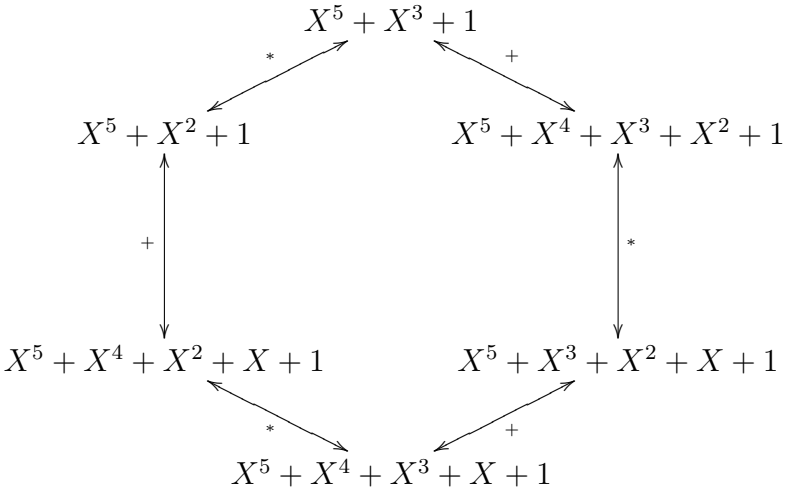


FIG. 3.6 – Hexagone à 6 éléments de degré 5

Pour calculer le nombre de ces hexagones pour un degré donné, nous commençons par rappeler la formule de Gauss [Gau63], qui renvoie le nombre $I(n)$ de polynômes irréductibles de degré n dans $\mathbb{F}_2[X]$:

$$I(n) = \frac{1}{n}\sum_{d|n}\mu(d)2^{\frac{n}{d}}. \tag{3.3}$$

Maintenant, en utilisant (3.3) et les formules h_1, h_2 et h_3 que nous avons données plus tôt, nous pouvons calculer le nombre $h_6(n)$ d'hexagones non dégénérés de degré n, $n \geq 2$:

$$h_6(n) = \frac{1}{6}[I(n) - h_1(n) - 2h_2(n) - 3h_3(n)].$$

Sur le site de Sloane, nous avons ajouté la suite des $h_6(n)$, pour $n \geq 2$, c'est la A165921.

3.6 Table récapitulative

En rassemblant les résultats énoncés dans les sections précédentes, nous pouvons déterminer, pour un degré n donné, $n \geq 2$, la façon dont les polynômes irréductibles sont répartis en hexagones. Pour illustrer cela, nous avons la Table 3.1 qui contient le nombre d'hexagones de chaque type, le nombre d'hexagones au total et le nombre d'irréductibles, pour les degrés allant de 2 à 30 :

n	$h_1(n)$	$h_2(n)$	$h_3(n)$	$h_6(n)$	$hex(n)$	$I(n)$
2	1	0	0	0	1	1
3	0	1	0	0	1	2
4	0	0	1	0	1	3
5	0	0	0	1	1	6
6	0	0	1	1	2	9
7	0	0	0	3	3	18
8	0	0	2	4	6	30
9	0	1	0	9	10	56
10	0	0	3	15	18	99
11	0	0	0	31	31	186
12	0	1	5	53	59	335
13	0	0	0	105	105	630
14	0	0	9	189	198	1161
15	0	2	0	363	365	2182
16	0	0	16	672	688	4080
17	0	0	0	1285	1285	7710
18	0	3	28	2407	2438	14532
19	0	0	0	4599	4599	27594
20	0	0	51	8704	8755	52377
21	0	6	0	16641	16647	99858
22	0	0	93	31713	31806	190557
23	0	0	0	60787	60787	364722
24	0	10	170	116390	116570	698870
25	0	0	0	223696	223696	1342176
26	0	0	315	429975	430290	2580795
27	0	19	0	828495	828514	4971008
28	0	0	585	1597440	1598025	9586395
29	0	0	0	3085465	3085465	18512790
30	0	33	1091	5964488	5965612	35790267

TAB. 3.1 – Répartition des polynômes irréductibles en hexagones jusqu'au degré 30

On peut constater que, d'une part, la très grande majorité des polynômes irréductibles de $\mathcal{I}$ est issue d'hexagones non dégénérés et d'autre part, parmi les polynômes invariants, on trouve proportionnellement bien plus d'invariants par l'action de l'un des sous-groupes de taille 2 de $\mathfrak{S}_3$ que par l'action du sous-groupe alterné.

Dans [Slo], la suite des $I(n)$ est la A1037 et celle des $hex(n)$ est la A11957. Étonnamment, cette dernière existait déjà, elle apparaît dans un papier de McLarnan [McL81] datant de 1981, qui traite des empilements d'atomes en chimie.

Deuxième partie

Génération de polynômes invariants

Dans cette seconde partie, nous allons nous intéresser à la génération des polynômes invariants présentés précédemment. Plus précisément, dans le Chapitre 4, nous allons donner, puis étudier, des transformations permettant de générer ces polynômes. Dans un premier temps, nous définirons les transformations quadratiques ϕ_p, ϕ_m et ϕ_r qui génèrent respectivement des polynômes périodiques, médians et réciproques à partir de polynômes de $\mathcal{I}$. Nous donnerons le critère d'irréductibilité de l'image d'un polynôme et nous expliquerons ce qu'il se passe dans l'autre cas. Nous utiliserons ensuite ces résultats pour prouver le Théorème 8 et construire des hexagones à 3 ou 6 éléments. Et nous donnerons d'autres transformations quadratiques pouvant jouer le même rôle que celles évoquées plus tôt.

De manière analogue, pour le cas des polynômes alternatifs, nous définirons la transformation cubique ψ qui permet de les obtenir. Nous préciserons la condition requise pour que ψ engendre un irréductible et ce que l'on obtient dans le cas contraire. Puis, en ce qui concerne les applications, nous continuerons le parallèle avec la première section en prouvant le Théorème 5 et en donnant un moyen de construire des hexagones à 2 et 6 éléments. En plus de cela, nous préciserons comment déterminer le type d'un polynôme alternatif irréductible. Enfin, nous terminerons en donnant d'autres transformations cubiques, équivalentes à ψ.

Le Chapitre 5 sera consacré à la génération de suites infinies de nos polynômes invariants. Nous commencerons par une introduction aux extensions algébriques infinies de corps finis et nous donnerons ensuite un moyen de générer des suites infinies de polynômes irréductibles réciproques, médians, périodiques et alternatifs. Ces suites permettront alors de définir toutes les extensions de $\mathbb{F}_2$ de la forme $\mathbb{F}_{2^{2^i p}}$ ou $\mathbb{F}_{2^{3^i p}}$, pour $i \geq 0$ et p un nombre premier quelconque.

L'essentiel des résultats présentés dans cette seconde partie se trouve dans l'article [MR10b]. Et là encore, plusieurs fonctions et exemples reprenant ces travaux sont proposés en Annexe B.

Chapitre 4

Transformations

Nous donnons dans ce chapitre un moyen de générer nos polynômes invariants. Pour chaque type d'invariance, nous proposons une transformation qui, à partir d'un polynôme irréductible, engendre un invariant, irréductible ou non. Nous précisons alors dans quel cas le polynôme est irréductible et ce que l'on obtient dans l'autre cas. Nous utilisons ensuite ces résultats pour diverses applications et nous terminons en donnant d'autres transformations, équivalentes à celles proposées.

4.1 Transformations quadratiques

4.1.1 Les transformations ϕ_p, ϕ_m et ϕ_r

Pour commencer, nous donnons les définitions suivantes :

Définition 7. *Soient P et Q, $P \neq Q$, 2 polynômes irréductibles, on dit que $\{P, Q\}$ est une **paire réciproque** (resp. **paire périodique**, **paire médiane**) si $Q = P^*$ (resp. $Q = P^+$, $Q = P^{*+*}$).*

Bien entendu, les polynômes issus d'une même paire sont de même degré, on pourra donc définir le degré d'une paire comme étant celui de ses polynômes.

Définition 8. *Nous définissons les transformations ϕ_p, ϕ_m, ϕ_r : $\mathbb{F}_2[X] \to \mathbb{F}_2[X]$ par*

$$\begin{aligned}
\phi_p(P(X)) &= P(X^2 + X) \\
\phi_m(P(X)) &= \phi_p(P(X))^* = X^{2n}\, P(\frac{X+1}{X^2}) \\
\phi_r(P(X)) &= \phi_p(P(X))^{*+} = (X^2+1)^n\, P(\frac{X}{X^2+1}).
\end{aligned}$$

Par définition, on voit que l'image par ϕ_p (resp. ϕ_m, ϕ_r) d'un polynôme de $\mathcal{I}(n)$ est un polynôme périodique (resp. médian, réciproque) de degré $2n$, cependant, il n'est pas toujours irréductible.

Proposition 5. *Soit $\mathcal{P} \subset \mathbb{F}_2[X]$ l'ensemble des polynômes périodiques dans $\mathbb{F}_2[X]$, alors $\mathcal{P}$ est une sous-algèbre de $\mathbb{F}_2[X]$ et $\phi_p : \mathbb{F}_2[X] \to \mathcal{P}$ est un isomorphisme d'algèbre.*

Démonstration. Il suffit de démontrer la surjectivité de ϕ_p, le reste étant trivial. Soit Q un polynôme périodique, son degré est un entier pair $2n$. Alors, $Q + (X^2 + X)^n$ est un polynôme périodique de degré $< 2n$. En itérant cela, on obtient un polynôme P de degré n tel que $\phi_p(P) = Q$. □

On appelle **trace** d'un polynôme $P \neq 0$ de degré n le coefficient de X^{n-1}. La trace de P sera notée $\mathrm{Tr}(P)$.

Le théorème et le corollaire suivants peuvent être vus comme une extension d'un résultat de Meyn (voir [Mey90], Lemme 4) :

Théorème 9. *Soit $P \in \mathcal{I}(n)$. Si $\mathrm{Tr}(P) = 1$, alors $\phi_p(P)$ est un polynôme périodique irréductible de degré $2n$, sinon, $\phi_p(P)$ est le produit de 2 polynômes irréductibles de degré n qui forment une paire périodique.*

Inversement, soit Q un polynôme irréductible périodique de degré $2n$ (resp. $\{R, R^+\}$ une paire périodique de degré n), alors, il existe un unique $P \in \mathcal{I}(n)$ tel que $\phi_p(P) = Q$ (resp. $\phi_p(P) = RR^+$).

Démonstration. Soient $P \in \mathcal{I}(n)$ et h une racine de $\phi_p(P)$, alors par définition, $h^2 + h$ est une racine de P et engendre le corps $\mathbb{F}_{2^n}$. Cela implique que $\mathbb{F}_2[h] \supset \mathbb{F}_2[h^2+h] = \mathbb{F}_{2^n}$. Ainsi, h ne peut pas être une racine d'un polynôme de degré $< n$. On en déduit que la décomposition de $\phi_p(P)$ en facteurs irréductibles ne contient que des polynômes de degré $\geq n$. On a alors 2 possibilités : soit $\phi_p(P)$ est irréductible de degré $2n$, soit c'est le produit de 2 polynômes irréductibles A et B de degré n.

Supposons que l'on soit dans le deuxième cas, étant donné que AB est périodique, soit $B = A^+$, soit A et B sont eux-mêmes périodiques. Ce dernier cas est impossible car si $\phi_p(P) = AB$ avec A et B périodiques et irréductibles, alors d'après la Proposition 5, il existe U et V tels que $\phi_p(U) = A$ et $\phi_p(V) = B$, auquel cas $\phi_p(P) = \phi_p(U)\phi_p(V) = \phi_p(UV)$ et $P = UV$, ce qui est en contradiction avec le fait que P soit irréductible.

Nous démontrons maintenant que l'irréductibilité de $\phi_p(P)$ dépend de la trace de P. Supposons que $\phi_p(P) = AB$, alors $h \in \mathbb{F}_{2^n}$. Soit $a = h^2 + h \in \mathbb{F}_{2^n}$, on a $\mathrm{Tr}(a) = \mathrm{Tr}(h^2) + \mathrm{Tr}(h) = 0$ et donc $\mathrm{Tr}(P) = 0$ puisque a est une racine de P. Inversement, si $\mathrm{Tr}(P) = 0$, alors $\mathrm{Tr}(a) = 0$ pour toute racine a de P. Dans ce cas, on sait que les racines de l'équation $X^2 + X = a$ sont dans $\mathbb{F}_{2^n}$ (en utilisant la "demi-trace"), ce qui veut dire que les racines de $\phi_p(P)$ appartiennent à $\mathbb{F}_{2^n}$, donc $\phi_p(P)$ est réductible.

Nous prouvons maintenant la deuxième partie du théorème.
Soient Q un polynôme irréductible périodique de degré $2n$ et h une racine de Q. Par définition, $h + 1$ est également une racine de Q et, d'après le Théorème 6, on sait que $h + 1 = h^{2^n}$. Si

$$\mathcal{E} = \{h^{2^i} | 0 \leq i < n\},$$

$$Q = \prod_{h\in\mathcal{E}}(X+h)(X+h+1) = \prod_{h\in\mathcal{E}}(X^2+X+h(h+1)).$$

Prenons

$$P = \prod_{h\in\mathcal{E}}(X+h(h+1)),$$

il est clair que $\phi_p(P) = Q$. Soit $h(h+1)$ une racine de P, alors, toute autre racine peut être écrite sous la forme $h^{2^k}(h^{2^k}+1) = [h(h+1)]^{2^k}$, pour un entier $k \geq 1$ donné. En d'autres termes, les racines de P sont conjuguées par Frobenius. Cela implique que $P \in \mathbb{F}_2[X]$. Si P est réductible, prenons $P = ST$, alors $\phi_p(P) = \phi_p(S)\phi_p(T) = Q$. Cette décomposition est triviale car Q est irréductible. Par conséquent, soit S, soit T est trivial et donc P est irréductible. Enfin, supposons que P ne soit pas unique, il existe un polynôme irréductible S tel que $\psi(S) = Q$. Alors par définition, $h(h+1)$ est une racine de S, donc P et S ont les mêmes racines, ce qui veut dire que $P = S$.

De la même manière, soient $\{R, R^+\}$ une paire périodique dans $\mathcal{I}(n)$ et $\mathcal{F}$ l'ensemble des n racines de R, alors en prenant

$$P = \prod_{a\in\mathcal{F}}(X+a(a+1)),$$

on obtient un $P \in \mathbb{F}_2[X]$ tel que $\phi_p(P) = RR^+$.

Supposons que $P = ST$, S et T étant 2 polynômes non constants dans $\mathbb{F}_2[X]$, alors

$$\phi_p(P) = \phi_p(S)\phi_p(T) = RR^+.$$

Par conséquent, on peut écrire $\phi_p(S) = R$, ce qui est une contradiction car $\phi_p(S)$ est périodique et R ne l'est pas, ainsi, P est irréductible. Enfin, P est unique pour les mêmes raisons que plus haut. □

Corollaire 5. *Soit $P \in \mathcal{I}(n)$, si $\mathrm{Tr}(P) = 1$, alors, $\phi_r(P)$(resp. $\phi_m(P)$) est un polynôme irréductible réciproque (resp. médian) de degré $2n$, sinon, c'est le produit de 2 polynômes irréductibles de degré n qui forment une paire réciproque (resp. médiane).*

Inversement, soit Q un polynôme irréductible réciproque (resp. médian) de degré $2n$, alors, il existe $P \in \mathcal{I}(n)$ tel que $\phi_r(P) = Q$ (resp. $\phi_m(P) = Q$). De même, soit $\{R, R^*\}$ (resp. $\{R, R^{+*+}\}$) une paire réciproque (resp. médiane) de degré n, alors, il existe un unique $P \in \mathcal{I}(n)$ tel que $\phi_r(P) = RR^*$ (resp. $\phi_m(P) = RR^{+*+}$).

Démonstration. Nous prouvons le corollaire seulement pour le cas réciproque, le cas médian étant similaire.

Si $\mathrm{Tr}(P) = 1$, d'après le Théorème 9, on sait que $\phi_p(P)$ est périodique et appartient à $\mathcal{I}(2n)$. Et par conséquent, d'après les Définitions 6 et 10, $\phi_r(P)$ est réciproque dans $\mathcal{I}(2n)$. Si $\mathrm{Tr}(P) = 0$, il existe une paire périodique $\{S, S^+\}$ de degré n telle que $\phi_p(P) = SS^+$. Maintenant, étant donné que les transformations $*$ et $+$ sont distributives par

rapport à la multiplication dans $\mathbb{F}_2[X]$, $\phi_r(P) = (SS^+)^{*+} = S^{*+}S^{+*+} = S^{*+}(S^{*+})^*$, qui est une paire réciproque de degré n.

De la même manière, en utilisant le Théorème 9 et les Définitions 6 et 10, on démontre facilement la deuxième partie du corollaire. □

4.1.2 Applications directes

Nous donnons ici quelques conséquences directes des résultats précédents.

Démonstration du Théorème 8

Tout d'abord, maintenant que nous avons énoncé le Théorème 9, nous pouvons donner une rapide preuve du Théorème 8 :

Démonstration du Théorème 8. Prenons

$$A(m) = \{P \in \mathcal{I}(m) \mid P \text{ n'est pas périodique, }\}$$

$$B(m) = \{P \in \mathcal{I}(m) \mid \operatorname{Tr}(P) = 0\}.$$

Par définition,

$$\operatorname{Card}(A(m)) = I(m) - h_3(m).$$

D'après le Théorème 9, nous savons que ϕ_p est une bijection de l'ensemble des polynômes irréductibles de degré m et de trace 0 dans l'ensemble des paires périodiques de degré m. Ainsi,

$$\operatorname{Card}(B(m)) = \frac{\operatorname{Card}(A(m))}{2},$$

et on en déduit alors simplement la valeur de $h_3(2m)$, qui est, d'après le Théorème 9, le nombre de polynômes irréductibles de degré m de trace 1 :

$$\begin{aligned} h_3(2m) &= \operatorname{Card}(\mathcal{I}(m) \setminus B(m)) \\ &= I(m) - \operatorname{Card}(B(m)) \\ &= I(m) - \frac{I(m) - h_3(m)}{2} \\ &= \frac{I(m) + h_3(m)}{2} \end{aligned}$$

□

Construction d'hexagones

Avec les résultats précédents, on obtient également une manière simple de construire des hexagones à 3 et 6 éléments : soit P un polynôme irréductible de degré n tel que $\mathrm{Tr}(P) = 1$, alors $\{\phi_r(P), \phi_m(P), \phi_p(P)\}$ est un hexagone dégénéré à 3 éléments de degré $2n$. Ceci est illustré par la Figure 4.1.

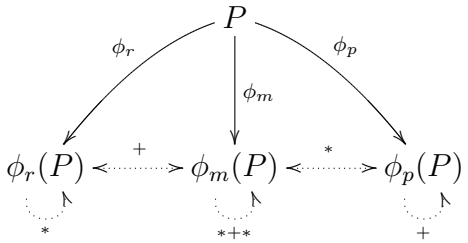


FIG. 4.1 – Construction d'un hexagone à 3 éléments par ϕ_r, ϕ_m et ϕ_p à partir d'un irréductible de trace 1.

Si $\mathrm{Tr}(P) = 0$, on a la Figure 4.2, où $\{Q_1, Q_2\}$, $\{Q_3, Q_4\}$ et $\{Q_5, Q_6\}$ sont les paires telles que $\phi_r(P) = Q_1Q_2$, $\phi_m(P) = Q_3Q_4$ et $\phi_p(P) = Q_5Q_6$ respectivement.

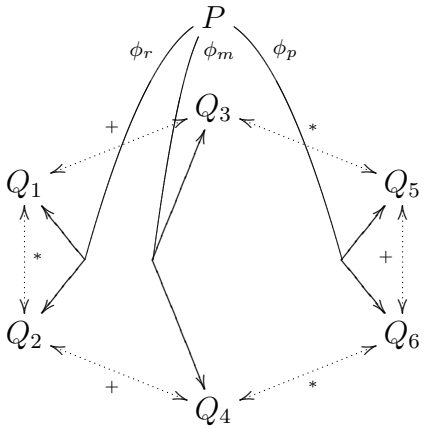


FIG. 4.2 – Construction d'un hexagone à 6 éléments par ϕ_r, ϕ_m et ϕ_p à partir d'un irréductible de trace 0.

4.1.3 Transformations quadratiques équivalentes

Dans la Définition 10, nous avons donné les définitions des transformations ϕ_p, ϕ_m et ϕ_r. Plus précisément, nous avons défini ϕ_m et ϕ_r à partir de ϕ_p, par une action gauche des éléments de $\mathfrak{S}_3$. Ce sont les seules que l'on peut définir de cette manière car :

$$+ \circ \phi_p = \phi_p$$

$$* \circ + \circ \phi_p = * \circ \phi_p = \phi_m$$

$$+ \circ * \circ + \circ \phi_p = + \circ * \circ \phi_p = \phi_r.$$

Cependant, d'autres transformations permettant de générer des polynômes périodiques peuvent être utilisées à la place de ϕ_p, on les obtient cette fois par une action droite des éléments de $\mathfrak{S}_3$ sur ϕ_p. On construit ainsi des fonctions ϕ'_p (qui sont au nombre de 5) et de la même manière, on construit des fonctions ϕ'_m et ϕ'_r. Parmi les ϕ'_r, on retrouve notamment la transformation

$$\phi'_r(P(X)) = \phi_r(P^*(X)) = X^n P(\frac{X^2+1}{X}) = X^n P(X + \frac{1}{X}),$$

que l'on rencontre plus fréquemment dans la littérature mathématique pour construire des polynômes réciproques.

Notre choix pour ϕ_p est simplement dû à la simplicité de la transformation. Ainsi, les résultats présentés précédemment peuvent être transposés (avec de légères modifications) aux autres transformations. Ces dernières sont présentées dans le Tableau 4.1 :

ϕ'_p	$\phi'_m = * \circ \phi'_p$	$\phi'_r = + \circ * \circ \phi'_p$
$P(X^2+X+1) = \phi_p(P^+)$	$X^{2n} P(\frac{X^2+X+1}{X^2})$	$(X^2+1)^n P(\frac{X^2+X+1}{X^2+1})$
$(X^2+X+1)^n P(\frac{1}{X^2+X+1}) = \phi_p(P^{*+})$	$(X^2+X+1)^n P(\frac{X^2}{X^2+X+1})$	$(X^2+X+1)^n P(\frac{X^2+1}{X^2+X+1})$
$(X^2+X+1)^n P(\frac{X^2+X}{X^2+X+1}) = \phi_p(P^{*+*})$	$(X^2+X+1)^n P(\frac{X+1}{X^2+X+1})$	$(X^2+X+1)^n P(\frac{X}{X^2+X+1})$
$(X^2+X)^n P(\frac{X^2+X+1}{X^2+X}) = \phi_p(P^{+*})$	$(X+1)^n P(\frac{X^2+X+1}{X+1})$	$X^n P(\frac{X^2+X+1}{X})$
$(X^2+X)^n P(\frac{1}{X^2+X}) = \phi_p(P^*)$	$(X+1)^n P(\frac{X^2}{X+1})$	$X^n P(\frac{X^2+1}{X})$

Tab. 4.1 – Autres transformations quadratiques

4.2 Transformations cubiques

4.2.1 La transformation ψ

Soit $P \in \mathcal{I}$, comme nous l'avons fait dans la section précédente, nous commençons par des définitions :

Définition 9. *Si P n'est pas alternatif, alors on dit que $\{P, P^{+*}, P^{*+}\}$ est un* ***triplet alternatif****.*

Là aussi, les polynômes d'un même triplet sont de même degré, ainsi, le degré d'un triplet sera celui de ses polynômes.

Définition 10. *Nous définissons la transformation* $\psi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]$ *par*

$$\psi(P)(X) = (X^2+X)^n\, P(\frac{X^3+X^2+1}{X^2+X}).$$

On vérifie facilement que $\psi(P)$ est un polynôme alternatif.

Dans la suite, nous appellerons ϵ et ϵ^2 les racines de X^2+X+1. Pour tout polynôme irréductible $P \neq X^2+X+1$ de $\mathbb{F}_2[X]$, on a $P(\epsilon) \in \{1, \epsilon, \epsilon^2\}$.

Le résultat principal de cette section est le théorème suivant :

Théorème 10. *Soit* $P \in \mathcal{I}(n)$, $n > 2$. *Si* $P(\epsilon) \neq 1$, *alors* $\psi(P)$ *est un polynôme irréductible alternatif de degré* $3n$, *sinon,* $\psi(P) = RST$, *où* $\{R, S, T\}$ *est un triplet alternatif de degré* n.

Inversement, soit $Q \in \mathcal{I}(3n)$, $n > 1$, *un polynôme alternatif (resp.* $\{R, R^{+*}, R^{*+}\}$ *un triplet alternatif de degré* n*), alors il existe un unique* $P \in \mathcal{I}(n)$ *tel que* $\psi(P) = Q$ *(resp.* $\psi(P) = RR^{+*}R^{*+}$*).*

Pour compléter le théorème, nous précisons que les polynômes irréductibles (alternatifs) de degré 3 sont obtenus à partir de X et $X+1$:

$$\psi(X) = X^3+X^2+1$$

$$\psi(X+1) = X^3+X+1,$$

et que, pour le cas particulier X^2+X+1 (dont la valeur en ϵ est 0) on a :

$$\psi(X^2+X+1) = (X^2+X+1)^3.$$

La démonstration du Théorème 10 étant longue, nous avons besoin d'établir quelques résultats avant de la commencer.

Soient $P \in \mathcal{I}(n)$, avec $n > 2$, $K = \mathbb{F}_{2^n}$ le corps de décomposition de P et h une racine de $\psi(P)$, alors $h \neq 0, 1$ et

$$a = \frac{h^3+h^2+1}{h^2+h} = h + \frac{1}{h} + \frac{1}{h+1} \tag{4.1}$$

est une racine de P. Cela implique que $K \subset K(h)$.

Et étant donné que $h \neq 0, 1$, c'est une racine du polynôme

$$T_a(X) = X^3 + (1+a)X^2 + aX + 1. \tag{4.2}$$

Démonstration de la première partie du Théorème 10

On commence par caractériser les racines de (4.2) :

Proposition 6. *Soit w une racine cubique de $(\epsilon+a)(\epsilon+a^2)$, les racines de (4.2) sont :*

$$h_i = 1 + a + \epsilon^i w + \frac{b}{\epsilon^i w},$$

avec $i = 0$, 1 ou 2 et $b = a^2 + a + 1$. De plus, elles vérifient les relations $h_1 = 1/(h_0 + 1)$ et $h_2 = 1 + 1/h_0$.

Démonstration. Les formules des h_i sont obtenues par la méthode de Cardan pour résoudre les équations du troisième degré.

La première étape est d'annuler le coefficient de X^2 dans

$$X^3 + (a+1)X^2 + aX + 1 = 0.$$

Donc on prend $X' = X + 1 + a$ et $b = 1 + a + a^2$:

$$X'^3 + bX' + b = 0.$$

La deuxième étape est d'utiliser 2 variables u, v et de poser $X' = u + v$:

$$u^3 + v^3 + (u+v)(uv + b) + b = 0.$$

En choisissant $uv = b$, si on peut résoudre

$$\begin{cases} uv & = b \\ u^3 + v^3 & = b \end{cases}$$

dans $\overline{K}$, nous aurons les racines de (4.2), ce seront les

$$1 + a + u + v.$$

On peut écrire :

$$\begin{cases} u^3 v^3 & = b^3 \\ u^3 + v^3 & = b, \end{cases}$$

ce qui est équivalent à un problème du second degré. Si $Y = u^3$, alors :

$$Y^2 + bY + b^3 = 0,$$

et en divisant par b^2, on obtient :

$$\frac{Y^2}{b^2} + \frac{Y}{b} + b = 0.$$

Prenons $Z = Y/b$ (ce qui est possible car $b \neq 0$) :

$$Z^2 + Z + b = 0$$

$$Z^2 + Z + 1 + a + a^2 = 0$$
$$(Z + a)^2 + (Z + a) + 1 = 0.$$

Donc les solutions sont $Z = a + \epsilon$ et $Z = a + \epsilon^2$, ainsi on peut prendre par exemple

$$u^3 = (1 + a + a^2)(a + \epsilon^2),$$

ce qui s'écrit également

$$\begin{aligned} u^3 &= (a + \epsilon)(a + \epsilon^2)(a + \epsilon^2) \\ &= (a + \epsilon)(a^2 + \epsilon). \end{aligned}$$

Donc on peut choisir u comme étant l'une des trois racines cubiques de $(a + \epsilon)(a^2 + \epsilon)$. La valeur de $v = b/u$ est alors déterminée de façon unique. Le rôle de v et u peuvent bien sûr être échangés.

Il reste maintenant à établir les relations entre les racines :

$$\begin{aligned} 1 + \frac{1}{h_0} &= h_0^2 + (1 + a)h_0 + a + 1 \quad \text{(from (4.2))} \\ &= w^2 + \frac{b^2}{w^2} + (1 + a)(w + \frac{b}{w}) + a + 1 \\ &= \frac{w^3}{w} + \frac{b^2 w}{w^3} + (1 + a)(w + \frac{b}{w}) + a + 1 \\ &= [\frac{b^2}{w^3} + 1 + a]w + [\frac{w^3}{b} + 1 + a]\frac{b}{w} + a + 1. \end{aligned}$$

Ainsi, puisque $b = (\epsilon + a)(\epsilon^2 + a)$ et $w^3 = (\epsilon + a)(\epsilon + a^2)$, on trouve :

$$1 + \frac{1}{h_0} = \epsilon^2 w + \frac{b}{\epsilon^2 w} + a + 1 = h_2.$$

La première relation est obtenue de la même manière. □

Lemme 1. *Si $P(\epsilon) = 1$ et n est pair (resp. impair), alors les racines cubiques de $(\epsilon + a)(\epsilon + a^2)$ sont dans $K = \mathbb{F}_{2^n}$ (resp. $K(\epsilon)$).*

Démonstration. Cas n pair : prenons $n = 2m$,

$$\begin{aligned} P(\epsilon) &= (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8)\dots(\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}}) \\ &= (\epsilon + a)(\epsilon + a^2)((\epsilon + a)(\epsilon + a^2))^4 \dots ((\epsilon + a)(\epsilon + a^2))^{2^{2m-2}}. \end{aligned}$$

Donc $P(\epsilon) = [(\epsilon + a)(\epsilon + a^2)]^k$, avec

$$k = 1 + 4 + \cdots + 2^{2(m-1)} = \frac{2^n - 1}{3}.$$

Soit w une racine cubique de $(\epsilon+a)(\epsilon+a^2)$ dans une extension de $\mathbb{F}_2$ (elle existe toujours), d'après ce que nous venons de voir,

$$w^{2^n-1} = w^{3.\frac{2^n-1}{3}} = P(\epsilon) = 1,$$

donc $w \in K$.

Cas n impair : prenons $n = 2m + 1$, on écrit $P(\epsilon)$ de deux manières différentes, en utilisant le Petit Théorème de Fermat :

$$P(\epsilon) = (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8)\dots(\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}})(\epsilon + a^{2^{2m}})$$
$$P(\epsilon) = (\epsilon + a^{2^{2m+1}})(\epsilon + a^{2^{2m+2}})(\epsilon + a^{2^{2m+3}})(\epsilon + a^{2^{2m+4}})\dots(\epsilon + a^{2^{4m}})(\epsilon + a^{2^{4m+1}}).$$

En multipliant ces égalités, on obtient

$$\begin{aligned} P(\epsilon)^2 &= [(\epsilon + a)(\epsilon + a^2)][(\epsilon + a)(\epsilon + a^2)]^4 \dots [(\epsilon + a)(\epsilon + a^2)]^{2^{4m}} \\ &= [(\epsilon + a)(\epsilon + a^2)]^k, \end{aligned}$$

où

$$k = 1 + 4 + \cdots + 2^{4m} = \frac{4^{2m+1} - 1}{3} = \frac{2^{2n} - 1}{3}.$$

Ainsi

$$w^{2^{2n}-1} = w^{3.\frac{2^{2n}-1}{3}} = P(\epsilon)^2 = 1,$$

et $w \in K(\epsilon)$ car $[K(\epsilon) : \mathbb{F}_2] = 2n$. □

Les deux résultats précédents nous permettent alors d'énoncer la proposition suivante :

Proposition 7. *Soit $P \in \mathcal{I}(n)$ tel que $P(\epsilon) = 1$, alors, $\psi(P)$ est réductible.*

Démonstration. Si n est pair, c'est une conséquence directe de la Proposition 6 et du Lemme 1.

Si n est impair, $w \in K(\epsilon)$ d'après le lemme précédent, donc d'après la Proposition 6, on a $K(h) \subset K(\epsilon)$. Si $\psi(P)$ est irréductible, alors, pour chacune de ses racines h, on a $[K(h) : \mathbb{F}_2] = 3n$ et $[K(h) : K] = 3$, ce qui est une contradiction, donc $\psi(P)$ est réductible. □

Nous allons maintenant montrer la réciproque de la Proposition 7. Pour cela, nous avons besoin du résultat suivant :

Proposition 8. *Soit $P \in \mathcal{I}(n)$, $n > 2$, le polynôme $\psi(P)$ a $3n$ racines distinctes et*

$$\psi(P) = \prod_{k=0}^{n-1} T_{a^{2^k}}(X),$$

où $a \in K$ est une racine de P.

Démonstration. Si a est une racine de P et si h est une racine de T_a, alors h est une racine de $\psi(P)$. Soit a' une autre racine de P, $a' \neq a$, d'après (4.1), l'ensemble des racines de T_a est disjoint de l'ensemble des racines de $T_{a'}$. Puisque P est irréductible, toutes ses racines sont conjuguées et distinctes, ce qui conclut la démonstration de la proposition. □

Nous pouvons ainsi énoncer :

Proposition 9. *Soit $P \in \mathcal{I}(n)$, $n > 2$, si $\psi(P)$ est réductible dans $\mathbb{F}_2[X]$, alors, $\psi(P) = RST$, où $\{R, S, T\}$ est un triplet alternatif de degré n, de plus $P(\epsilon) = 1$.*

Démonstration. Soit h une racine de $\psi(P)$, nous avons vu que $K \subset K(h)$. Ainsi, le degré du polynôme minimal de h est divisible par n et est $\leq 3n$. Cela implique que les facteurs irréductibles de $\psi(P)$ dans $\mathbb{F}_2[X]$ sont au moins de degré n, $< 3n$ et multiples de n. Par conséquent, l'un d'entre eux est de degré n. Nous appelons R ce facteur.

Prenons R^{*+} et R^{+*}. Ce sont des polynômes de $\mathbb{F}_2[X]$ de degré n et leurs racines sont des racines de $\psi(P)$, ils divisent donc $\psi(P)$. Si R n'est pas alternatif, alors on obtient un triplet alternatif $\{R, R^{*+}, R^{+*}\}$ de degré n, comme énoncé.

Supposons maintenant que R soit un polynôme alternatif. Soient h une racine de R et a tel que

$$a = \frac{h^3 + h^2 + 1}{h^2 + h},$$

alors, comme précédemment, a est une racine de P et $T_a(X) | R$ car h, $\frac{1}{h+1}$ et $\frac{h+1}{h}$ sont des racines distincte de R. Étant donné que $R \in \mathbb{F}_2[X]$ est irréductible de degré n, ses racines sont les h^{2^k}, avec $0 \leq k \leq n-1$. Donc, puisque Frobenius commute avec nos transformations de groupe, $T_{a^{2^k}} | R$ pour tout k. D'après la proposition précédente, les $T_{a^{2^k}}$ sont distincts. Il en résulte que R a $3n$ racines distinctes, ce qui est une contradiction. Donc R n'est pas alternatif et on a notre résultat.

Reste à prouver que $P(\epsilon) = 1$. D'après ce que l'on vient de voir, on peut écrire $\psi(P)$ de la manière suivante :

$$\psi(P) = R(X)(X+1)^n R\Big(\frac{1}{X+1}\Big) X^n R\Big(\frac{X+1}{X}\Big),$$

avec $R \in \mathbb{F}_2[X]$ irréductible de degré $n > 2$, ainsi $\psi(P)(\epsilon) = \epsilon^{3n} R(\epsilon)^3 = R(\epsilon)^3 = 1$.

Ensuite, en remplaçant X par ϵ dans la définition de ψ, on obtient $\psi(P)(\epsilon) = P(\epsilon^2)$. Par conséquent, $P(\epsilon^2) = P(\epsilon)^2 = 1$ et $P(\epsilon) = 1$. □

Les Propositions 7 et 9 démontrent la première partie de Théorème 10.

Démonstration de la deuxième partie du Théorème 10

La proposition suivante énonce la deuxième partie du théorème. Sa démonstration est similaire à celle de la deuxième partie du Théorème 9.

Proposition 10. *Soit $Q \in \mathcal{I}(3n)$, $n > 1$ un polynôme alternatif (resp. $\{R, R^{+*}, R^{*+}\}$ un triplet alternatif de degré n), alors il existe un unique $P \in \mathcal{I}(n)$ tel que $\psi(P) = Q$ (resp. $\psi(P) = RR^{+*}R^{*+}$).*

Démonstration. Soit a une racine de Q, on suppose que Q est de type 1 (le type 2 est similaire), on sait que $1/(1+a)$ et $1+1/a$ sont aussi racines de Q, de plus, d'après le Corollaire 1, on sait que $1+1/a = a^{2^n}$ et que $1/(1+a) = a^{2^{2n}}$. Maintenant, prenons

$$\mathcal{E} = \{a^{2^i} | 0 \leq i < n\},$$

d'après ce que nous venons de voir, nous pouvons écrire

$$\begin{aligned}
Q &= \prod_{a\in\mathcal{E}} (X+a)(X+1+\frac{1}{a})(X+\frac{1}{1+a}) \\
&= \prod_{a\in\mathcal{E}} \Big(\frac{a^3(X^2+X)+a^2(X^3+X+1)+a(X^3+X^2+1)+X^2+X}{a^2+a}\Big) \\
&= (X^2+X)^n \prod_{a\in\mathcal{E}} \Big(\frac{a^3(X^2+X)+a^2(X^3+X+1)+a(X^3+X^2+1)+X^2+X}{(a^2+a)(X^2+X)}\Big) \\
&= (X^2+X)^n \prod_{a\in\mathcal{E}} \Big(\frac{X^3+X^2+1}{X^2+X} + \frac{a^3+a^2+1}{a^2+a}\Big).
\end{aligned}$$

On prend alors

$$P = \prod_{a\in\mathcal{E}} \Big(X + \frac{a^3+a^2+1}{a^2+a}\Big),$$

il est évident que $\psi(P) = Q$. Soit $\frac{a^3+a^2+1}{a^2+a}$ une racine de P, toutes les autres racines peuvent s'écrire $a^{2^k}(1+1/a^{2^k})(1/(1+a^{2^k})) = [a(1+1/a)(1/(1+a))]^{2^k}$, où k est un entier ≥ 1. Autrement dit, les racines de P sont conjuguées par Frobenius, ce qui implique que $P \in \mathbb{F}_2[X]$.

Pour montrer que P est irréductible, on suppose que $P = ST$, où S et T sont deux polynômes non-constants de $\mathbb{F}_2[X]$, alors, puisque $\deg(ST) = \deg(S) + \deg(T)$:

$$\psi(P) = \psi(S)\psi(T) = Q,$$

et cette décomposition n'est pas triviale, ce qui est impossible car Q est irréductible, donc P est irréductible.

Et pour montrer que P est unique, on suppose qu'il existe un autre polynôme irréductible S tel que $\psi(S) = Q$, alors par définition, $\frac{a^3+a^2+1}{a^2+a}$ est une racine de S, donc P et S ont les mêmes racines et par conséquent $P = S$.

De la même manière, soit $\{R, R^{+*}, R^{*+}\}$ un triplet alternatif de degré n et $\mathcal{F}$ l'ensemble des n racines de R, alors en prenant

$$P = \prod_{a \in \mathcal{F}} \left(X + \frac{a^3 + a^2 + 1}{a^2 + a}\right),$$

on obtient un polynôme tel que $\psi(P) = RR^{+*}R^{*+}$ et $P \in \mathbb{F}_2[X]$.

Si P est réductible, on peut écrire $P = ST$, où S et T sont deux polynômes non-constants de $\mathbb{F}_2[X]$, dans ce cas

$$\psi(P) = \psi(S)\psi(T) = RR^{+*}R^{*+}.$$

Par conséquent, sans perte de généralité, on peut écrire $\psi(S) = R$, ce qui est une contradiction car $\psi(S)$ est alternatif et R ne l'est pas, ainsi P est irréductible. Enfin, on montre que P est unique de la même manière que précédemment. □

Ceci complète la démonstration du Théorème 10.

4.2.2 Applications directes

Démonstration du Théorème 5

À l'aide du Théorème 10, il est maintenant possible de démontrer le Théorème 5 :

Démonstration du Théorème 5. Prenons

$$A(m) = \{P \in \mathcal{I}(m) \mid P \text{ n'est pas alternatif, }\}$$

$$B(m) = \{P \in \mathcal{I}(m) \mid P(\epsilon) = 1\}.$$

Par définition,

$$\text{Card}(A(m)) = I(m) - 2h_2(m).$$

D'après le Théorème 10, on sait que ψ est une bijection de l'ensemble des polynômes irréductibles de degré m et dont la valeur en ϵ est 1 dans l'ensemble des triplets alternatifs de degré m. Ainsi,

$$\text{Card}(B(m)) = \frac{\text{Card}(A(m))}{3},$$

et on en déduit alors simplement la valeur de $h_2(3m)$, qui est, d'après le Théorème 10, la moitié du nombre de polynômes irréductibles de degré m dont la valeur en ϵ est différente de 1 :

$$\begin{aligned} h_2(3m) &= \frac{\mathrm{Card}(\mathcal{I}(m) \setminus B(m))}{2} \\ &= \frac{I(m) - \mathrm{Card}(B(m))}{2} \\ &= \frac{I(m) - \frac{I(m)-2h_2(m)}{3}}{2} \\ &= \frac{I(m) + h_2(m)}{3} \end{aligned}$$

□

Construction d'hexagones

Aussi, à l'image de ce que nous avons fait dans la section précédente, nous proposons une manière simple de construire des hexagones à 2 et à 6 éléments.

Dans un premier temps, on remarque que $\psi \circ + = + \circ \psi$ (cela se vérifie rapidement par le calcul), maintenant, soit $P \in \mathcal{I}(n)$, $P \neq X^2+X+1$, tel que $P(\epsilon) \neq 1$, alors d'après le Théorème 10, on sait que $\{\psi(P), \psi(P^+)\}$ est un hexagone dégénéré à 2 éléments de degré $3n$. Ceci est illustré par la Figure 4.3 :

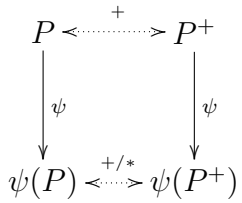


FIG. 4.3 – Construction d'un hexagone à 2 éléments par ψ à partir d'un polynôme irréductible P tel que $P(\epsilon) \neq 1$.

D'un autre côté, si $P(\epsilon) = 1$, nous obtenons la Figure 4.4, où $\{Q_1, Q_3, Q_5\}$ et $\{Q_2, Q_4, Q_6\}$ sont les triplets alternatifs tels que $\psi(P) = Q_1Q_3Q_5$ et $\psi(P^+) = Q_2Q_4Q_6$ respectivement :

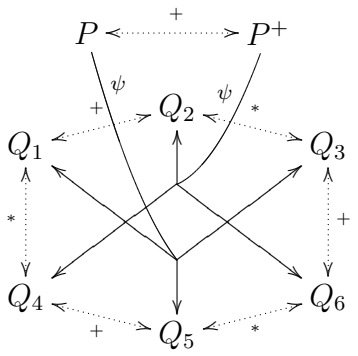


FIG. 4.4 – Construction d'un hexagone à 6 éléments par ψ à partir d'un polynôme irréductible P tel que $P(\epsilon) = 1$.

Calcul du type des polynômes irréductibles alternatifs

Une autre conséquence du Théorème 10 est qu'il donne une manière simple de calculer le type d'un irréductible alternatif :

Théorème 11. *Soit Q un polynôme irréductible alternatif de degré > 2, alors, Q est de type 1 (resp. 2) si et seulement si $Q(\epsilon) = \epsilon$ (resp. $Q(\epsilon) = \epsilon^2$).*

Démonstration. Si $\deg(Q) = 3$, on vérifie le théorème par le calcul. On suppose maintenant que $\deg(Q) = 3n$, $n > 1$. D'après ce qui précède, on sait que $Q = \psi(P) \in \mathcal{I}(3n)$ pour un polynôme irréductible P de degré n et que $Q(\epsilon) = P(\epsilon)^2$.

Si n est pair, soit h_0 une racine de Q, alors, avec les notations utilisées dans la Proposition 6, on a $h_0 = 1 + a + w + \frac{b}{w}$. Par conséquent :

$$h_0^{2^n} = 1 + a + w^{2^n} + \frac{b}{w^{2^n}}.$$

D'après la démonstration du Lemme 1, on a $w^{2^n} = P(\epsilon)w$ et

$$h_0^{2^n} = 1 + a + P(\epsilon)w + \frac{b}{P(\epsilon)w}.$$

Si $Q(\epsilon) = \epsilon$ (resp. ϵ^2), alors $P(\epsilon) = \epsilon^2$ (resp. ϵ) et en utilisant une nouvelle fois le Théorème 10 :

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{ resp. } h_0^{2^n} = \frac{1}{h_0 + 1}\ ).$$

Ceci revient à dire que Q est de type 1 (resp. 2).

Si n est impair, la démonstration est basée sur le même principe mis à part le fait que l'on doit utiliser $w^{2^{2n}} = P(\epsilon)^2 w = Q(\epsilon)w$. On calcule :

$$h_0^{2^{2n}} = 1 + a + Q(\epsilon)w + \frac{b}{Q(\epsilon)w}.$$

Si $Q(\epsilon) = \epsilon$ (resp. ϵ^2), alors $P(\epsilon) = \epsilon^2$ (resp. ϵ). On obtient :

$$h_0^{2^{2n}} = \frac{1}{h_0 + 1} \quad (\text{ resp. } h_0^{2^{2n}} = 1 + \frac{1}{h_0}\ ).$$

Ce qui implique (par itération par exemple) que :

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{ resp. } h_0^{2^n} = \frac{1}{h_0 + 1}\ ),$$

et Q est de type 1 (resp. 2). □

4.2.3 Transformations cubiques équivalentes

D'autres transformations permettant de générer des polynômes alternatifs peuvent être utilisées à la place de ψ. Comme dans la section précédente, on les obtient par une action droite des éléments de $\mathfrak{S}_3$ sur ψ et les résultats que l'on vient de voir peuvent être transposés à ces autres transformations, présentées dans le Tableau 4.2 :

ψ'
$(X^2+X)^n P(\frac{X^3+X+1}{X^2+X}) = \psi(P^+)$
$(X^3+X+1)^n P(\frac{X^2+X}{X^3+X+1}) = \psi(P^{*+})$
$(X^3+X+1)^n P(\frac{X^3+X^2+1}{X^3+X+1}) = \psi(P^{*+*})$
$(X^3+X^2+1)^n P(\frac{X^3+X+1}{X^3+X^2+1}) = \psi(P^{+*})$
$(X^3+X^2+1)^n P(\frac{X^2+X}{X^3+X^2+1}) = \psi(P^*)$

TAB. 4.2 – Autres transformations cubiques.

Chapitre 5

Suites infinies

Dans ce chapitre, nous commençons par une introduction aux extensions algébriques infinies de corps finis. Puis, nous donnons un moyen de générer des suites infinies de polynômes irréductibles invariants, pour chaque type d'invariance, en utilisant les résultats du chapitre précédent.

5.1 Introduction aux extensions algébriques infinies de corps finis

Nous présentons ici les extensions algébriques infinies de corps finis, pour une introduction plus détaillée sur le sujet, le lecteur pourra consulter le livre de Brawley et Schnibben [BS89].

Une **clôture algébrique** d'un corps $\mathbb{F}_q$ est une extension de $\mathbb{F}_q$ dans laquelle tous les polynômes non-constants définis sur $\mathbb{F}_q$ ont leurs racines. Tout corps admet une clôture algébrique, elle est unique, à un isomorphisme près, et on la note $\overline{\mathbb{F}_q}$. Si $\mathbb{F}_q$ est une extension d'un corps premier $\mathbb{F}_p$, alors $\overline{\mathbb{F}_q} = \overline{\mathbb{F}_p}$. On peut définir $\overline{\mathbb{F}_q}$ ainsi :

$$\overline{\mathbb{F}_q} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}.$$

Nous souhaiterions maintenant caractériser les sous-corps de $\overline{\mathbb{F}_q}$. Nous utiliserons pour cela une façon étendue de concevoir les entiers positifs, introduite par Steinitz dans [Ste10] :

Définition 11. *Un **nombre de Steinitz** est un nombre écrit sous la forme*

$$N = p_1^{k_1} p_2^{k_2} p_3^{k_3} ... = \prod_{i=1}^{\infty} p_i^{k_i},$$

où p_i est le i-ème nombre premier et $k_i \in \{0, 1, 2, ..., \infty\}$. L'ensemble des nombres de Steinitz est noté $\mathbb{E}$.

L'avantage de cette notation est que l'on va pouvoir préciser en quoi un nombre entier positif est infini. Par exemple, 5^∞, $2^5 3^\infty$ et $\prod_{i=1}^{\infty} p_i$ sont trois nombres de Steinitz représentant des infinis différents. Pour les entiers positifs finis, il s'agit simplement de leur décomposition en facteurs premiers. Concernant les opérations sur ces nombres, la multiplication, la division et les calculs de plus petit commun multiple et de plus grand commun diviseur se définissent naturellement (voir [BS89]). Nous utilisons maintenant les nombres de Steinitz pour définir les extensions de $\mathbb{F}_q$:

Définition 12. *Soit N un nombre de Steinitz, on définit $\mathbb{F}_{q^N}$ de la manière suivante :*

$$\mathbb{F}_{q^N} = \bigcup_{d|N} \mathbb{F}_{q^d},$$

où les diviseurs d de N sont des entiers positifs finis.

À partir de maintenant, nous considérons que N représente un nombre de Steinitz. Nous décrivons la structure des sous-corps de $\overline{\mathbb{F}_q}$ par l'intermédiaire du théorème suivant :

Théorème 12 (Steinitz, [Ste10])**.** *Soit f l'application de $\mathbb{E}$ dans l'ensemble des sous-corps de $\overline{\mathbb{F}_q}$ définie par*

$$f(N) = \mathbb{F}_{q^N}.$$

Alors f est une bijection entre $\mathbb{E}$ et l'ensemble des sous-corps de $\overline{\mathbb{F}_q}$ contenant $\mathbb{F}_q$. De plus :

- *$\mathbb{F}_{q^N}$ est fini si et seulement si N est fini,*
- *$\mathbb{F}_{q^N} \subseteq \mathbb{F}_{q^M}$ si et seulement si $N|M$,*
- *$\mathbb{F}_{q^N} \cap \mathbb{F}_{q^M} = \mathbb{F}_{q^D}$, où $D = pgcd(N, M)$,*
- *$< \mathbb{F}_{q^N} \cup \mathbb{F}_{q^M} >= \mathbb{F}_{q^L}$, où $L = ppcm(N, M)$.*

Étant donné qu'il est impossible de définir concrètement $\overline{\mathbb{F}_q}$ (on ne peut pas donner une base de $\overline{\mathbb{F}_q}$ ou un polynôme irréductible qui la génère), il serait néanmoins intéressant de pouvoir définir les sous-corps de $\overline{\mathbb{F}_q}$. Dans cet objectif, nous allons voir que nous pouvons définir des extensions algébriques infinies de $\mathbb{F}_q$. Nous introduisons pour cela les notions de suites de diviseurs et de présentation itérées :

Définition 13. *Une **suite de diviseurs** est une suite (finie ou non) d'entiers positifs $d_1, d_2, d_3, ...$ vérifiant $d_i|d_{i+1}$ pour $i \in \{1, 2, ...\}$. Elle converge vers le nombre de Steinitz N si et seulement si $d_i|N$ pour tout $i \in \{1, 2, ...\}$ et pour tout diviseur d de N, d divise d_i pour un certain i.*

Par exemple, $1, 3, 3^2 7$ et $3, 3^2, 3^2 7$ sont deux suites de diviseurs convergeant vers $3^2 7$. Pour la seconde définition, on suppose que le corps $\mathbb{F}_q$ est défini (on connaît ses éléments et on sait faire les opérations habituelles sur eux).

Définition 14. *Une* ***présentation itérée*** *de $\mathbb{F}_{q^N}$ sur $\mathbb{F}_q$ est un couple de suites $(d_i; P_i(X))$, où d_0=1,$d_1, d_2, ...$ est une suite de diviseurs convergeant vers N et $P_1, P_2, ...$ est une suite de polynômes telle que $\forall i \geq 0$, $P_{i+1}(X)$ est irréductible de degré d_{i+1}/d_i sur $\mathbb{F}_{q^{d_i}}$.*

Une présentation itérée de $\mathbb{F}_{q^N}$ sur $\mathbb{F}_q$ permet donc de définir l'ensemble des $\mathbb{F}_{q^{d_i}}$, où les d_i sont issus de la suite de diviseurs convergeant vers N. Voici deux exemples de présentations itérées, le premier est une présentation donnée par Wiedemann dans [Wie88] :

Exemple 6. *La suite de diviseurs est d_i=2^i, pour $i \geq 0$ et la suite de polynômes est P_1=$X^2 + X + 1$, P_i=$X^2 + \alpha_i X + 1$, pour $i > 1$, où α_i est une racine de P_{i-1}, forment une présentation itérée de $\mathbb{F}_{2^{2^\infty}}$ sur $\mathbb{F}_2$.*

Le second, donné dans [BS89], diffère du premier car cette fois, nous avons une suite infinie de polynômes irréductibles sur $\mathbb{F}_2$ et chaque polynôme va engendrer une présentation itérée d'un $\mathbb{F}_{2^{2.3^k}}$, pour un certain $k \geq 0$. Cette méthode nous permet donc de définir toutes les extensions algébriques de $\mathbb{F}_2$ de la forme $\mathbb{F}_{2^{2.3^k}}$, $k \geq 0$:

Exemple 7. *On sait que les polynômes $Q_k(X) = X^{2.3^k} + X^{3^k} + 1$ sont irréductibles sur $\mathbb{F}_2$. Ainsi, $\forall k \geq 0$ et $N = 2.3^k$, d_0=1, d_1=N et $P_1(X)$=$Q_k(X)$ forment une présentation itérée de $\mathbb{F}_{2^N}$ sur $\mathbb{F}_2$.*

C'est en appliquant le principe de ce second exemple que nous utiliserons les suites données dans la section suivante pour définir les extensions de $\mathbb{F}_2$ de la forme $\mathbb{F}_{2^{2^k p}}$ et $\mathbb{F}_{2^{3^k p}}$, pour $k \geq 0$ et où p est un nombre premier quelconque.

5.2 Génération de suites infinies de polynômes irréductibles invariants

Dans cette section, nous utilisons simplement les résultats du Chapitre 4 afin de générer des suites de polynômes irréductibles réciproques, médians et périodiques dans un premier temps et alternatifs dans un deuxième temps.

5.2.1 Suites de réciproques, médians et périodiques

Soit $P \in \mathcal{I}(n)$, on appelle $c_i(P)$ le coefficient de X^i dans P.

Des suites de polynômes irréductibles invariants apparaissent implicitement dans Varshamov [Var84] et plus explicitement dans Wiedemann [Wie88], Meyn [Mey90] et Cohen [Coh92]. Ces suites apparaissent dans des papiers consacrés au problème plus général qu'est la construction de polynômes irréductibles (voir Kyuregyan [Kyu02] et [Kyu04] pour des références récentes à ce sujet).

Notre approche montre que, en fait, il y a trois familles complètement analogues de polynômes irréductibles invariants correspondant aux trois sous-groupes de $\mathfrak{S}_3$ de taille 2. Le théorème suivant étend de façon simple la construction de suites de polynômes irréductibles réciproques donnée par Meyn et Cohen aux polynômes médians et périodiques.

Théorème 13. *Soit $P \in \mathcal{I}(n)$ tel que $\mathrm{c}_1(P) = \mathrm{Tr}(P) = 1$. À partir de $\phi_r(P)$ (resp. $\phi_m(P)$, $\phi_p(P)$) et en itérant la transformation $P \to \phi_r(P)$ (resp. $P \to \phi_m(P^+)$, $P \to \phi_p(P^{*+})$), on génère une suite infinie de polynômes irréductibles réciproques (resp. médians, périodiques) de degré $2^i n$, $i > 0$.*

Démonstration. On sait d'après le Corollaire 5 que $\phi_r(P)$ est réciproque et irréductible. Par le calcul, on voit que $\mathrm{Tr}(\phi_r(P)) = 1$ et du fait de la réciprocité, $\mathrm{c}_1(\phi_r(P)) = 1$. Donc par récurrence, on obtient une suite de polynômes irréductibles réciproques. Ensuite, en utilisant les Définitions 6 et 10, on obtient des suites de polynômes médians et périodiques. □

La figure 5.1 illustre le Théorème 13 : à partir d'un polynôme irréductible P tel que $\mathrm{c}_1(P) = \mathrm{Tr}(P) = 1$, on construit une suite $(P_1, P_2, ...)$ d'irréductibles réciproques en itérant ϕ_r et donc, d'après la structure d'un hexagone à 3 éléments, $(P_1^+, P_2^+, ...)$ est une suite de médians et $(P_1^{+*}, P_2^{+*}, ...)$ est une suite de périodiques.

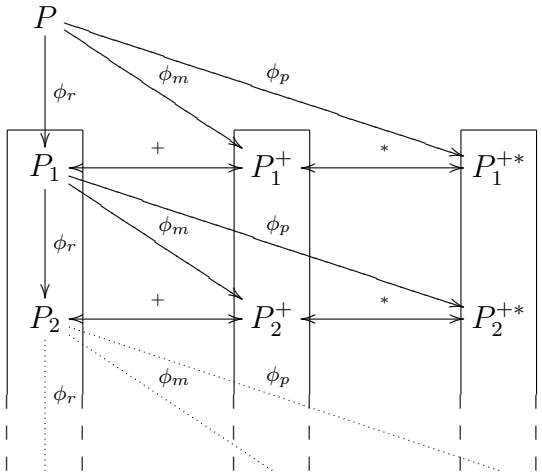


FIG. 5.1 – Construction de suites infinies de polynômes irréductibles réciproques, médians et périodiques à partir d'un polynôme P tel que $\mathrm{c}_1(P) = \mathrm{Tr}(P) = 1$.

Exemple 8. *Nous donnons ici l'exemple le plus simple : les suites engendrées par le polynôme $X^2 + X + 1$. On y retrouve notamment la suite de polynômes irréductibles réciproques donnée par Wiedemann dans [Wie88] :*

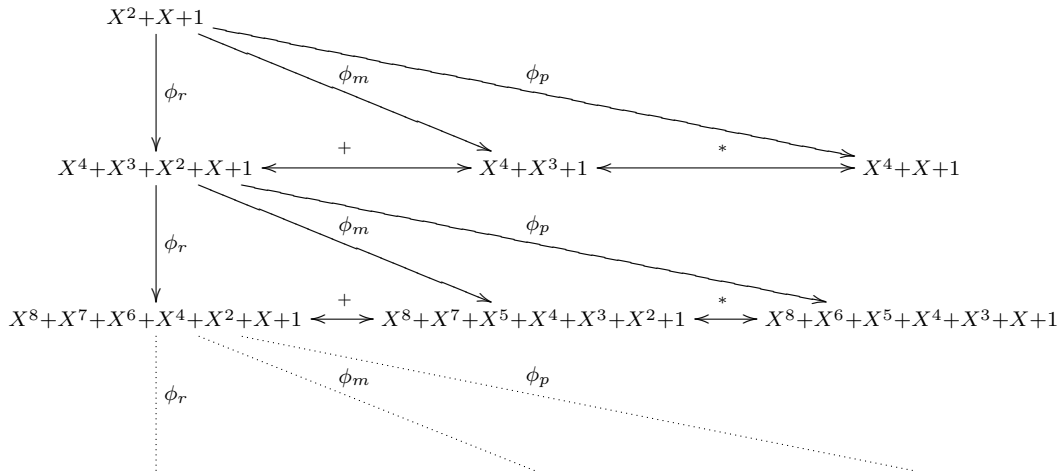


FIG. 5.2 – Construction de suites infinies de polynômes irréductibles réciproques, médians et périodiques à partir de $X^2 + X + 1$.

Comme nous l'avons vu dans la section précédente, les suites infinies de polynômes irréductibles que l'on peut construire vont permettre de définir effectivement toutes les extensions de $\mathbb{F}_2$ de la forme $\mathbb{F}_{2^{2^i p}}$, avec $i \geq 0$ et p un nombre premier. Il suffit pour cela de prendre un polynôme irréductible Q_0 de degré p tel que $\mathrm{c}_1(Q_0) = \mathrm{Tr}(Q_0) = 1$. On pose ensuite $Q_1 = \phi_r(Q_0)$ (resp. $\phi_m(Q_0)$, $\phi_p(Q_0)$) et $Q_i = \phi_r(Q_{i-1})$ (resp. $\phi_m(Q^+_{i-1})$, $\phi_p(Q^{*+}_{i-1})$), $i \geq 2$. Maintenant, avec les notations de l'Exemple 7, $\forall i \geq 0$ et $N = 2^i p$, $d_0 = 1$, $d_1 = N$ et $P_1 = Q_i$ forment une présentation itérée de $\mathbb{F}_{2^N}$ sur $\mathbb{F}_2$ et dans ce cas, si α est une racine de P_1, alors $\{\alpha^i, i = 0, ..., N-1\}$ est une base de $\mathbb{F}_{2^N}$ sur $\mathbb{F}_2$.

Pour compléter cette partie, nous ajoutons les formules que Niederreiter a données dans [Nie90], permettant de calculer le nombre $A(n)$ de polynômes irréductibles $P \in \mathbb{F}_2[X]$ de degré n et tels que $\mathrm{c}_1(P) = \mathrm{Tr}(P) = 1$. Si n est une puissance de 2, on a la première formule :

$$A(n) = \frac{2^n + 1}{4n} - \frac{1}{2^{n+1} n} \sum_{j=0}^{n/2} (-1)^j \binom{n}{2j} 7^j.$$

Dans le cas contraire, on écrit $n = 2^h m$, où $h \geq 0$ et m est un entier impair > 1. On a alors :

$$A(n) = \frac{1}{4n} \sum_{d|m} \mu\left(\frac{m}{d}\right) \left(2^{2^h d} - 2^{1-2^h d} \sum_{j=0}^{2^{h-1} d} (-1)^{2^h d + j} \binom{2^h d}{2j} 7^j\right).$$

Ces formules démontrent que pour tout $n \geq 2$, $n \neq 3$, $A(n) > 0$. Ainsi, d'après le Théorème 13, il est possible de construire des polynômes irréductibles réciproques, médians et périodiques de degré $2^i n$, $\forall i > 0$ et $\forall n \geq 2, n \neq 3$.

5.2.2 Suites d'alternatifs

Nous allons maintenant donner le moyen de construire des suites de polynômes irréductibles alternatifs. Cela découle simplement de nos précédents résultats. Nous commençons par énoncer la proposition suivante :

Proposition 11. *Si P est un polynôme irréductible alternatif de degré > 2, alors $\psi(P)$ est également irréductible alternatif.*

Démonstration. Puisque P est un polynôme irréductible alternatif (différent de $X^2 + X + 1$), on sait, d'après le Théorème 10, qu'il existe un polynôme irréductible Q tel que $P = \psi(Q)$. Or on sait aussi que $Q(\epsilon) \in \{\epsilon, \epsilon^2\}$ et que $P(\epsilon) = Q(\epsilon)^2$. Ceci implique que $P(\epsilon) \in \{\epsilon, \epsilon^2\}$ et, toujours d'après le Théorème 10, $\psi(P)$ est un polynôme irréductible alternatif. □

S'ensuit alors le théorème :

Théorème 14. *Soit $P \in \mathcal{I}(n)$ tel que $P(\epsilon) \in \{\epsilon, \epsilon^2\}$, alors l'itération de ψ sur P génère une suite de polynômes irréductibles alternatifs de degré $3^i n$, $i > 0$.*

Démonstration. Le Théorème 10 et la Proposition 11 démontrent ce théorème. □

Exemple 9. *Nous illustrons le théorème précédent par les premiers termes de la suite engendrée par $X^3 + X + 1$:*

$$X^3 + X + 1$$
$$\downarrow \psi$$
$$X^9 + X^8 + 1$$
$$\downarrow \psi$$
$$X^{27} + X^{25} + X^{24} + X^{19} + X^{18} + X^{16} + X^{10} + X^9 + X^3 + X + 1$$
$$\downarrow \psi$$
$$X^{81} + X^{80} + X^{65} + X^{17} + 1$$
$$\vdots \psi$$

FIG. 5.3 – Suite des polynômes irréductibles alternatifs engendrée par $X^3 + X + 1$.

Remarque: D'après ce que nous avons vu, nous savons que dans une suite, deux polynômes consécutifs vont être de type différent. Ainsi, si nous souhaitons engendrer une suite de polynômes alternatifs de même type, il suffit d'itérer la fonction $+ \circ \psi$.

Comme précédemment, ces suites vont permettre de définir effectivement toutes les extensions de $\mathbb{F}_2$ de la forme $\mathbb{F}_{2^{3^i p}}$, avec $i \geq 0$ et p un nombre premier. Il suffit pour cela de prendre un polynôme irréductible Q_0 de degré p tel que $Q_0(\epsilon) \in \{\epsilon, \epsilon^2\}$. On pose ensuite $Q_i = \psi(Q_{i-1})$, $i \geq 1$. Avec les notations de l'Exemple 7, $\forall i \geq 0$ et $N = 3^i p$, $d_0 = 1$, $d_1 = N$ et $P_1 = Q_i$ forment une présentation itérée de $\mathbb{F}_{2^N}$ sur $\mathbb{F}_2$ et dans ce cas, si α est une racine de P_1, alors $\{\alpha^i, i = 0, ..., N-1\}$ est une base de $\mathbb{F}_{2^N}$ sur $\mathbb{F}_2$.

Troisième partie

Interprétations des transformations

À toute transformation T sur les polynômes irréductibles, on peut associer un graphe Γ_T orienté dont l'ensemble des sommets est l'ensemble $\mathcal{I}$ et où, pour tout polynôme $P \in \mathcal{I}$, un arc joint P à chaque facteur irréductible de $T(P)$.

Tout d'abord, dans le Chapitre 6, nous montrerons que les transformations que nous avons vues précédemment, y compris les transformations équivalentes données dans les Tableaux 4.1 et 4.2, n'engendrent en fait que cinq graphes différents, à isomorphisme près. Nous donnerons la table regroupant les transformations en fonction de la forme de leur graphe.

Ensuite, dans le Chapitre 7, nous étudierons le cas des transformations quadratiques. Nous introduirons dans un premier temps la courbe elliptique $\mathcal{K}$ et nous expliquerons en quoi elle est liée à nos travaux. Ensuite, après une rapide étude de la courbe, nous montrerons que l'on retrouve les graphes de ϕ_r et de ϕ_m à travers les calculs d'une 2-isogénie ou du doublement sur ses points. Puis, pour illustrer cela, nous donnerons le graphe de ϕ_r sur les polynômes de degré 2^i, $1 \leq i \leq 3$, et nous expliquerons sa forme par l'étude des groupes $\mathcal{K}(\mathbb{F}_{2^{2^i}})$, $0 \leq i \leq 4$. Nous donnerons également le graphe de ϕ_m à titre d'information. Enfin, bien que nous pensons qu'il existe, nous n'avons pour le moment pas fait le lien entre $\mathcal{K}$ et ϕ_p. Néanmoins, nous présenterons le graphe de cette dernière et nous étudierons le cas des polynômes de degré une puissance de 2 par une approche totalement différente.

Le Chapitre 8 est consacré aux transformations ψ et $\psi' = + \circ \psi$. Nous ferons une étude de ψ, inspirée de celle de ϕ_r et ϕ_m, en introduisant la courbe supersingulière $\mathcal{S}$ et en montrant que l'on retrouve ψ à travers la construction d'une isogénie de degré 3 sur $\mathcal{S}$. Nous donnerons également les graphes de ces transformations sur les polynômes de degré 3 et 9.

Concernant les courbes elliptiques, le lecteur pourra retrouver toutes les notions abordées dans cette partie dans les livres de Silverman [Sil86] ou de Washington [Was08] par exemple.

Chapitre 6

Graphes isomorphes

Prenons les cinq transformations ϕ_r, ϕ_m, ϕ_p, ψ et $\psi' = + \circ \psi$. Dans ce chapitre, nous allons montrer que pour chacune des transformations équivalentes présentées dans les Tableaux 4.1 et 4.2, le graphe qui lui est associé sera isomorphe au graphe de l'une de ces cinq transformations.

Pour cela, il suffit de prouver la proposition suivante :

Proposition 12. *Soit $t \in \{\phi_p, \phi_m, \phi_r, \psi, \psi'\}$, pour tout élément $S \in \mathfrak{S}_3$, le graphe de la transformation conjuguée $S \circ t \circ S^{-1}$ est isomorphe à celui de t.*

Démonstration. On a une transformation $t \in \{\phi_p, \phi_m, \phi_r, \psi, \psi'\}$ définie sur $\mathcal{I}$, soient S un élément de $\mathfrak{S}_3$ et $f = S \circ t \circ S^{-1}$. On sait que S est une bijection de $\mathcal{I}$ (bien évidemment, S^{-1} aussi). Pour tout $P \in \mathcal{I}$, on a $f(S(P)) = S \circ t \circ S^{-1} \circ S(P) = S(t(P))$ donc le graphe de f est l'image du graphe de t par S et ces graphes sont isomorphes. □

Nous rappelons maintenant quelques propriétés de nos transformations :

$$\phi_p = + \circ \phi_p = * \circ \phi_m = * \circ + \circ \phi_r$$

$$\phi_m = * \circ + \circ * \circ \phi_m = * \circ \phi_p = + \circ \phi_r$$

$$\phi_r = * \circ \phi_r = + \circ \phi_m = + \circ * \circ \phi_p$$

$$\begin{cases} \psi = * \circ + \circ \psi = + \circ * \circ \psi \\ + \circ \psi = * \circ \psi = * \circ + \circ * \circ \psi \\ \psi = + \circ \psi \circ + \end{cases}$$

Ainsi, à l'aide de ces propriétés et de la Proposition 12, nous pouvons dresser le tableau suivant, qui classe les transformations en fonction de la forme des graphes qu'elles engendrent :

type de graphe	transformations conjuguées	transformations correspondantes
graphe de ϕ_p	ϕ_p $* \circ \phi_p \circ *$ $+ \circ * \circ \phi_p \circ * \circ +$ $* \circ + \circ * \circ \phi_p \circ * \circ + \circ *$ $* \circ + \circ \phi_p \circ + \circ *$ $+ \circ \phi_p \circ +$	ϕ_p $\phi_m \circ *$ $\phi_r \circ * \circ +$ $\phi_r \circ * \circ + \circ *$ $\phi_m \circ + \circ *$ $\phi_p \circ +$
graphe de ϕ_m	ϕ_m $* \circ \phi_m \circ *$ $+ \circ * \circ \phi_m \circ * \circ +$ $* \circ + \circ * \circ \phi_m \circ * \circ + \circ *$ $* \circ + \circ \phi_m \circ + \circ *$ $+ \circ \phi_m \circ +$	ϕ_m $\phi_p \circ *$ $\phi_p \circ * \circ +$ $\phi_m \circ * \circ + \circ *$ $\phi_r \circ + \circ *$ $\phi_r \circ +$
graphe de ϕ_r	ϕ_r $* \circ \phi_r \circ *$ $+ \circ * \circ \phi_r \circ * \circ +$ $* \circ + \circ * \circ \phi_r \circ * \circ + \circ *$ $* \circ + \circ \phi_r \circ + \circ *$ $+ \circ \phi_r \circ +$	ϕ_r $\phi_r \circ *$ $\phi_m \circ * \circ +$ $\phi_p \circ * \circ + \circ *$ $\phi_p \circ + \circ *$ $\phi_m \circ +$
graphe de ψ	ψ $= + \circ \psi \circ +$ $* \circ \psi \circ *$ $= * \circ + \circ \psi \circ + \circ *$ $+ \circ * \circ \psi \circ * \circ +$ $= * \circ + \circ * \circ \psi \circ * \circ + \circ *$	ψ $\psi \circ + \circ *$ $\psi \circ * \circ +$
graphe de ψ'	ψ' $= + \circ \psi' \circ +$ $* \circ \psi' \circ *$ $= * \circ + \circ \psi' \circ + \circ *$ $+ \circ * \circ \psi' \circ * \circ +$ $= * \circ + \circ * \circ \psi' \circ * \circ + \circ *$	$\psi \circ +$ $\psi \circ *$ $\psi \circ * \circ + \circ *$

TAB. 6.1 – Classement des transformations en fonction de la forme de leur graphe.

Chapitre 7

La courbe elliptique $\mathcal{K}$ et les graphes des transformations quadratiques

Ce chapitre est consacré aux graphes des transformations quadratiques. Nous introduisons pour cela la courbe $\mathcal{K}$ et nous montrons que l'on retrouve les graphes de ϕ_r et ϕ_m sur les points de $\mathcal{K}$, par l'intermédiaire d'une 2-isogénie ou du doublement. Aussi, pour ϕ_p, à défaut de faire également le lien avec $\mathcal{K}$, nous donnons un résultat intéressant concernant les polynômes de degré une puissance de 2.

7.1 Présentation de la courbe $\mathcal{K}$

À la fin de la section 5.2.1, il est précisé que Niederreiter a donné, dans [Nie90], les formules permettant de calculer le nombre de polynômes irréductibles $P \in \mathbb{F}_2[X]$ tels que $\mathrm{c}_1(P) = \mathrm{Tr}(P) = 1$ pour un degré donné. Dans sa démonstration, il calcule de manière explicite certaines sommes de Kloosterman. C'est par l'intermédiaire de l'une de ces sommes que nous allons introduire notre courbe elliptique.

Les sommes de Kloosterman sur $\mathbb{F}_2$ sont des sommes de valeurs de caractères du groupe additif $(\mathbb{F}_{2^n}, +)$ en certains points du corps $\mathbb{F}_{2^n}$. Il est facile de construire un caractère de ce groupe :

$$\psi_n(x) = (-1)^{\mathrm{Tr}_n(x)},$$

où $x \in \mathbb{F}_{2^n}$ et Tr_n est la trace $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}$. Tous les autres caractères sont de la forme $\psi_n(cx)$, avec $c \in \mathbb{F}_{2^n}$. La somme de Kloosterman est

$$K_n(a,b) = \sum_{x \in \mathbb{F}_{2^n}^*} \psi_n(ax + b/x)$$

avec $a, b \in \mathbb{F}_{2^n}$. On désire évaluer cette somme. Les cas triviaux sont faciles :

$$K_n(0,0) = 2^n - 1 \text{ et } K_n(0,b) = K_n(a,0) = -1 \text{ si } a, b \in \mathbb{F}_{2^n}^*$$

Le calcul de $K_n(1,1)$ est légèrement plus compliqué, on a :

$$K_n(1,1) = -\omega_1^n - \omega_2^n,$$

avec

$$\omega_1 = \frac{-1 \pm i\sqrt{7}}{2} \text{ et } \omega_2 = \overline{\omega_1}.$$

À partir de là, en suivant ce que fait Serre dans [Ser77], on introduit la courbe $\mathcal{K}$:

$$\mathcal{K} : Y^2 + Y = X + \frac{1}{X}.$$

C'est un cas particulier des courbes d'Artin-Schreier sur $\mathbb{F}_2$ qui ont la forme générale $Y^2 + Y = f(X)$ avec $f(X) \in \mathbb{F}_2[X]$. Étant donné que $\mathcal{K}$ possède 4 points rationnels sur $\mathbb{F}_2$, sa fonction zéta est (voir [Sil86] par exemple)

$$Z(\mathcal{K}, t) = \frac{2t^2 + t + 1}{(1-t)(1-2t)} = \frac{(1-\omega_1 t)(1-\omega_2 t)}{(1-t)(1-2t)},$$

où l'on retrouve les ω_1 et ω_2 de la somme de Kloosterman. En prenant le logarithme, on obtient la formule classique du calcul du nombre de points de la courbe :

$$\nu_n = \mathrm{Card}(\mathcal{K}(\mathbb{F}_{2^n})) = 2^n + 1 - \omega_1^n - \omega_2^n. \tag{7.1}$$

Les premières valeurs de ν_n sont données par le tableau suivant :

n	1	2	3	4	5	6	7	8
ν_n	4	8	4	16	44	56	116	288

donc

$$\log Z(\mathcal{K}, t) = 4t + 8\frac{t^2}{2} + 4\frac{t^3}{3} + \cdots + \frac{\nu_n t^n}{n} + \dots .$$

On a ainsi une interprétation de la somme de Kloosterman $K_n(1,1)$ par l'intermédiaire du nombre de points de la courbe elliptique $\mathcal{K}$.

Nous étudions maintenant brièvement les points de notre courbe. En faisant la complétion projective de $\mathcal{K}$, on obtient une courbe elliptique (non singulière et non supersingulière) sur $\mathbb{F}_2$:

$$XY^2 + XYZ = X^2Z + Z^3.$$

Pour passer sous la forme de Weierstrass, elle peut être ramenée à la courbe E_0 suivante (qui est une courbe de Köblitz [HMV04]) :

$$E_0 : S^2 + RS = R^3 + 1,$$

en faisant tout d'abord le changement de repère

$$(X : Y : Z) \to (R : S : T) = (Z : Y + X : X),$$

puis, en prenant sa partie affine ($T = 1$). Le point à l'infini $(0 : 1 : 0)$ de E_0 correspond au point au point à l'infini $\Omega = (0 : 1 : 0)$ de $\mathcal{K}$, mais $\mathcal{K}$ possède un second point à l'infini $O = (1 : 0 : 0)$.

Si on a un point rationnel $A = (\alpha : \beta : 1) \in \mathcal{K}(\mathbb{F}_{2^n})$ alors $A' = (\alpha : \beta+1 : 1) \in \mathcal{K}(\mathbb{F}_{2^n})$ et ces deux points sont sur la droite $X = \alpha$, qui coupe la courbe en un troisième point qui est Ω. Donc la loi de groupe sur $\mathcal{K}$, en prenant Ω pour élément neutre, nous dit que

$$A + A' = \Omega,$$

c'est à dire que A' est l'opposé de A.

Aussi, si $\alpha \neq 0$, le point $B = (1/\alpha : \beta : 1) \in \mathcal{K}(\mathbb{F}_{2^n})$ et la droite AB passe par O, donc on a

$$A + B = O.$$

Sur $\mathbb{F}_2$, on a

$$\mathcal{K}(\mathbb{F}_2) = \{\Omega,\ O,\ (1 : 0 : 1),\ (1 : 1 : 1)\},$$

qui est un groupe cyclique d'ordre 4, où le point O est d'ordre 2 et les deux derniers points sont d'ordre 4.

À partir de maintenant, pour un élément a d'un corps fini, nous noterons P_a son polynôme minimal. Aussi, pour simplifier les notations dans ce qui va suivre, nous appellerons ϕ'_r la transformation $\phi_r \circ *$.

Définition 15. *Soient $a \in \mathbb{F}_{2^n}$ et $\mathcal{P} = (a, b)$ un point de $\mathcal{K}$, on définit les **degrés** de a et de $\mathcal{P}$ de la manière suivante :*

$$\deg(a) = \deg(P_a),$$

$$\deg(\mathcal{P}) = \max(\deg(a), \deg(b)).$$

Nous allons maintenant caractériser les points de $\mathcal{K}(\mathbb{F}_{2^n})$ dont "l'abscisse" est de degré n, ceci nous servira lors de l'interprétation du graphe de ϕ_r. Soit $\mathcal{P} = (a, b)$ un point de $\mathcal{K}(\mathbb{F}_{2^n})$ et u tel que $a+1/a = b^2+b = u$. On a $P_u(a+1/a) = 0$ donc $P_a | \phi'_r(P_u)$, de même, $P_u(b^2 + b) = 0$ donc $P_b | \phi_p(P_u)$.

Supposons que a soit de degré n. Dans ce cas, u appartient aussi à $\mathbb{F}_{2^n}$ mais il peut être dans un sous-corps de $\mathbb{F}_{2^n}$. Posons $\deg(u) = m$. Le polynôme P_u est irréductible dans $\mathbb{F}_2[X]$ et donc, par le Théorème 9 et le Corollaire 5 :

- si $c_1(P_u) = 1$ alors P_a est le polynôme irréductible réciproque $\phi'_r(P_u)$ et $m = n/2$. Ensuite, si $\mathrm{Tr}(P_u) = 0$, alors P_b est de degré m et n'est pas périodique et P_a est de trace 0 (démonstration triviale). D'autre part, si $\mathrm{Tr}(P_u) = 1$, alors P_b est périodique de degré n et P_a est de trace 1.

– si $\mathrm{c}_1(P_u) = 0$, alors $\phi'_r(P_u) = QQ^*$, où Q est irréductible de degré m. Dans ce cas on a $m = n$ et $P_a = Q$ ou Q^*. Aussi, étant donné que $\mathcal{P} \in \mathcal{K}(\mathbb{F}_{2^n})$, $\deg(\mathcal{P}) \leq n$ et donc P_b ne peut pas être périodique de degré $2n$, ainsi, $\mathrm{Tr}(P_u) = 0$, ce qui implique que $\mathrm{c}_1(P_a) = \mathrm{Tr}(P_a)$ (là encore, la démonstration est simple).

Ainsi, pour résumer, si $\mathcal{P} = (a, b)$ est un point de $\mathcal{K}(\mathbb{F}_{2^n})$, soit P_a est de degré n, auquel cas $\mathrm{c}_1(P_a) = \mathrm{Tr}(P_a)$, soit $\deg(P_a) < n$.

7.2 Graphe de ϕ_r et interprétation

Nous commençons par un bref rappel sur la construction d'isogénies. À partir d'un sous-groupe fini F de l'ensemble des points d'une courbe elliptique E_1 définie sur un corps commutatif algébriquement clos $\mathbb{K}$, Vélu [Vél71] a donné le moyen de construire une isogénie de noyau F entre E_1 et une autre courbe E_2, E_1 et E_2 étant des courbes de Weierstrass. Cela se fait de la manière suivante :

$$\begin{array}{ccc} E_1(\mathbb{K}) & \to & E_2(\mathbb{K}) \\ \mathcal{P} & \mapsto & \begin{cases} \Omega_{E_2} & \text{si } \mathcal{P} \in F, \\ \big(X_{\mathcal{P}} + \displaystyle\sum_{\mathcal{Q} \in F \setminus \{\Omega_{E_1}\}} X_{\mathcal{P}+\mathcal{Q}} - X_{\mathcal{Q}}, & \\ \quad Y_{\mathcal{P}} + \displaystyle\sum_{\mathcal{Q} \in F \setminus \{\Omega_{E_1}\}} Y_{\mathcal{P}+\mathcal{Q}} - Y_{\mathcal{Q}}\big) & \text{sinon,} \end{cases} \end{array} \tag{7.2}$$

où $\mathcal{P}$ est un point de coordonnées $(X_{\mathcal{P}}, Y_{\mathcal{P}})$ et où Ω_{E_1} (resp. Ω_{E_2}) est l'élément neutre de E_1 (resp. E_2).

En utilisant cette construction sur les points de $\mathcal{K}$ avec $F = \{\Omega, O\}$, on construit une isogénie $\mathfrak{I}$ de degré 2 de $\mathcal{K}$ dans elle-même. Le théorème suivant permet de faire le lien avec nos transformations :

Théorème 15. *Soient $\mathcal{P} = (a, b)$ et $\mathcal{P}' = (a', b')$ deux points de $\mathcal{K}$ tels que $\mathcal{P}'$ est l'image de $\mathcal{P}$ par l'isogénie $\mathfrak{I}$. Alors, $P_a | \phi_r(P_{a'})$ et $P_b | (\phi_p \circ *)(P_{a'})$.*

Démonstration. À l'aide des formules 7.2 et de la loi de groupe pour les courbes sous la forme de Weierstrass (voir [Sil86]), on obtient

$$a' = \frac{a}{a^2 + 1} = \frac{1}{b^2 + b} \text{ et } b' = b + \frac{a}{a + 1},$$

autrement dit, a est racine de $\phi_r(P_{a'})$ et b est racine de $(\phi_p \circ *)(P_{a'})$. □

Le même résultat est obtenu par le doublement :

Théorème 16. *Soient $\mathcal{P} = (a, b)$ et $\mathcal{P}' = (a', b')$ deux points de $\mathcal{K}$ tels que $\mathcal{P}' = 2 * \mathcal{P}$. Alors, $P_a | \phi_r(P_{a'})$ et $P_b | (\phi_p \circ *)(P_{a'})$.*

Démonstration. Avec les formules de doublement, on trouve

$$a' = \left(\frac{a}{a^2+1}\right)^2 = \left(\frac{1}{b^2+b}\right)^2 \text{ et } b' = \left(b + \frac{a}{a+1}\right)^2,$$

autrement dit, a est racine de $\phi_r(P_{a'})$ et b est racine de $(\phi_p \circ *)(P_{a'})$. □

Remarque: Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux courbes elliptiques. On sait que si $f : \mathcal{C}_1 \to \mathcal{C}_2$ est une isogénie de degré d, alors, sa duale $f^\# : \mathcal{C}_2 \to \mathcal{C}_1$ est telle que $f \circ f^\#$ est la multiplication par d des points de $\mathcal{C}_1$. D'après les preuves des théorèmes précédents, on constate que la duale de $\mathfrak{I}$ est un cas particulier puisqu'il s'agit de l'automorphisme de Frobenius.

Soit Γ le graphe dont les sommets sont les polynômes de $\mathcal{I}$ et où il existe un arc allant du polynôme P_1 au polynôme P_2 si et seulement s'il existe deux points $\mathcal{P}_1$ et $\mathcal{P}_2$ de $\mathcal{K}(\overline{\mathbb{F}_2})$ dont les abscisses sont respectivement racines de P_1 et P_2 et tels que $\mathcal{P}_1 = 2 * \mathcal{P}_2$. Alors d'après le Théorème 16, Γ est le graphe de ϕ_r.

Pour illustrer cela, nous allons interpréter le graphe de ϕ_r pour les polynômes irréductibles de degré 2^k, $1 \leq k \leq 3$ (Figure 7.1). Chaque polynôme est représenté par un nombre, la correspondance étant donnée dans l'Annexe C.1. Les lignes horizontales en pointillés regroupent les polynômes par degré.

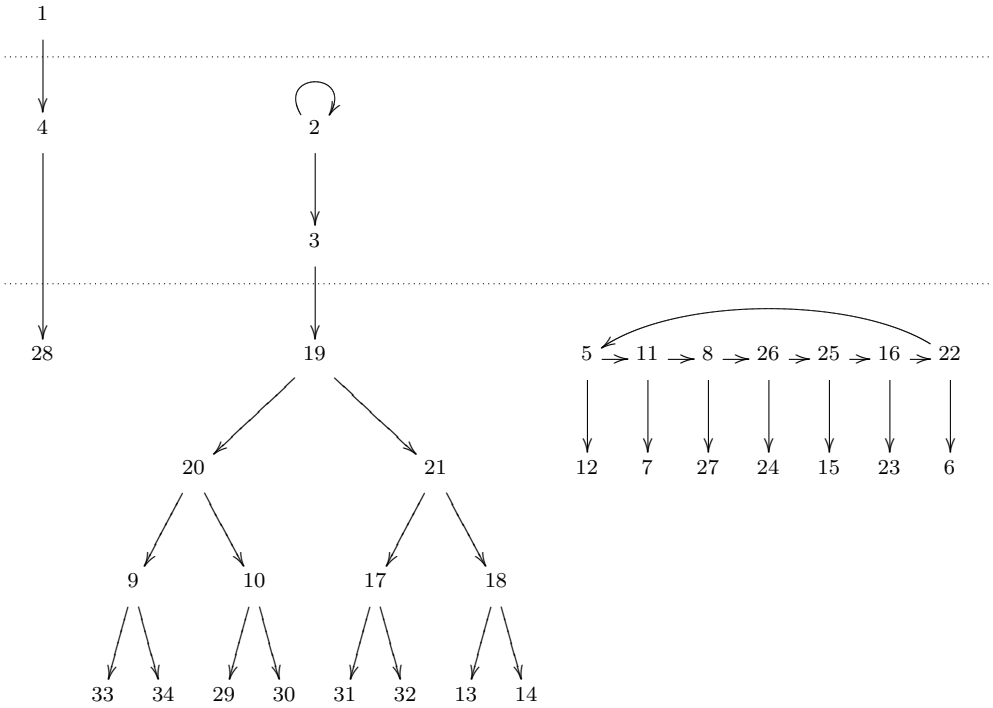


FIG. 7.1 – Graphe de ϕ_r.

Pour notre interprétation, nous allons étudier les groupes $\mathcal{K}(\mathbb{F}_{2^{2^i}})$, $0 \leq i \leq 4$. Pour simplifier l'écriture, nous dirons que le polynôme minimal de l'abscisse d'un point est le polynôme associé au point et inversement, les points dont les abscisses sont racines d'un polynôme seront les points associés au polynôme.

Le groupe $\mathcal{K}(\mathbb{F}_2)$

Comme nous l'avons vu plus tôt, on a

$$\mathcal{K}(\mathbb{F}_2) = \{\Omega,\ O,\ (1:0:1),\ (1:1:1)\},$$

où Ω est l'élément neutre, O est d'ordre 2 et les deux autres points sont d'ordre 4. On connaît la structure du groupe $\mathcal{K}[2^k]$ des points de 2^k-division (voir [Was08] par exemple) :

$$\mathcal{K}[2^k] \simeq \mathbb{Z}/2^k\mathbb{Z},$$

donc

$$\mathcal{K}[2] = \{\Omega, O\},$$

et

$$\mathcal{K}[4] = \mathcal{K}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Cependant, étant donné que les polynômes de $\mathcal{I}$ sont de degré ≥ 2, les polynômes associés aux points de $\mathcal{K}(\mathbb{F}_2)$ n'interviennent pas dans le graphe de ϕ_r.

Le groupe $\mathcal{K}(\mathbb{F}_{2^2})$

D'après la formule 7.1, on sait que $\text{Card}(\mathcal{K}(\mathbb{F}_{2^2})) = 8$ et puisque $\mathcal{K}[8] \simeq \mathbb{Z}/8\mathbb{Z}$, on en déduit que $\mathcal{K}(\mathbb{F}_{2^2}) = \mathcal{K}[8]$. Parmi ces 8 points, on compte les 4 points de $\mathcal{K}(\mathbb{F}_2)$ et les 4 points d'ordre 8 de $\mathcal{K}$. Ces derniers sont tous associés au polynôme 1 dans la Figure 7.1.

Le groupe $\mathcal{K}(\mathbb{F}_{2^4})$

On a $\text{Card}(\mathcal{K}(\mathbb{F}_{2^4})) = 16$ donc $\mathcal{K}(\mathbb{F}_{2^4}) = \mathcal{K}[16]$. Ainsi, $\mathcal{K}(\mathbb{F}_{2^4})$ est constitué des 8 points de $\mathcal{K}(\mathbb{F}_{2^2})$ et des 8 points d'ordre 16 de $\mathcal{K}$. D'après le Théorème 16, on sait que ces 8 points sont associés au polynôme $\phi_r(1) = 4$. On a donc un arc allant du 1 au 4 dans le graphe.

Le groupe $\mathcal{K}(\mathbb{F}_{2^8})$

Cette fois, $\text{Card}(\mathcal{K}(\mathbb{F}_{2^8})) = 288$ et $\mathcal{K}(\mathbb{F}_{2^8})$ n'est plus un groupe cyclique. Plus précisément, on a

$$\mathcal{K}(\mathbb{F}_{2^8}) \simeq \mathbb{Z}/96\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Parmi les 288 points, on a le sous-groupe cyclique $\mathcal{K}[32]$ constitué des 16 points de $\mathcal{K}(\mathbb{F}_{2^4})$ et des 16 points d'ordre 32 de $\mathcal{K}$. Ces derniers sont tous associés au polynôme $\phi_r(4) = 28$.

Ensuite, d'après ce que l'on a vu précédemment, on retrouve les points associés aux polynômes de degré 4 dont la trace est différente du coefficient de X. On compte 2 tels polynômes (2 et 3), ce qui fait 16 points. Et en particulier, les points associés au polynôme 2 sont les 8 points d'ordre 3, en les divisant par 2 on obtient les mêmes points auxquels s'ajoutent les 8 points d'ordre 6 associés au polynôme 3.

Enfin, il reste les 240 points associés aux 15 polynômes de degré 8 (mis à part le 28), tels que leur trace et le coefficient de X sont égaux. Ces polynômes constituent l'arbre de la Figure 7.1, on y trouve le 19, réciproque, dont les points associés sont d'ordre 12, les 20 et 21, dont les points sont d'ordre 24, les 9, 10 17 et 18 associés aux points d'ordre 48 et enfin, les polynômes 33, 34, 29, 30, 31, 32, 13 et 14 associés aux points d'ordre 96.

Le groupe $\mathcal{K}(\mathbb{F}_{2^{16}})$

Pour terminer les explications sur le graphe de la Figure 7.1, nous nous limiterons aux points de $\mathcal{K}(\mathbb{F}_{2^{16}}) \setminus \mathcal{K}(\mathbb{F}_{2^8})$ associés à des polynômes de degré 8.

Le groupe $\mathcal{K}(\mathbb{F}_{2^{16}})$ compte 65088 éléments, il n'est pas cyclique et sa structure est

$$\mathcal{K}(\mathbb{F}_{2^{16}}) \simeq \mathbb{Z}/21696\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Il y a $\varphi(113) = 112$ points d'ordre 113 et autant d'ordre 226. Les premiers sont associés aux 7 polynômes formant le cycle dans le graphe (les polynômes 5, 11, 8, 26, 25, 16 et 22), les seconds sont associés aux 7 polynômes attachés au cycle (les numéros 12, 7, 27, 24, 15, 23 et 6). Les $65088 - 288 - 2 * 112 = 64576$ points restant sont associés aux 2018 polynômes de degré 16 dont la trace et le coefficient de X sont égaux.

7.3 Graphe de ϕ_m

Les Théorèmes 15 et 16 démontrent que l'on retrouve la transformation $\phi_p \circ *$ à travers les calculs d'une 2-isogénie ou du doublement sur $\mathcal{K}$. Ainsi, à l'image de ce que nous avons fait précédemment, soit Γ le graphe dont les sommets sont les polynômes de $\mathcal{I}$ et où il existe un arc allant du polynôme P_1 au polynôme P_2 si et seulement s'il existe deux points $\mathcal{P}_1$ et $\mathcal{P}_2$ de $\mathcal{K}(\overline{\mathbb{F}_2})$ tels que l'abscisse de $\mathcal{P}_1$ est racine de P_1, l'ordonnée de $\mathcal{P}_2$ est racine de P_2 et $\mathcal{P}_1 = 2 * \mathcal{P}_2$. Alors d'après le Théorème 16, Γ est le graphe de $\phi_p \circ *$. Or, d'après le Tableau 6.1, on sait que $\phi_p \circ *$ et ϕ_m ont des graphes isomorphes, par conséquent, Γ est un graphe isomorphe à celui de ϕ_m.

Nous ne faisons pas, ici, l'étude du graphe comme nous l'avons faite pour ϕ_r, nous donnons simplement le graphe de ϕ_m, pour lequel nous rappelons que la correspondance entre les numéros et les polynômes est en Annexe C.1.

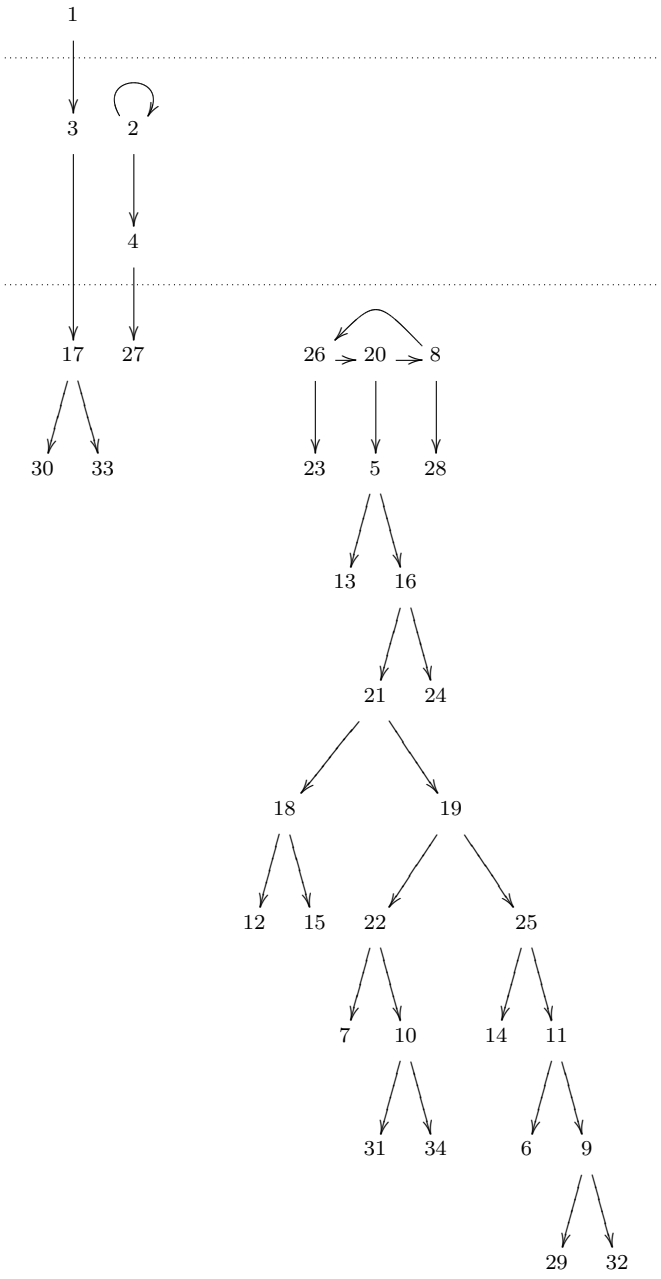


FIG. 7.2 – Graphe de ϕ_m.

7.4 Graphe de ϕ_p

Pour l'étude de la transformation ϕ_p, nous nous limiterons aux polynômes de degré $n = 2^k$, $k \geq 1$.

Soit $K = \mathbb{F}_{2^n}$, nous considérons l'application

$$f = \sigma + Id : \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^2 + x, \end{array}$$

où σ est l'automorphisme de Frobenius et Id est l'identité. On a donc, si $P \in \mathcal{I}(n)$:

$$\phi_p(P) = P \circ f.$$

On reconnaît en f l'application dite d'Artin-Schreier, souvent noté $\wp$, pour les corps de caractéristique 2. La théorie d'Artin-Schreier, caractérise les extensions cycliques de degré p (ici $p = 2$) des corps de caractéristique p, appelées extensions d'Artin-Schreier [Lan02].

Ainsi l'étude de la transformation ϕ_p sur les polynômes irréductibles de $\mathbb{F}_2[X]$ reflète la théorie d'Artin-Schreier appliquée aux corps finis de caractéristique 2.

Si on voit $(K, +)$ comme un $\mathbb{F}_2$-espace vectoriel de dimension n, alors f est un endomorphisme $\mathbb{F}_2$-linéaire de $(K, +)$, son noyau est $\mathbb{F}_2$ et son image est de dimension $n - 1$, c'est l'espace des éléments de trace nulle de K (Théorème 90 additif de Hilbert). De plus f et σ commutent :

$$f \circ \sigma = \sigma \circ f.$$

Cette propriété est très importante. Par exemple, elle implique que $Ker(f)$ et $Im(f)$ sont des $\mathbb{F}_2$-sous-espaces de K, stables par Frobenius.

On remarque d'une part que $Ker(f) = \mathbb{F}_2$ et d'autre part, que $f \circ f(K)$ est inclus dans $f(K)$ et c'est un sous-espace de dimension $n - 2$ de K. De même, $f \circ f \circ f(K)$ est inclus dans $f \circ f(K)$ et c'est un sous-espace de dimension $n - 3$ de K, etc.

Proposition 13. *Si le degré n est une puissance de 2, alors $f^n = 0$ (f est nilpotente).*

Démonstration. On utilise la théorie des 2-polynômes (voir [Ore34]). Si $\otimes$ désigne le *produit symbolique* des 2-polynômes (c'est-à-dire la composition), $f^n(x) = (x^2 + x) \otimes \cdots \otimes (x^2 + x)$ (n fois) est le linéarisé de $(x + 1)^n$, or n est une puissance de 2 donc $(x + 1)^n = x^n + 1$ et $f^n(x) = x^{2^n} + x$. Ainsi d'après le Petit Théorème de Fermat, f est identiquement nulle sur $\mathbb{F}_{2^n}$. □

On a donc $n + 1$ $\mathbb{F}_2$-espaces vectoriels inclus les uns dans les autres :

$$L_n = K \supset L_{n-1} = f(L_n) \supset L_{n-2} = f(L_{n-1}) \supset ... \supset L_0 = \{0\}, \tag{7.3}$$

et ils sont tous de codimension 1. Ainsi, les itérations de f donnent des images qui forment une suite décroissante de $\mathbb{F}_2$-sous-espaces qui sont stables par Frobenius (à cause de la commutation ci-dessus).

Nous pouvons donc regarder cette filtration du point de vue des polynômes irréductibles de $\mathbb{F}_2[X]$.

Définition 16. *Soient $P \in \mathcal{I}(n)$, et a une racine de P, on appelle* ***rang*** *de P (resp. de a), noté $\mathrm{rg}(P)$ (resp. $\mathrm{rg}(a)$), le rang sur $\mathbb{F}_2$ de l'ensemble de ses n racines $\{a, a^2, \ldots, a^{2^{n-1}}\}$ dans le $\mathbb{F}_2$-espace vectoriel K.*

Posons $R_i = L_i \setminus L_{i-1}$, $1 \leq i \leq n$. Les ensembles R_i sont stables par Frobenius puisque L_i et L_{i-1} sont stables. On remarque que R_n est la réunion des bases normales de K.

Théorème 17. *L_i est l'ensemble des racines des polynômes irréductibles de degré $2^k \leq n$ et de rang $\leq i$ et*

$$\prod_{x \in L_i} (X - x) = (X^2 + X)^{\otimes i}.$$

R_i est l'ensemble des racines des polynômes irréductibles de $\mathbb{F}_2[X]$ de rang égal à i et

$$\prod_{x \in R_i} (X - x) = (X^2 + X)^{\otimes i} / (X^2 + X)^{\otimes i-1}.$$

Démonstration. La seconde assertion résulte évidemment de la première. Démontrons la première.

Puisque $\dim(L_i) = i$ et que L_i est stable par Frobenius, L_i est l'ensemble des zéros d'un 2-polynôme. D'autre part la décomposition prouvée précédemment :

$$X^{2^n} - X = (X^2 + X)^{\otimes n},$$

est une décomposition irréductible symbolique (car $X^2 + X$ est un 2-polynôme symboliquement irréductible). D'après l'unicité de la décomposition symbolique ([Ore34]), on en déduit que L_i est l'ensemble des racines d'un 2-polynôme de la forme :

$$(X^2 + X)^{\otimes j} \text{ avec } j \leq n.$$

Puisque $\mathrm{Card}(L_i) = 2^i$, on en déduit que $j = i$ et que le rang des éléments de L_i est $\leq i$. □

Corollaire 6. *Les éléments de R_i, $i \geq 2$, sont les racines des polynômes $\phi_p^{i-2}(X^2 + X + 1)$.*

Démonstration. On a

$$\begin{aligned}
X^2 + X &= X(X+1), \\
(X^2 + X)^{\otimes 2} &= X^4 + X = (X^2 + X + 1)(X^2 + X), \\
&\cdots \\
(X^2 + X)^{\otimes i} &= (X^2 + X)^{\otimes 2} \otimes (X^2 + X)^{\otimes i-2} \\
&= [(X^2 + X + 1)(X^2 + X)] \otimes (X^2 + X)^{\otimes i-2} \\
&= \phi_p^{i-2}(X^2 + X + 1).(X^2 + X)^{\otimes i-1}.
\end{aligned}$$

Pour établir la dernière égalité, nous utilisons le fait que la composition des polynômes vérifie $(A.B) \circ C = (A \circ C).(B \circ C)$, le corollaire résulte alors de l'expression de R_i dans le théorème précédent. □

On remarque ainsi que tous les polynômes irréductibles dont le degré est une puissance de 2 sont obtenus par itération de ϕ_p sur $X^2 + X + 1$.

Voici le graphe de ϕ_p (Figure 7.3) pour les polynômes irréductibles de degré 2^k, $1 \leq k \leq 3$. La correspondance entre les polynômes et les nombres les représentant se trouve en Annexe C.1.

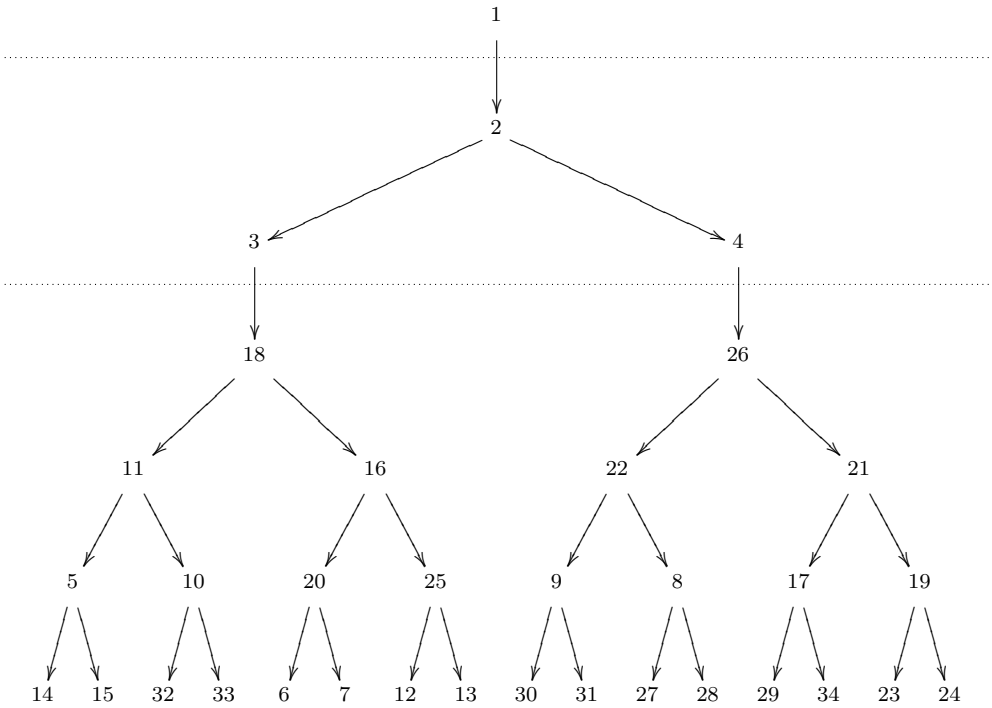


FIG. 7.3 – Graphe de ϕ_p.

Nous pouvons alors remarquer que pour chaque degré, les polynômes de rang minimal sont les polynômes périodiques. Plus précisément, les périodiques de degré 2^k sont de rang $2^{k-1} + 1$, ils sont racines d'arbres binaires de hauteur 2^{k-1} dont les feuilles, qui sont les polynômes de trace 1, sont également les polynômes normaux pour le degré 2^k.

Cette forme de graphe "pyramidale" ne s'applique qu'aux polynômes de degré 2^k. Étendre cette étude aux autres degrés engendre quelques complications mais est tout à fait faisable.

Aussi, il devrait être possible de retrouver ϕ_p (ou tout du moins son graphe) par l'intermédiaire de $\mathcal{K}$, mais nous n'avons pas encore clarifié la situation à ce jour.

Chapitre 8

Graphes des transformations cubiques

Dans ce chapitre, nous donnons les graphes de ψ et de $\psi' = + \circ \psi$ et nous traitons le cas de ψ en nous inspirant du travail du Chapitre 7, mais de manière moins détaillée. Ainsi, nous montrons qu'il est possible d'obtenir le graphe de ψ par l'intermédiaire d'une courbe elliptique, par contre, nous ne donnons pas d'explications quant à la forme du graphe.

Tout d'abord, nous introduisons la courbe $\mathcal{S}$ suivante :

$$\mathcal{S} : Y^2 + Y = X^3.$$

C'est une courbe supersingulière dont $\Omega = (0 : 1 : 0)$ est le seul point à l'infini. On a

$$\mathcal{S}(\mathbb{F}_2) = \{\Omega,\ (0 : 0 : 1),\ (0 : 1 : 1)\},$$

qui est un groupe d'ordre 3.

En utilisant la construction d'isogénie du chapitre précédent sur les points de la courbe $\mathcal{S}$ avec le noyau $F = \mathcal{S}(\mathbb{F}_2)$, on construit une isogénie $\mathfrak{J}$ de degré 3 qui envoie $\mathcal{S}$ sur une autre courbe supersingulière d'équation

$$Y^2 + Y = X^3 + 1.$$

Le lien avec ψ est donné par le théorème suivant :

Théorème 18. *Soient $\mathcal{P} = (x, y)$ un point de $\mathcal{S}$ et $\mathcal{P}' = (x', y')$ son image par la 3-isogénie $\mathfrak{J}$, alors, $P_y | \psi(P_{y'})$.*

Démonstration. D'après les formules de la loi de groupe pour les courbes elliptiques et la construction donnée en 7.2, on trouve que

$$y' = \frac{y^3 + y^2 + 1}{y^2 + y},$$

autrement dit, y est racine de $\psi(P_{y'})$. □

Ainsi, soit Γ le graphe dont les sommets sont les polynômes de $\mathcal{I}$ et où il existe un arc allant du polynôme P' au polynôme P si et seulement s'il existe un point $\mathcal{P} \in \mathcal{S}(\overline{\mathbb{F}_2})$ dont l'ordonnée est racine de P et tel que son image par $\mathfrak{J}$ ait une ordonnée racine de P'. Alors d'après le Théorème 18, Γ est le graphe de ψ.

Voici les graphes de ψ et de ψ' pour les polynômes irréductibles de degré 3 et 9. Les polynômes correspondant aux numéros des graphes se trouvent en Annexe C.2.

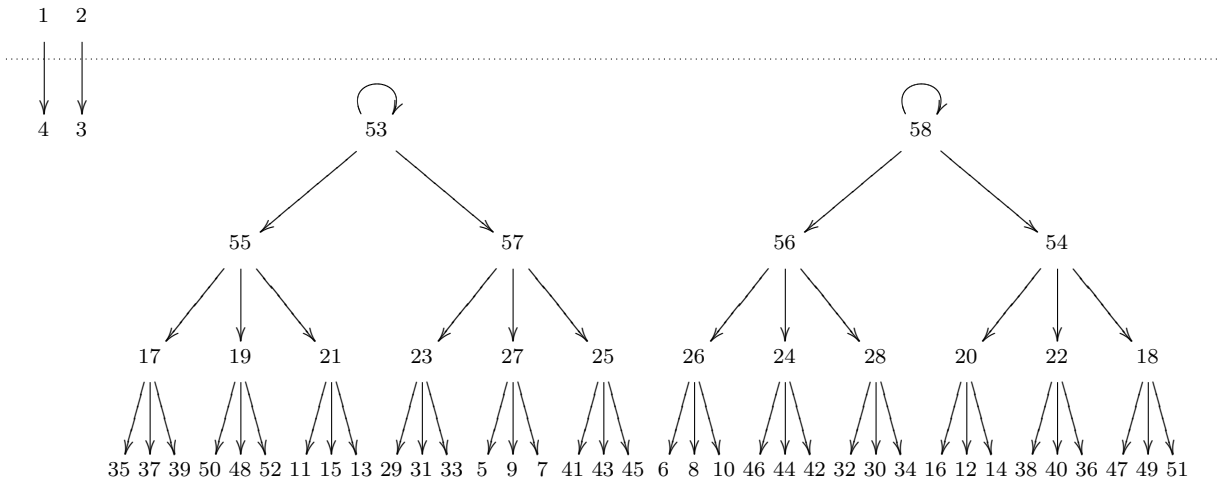


FIG. 8.1 – Graphe de ψ.

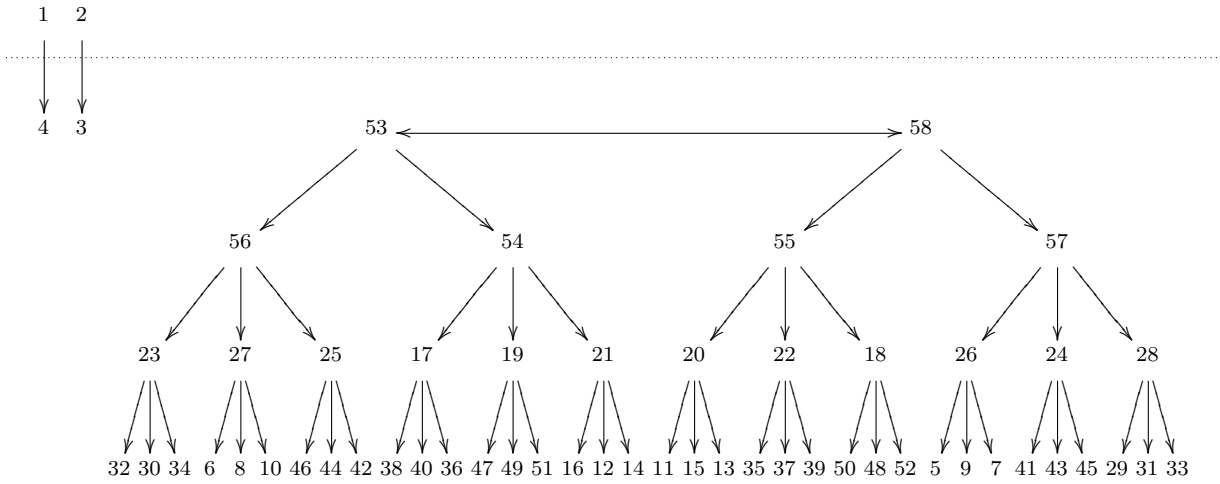


FIG. 8.2 – Graphe de ψ'.

Conclusion

Dans cette thèse nous avons essayé de dégager quelques propriétés élémentaires et quelques conséquences de l'action du groupe $\mathfrak{S}_3$ sur $\mathbb{P}^1(\mathbb{F}_2)$. Ce point de vue peut sembler très particulier mais le lecteur connaisseur de la Théorie des Nombres et de la Géométrie Algébrique fait aisément le lien avec des notions classiques de la façon suivante : les polynômes irréductibles binaires sont les points fermés de la droite affine $\mathbb{A}^1(\mathbb{F}_2)$ (vue comme schéma affine). La transformation $X \to 1/X$ s'interprète sur un schéma non affine qui est $\mathbb{P}^1$. Le groupe G des automorphismes de $\mathbb{P}^1$ est PGL_2.

La formule classique d'énumération des polynômes irréductibles de degré donné dans $\mathbb{F}_q[X]$, pour $\mathbb{F}_q$ un corps fini quelconque, est de démonstration élémentaire. Cette formule est équivalente au fait que la fonction zéta de $\mathbb{A}^1(\mathbb{F}_q)$ est la fonction complexe :

$$\zeta(\mathbb{A}^1(\mathbb{F}_q), s) = \frac{1}{1 - q^{1-s}},$$

où $s \in \mathbb{C} \setminus \{1\}$, qu'on écrit souvent en posant $T = q^{-s}$:

$$Z(\mathbb{A}^1(\mathbb{F}_q), T) = \frac{1}{1 - qT}.$$

Elle peut aussi se traduire sur la droite projective par

$$Z(\mathbb{P}^1(\mathbb{F}_q), T) = \frac{1}{(1 - T)(1 - qT)}.$$

Puisque G (et aussi tous ses sous-groupes) opère naturellement sur $\mathbb{P}^1$ la théorie des fonctions L d'Artin peut s'appliquer [Ser77]. La fonction zéta ci-dessus s'écrit comme un produit fini de fonction L. Chaque fonction L donnera des formules d'énumération de certaines familles de polynômes invariants. Ainsi l'énumération des polynômes réciproques irréductibles fait intervenir les coefficients d'une fonction L appelés sommes de Kloosterman et dans notre cas (sur $\mathbb{F}_2$), il s'avère que cette fonction L est aussi la fonction zéta d'une courbe elliptique (la courbe $\mathcal{K}$ de cette thèse). La transformation ϕ_r reflète alors le calcul de l'unique 2-isogénie sur cette courbe.

L'objectif de ce travail n'était pas de pousser l'explication "abstraite" au maximum car les connaissances mathématiques nécessaires sont trop importantes, mais nous avons

essayé de poser le problème de l'invariance des polynômes irréductibles binaires par $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ et de trouver des réponses très concrètes en nous aidant de l'outil informatique. Il s'avère que quelques résultats nouveaux sont apparus grâce à cette démarche :

- l'existence des fonctions "alternatives" et leur énumération,
- les interprétations des transformations ϕ et ψ en termes de "rang" ou de 2 ou 3-isogénies de certaines courbes elliptiques.

Cependant, même pour le cas binaire, notre tableau n'est pas tout à fait complet. Il reste

- à approfondir le cas du "rang" d'un polynôme irréductible (correspondant à la transformation $X \to X + 1$),
- à décrire les sommes de Kloosterman dans le cas des transformations cubiques.

Aussi, il existe de nombreuses méthodes permettant de construire des polynômes irréductibles, il serait intéressant d'y réfléchir en utilisant nos idées.

Nous espérons que ce travail sera considéré comme une extension significative des travaux antérieurs dans ce domaine.

Annexe A

Inversion de Möbius et caractères de Dirichlet

Pour compléter ce manuscrit, en particulier la démonstration de la Formule 3.2, nous rappelons certains résultats sur l'inversion de Möbius et les caractères de Dirichlet. Pour plus de détails, le lecteur pourra par exemple consulter les livres de Lang [Lan02] et de Lidl et Niederreiter [LN94].

Une **fonction arithmétique** est une fonction $f : \mathbb{N} - \{0\} \to \mathbb{Z}$.

Étant données deux fonctions arithmétiques $f, g : \mathbb{N} - \{0\} \to \mathbb{Z}$, on définit leur **convolution** (de Dirichlet) ainsi :

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}),$$

pour tout entier $n \geq 1$. La convolution est associative, commutative, distributive par rapport à la somme et la fonction arithmétique

$$\delta(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon,} \end{cases}$$

est l'élément neutre de la convolution.

La **fonction identité de Möbius** μ se définit comme suit :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est divisible par } k \text{ nombres premiers distincts,} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

On a alors :

$$\sum_{d|n} \mu(d) = \delta(n),$$

ce qui peut se traduire par

$$1 * \mu = \delta,$$

autrement dit, μ est l'inverse de la fonction constante 1. La **formule d'inversion de Möbius** en est une conséquence immédiate :

$$f = 1 * g \Rightarrow g = f * \mu.$$

On définit le caractère **principal** de Dirichlet modulo n comme suit :

$$\chi_n(a) = \begin{cases} 1 \text{ si } a \equiv 1 \mod n \\ 0 \text{ sinon.} \end{cases}$$

Étant données deux fonctions arithmétiques f et g, on écrit fg la multiplication ordinaire de ces deux fonctions.

Proposition 14. *Pour un nombre premier p et deux fonctions arithmétiques f et g :*

$$(f\chi_p) * (g\chi_p) = (f * g)\chi_p.$$

En particulier, en prenant $f = 1$ et $g = \mu$, on obtient :

Corollaire 7.

$$\chi_p * (\mu\chi_p) = \delta\chi_p = \delta.$$

L'inverse de χ_p pour la convolution est $\mu\chi_p$.

Annexe B

Mise en œuvre

Nous avons écrit de nombreuses fonctions, à l'aide du logiciel mathématique SAGE [Sag], afin de pouvoir tester nos travaux. Voici une partie de ces fonctions, que le lecteur pourra utiliser s'il souhaite travailler sur les différents sujets présentés dans cette thèse.

Nous commençons par déclarer $\mathbb{F}_2$ et l'anneau des polynômes à coefficients dans $\mathbb{F}_2$:

```
F2 = FiniteField(2)
R.<X> = PolynomialRing(F2)
```

Nous définissons les opérations + et * :

```
def star(pol):
  return pol.reverse()

def plus(pol):
  return pol.subs(X=X+1)
```

Ensuite, nous donnons quelques fonctions triviales. Les premières testent le type d'un polynôme :

```
>def is_rec(pol):
  return pol == star(pol)

>def is_med(pol):
  return pol == star(plus(star(pol)))

>def is_per(pol):
  return pol == plus(pol)

>def is_alt(pol):
  return pol == plus(star(pol))
```

Les fonctions suivantes renvoient les polynômes $B_k(X)$, $H_{r,k}(X)$, $H_{m,k}(X)$ et $H_{p,k}(X)$:

```
>def B(k):
  return (X^(2^k+1)+X+1)

>def Hr(k):
  return (X^(2^k+1)+1)

>def Hm(k):
  return (X^(2^k)+X^(2^k-1)+1)

>def Hp(k):
  return (X^(2^k)+X+1)
```

Ensuite, nous donnons une fonction permettant de lister tous les polynômes irréductibles d'un même degré. Cependant, la méthode utilisée ne permet pas de le faire pour de grands degré (k doit être inférieur à 16) :

```
>def Irr(k):
  l = []
  f = (X^(2k-1)+1).factor()
  for e in f:
    if e[0].degree() == k:
      l.append(e[0])
  return l

>for po in Irr(6):
  print po
X^6 + X + 1
X^6 + X^3 + 1
X^6 + X^4 + X^2 + X + 1
X^6 + X^4 + X^3 + X + 1
X^6 + X^5 + 1
X^6 + X^5 + X^2 + X + 1
X^6 + X^5 + X^3 + X^2 + 1
X^6 + X^5 + X^4 + X + 1
X^6 + X^5 + X^4 + X^2 + 1
```

Les deux fonctions ci-dessous génèrent des hexagones. La première renvoie l'hexagone d'un polynôme :

```
>def hexa(pol):
  if not pol.is_irreducible():
```

```
    return []
  else:
    hex = []
    hex.append(pol)
    for i in range(2):
      pol = star(pol)
      if pol not in hex:
        hex.append(pol)
      pol = plus(pol)
      if pol not in hex:
        hex.append(pol)
    pol = star(pol)
    if pol not in hex:
      hex.append(pol)
    return hex

>for po in hexa(X^7+X+1):
  print po
X^7 + X + 1
X^7 + X^6 + 1
X^7 + X^5 + X^3 + X + 1
X^7 + X^6 + X^4 + X^2 + 1
X^7 + X^5 + X^4 + X^3 + X^2 + X + 1
X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1
```

La seconde les génère tous pour un degré donné (cette fois encore, le degré doit être assez petit) :

```
>def hexas(k) :
  l = Irr(k)
  list_hexas = []
  while l != []:
    pol = l[0]
    hex = hexa(pol)
    for po in hex:
      l.pop(l.index(po))
    list_hexas.append(hex)
  return list_hexas

>for h in hexas(6):
  for po in h:
    print po
```

```
  print ''
X^6 + X + 1
X^6 + X^5 + 1
X^6 + X^5 + X^2 + X + 1
X^6 + X^5 + X^4 + X + 1
X^6 + X^5 + X^4 + X^2 + 1
X^6 + X^4 + X^2 + X + 1

X^6 + X^3 + 1
X^6 + X^4 + X^3 + X + 1
X^6 + X^5 + X^3 + X^2 + 1
```

Nous donnons maintenant les fonctions renvoyant le nombre de polynômes irréductibles, d'hexagones de chaque type et de tous les hexagones pour un degré donné :

```
>def irr(k):
  res = 0
  for i in divisors(k):
    res += moebius(k/i)*2^i
  res /= k
  return res

>def h2(k):
  if mod(k,3) != 0 or k<1:
    return 0
  res = 0
  for i in divisors(k/3):
    if mod(i,3) != 0:
      res += moebius(i)*(2^(k/(3*i))-(-1)^(k/(3*i)))
  res /= k
  return res

>def h3(k):
  if mod(k,2) == 1 or k<4:
    return 0
  res = 0
  for i in divisors (k/2):
    if mod(i,2) == 1 :
      res += moebius(i)*2^(k/(2*i))
  res /= k
  return res
```

```
>def h6(k):
  if k<5:
    return 0
  else:
    return (irr(k)-2*h2(k)-3*h3(k))/6

>def hex(k):
  if k < 2:
    return 0
  if k == 2:
    return 1
  he2 = h2(k)
  he3 = h3(k)
  he6 = h6(k)
  return he2+he3+he6

>def decomp_hex(k):
  print 'degré',k,': h2 =',h2(k),', h3 =',h3(k),', h6 =',h6(k),',
hex =',hex(k),'et I =',irr(k)

>decomp_hex(6)
degré 6 : h2 = 0 , h3 = 1 , h6 = 1 , hex = 2 et I = 9

>decomp_hex(18)
degré 18 : h2 = 3 , h3 = 28 , h6 = 2407 , hex = 2438 et I = 14532
```

Ensuite, nous définissons la trace et nos transformations quadratiques :

```
>def tr(pol):
  return pol[pol.degree()-1]

>def phi_r(pol):
  return ((pol.subs(X=X/(X^2+1)))*(X^2+1)^pol.degree()).numerator()

>def phi_m(pol):
  return ((pol.subs(X=(X+1)/X^2))*(X^2)^pol.degree()).numerator()

>def phi_p(pol):
  return pol.subs(X=X^2+X)
```

Et nous illustrons par deux exemples les constructions d'hexagones évoquées dans la Section 4.1.2. Le premier exemple est la construction d'un hexagone dégénéré à 3 éléments à partir d'un polynôme irréductible de trace 1 :

```
>tr(X^7+X^6+1)
1

>phi_r(X^7+X^6+1).factor()
X^14 + X^12 + X^10 + X^7 + X^4 + X^2 + 1

>phi_m(X^7+X^6+1).factor()
X^14 + X^8 + X^7 + X^5 + X^3 + X + 1

>phi_p(X^7+X^6+1).factor()
X^14 + X^13 + X^11 + X^9 + X^7 + X^6 + 1

>for po in hexa(phi_r(X^7+X^6+1)):
  print po
X^14 + X^12 + X^10 + X^7 + X^4 + X^2 + 1
X^14 + X^8 + X^7 + X^5 + X^3 + X + 1
X^14 + X^13 + X^11 + X^9 + X^7 + X^6 + 1
```

Le second illustre la construction d'un hexagone à 6 éléments à partir d'un polynôme irréductible de trace 0 :

```
>tr(X^7+X^4+1)
0

>phi_r(X^7+X^4+1).factor()
(X^7 + X^4 + X^3 + X^2 + 1) * (X^7 + X^5 + X^4 + X^3 + 1)

>phi_m(X^7+X^4+1).factor()
(X^7 + X^6 + X^4 + X + 1) * (X^7 + X^6 + X^5 + X^2 + 1)

>phi_p(X^7+X^4+1).factor()
(X^7 + X^5 + X^2 + X + 1) * (X^7 + X^6 + X^3 + X + 1)

>for po in hexa(X^7+X^4+X^3+X^2+1):
  print po
X^7 + X^4 + X^3 + X^2 + 1
X^7 + X^5 + X^4 + X^3 + 1
X^7 + X^6 + X^4 + X + 1
X^7 + X^6 + X^3 + X + 1
X^7 + X^5 + X^2 + X + 1
X^7 + X^6 + X^5 + X^2 + 1
```

Nous donnons maintenant une fonction qui renvoie la valeur d'un polynôme $pol \in \mathcal{I}$ en ϵ. Si $pol(\epsilon)$ vaut : 0, on renvoie 0, 1, on renvoie 1, ϵ, on renvoie 2 et ϵ^2, on renvoie 3. Nous définissons aussi la transformation ψ :

```
>def eps(pol):
  res = [0,0,0]
  for i in range(pol.degree()+1):
    if pol[i]:
      res[mod(i,3)] += 1
  for i in range(3):
    res[i] = int(mod(res[i],2))
  if res[2]:
    return 3
  if res[1]:
    return 2
  if res[0]:
    return 1
  else:
    return 0

>def psi(pol):
  return ((pol.subs(X=(X^3+X^2+1)/(X^2+X)))*(X^2+X)^pol.degree())
.numerator()
```

Et nous illustrons les constructions présentées dans la Section 4.2.2 par deux exemples. Le premier pour la construction d'un hexagone à 2 éléments à partir d'un polynôme irréductible dont la valeur en ϵ est ϵ ou ϵ^2 :

```
>eps(X^6+X^5+1)
3

>psi(X^6+X^5+1).factor()
X^18 + X^17 + X^16 + X^15 + X^12 + X^11 + X^9 + X^5 + X^4 + X^3 + X^2 +
X + 1

>psi(plus(X^6+X^5+1)).factor()
X^18 + X^17 + X^16 + X^15 + X^14 + X^13 + X^9 + X^7 + X^6 + X^3 + X^2 +
X + 1

>for po in hexa(psi(X^6+X^5+1)):
  print po
X^18 + X^17 + X^16 + X^15 + X^12 + X^11 + X^9 + X^5 + X^4 + X^3 + X^2 +
```

```
X + 1
X^18 + X^17 + X^16 + X^15 + X^14 + X^13 + X^9 + X^7 + X^6 + X^3 + X^2 +
X + 1
```

Le second pour la construction d'un hexagone à 6 éléments à partir d'un irréductible dont la valeur en ϵ est 1 :

```
>eps(X^7+X+1)
1

>psi(X^7+X+1).factor()
(X^7 + X^3 + 1) * (X^7 + X^3 + X^2 + X + 1) * (X^7 + X^6 + X^5 + X^3 +
X^2 + X + 1)

>psi(plus(X^7+X+1)).factor()
(X^7 + X^4 + 1) * (X^7 + X^6 + X^5 + X^4 + 1) * (X^7 + X^6 + X^5 + X^4 +
X^2 + X + 1)

>for po in hexa(X^7+X^3+1):
  print po
X^7 + X^3 + 1
X^7 + X^4 + 1
X^7 + X^6 + X^5 + X^3 + X^2 + X + 1
X^7 + X^6 + X^5 + X^4 + X^2 + X + 1
X^7 + X^3 + X^2 + X + 1
X^7 + X^6 + X^5 + X^4 + 1
```

Nous donnons maintenant les fonctions faisant les transformations inverses. Dans ce cas, nous supposons que le polynôme est invariant et qu'il n'est pas divisible par X ou $X+1$ (ni par X^2+X+1 pour le cas alternatif) :

```
>def inv_phi_r(pol):
  if not is_rec(pol):
    return -1
  res = 0
  num = X
  den = X^2+1
  d = pol.degree()/2
  while pol != 0:
    while den.divides(pol):
      pol = (pol/den).numerator()
      d -= 1
```

```
    res += X^d
    pol += num^d
  return res

>def inv_phi_m(pol):
  if not is_med(pol):
    return -1
  res = 0
  num = X+1
  den = X^2
  d = pol.degree()/2
  while pol != 0:
    while den.divides(pol):
      pol = (pol/den).numerator()
      d -= 1
    res += X^d
    pol += num^d
  return res

>def inv_phi_p(pol):
  if not is_per(pol):
    return -1
  res = 1
  tmp = pol
  while tmp != 1:
    d = tmp.degree()
    res += X^(d/2)
    tmp += (X+X^2)^(d/2)
  return res

>def inv_psi(pol):
  if not is_alt(pol):
    return -1
  res = 0
  num = X^3+X^2+1
  den = X^2+X
  d = pol.degree()/3
  while pol != 0:
    while den.divides(pol):
      pol = (pol/den).numerator()
      d -= 1
```

```
    res += X^d
    pol += num^d
  return res
```

Enfin, nous terminons par les fonctions qui permettent de générer des suites de polynômes irréductibles invariants (pour chaque type d'invariance) et nous illustrons chacune d'entre elles par un exemple. Le paramètre k est la taille de la suite que l'on souhaite. Nous commençons par le cas réciproque :

```
>def seq_r(pol, k):
  if tr(pol) and pol[1] and pol.is_irreducible():
    seq = []
    pol = phi_r(pol)
    seq.append(pol)
    for i in range(k-1):
      pol = phi_r(pol)
      seq.append(pol)
    return seq
  else:
    return -1

>for po in seq_r(X^2+X+1,4):
  print po
X^4 + X^3 + X^2 + X + 1
X^8 + X^7 + X^6 + X^4 + X^2 + X + 1
X^16 + X^15 + X^14 + X^13 + X^12 + X^11 + X^8 + X^5 + X^4 + X^3 + X^2 +
X + 1
X^32 + X^31 + X^30 + X^28 + X^27 + X^26 + X^24 + X^22 + X^17 + X^16 +
X^15 + X^10 + X^8 + X^6 + X^5 + X^4 + X^2 + X + 1
```

Puis, le cas médian :

```
>def seq_m(pol, k):
  if tr(pol) and pol[1] and pol.is_irreducible():
    seq = []
    pol = phi_m(pol)
    seq.append(pol)
    for i in range(k-1):
      pol = phi_m(plus(pol))
      seq.append(pol)
    return seq
  else:
```

```
    return -1

>for po in seq_m(X^2+X+1,4):
  print po
X^4 + X^3 + 1
X^8 + X^7 + X^5 + X^4 + X^3 + X^2 + 1
X^16 + X^15 + X^10 + X^9 + X^7 + X^5 + X^3 + X^2 + 1
X^32 + X^31 + X^29 + X^28 + X^23 + X^22 + X^21 + X^18 + X^17 + X^16 +
X^14 + X^11 + X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1
```

Ensuite, le cas périodique :

```
>def seq_p(pol, k):
  if tr(pol) and pol[1] and pol.is_irreducible():
    seq = []
    pol = phi_p(pol)
    seq.append(pol)
    for i in range(k-1):
      pol = phi_p(plus(star(pol)))
      seq.append(pol)
    return seq
  else:
    return -1

>for po in seq_p(X^2+X+1,4):
  print po
X^4 + X + 1
X^8 + X^6 + X^5 + X^4 + X^3 + X + 1
X^16 + X^14 + X^13 + X^11 + X^9 + X^7 + X^6 + X + 1
X^32 + X^30 + X^29 + X^27 + X^26 + X^24 + X^23 + X^21 + X^18 + X^16 +
X^15 + X^14 + X^11 + X^10 + X^9 + X^4 + X^3 + X + 1
```

Et pour finir, le cas alternatif :

```
>def seq_a(pol, k):
  if eps(pol)>1 and pol.is_irreducible():
    seq = []
    pol = psi(pol)
    seq.append(pol)
    for i in range(k-1):
      pol = psi(pol)
      seq.append(pol)
```

```
    return seq
  else:
    return -1

>for po in seq_a(X^3+X+1,3):
  print po
X^9 + X^8 + 1
X^27 + X^25 + X^24 + X^19 + X^18 + X^16 + X^10 + X^9 + X^3 + X + 1
X^81 + X^80 + X^65 + X^17 + 1
```

Annexe C

Listes indexées de polynômes irréductibles

C.1 Liste des polynômes de degré 2, 4 et 8

La liste suivante est utilisée pour les graphes engendrés par les transformations quadratiques ϕ_r, ϕ_m et ϕ_p, les polynômes sont regroupés par hexagones pour faciliter la lecture des graphes :

```
1  : z^2 + z + 1

2  : z^4 + z + 1
3  : z^4 + z^3 + 1
4  : z^4 + z^3 + z^2 + z + 1

5  : z^8 + z^4 + z^3 + z + 1
6  : z^8 + z^7 + z^5 + z^4 + 1
7  : z^8 + z^7 + z^6 + z^4 + z^3 + z^2 + 1
8  : z^8 + z^6 + z^5 + z^4 + z^2 + z + 1
9  : z^8 + z^6 + z^5 + z^4 + 1
10 : z^8 + z^4 + z^3 + z^2 + 1

11 : z^8 + z^5 + z^3 + z + 1
12 : z^8 + z^7 + z^5 + z^3 + 1
13 : z^8 + z^7 + z^6 + z + 1
14 : z^8 + z^7 + z^2 + z + 1
15 : z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + 1
16 : z^8 + z^5 + z^4 + z^3 + z^2 + z + 1
```

```
17 : z^8 + z^5 + z^3 + z^2 + 1
18 : z^8 + z^6 + z^5 + z^3 + 1
19 : z^8 + z^5 + z^4 + z^3 + 1

20 : z^8 + z^6 + z^3 + z^2 + 1
21 : z^8 + z^6 + z^5 + z^2 + 1
22 : z^8 + z^6 + z^5 + z + 1
23 : z^8 + z^7 + z^3 + z^2 + 1
24 : z^8 + z^7 + z^6 + z^5 + z^4 + z^2 + 1
25 : z^8 + z^6 + z^4 + z^3 + z^2 + z + 1

26 : z^8 + z^6 + z^5 + z^4 + z^3 + z + 1
27 : z^8 + z^7 + z^5 + z^4 + z^3 + z^2 + 1
28 : z^8 + z^7 + z^6 + z^4 + z^2 + z + 1

29 : z^8 + z^7 + z^3 + z + 1
30 : z^8 + z^7 + z^5 + z + 1
31 : z^8 + z^7 + z^6 + z^3 + z^2 + z + 1
32 : z^8 + z^7 + z^6 + z^5 + z^2 + z + 1
33 : z^8 + z^7 + z^4 + z^3 + z^2 + z + 1
34 : z^8 + z^7 + z^6 + z^5 + z^4 + z + 1
```

C.2 Liste des polynômes de degré 3 et 9

La liste suivante est utilisée pour les graphes engendrés par les transformations cubiques ψ et $\psi' = + \circ \psi$, là encore, les polynômes sont regroupés par hexagones :

```
1  : z^3 + z + 1
2  : z^3 + z^2 + 1

3  : z^9 + z + 1
4  : z^9 + z^8 + 1

5  : z^9 + z^4 + 1
6  : z^9 + z^5 + 1
7  : z^9 + z^8 + z^5 + z^4 + 1
8  : z^9 + z^5 + z^4 + z + 1
9  : z^9 + z^8 + z^5 + z + 1
10 : z^9 + z^8 + z^4 + z + 1
```

```
11 : z^9 + z^4 + z^2 + z + 1
12 : z^9 + z^8 + z^7 + z^5 + 1
13 : z^9 + z^7 + z^6 + z^3 + z^2 + z + 1
14 : z^9 + z^8 + z^7 + z^6 + z^3 + z^2 + 1
15 : z^9 + z^7 + z^5 + z + 1
16 : z^9 + z^8 + z^4 + z^2 + 1

17 : z^9 + z^4 + z^3 + z + 1
18 : z^9 + z^8 + z^6 + z^5 + 1
19 : z^9 + z^6 + z^5 + z^2 + 1
20 : z^9 + z^7 + z^4 + z^3 + 1
21 : z^9 + z^8 + z^7 + z^6 + z^5 + z + 1
22 : z^9 + z^8 + z^4 + z^3 + z^2 + z + 1

23 : z^9 + z^5 + z^3 + z^2 + 1
24 : z^9 + z^7 + z^6 + z^4 + 1
25 : z^9 + z^8 + z^7 + z^5 + z^4 + z^3 + 1
26 : z^9 + z^6 + z^5 + z^4 + z^2 + z + 1
27 : z^9 + z^8 + z^6 + z^5 + z^4 + z + 1
28 : z^9 + z^8 + z^5 + z^4 + z^3 + z + 1

29 : z^9 + z^6 + z^3 + z + 1
30 : z^9 + z^8 + z^6 + z^3 + 1
31 : z^9 + z^6 + z^4 + z^3 + 1
32 : z^9 + z^6 + z^5 + z^3 + 1
33 : z^9 + z^8 + z^6 + z^5 + z^3 + z + 1
34 : z^9 + z^8 + z^6 + z^4 + z^3 + z + 1

35 : z^9 + z^6 + z^4 + z^3 + z^2 + z + 1
36 : z^9 + z^8 + z^7 + z^6 + z^5 + z^3 + 1
37 : z^9 + z^7 + z^4 + z^2 + 1
38 : z^9 + z^7 + z^5 + z^2 + 1
39 : z^9 + z^8 + z^7 + z^6 + z^3 + z + 1
40 : z^9 + z^8 + z^6 + z^3 + z^2 + z + 1

41 : z^9 + z^6 + z^5 + z^3 + z^2 + z + 1
42 : z^9 + z^8 + z^7 + z^6 + z^4 + z^3 + 1
43 : z^9 + z^7 + z^5 + z^4 + z^2 + z + 1
44 : z^9 + z^8 + z^7 + z^5 + z^4 + z^2 + 1
45 : z^9 + z^7 + z^6 + z^4 + z^3 + z + 1
46 : z^9 + z^8 + z^6 + z^5 + z^3 + z^2 + 1
```

```
47 : z^9 + z^6 + z^5 + z^4 + z^3 + z^2 + 1
48 : z^9 + z^7 + z^6 + z^5 + z^4 + z^3 + 1
49 : z^9 + z^8 + z^7 + z^2 + 1
50 : z^9 + z^7 + z^2 + z + 1
51 : z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z + 1
52 : z^9 + z^8 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1

53 : z^9 + z^7 + z^5 + z^3 + z^2 + z + 1
54 : z^9 + z^8 + z^7 + z^6 + z^4 + z^2 + 1
55 : z^9 + z^7 + z^5 + z^4 + z^3 + z^2 + 1
56 : z^9 + z^7 + z^6 + z^5 + z^4 + z^2 + 1
57 : z^9 + z^8 + z^7 + z^3 + z^2 + z + 1
58 : z^9 + z^8 + z^7 + z^6 + z^2 + z + 1
```

Bibliographie

[BS89] J. V. Brawley et G. E. Schnibben : *Infinite Algebraic Extensions of Finite Fields*, volume 95 de *Contemporary Mathematics*. Amer. Math. Soc., 1989.

[Car67] L. Carlitz : Some theorems on irreducible reciprocal polynomials over a finite field. *J. Reine Angew. Math.*, 227:212–220, 1967.

[Coh92] S. D. Cohen : The explicit construction of irreducible polynomials over finite fields. *Designs, Codes and Cryptography*, 2:169–174, 1992.

[Coh03] P. M. Cohn : *Basic Algebra, Groups, Rings and Fields*. Springer Verlag, 2003.

[Gau63] C. F. Gauss : *Disquisitiones generales de congruentiis. Werke II*. 1863. (pour cette référence, nous remercions http ://gdz.sub.uni-goettingen.de/en/gdz/).

[HMV04] D. Hankerson, A. Menezes et S. Vanstone : *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[Kyu02] M. K. Kyuregyan : Recurrent methods for constructing irreducible polynomials over GF(2^s). *Finite Fields and Their Applications*, 8:52–68, 2002.

[Kyu04] M. K. Kyuregyan : Iterated constructions of irreducible polynomials over finite fields with linearly independent roots. *Finite Fields and Their Applications*, 10:323–341, 2004.

[Lan02] S. Lang : *Algebra*, volume 211 de *Graduate Text in Mathematics*. Springer Verlag, 2002.

[LN94] R. Lidl et H. Niederreiter : *Introduction to finite fields and their applications*. Cambridge University Press, revised edition, 1994.

[McL81] T. J. McLarnan : The numbers of polytypes in close-packings and related structures. *Zeitschr. f. Kristall.*, 155:269–291, 1981.

[Mey90] H. Meyn : On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Eng. Comm. Comp.*, 1:43–53, 1990.

[MG90] H. Meyn et W. Götz : Self-reciprocal polynomials over finite fields. *Publ. I.R.M.A. Strasbourg*, 413/S-21:82–90, 1990.

[MR10a] J.-F. Michon et P. Ravache : On different families of invariant irreducible polynomials over GF(2). *Finite Fields and Their Applications*, 16(3):163–174, 2010.

[MR10b] J.-F. Michon et P. Ravache : Transformations on irreducible binary polynomials. *Lecture Notes in Computer Science, proceedings de SETA2010*, 2010.

[Nie90] H. Niederreiter : An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field. *Appl. Algebra Eng. Comm. Comp.*, 1:119–124, 1990.

[Ore34] O. Ore : Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.*, pages 243–274, 1934.

[Sag] Sage : Open source mathematics software. http://www.sagemath.org.

[Ser77] J.-P. Serre : Majoration de sommes exponentielles. *Journées arithmétiques de Caen, Astérisque 41-42*, pages 111–126, 1977.

[Sil86] J. H. Silverman : *The Arithmetic of Elliptic Curves*, volume 106 de *Graduate Text in Mathematics*. Springer Verlag, 1986.

[Slo] N. J. A. Sloane : The on-line encyclopedia of integer sequences. http://www.research.att.com/~njas/sequences.

[Ste10] E. Steinitz : Algebraische Theorie der Körper. *J. Reine Angew. Math.*, 137:167–309, 1910.

[Var84] R. R. Varshamov : A general method of synthesis for irreducible polynomials over galois fields. *Soviet Math. Dokl.*, 29:334–336, 1984.

[Vél71] J. Vélu : Isogénies entre courbes elliptiques. *Comptes rendus de l'Académie des Sciences de Paris, Série A*, 273:238–241, 1971.

[Was08] L. C. Washington : *Elliptic Curves, Number Theory and Cryptography*. Chapman and Hall/CRC, Second Edition, 2008.

[Wie88] D. Wiedemann : An iterated quadratic extension of GF(2). *Fibonacci Quart.*, 26:290–295, 1988.

Automorphismes projectifs et polynômes binaires irréductibles

Cette thèse porte sur l'étude de certaines propriétés structurelles de l'ensemble des polynômes irréductibles à coefficients dans $\mathbb{F}_2$. La première partie classifie ces polynômes par rapport à l'action du groupe des automorphismes de la droite projective $\mathbb{P}^1(\mathbb{F}_2)$, à savoir $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$. Nous obtenons quatre familles de polynômes invariants par l'action des quatre sous-groupes non triviaux de $\mathfrak{S}_3$, ce qui généralise la notion de polynôme réciproque. De plus, nous donnons une formule de dénombrement qui complète celle de Carlitz (qui a traité le cas réciproque). Dans la seconde partie, nous donnons des transformations permettant de générer nos polynômes invariants ainsi que le théorème général décrivant leur action précise sur les polynômes irréductibles. Cela donne deux partitions différentes par des relations simples sur leurs coefficients. Nous proposons également des moyens de construire des suites infinies explicites d'irréductibles invariants en généralisant ce qui existait pour les réciproques. Dans la troisième partie, nous étudions plus en détail nos transformations. En particulier, nous retrouvons deux d'entre elles au travers d'opérations sur les points de deux courbes elliptiques.

Mots clés : polynômes irréductibles, polynômes invariants, polynômes réciproques, corps finis, courbes elliptiques, isogénies, caractéristique 2.

Projective automorphisms and irreducible binary polynomials

This Ph.D. is a study of some structural properties of the set of irreducible polynomials with coefficients in $\mathbb{F}_2$. The first part classify these polynomials under the action of the automorphisms group of the projective line $\mathbb{P}^1(\mathbb{F}_2)$, i.e. $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$. We obtain four families of invariant polynomials under each non trivial subgroup of $\mathfrak{S}_3$, which generalize the notion of self-reciprocal polynomials. Moreover, we give an enumeration formula that completes Carlitz' one (which concerns the self-reciprocal polynomials). In the second part, we give transformations that generate our invariant polynomials and the general theorem describing their action on the irreducible polynomials. That gives two different partitions by easy relations on their coefficients. We also propose ways to construct infinite sequences of irreducible invariant polynomials, generalizing what was known for self-reciprocal polynomials. In the third part, we study more deeply our transformations. In particular, we show that we can find two of them through operations on the points of two elliptic curves.

Keywords : irreducible polynomials, invariant polynomials, self-reciprocal polynomials, finite fields, elliptic curves, isogenies, characteristic 2.