Algèbres Quadratiques

Résumé

Les résultats présentés dans ce document concerne le nombre et le type des algèbres quadratiques définies sur un corps commutatif.
Bien que similaires, les théorèmes principaux pour les corps de caractéristique 2 et les autres (y compris 0) sont différents.

1 Introduction

1.1 L'espace vectoriel $\mathbb{K}^2$

Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif, il est facile de munir $\mathbb{K}^2$ d'une structure d'espace vectoriel (c'est la méthode usuelle, les démonstrations se trouvent partout) de dimension 2 (sur $\mathbb{K}$) en définissant une addition interne notée $+$ et une multiplication externe notée aussi $\cdot$ (voire omise) et définies par

$$\begin{array}{ccccc} (x,y) & + & (x',y') & = & (x+x', y+y') \\ \lambda & \cdot & (x,y) & = & (\lambda \cdot x, \lambda \cdot y) \end{array}$$

La base canonique de cet espace vectoriel est, évidemment, $\{(1,0),(0,1)\}$ et donc tout élément de $\mathbb{K}^2$ s'écrit naturellement :

$$(x,y) = x \cdot (1,0) + y \cdot (0,1)$$

Par la suite nous oublierons, quand ce n'est pas toxique, le signe $\cdot$ pour la multiplication externe, par exemple :

$$(x,y) = x(1,0) + y(0,1)$$

1.2 Algèbre sur un corps

1.2.1 Généralités

Une algèbre sur un corps commutatif est un espace vectoriel sur ce corps, sur lequel on définit en plus une multiplication interne (partout définie), notée $\times$ ci-dessous, qui soit bilinéaire.

Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif, $(\mathcal{A}, +, \cdot, \times)$ est une algèbre sur $\mathbb{K}$ (ou $\mathbb{K}$-algèbre), si :

- $(\mathcal{A}, +, \cdot)$ est un espace vectoriel sur $\mathbb{K}$
- $\times : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ est une application
- $\forall (x,y,z) \in \mathcal{A}^3 \ ((x+y) \times z = (x \times z) + (y \times z))$
- $\forall (x,y,z) \in \mathcal{A}^3 \ (x \times (y+z) = (x \times y) + (x \times z))$
- $\forall (x,y) \in \mathcal{A}^2 \ \forall (\alpha, \beta) \in \mathbb{K}^2 \ ((\alpha \cdot x) \times (\beta \cdot y) = (\alpha \cdot \beta) \cdot (x \times y))$

1.2.2 L'algèbre $\mathbb{K}^2$

Les algèbres de dimension 2 sur $\mathbb{K}$ sont des cas particuliers d'hypercomplexes de la forme $\mathbb{K} \oplus \mathbb{K}$ en tant qu'espace vectoriel.

Il y a deux façons naturelles de représenter un élément de $\mathbb{K} \oplus \mathbb{K}$:

- Un couple : $z = (x_0, x_1)$, où $(x_0, x_1) \in \mathbb{K}^2$
- Une combinaison linéaire d'éléments d'une base de l'espace vectoriel $\mathbb{K} \oplus \mathbb{K}$: $z = x_0 \cdot e_0 + x_1 \cdot e_1$

Les deux représentations sont parfaitement interchangeables grace à l'identification :
$(1, 0) = e_0$ et $(0, 1) = e_1$.

Il est d'usage d'identifier $\mathbb{K}$ avec la première composante de $\mathbb{K}^2$ ($(\mathbb{K}, +, \cdot, \times) \hookrightarrow (\mathbb{K}^2, +, \cdot, \times)$), c'est à dire que si $x \in \mathbb{K}$, on identifie x et $(x, 0)$, et comme $(x, 0) = x \cdot (1, 0)$, on identifie aussi x et $x \cdot e_0$, et en particulier 1 et e_0 (ou encore, on identifie $1_{\mathbb{K}}$ et $1_{\mathbb{K}^2}$), de ce fait, la méthode la plus pratique pour représenter un élément de $\mathbb{K}^2$ est $z = x_0 + x_1 \cdot e_1$, et même $z = x_0 + e x_1$ (sur le modèle des nombres complexes). C'est cette représentation que nous utiliserons par la suite.

Pour définir complètement la structure d'algèbre sur $\mathbb{K}^2$, il reste à définir la multiplication de deux éléments, et grace aux propriétés de la multiplication, il suffit de définir la multiplication sur les éléments d'une base, comme, de plus, 1 est l'élément neutre de cette multiplication (les algèbres quadratiques sont unitaires), nous avons forcément $1 \cdot 1 = 1$ et $1 \cdot e = e \cdot 1 = e$, il ne reste plus qu'à définir $e \cdot e$ ce que nous pouvons résumer par la table de multiplication :

$\cdot$	1	e
1	1	e
1	e	$a + eb$

$(\mathbb{K}^2)_{a,b}$

Nous noterons $\mathbb{K}^2_{(a,b)}$ pour l'algèbre $\mathbb{K}^2$ munie de la multiplication précédente.

Les algèbres quadratiques sur un corps commutatif sont distributives et commutatives (les démonstrations sont triviales).

2 Algèbres quadratiques

2.1 Corps de caractéristique différente de 2

Soit $\overset{2}{\simeq}$ la relation définie sur $\mathbb{K}$ par : $(x \overset{2}{\simeq} y) \Longleftrightarrow \exists k((k \neq 0) \wedge (x = k^2 y))$.

La relation $\overset{2}{\simeq}$ est trivialement une relation d'équivalence. La classe d'un élément x sera notée $\overline{x}$, en particulier la classe de 1 est constituée des carrés (de $\mathbb{K}$)

Une question naturelle consiste à se demander à quelle(s) condition(s) sur a, b et δ il existe un isomorphisme φ entre $\mathbb{K}^2_{(a,b)}$ et $\mathbb{K}^2_{(\delta,0)}$.

Par définition d'un isomorphisme d'algèbre, φ vérifie les propriété suivantes (nous noterons f le deuxième élément de la base de $\mathbb{K}^2_{(\delta,0)}$, et donc $f^2 = \delta$) :

1. $\varphi(1) = 1$
2. $\varphi(a + eb) = a + b \cdot \varphi(e)$
3. $\varphi(e^2) = (\varphi(e))^2$
4. $\exists \alpha \in \mathbb{R}\ \exists \beta \in \mathbb{R}^*\ (\varphi(e) = \alpha + f\beta)$

β doit être différent de 0 sinon φ ne serait pas une bijection.

On a donc :

$\varphi(e^2) = \varphi(a + eb) = a + b \cdot \varphi(e) = a + b(\alpha + f\beta) = a + b\alpha + fb\beta$
$(\varphi(e))^2 = (\alpha + f\beta)^2 = \alpha^2 + \delta\beta^2 + 2f\alpha\beta$

Nous devons donc résoudre $a + b\alpha + fb\beta = \alpha^2 + \delta\beta^2 + 2f\alpha\beta$, ce qui est équivalent au système (a et b sont des paramètres réels et α et β les inconnues réelles) :

$$\begin{cases} a + b\alpha & = & \alpha^2 + \delta\beta^2 \\ b\beta & = & 2\alpha\beta \\ \beta & \neq & 0 \end{cases}$$

Or $\beta \neq 0$, nous obtenons donc le système $\begin{cases} a + b\alpha & = & \alpha^2 + \delta\beta^2 \\ b & = & 2\alpha \\ \beta & \neq & 0 \end{cases}$

Si $\mathbb{K}$ est de caractéristique différente de 2 (le cas de $\mathbb{F}_{2^p}$ sera vu spécifiquement), et après quelque calculs élémentaires le système devient

$$\begin{cases} 4a + b^2 & = & 4\delta\beta^2 \\ \frac{b}{2} & = & \alpha \\ \beta & \neq & 0 \end{cases} \tag{1}$$

Système qui a des solutions sous une seule condition : $4a + b^2 \overset{2}{\simeq} \delta$, le nombre d'algèbres quadratiques sur $\mathbb{K}$ non isomorphe est donc égal au nombre de classe de $\overset{2}{\simeq}$ sur $\mathbb{K}$.

Théorème

Dans tous les cas, en caractéristique différente de 2, $\mathbb{K}^2_{(a,b)} = \mathbb{K}^2_{(4a+b^2,0)}$ et ne dépend que de $\overline{4a + b^2}$.

Pour tous les corps, $\overset{2}{\simeq}$ possède toujours au moins deux classes, celle de 0 et celle de 1 (qui contient tous les carrés de $\mathbb{K}$.)

$\mathbb{K}^2_{(0,0)}$ contient toujours des élément nil-carrés (les éléments de la forme ey par exemple).

$\mathbb{K}^2_{(1,0)}$ contient toujours des diviseurs de zéro : $(1+e)(1-e) = 1-e^2 = 0$

$\mathbb{K}^2_{(1,0)}$ ne contient pas d'élément nil-carré non trivial : $(x+ey)^2 = x^2+y^2+2exy = 0$, équation équivalente à $\begin{cases} x^2+y^2 &= 0 \\ 2xy &= 0 \end{cases}$ qui n'a pas de solution différente de $x = y = 0$.

Par la suite nous appelerons « Algèbre Duale » les algèbres contenant des nil-carrés, et « Algèbre Fendue » les algèbres contenant des diviseurs de zéro mais pas de nil-carrés

Si $\mathbb{K}$ possède d'autres classes, soit $k \neq 0$ et $k \notin \overline{1}$, autrement dit k n'est pas un carré alors tous les élements de $\mathbb{K}^2_{(k,0)}$ ont un inverse et donc $\mathbb{K}^2_{(k,0)}$ est un corps :

$\alpha^2 - k\beta^2 \neq 0$, sinon k serait un carré et donc $(\alpha+e\beta)(\alpha-e\beta)(\alpha^2-k\beta^2)^{-1} = 1$

2.1.1 $\mathbb{K} = \mathbb{R}$

Sur $\mathbb{R}$, la relation $\overset{2}{\simeq}$ possède 3 classes : $\mathbb{R}/\underset{\sim}{2} = \{\overline{-1}, \overline{0}, \overline{1}\}$

Ces trois classes correspondent respectivement à $\mathbb{C}$, $\mathbb{D}_1$ et $\mathbb{C}$:

$\cdot$	1	e
1	1	e
e	e	-1

Complexe : $\mathbb{C}$

$\cdot$	1	e
1	1	e
e	e	0

Dual complexe : $\mathbb{D}_1$

$\cdot$	1	e
1	1	e
e	e	1

Complexe fendu : $\mathbb{C}$

Ces trois structures ne sont pas isomorphes 2 à 2 :

▷ $(\mathbb{C}, +, \cdot)$ est un corps

▷ $(\mathbb{D}_1, +, \cdot)$ contient des éléments non nuls vérifiant $x^2 = 0$ (par exemple e)

▷ $(\mathbb{C}, +, \cdot)$ contient des diviseurs de zéro (par exemple $(1-e)\cdot(1+e) = 0$), mais pas d'éléments non nuls vérifiant $x^2 = 0$

Il est d'usage de noter $e = i$ dans le cas $\mathbb{C}$, $e = \varepsilon$ dans le cas $\mathbb{D}_1$ et $e = j$ dans le cas $\mathbb{C}$.

Résumé : 3 cas possibles

☞ Un corps : $\mathbb{C}$

☞ Une algèbre contenant des nil-carrés : $\mathbb{D}_1$

☞ Une algèbre contenant des diviseurs de 0, mais pas de nil-carrés : $\mathbb{C}$

2.1.2 $\mathbb{K} = \mathbb{Q}$

La relation $\overset{2}{\simeq}$ posséde $\aleph_0$ classes (tous les nombres premiers sont dans des classes différentes), toutes de cardinal $\aleph_0$, sauf la classe de 0 qui est réduite à $\{0\}$.

Résumé : $\aleph_0$ cas possibles

☞ Une algèbre contenant des nil-carrés.

☞ Une algèbre contenant des diviseurs de 0, mais pas de nil-carrés.

☞ $\aleph_0$ corps non isomorphes.

2.1.3 $\mathbb{K} = \mathbb{C}$

La relation $\overset{2}{\simeq}$ posséde 2 classes (c'est le cas de tous les corps algèbriquement clos), sur $\mathbb{C}$: $\mathbb{C}/\underset{\sim}{2} = \{\overline{0}, \overline{1}\}$, qui correspondent respectivement aux Complexes duaux et aux BiComplexes

En particulier, on voit que le corps des Quaternions n'est pas une $\mathbb{C}$-algèbre.

Résumé : 2 cas possibles

- ☞ Complexes duaux $\mathbb{D}_2$
- ☞ BiComplexes $\mathbb{C}_2$

2.1.4 Corps finis $\mathbb{K} = \mathbb{F}_{p^n}$ pour p premier, $p > 2$, $n > 0$

Un nombre premier strictement plus grand que 2 est impair.

Dans tous les corps $\mathbb{F}_{p^n}$ avec $p > 2$, et $n > 0$, -1 est différent de 1, et donc

$$\forall x \in \mathbb{F}_{p^n}((x \neq 0) \Longrightarrow ((x \neq -x) \wedge (x^2 = (-x)^2)))$$

il y a donc exactement $\dfrac{p^n - 1}{2}$ éléments non nuls qui sont des carrés (dont 1), et donc $\dfrac{p^n - 1}{2}$ qui ne sont pas des carrés.

Soit x un élément non carré de $\mathbb{F}_{p^n}$ alors l'ensemble $\{k^2 x | k \in \mathbb{F}_{p^n}\}$ possède $\dfrac{p^n - 1}{2}$ éléments dont aucun n'est un carré, c'est donc exactement l'ensemble des non carrés, qui par conséquent sont tous équivalents pour $\overset{2}{\simeq}$

Dans la suite k désigne un élément de $\mathbb{F}_{p^n}$ qui n'est pas un carré.

Dans le corps $\mathbb{F}_{p^n}$, pour $p > 2$, et $n > 0$, la relation $\overset{2}{\simeq}$ possède 3 classes : $\mathbb{F}_{p^n}/\underset{\sim}{2} = \{\overline{k}, \overline{0}, \overline{1}\}$

Résumé : 3 cas possibles

- ☞ Un corps : $\mathbb{F}_{p^{2n}}$.
- ☞ Une algèbre contenant des nil-carrés.
- ☞ Une algèbre contenant des diviseurs de 0, mais pas de nil-carrés.

On peut noter que :

- $|\overline{0}| = 1$
- $|\overline{1}| = \frac{p^n - 1}{2}$
- $|\overline{k}| = \frac{p^n - 1}{2}$

2.1.4.1 Comptages

2.1.4.1.1 Nombres de copies

En repartant de l'équation (1) et du résultat : $\mathbb{K}^2_{(a,b)} = \mathbb{K}^2_{(4a+b^2,0)}$ et ne dépend que de $\overline{4a+b^2}$.

Cas $\overline{0}$

Pour chacune des p^n valeurs de b, il existe une et une seule valeur de a telle que $4a+b^2=0$: $a=-b^2 4^{-1}$, il y a donc p^n possibilités pour construire une algèbre duale isomorphe à $\mathbb{F}^2_{p^n,(0,0)}$

Cas $\overline{1}$

Pour chacune des p^n valeurs de b, et chacun des $\frac{p^n-1}{2}$ carrés ($\lambda \neq 0$) il existe une et une seule valeur de de a telle que $4a+b^2=\lambda$, il y a donc $\frac{p^n(p^n-1)}{2}$ possibilités pour construire une algèbre fendue isomorphe à $\mathbb{F}^2_{p^n,(1,0)}$

Cas $\overline{k}$

Pour chacune des p^n valeurs de b, et chacun des $\frac{p^n-1}{2}$ valeurs qui ne sont pas des carrés (λ) il existe une et une seule valeur de a telle que $4a+b^2=\lambda$, il y a donc $\frac{p^n(p^n-1)}{2}$ possibilités pour construire un corps isomorphe à $\mathbb{F}^2_{p^n,(k,0)}$

2.1.4.1.2 Nombres d'inversibles

Un élément inversible est un élément x (forcément $x \neq 0$) tel qu'il existe un élément y (forcément $y \neq 0$) vérifiant $xy=1$. Dans les corps c'est le cas de tous les éléments non nuls.

Dans $\mathbb{F}^2_{p^n,(\delta,0)}$, cela s'écrit $(x+ey)(x'+ey')=1=xx'+e^2yy'+e(xy'+x'y)$

Ce qui mène à :

$$\begin{cases} xx'+\delta yy' & = & 1 \\ xy'+x'y' & = & 0 \\ x\neq 0 & \vee & y\neq 0 \\ x'\neq 0 & \vee & y'\neq 0 \end{cases} \tag{2}$$

Cas $\delta = 0$:

Le système (2) devient

$$\begin{cases} xx' & = & 1 \\ x'y+xy' & = & 0 \\ x\neq 0 & \vee & y\neq 0 \\ x'\neq 0 & \vee & y'\neq 0 \end{cases}$$

On doit donc avoir $x \neq 0$ d'où

$$\begin{cases} xx' & = & 1 \\ y+x^2y' & = & 0 \\ x\neq 0 & \vee & y\neq 0 \\ x'\neq 0 & \vee & y'\neq 0 \end{cases}$$

Pour chacune des p^n-1 valeur de $x \neq 0$ et chacune des p^n valeurs de y, on peut prendre : $(x'=x^{-1}) \wedge (y'=-yx^{-2})$, il y a donc $p^n(p^n-1)$ éléments inversibles.

Cas $\delta = 1$:

Le système (2) devient

$$\begin{cases} xx' + yy' & = & 1 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Vu comme un système à deux inconnus (x' et y') et deux paramètres (x et y), il faut et il suffit, pour qu'il ait des solutions, que $x^2 - y^2 \neq 0$, soit

1. $x = 0$: chacune des $p^n - 1$ valeurs non nulles de y convient
2. $x \neq 0$: pour chacune des $p^n - 1$ valeurs de x, chacune des $p^n - 2$ valeurs de y différentes de x et -x convient

Soit un total de $(p^n - 1) + (p^n - 1)(p^n - 2) = (p^n - 1)^2$ solutions.

Cas $\delta = k$:
Dans le cas d'un corps tous les éléments non nuls sont inversibles :
Le système (2) devient

$$\begin{cases} xx' + kyy' & = & 1 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Vu comme un système à deux inconnus (x' et y') et deux paramètres (x et y), il faut et il suffit, pour qu'il ait des solutions, que $x^2 - ky^2 \neq 0$, ce qui est toujours le cas (sinon k serait un carré), sauf si $x = y = 0$, ce qui donne bien $p^{2n} - 1$ éléments inversibles.

$\delta = 0$	Algèbre duale	$p^n(p^n - 1)$ solutions
$\delta = 1$	Algèbre fendue	$(p^n - 1)^2$ solutions
$\delta = k$	Corps	$p^{2n} - 1$ solutions, comme dans tous les corps

2.1.4.1.3 Nombres de diviseurs de zéro

Un élément diviseur de zéro est un élément $x \neq 0$ tel qu'il existe un élément $y \neq 0$ vérifiant $xy = 0$. Dans les corps il n'y en a pas.
Dans $\mathbb{F}^2_{p^n,(\delta,0)}$, cela s'écrit $(x + ey)(x' + ey') = 0 = xx' + e^2yy' + e(xy' + x'y)$

Ce qui mène à :

$$\begin{cases} xx' + \delta yy' & = & 0 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases} \tag{3}$$

Cas $\delta = 0$:

Si $x \neq 0$ le système (3) devient

$$\begin{cases} x' & = & 0 \\ y' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

sytème n'ayant aucune solution.

Si $x = 0$ le système (3) devient

$$\begin{cases} x & = & 0 \\ x'y & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

système dont les solutions sont $x = x' = 0$, soit les éléments de la forme ey pour chacune des $p^n - 1$ valeurs non nulles de y.

Cas $\delta = 1$
Le système (3) devient

$$\begin{cases} xx' + yy' & = & 0 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Ce qui revient à trouver les valeurs de x et de y pour lesquels le système précédent a des solutions non nulles pour x' et y' autrement dit, il faut et il suffit que $x^2 - y^2 = 0$; pour chacune des valeurs non nulles de x, y peut prendre les deux valeurs x et $-x$ ce qui donne $2(p^n - 1)$

Cas $\delta = k$
Comme nous sommes dans le cas d'un corps il n'y a pas de diviseur de zéro, faisons les calculs néanmoins :
le système (3) devient

$$\begin{cases} xx' + kyy' & = & 0 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Ce qui revient à trouver les valeurs de x et de y pour lesquels le système précédent a des solutions non nulles pour x' et y' autrement dit, il faut et il suffit que $x^2 - ky^2 = 0$, ce qui est impossible, sinon k serait un carré.

$\delta = 0$	Algèbre duale	$(p^n - 1)$ solutions
$\delta = 1$	Algèbre fendue	$2(p^n - 1)$ solutions
$\delta = k$	Corps	0 solution, comme dans tous les corps

2.1.4.1.4 Nombres d'éléments d'ordre 2

Un élément d'ordre 2 est un élément tel que $x^2 = 1$, il y a donc toujours 1 (et -1 s'il est différent de 1).

Dans $\mathbb{F}^2_{n,(\delta,0)}$, cela s'écrit $(x + ey)^2 = 1 = x^2 + e^2y^2 + 2exy$

Ce qui mène à :

$$\begin{cases} x^2 + \delta y^2 & = & 1 \\ 2xy & = & 0 \end{cases} \tag{4}$$

Si $y = 0$ on obtient $x^2 = 1$ dont les seules solution sont 1 et -1 (qui est différent de 1, puisque $p > 2$).

Si $y \neq 0$, alors $x = 0$ et l'équation (4) devient

$$\begin{cases} \delta y^2 &= 1 \\ x &= 0 \end{cases}$$

Si $\delta \in \{0, k\}$, il n'y a pas de solution en plus des deux précédentes, et si $\delta = 1$ les solutions sont $y = \pm 1$, ce qui rajoute les solution e et $-e$)

$\delta = 0$	Algèbre duale	2 solutions (1 et -1)
$\delta = 1$	Algèbre fendue	4 solutions (1, -1, e et $-e$)
$\delta = k$	Corps	2 solutions (1 et -1)

2.1.4.1.5 Nombres d'éléments nil-carrés

Un nil-carré non trivial est un élément $x \neq 0$ tel que $x^2 = 0$

Dans $\mathbb{F}^2_{p^n,(\delta,0)}$, cela s'écrit $(x + ey)^2 = 0 = x^2 + e^2y^2 + 2exy$

Ce qui mène à :

$$\begin{cases} x^2 + \delta y^2 &= 0 \\ 2xy &= 0 \end{cases} \tag{5}$$

Si $y = 0$ on obtient $x^2 = 0$ dont la seules solution est 0, on en déduit que $y \neq 0$ et donc que $x = 0$

L'équation (5) devient

$$\begin{cases} \delta y^2 &= 0 \\ x &= 0 \end{cases}$$

Si $\delta \neq 0$, il n'y a pas de solution, et si $\delta = 0$ toutes les valeurs de $y \neq 0$ sont solutions

$\delta = 0$	Algèbre duale	$(p^n - 1)$ solutions (ey)
$\delta = 1$	Algèbre fendue	0 solution
$\delta = k$	Corps	0 solution (comme dans tous les corps)

2.1.4.1.6 Nombres d'idempotents non triviaux

Un idempotent non trivial est un élément $x \notin \{0, 1\}$ tel que $x^2 = x$

Dans $\mathbb{F}^2_{p^n,(\delta,0)}$, cela s'écrit $(x + ey)^2 = (x + ey) = x^2 + e^2y^2 + 2exy$

Ce qui mène à :

$$\begin{cases} x^2 + \delta y^2 &= x \\ 2xy &= y \end{cases} \tag{6}$$

Si $y = 0$ on obtient $x^2 = x$ dont les seules solutions sont les idempotents triviaux de $\mathbb{F}_{p^n}$, on en déduit que $y \neq 0$ et donc que $x = 2^{-1}$

L'équation (6) devient

$$\begin{cases} \delta y^2 &= 2^{-1} - 2^{-2} \\ x &= 2^{-1} \end{cases}$$

or $2^{-1} - 2^{-2} = 2^{-2}(2 - 1) = 2^{-2}$ d'où

$$\begin{cases} \delta y^2 &= 2^{-2} \\ x &= 2^{-1} \end{cases}$$

Equation qui n'a de solution que si $\delta = 1$.

$\delta = 0$	Algèbre duale	0 solution
$\delta = 1$	Algèbre fendue	2 solutions ($2^{-1} \pm 2^{-1}e$)
$\delta = k$	Corps	0 solution (comme dans tous les corps)

2.1.4.1.7 Synthèse

$\mathbb{F}^2_{n,(\delta,0)}$	Corps	Algèbre duale	Algèbre Fendue
Nombre copies	$\frac{p^n(p^n-1)}{2}$	p^n	$\frac{p^n(p^n-1)}{2}$
Inversibles	$p^{2n}-1$	$p^n(p^n-1)$	$(p^n-1)^2$
Diviseurs de 0	0	p^n-1	$2(p^n-1)$
Ordre 2	2	2	4
Nil-carré	0	p^n-1	0
Idempotent	0	0	2

2.2 Corps de caractéristique 2

Soit $\overset{2}{\simeq}$ la relation définie sur $\mathbb{K}$ par : $(x \overset{2}{\simeq} y) \Longleftrightarrow \exists k(k^2+k+x+y=0)$.

La relation $\overset{2}{\simeq}$ est une relation d'équivalence (pour la transitivité, seule propriété pas absolument triviale, si $(k^2+k+x+y=0) \wedge (k'^2+k'+y+z=0)$ alors $(k+k')^2+(k+k')+x+y+y+z=0$).

La classe d'un élément x sera notée $\overline{x}$.

Dans les corps de caractéristique 2 l'application définie par $x \mapsto x^2$ est une bijection (en effet : $x^2 = y^2 \Rightarrow (x+y)^2 = 0 \Rightarrow (x=y)$)

Dans les corps $\mathbb{F}_{2^p}$ l'application définie par $\varphi : x \mapsto x^2 + x$ vérifie $\varphi(x) = \varphi(x+1)$ et $|Im(\varphi)| = 2^{p-1}$ (en effet : $x^2+x = y^2+y \Rightarrow (x+y)^2 = (x+y) \Rightarrow ((x=y) \vee (x=y+1))$. De plus, $((a \notin Im(\varphi)) \wedge (b \notin Im(\varphi))) \Rightarrow ((a+b) \in Im(\varphi))$. $\overset{2}{\simeq}$ possède deux classes qui séparent $\mathbb{F}_{2^p}$ en deux sous ensembles de même cardinal.

Remarque : $|\overline{0}| = 2^{p-1}$ et si $k \notin \overline{0}$ alors $|\overline{k}| = 2^{p-1}$.

On peut aussi noter que $0 \in Im(\varphi)$ quelque soit $p > 0$

Soit φ un isomorphisme entre $(\mathbb{K}^2_{(a,b)}, +, \cdot, \times)$ et $(\mathbb{K}^2_{(a',b')}, +, \cdot, \times)$ Par définition d'un isomorphisme d'algèbre, φ vérifie les propriété suivantes (nous noterons f le deuxième élément de la base de $(\mathbb{K}^2_{(a',b')}, +, \cdot, \times)$

1. $\varphi(1) = 1$
2. $\varphi(a + eb) = a + b \cdot \varphi(e)$
3. $\varphi(e^2) = (\varphi(e))^2$
4. $\exists \alpha \in \mathbb{K}\ \exists \beta \in \mathbb{K}^*\ (\varphi(e) = \alpha + f\beta)$

β doit être différent de 0 sinon φ ne serait pas une bijection.

On doit donc avoir :

$$\begin{cases} \varphi(e^2) & = & a + b\varphi(e) & = & a + b(\alpha + f\beta) & = & a + b\alpha + fb\beta \\ (\varphi(e))^2 & = & (\alpha + f\beta)^2 & = & \alpha^2 + f^2\beta^2 & = & \alpha^2 + (a' + fb')\beta^2 \quad = \quad \alpha^2 + a'\beta^2 + fb'\beta^2 \end{cases}$$

$$\begin{cases} a + b\alpha & = & \alpha^2 + a'\beta^2 \\ b\beta & = & b'\beta^2 \\ \beta & \neq & 0 \end{cases} \tag{7}$$

Du système (7) on déduit immédiatement que $b = b'\beta$.

Soit $b = 0$ et alors $b' = 0$
Soit $b \neq 0$ alors :

$$\begin{cases} a + b\alpha & = & \alpha^2 + \frac{a'b^2}{b'^2} \\ b & = & b'\beta \end{cases} \tag{8}$$

Dans l'équation (8), en posant $bX = \alpha$: $b^2X^2 + b^2X + a + \frac{a'b^2}{b'^2} = 0$ et en divisant tout par b^2 on obtient $X^2 + X + \frac{a}{b^2} + \frac{a'}{b'^2} = 0$ autrement dit X existe (et donc l'isomorphisme existe) si et seulement si $\frac{a}{b^2} \overset{2}{\simeq} \frac{a'}{b'^2}$

Théorème

Dans le cas de la caractéristique 2, $\mathbb{K}^2_{(a,b)}$ ne dépend que de $\overline{\left(\frac{a}{b^2}\right)}$ si b est différent de 0.
Et $\mathbb{K}^2_{(a,0)} = \mathbb{K}^2_{(0,0)}$

2.2.1 $\mathbb{K} = \mathbb{F}_2$

·	0	1	e	1 + e
0	0	0	0	0
1	0	1	e	1 + e
e	0	e	0	e
1 + e	0	1 + e	e	1

$e^2 = 0$

·	0	1	e	1 + e
0	0	0	0	0
1	0	1	e	1 + e
e	0	e	e	0
1 + e	0	1 + e	0	1 + e

$e^2 = e$

·	0	1	e	1 + e
0	0	0	0	0
1	0	1	e	1 + e
e	0	e	1	1 + e
1 + e	0	1 + e	1 + e	0

$e^2 = 1$

·	0	1	e	1 + e
0	0	0	0	0
1	0	1	e	1 + e
e	0	e	1 + e	1
1 + e	0	1 + e	1	e

$e^2 = 1 + e$

L'application de $\varphi : \mathbb{F}^2_{2,(0,0)} \to \mathbb{F}^2_{2,(1,0)}$:

$$\begin{aligned}\varphi(0) &= 0\\ \varphi(1) &= 1\\ \varphi(e) &= e+1\\ \varphi(e+1) &= e\end{aligned}$$

est un isomorphisme d'algèbre.

Le cas $e^2 = e$ correspond à $\mathbb{F}^2_{2,(0,1)}$ c'est à dire que $\dfrac{a}{b^2} = 0$ et, bien sûr, $X^2 + X = 0$ possède des solutions.

Le cas $e^2 = 1 + e$ correspond à $\mathbb{F}^2_{2,(1,1)}$ c'est à dire que $\dfrac{a}{b^2} = 1$ et, bien sûr, $X^2 + X + 1 = 0$ ne possède pas de solutions dans $\mathbb{F}_2$.

Résumé : 3 cas possibles

- ☞ Un corps : $\mathbb{F}_4$ (obtenu d'une seule façon).
- ☞ Une algèbre Duale (obtenue de deux façons différentes).
- ☞ Une algèbre Fendue (obtenue d'une seule façon).

2.2.2 $\mathbb{K} = \mathbb{F}_{2^p}$ pour $p > 1$

On peut noter qu'il y a 3 algèbres différentes (à isomorphisme près) pour $\mathbb{K} = \mathbb{F}_{2^p}$, correspondant aux 3 classes de $\overset{2}{\simeq}$:

Dans le cas $\mathbb{F}^2_{2^p,(a,b)}$ où $\dfrac{a}{b^2} \notin \overline{0}$, si $y = 0$ le symétrique de x est $x^{-1} + 0e$ (c'est le symétrique dans $\mathbb{F}_{2^p}$), sinon $(x + ey)(x + by + ey) = x^2 + bxy + ay^2$, or

$$x^2 + bxy + ay^2 = b^2y^2\left(\left(\frac{x}{by}\right)^2 + \frac{x}{by} + \frac{a}{b^2}\right) \neq 0$$

Autrement dit, dans tous les cas $(x + ey \neq 0) \Rightarrow (x + ey)^{-1} = \dfrac{(x + by + ey)}{x^2 + bxy + ay^2}$

- ▷ $\mathbb{F}^2_{2^p,(0,0)}$ qui contient des éléments nil-carrés (tous les éléments de la forme eb).
- ▷ $\mathbb{F}^2_{2^p,(0,1)}$ qui contient des diviseurs de 0 (comme $e(1 + e) = e + e^2 = e + e = 0$), mais pas de nil-carré ($(a + eb)^2 = a^2 + e^2b^2 = a^2 + eb^2 = 0$ a pour unique solution $a = b = 0$).
- ▷ $\mathbb{F}^2_{2^p,(a,1)}$ où $a \notin \overline{0}$ qui est le corps $\mathbb{F}_{2^{2p}}$

Résumé : 3 cas possibles

- ☞ Une algèbre Duale.
- ☞ Une algèbre Fendue.
- ☞ Un corps : $\mathbb{F}_{2^{2p}}$.

2.2.2.1 Comptages

2.2.2.1.1 Nombres de copies

En repartant de l'équation (8) et du résultat : $\mathbb{K}^2_{(a,b)}$ ne dépend que de $\overline{\frac{a}{b^2}}$ ou $b = 0$.

Cas $\mathbb{F}^2_{2^p,(a,0)}$

Pour chacune des 2^p valeurs de a, on obtient une algèbre isomorphe à $\mathbb{F}^2_{2^p,(0,0)}$, il y a donc 2^p possibilités pour construire $\mathbb{F}^2_{2^p,(0,0)}$

Cas $\mathbb{F}^2_{2^p,(0,b)}$, $b \neq 0$

Pour chacune des $2^p - 1$ valeurs de $b \neq 0$, et chacun des 2^{p-1} éléments λ de $\overline{0}$ il existe une et une seul valeur de a telle que $a = \lambda b^2$, il y a donc $2^{p-1}(2^p - 1)$ possibilités pour construire une algèbre fendue isomorphe à $\mathbb{F}^2_{2^p,(0,1)}$

Cas $\mathbb{F}^2_{2^p,(a,1)}$, $a \neq 0$, $a \notin \overline{0}$

Pour chacune des $2^p - 1$ valeurs de $b \neq 0$, et chacun des 2^{p-1} éléments $\lambda \notin \overline{0}$ il existe une et une seul valeur de a telle que $a = \lambda b^2$, il y a donc $2^{p-1}(2^p - 1)$ possibilités pour construire une algèbre fendue isomorphe à $\mathbb{F}^2_{2^p,(a,1)}$

2.2.2.1.2 Nombres d'inversibles

Un élément inversible est un élément x (forcément $x \neq 0$) tel qu'il existe un élément y (forcément $y \neq 0$) vérifiant $xy = 1$.

Dans $\mathbb{F}^2_{2^p,(a,b)}$, cela s'écrit :

$$(x + ey)(x' + ey') = 1 = xx' + e^2yy' + e(xy' + x'y) = xx' + (a + eb)yy' + e(xy' + x'y)$$

Ce qui mène à :

$$\begin{cases} xx' + ayy' & = & 1 \\ xy' + x'y + byy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases} \tag{9}$$

Cas $\mathbb{F}^2_{2^p,(0,0)}$

Le système (9) devient

$$\begin{cases} xx' & = & 1 \\ xy' + x'y & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Dont les solutions sont $x' = x^{-1}$ (donc $x \neq 0$) et $y' = x^{-2}y$, tous les éléments tels que $x \neq 0$ ont un inverse, soit $2^p(2^p - 1)$ éléments

Cas $\mathbb{F}^2_{2^p,(0,1)}$

Le système (9) devient

$$\begin{cases} xx' & = & 1 \\ xy' + x'y + yy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Dont les solutions sont $x' = x^{-1}$ (donc $x \neq 0$) et $y' = x^{-1}y(x+y)^{-1}$ (donc $x \neq y$), tous les éléments tels que $x \neq 0$ et $x \neq y$ont un inverse, soit $(2^p-1)^2$ éléments

Cas $\mathbb{F}^2_{2^p,(a,1)}$, $a \neq 0$, $a \notin \overline{0}$

Ce cas a été traité au paragraphe $\mathbb{K} = \mathbb{F}_{2^p}$ pour $p > 1$: tous les éléments différents de 0 ont un inverse, soit $2^{2p} - 1$

$\mathbb{F}^2_{2^p,(0,0)}$	Algèbre duale	$2^p(2^p-1)$ solutions
$\mathbb{F}^2_{2^p,(0,1)}$	Algèbre fendue	$(2^p-1)^2$ solutions
$\mathbb{F}^2_{2^p,(a,0)}$	Corps	2^{2p} solutions, comme dans tous les corps

2.2.2.1.3 Nombres de diviseurs de zéro

Un élément diviseur de zéro est un élément $x \neq 0$ tel qu'il existe un élément $y \neq 0$ vérifiant $xy = 0$. Dans les corps il n'y en a pas.

Dans $\mathbb{F}^2_{2^p,(a,b)}$, cela s'écrit :

$$(x+ey)(x'+ey') = 0 = xx' + e^2yy' + e(xy' + x'y) = xx' + (a+eb)yy' + e(xy' + x'y)$$

Ce qui mène à :

$$\begin{cases} xx' + ayy' & = & 0 \\ x'y + xy' + byy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases} \tag{10}$$

Cas $\mathbb{F}^2_{2^p,(0,0)}$

Le système (10) devient

$$\begin{cases} xx' & = & 0 \\ x'y + xy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Dont les seules solutions sont $x = x' = 0$ et $y \neq 0$ et $y' \neq 0$, soit $2^p - 1$ possibilités

Cas $\mathbb{F}^2_{2^p,(0,1)}$

Le système (10) devient

$$\begin{cases} xx' & = & 0 \\ x'y + xy' + yy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Les solutions sont $x = 0$ et $y(x'+y') = 0$ soit $(2^p-1) + (2^p-1) = 2(2^p-1)$

Cas $\mathbb{F}^2_{2^p,(a,1)}$, $a \neq 0$, $a \notin \overline{0}$

$$\begin{cases} xx' + ayy' & = & 0 \\ x'y + xy' + yy' & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

$\mathbb{F}^2_{2^p,(0,0)}$	Algèbre duale	(2^p-1) solutions
$\mathbb{F}^2_{2^p,(0,1)}$	Algèbre fendue	$2(2^p-1)$ solutions
$\mathbb{F}^2_{2^p,(a,0)}$	Corps	0 solution, comme dans tous les corps

2.2.2.1.4 Nombres d'éléments d'ordre 2

Un élément d'ordre 2 est un élément tel que $x^2 = 1$, il y a donc toujours 1 (et -1 s'il est différent de 1).

Dans $\mathbb{F}^2_{2^p,(a,b)}$, cela s'écrit $(x+ey)^2 = 1 = x^2 + e^2y^2 = x^2 + (a+eb)y^2$

Ce qui mène à :

$$\begin{cases} x^2 + ay^2 &= 1 \\ by^2 &= 0 \end{cases} \tag{11}$$

Cas $\mathbb{F}^2_{2^p,(0,0)}$

Le système (11) devient

$$\begin{cases} x^2 &= 1 \\ 0 &= 0 \end{cases}$$

C'est à dire $x = 1$ et y n'importe laquelle des 2^p valeurs possibles

Cas $\mathbb{F}^2_{2^p,(0,1)}$

Le système (11) devient

$$\begin{cases} x^2 &= 1 \\ y^2 &= 0 \end{cases}$$

Système qui n'a qu'une seule solution : 1.

Cas $\mathbb{F}^2_{2^p,(a,1)}$**,** $a \neq 0$**,** $a \notin \overline{0}$

Le système (11) devient

$$\begin{cases} x^2 + ay^2 &= 1 \\ y^2 &= 0 \end{cases}$$

Système qui n'a qu'une seule solution : 1.

$\mathbb{F}^2_{2^p,(0,0)}$	Algèbre duale	2^p solutions
$\mathbb{F}^2_{2^p,(0,1)}$	Algèbre fendue	1 solution (1)
$\mathbb{F}^2_{2^p,(a,1)}$	Corps	1 solution (1)

2.2.2.1.5 Nombres d'éléments nil-carrés Un nil-carré non trivial est un élément $x \neq 0$ tel que $x^2 = 0$

Dans $\mathbb{F}^2_{2^p,(a,b)}$, cela s'écrit $(x+ey)^2 = 0 = x^2 + e^2y^2 = x^2 + (a+eb)y^2$

Ce qui mène à :

$$\begin{cases} x^2 + ay^2 & = & 0 \\ by^2 & = & 0 \end{cases} \tag{12}$$

Cas $\mathbb{F}^2_{2^p,(0,0)}$

Le système (12) devient

$$\begin{cases} x^2 & = & 0 \\ 0 & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Système dont les solutions sont $x = 0$ et $y \neq 0$, soit $(2^p - 1)$ solutions

Cas $\mathbb{F}^2_{2^p,(0,1)}$

Le système (12) devient

$$\begin{cases} x^2 & = & 0 \\ y^2 & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Système qui n'a pas de solution.

Cas $\mathbb{F}^2_{2^p,(a,1)}$**,** $a \neq 0$**,** $a \notin \overline{0}$

Le système (12) devient

$$\begin{cases} x^2 + ay^2 & = & 0 \\ y^2 & = & 0 \\ x \neq 0 & \vee & y \neq 0 \\ x' \neq 0 & \vee & y' \neq 0 \end{cases}$$

Système qui n'a pas de solution.

$\mathbb{F}^2_{2^p,(0,0)}$	Algèbre duale	$(2^p - 1)$ solutions (ey)
$\mathbb{F}^2_{2^p,(0,1)}$	Algèbre fendue	0 solution
$\mathbb{F}^2_{2^p,(a,1)}$	Corps	0 solution (comme dans tous les corps)

2.2.2.1.6 Nombres d'idempotents non triviaux Un idempotent non trivial est un élément $x \notin \{0,1\}$ tel que $x^2 = x$

Dans $\mathbb{F}^2_{2^p,(a,b)}$, cela s'écrit $(x+ey)^2 = (x+ey) = x^2 + e^2b^2 = x^2 + (a+eb)y^2$

Ce qui mène à :

$$\begin{cases} x^2 + ay^2 &= x \\ by^2 &= y \end{cases} \tag{13}$$

$\mathbb{F}^2_{2^p,(0,0)}$

Le système (13) devient

$$\begin{cases} x^2 &= x \\ 0 &= y \end{cases}$$

Système dont les seules solutions sont les idempotents triviaux.

Cas $\mathbb{F}^2_{2^p,(0,1)}$

Le système (13) devient

$$\begin{cases} x^2 &= x \\ y^2 &= y \end{cases}$$

Système dont les solution sont $0, 1, e, 1+e$, soit deux idempotents non triviaux.

Cas $\mathbb{F}^2_{2^p,(a,1)}$, $a \neq 0$, $a \notin \overline{0}$

Le système (13) devient

$$\begin{cases} x^2 + ay^2 &= x \\ y^2 &= y \end{cases}$$

Si $y = 0$ on retrouve les idempotents triviaux et si $y = 1$ on obtient l'équation $x^2 + x + a = 0$ qui n'a pas de solution par définition de a.

$\mathbb{F}^2_{2^p,(0,0)}$	Algèbre duale	0 solution
$\mathbb{F}^2_{2^p,(0,1)}$	Algèbre fendue	2 solutions $(e, 1+e)$
$\mathbb{F}^2_{2^p,(a,1)}$	Corps	0 solution (comme dans tous les corps)

2.2.2.1.7 Synthèse

$\mathbb{F}^2_{n,(\delta,0)}$	Corps	Algèbre duale	Algèbre Fendue
Nombre copies	$2^{p-1}(2^p-1)$	2^p	$2^{p-1}(2^p-1)$
Inversibles	$2^{2p}-1$	$2^p(2^p-1)$	$(2^p-1)^2$
Diviseurs de 0	0	2^p-1	$2(2^p-1)$
Ordre 2	1	2^p	1
Nil-carré	0	2^p-1	0
Idempotent	0	0	2