الجمهورية الجزائرية الديموقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/12***

Mémoire de fin d'étude

Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

Corps Finis et Leur Application en Théorie des Codes

Présenté par :
1 - Barkat Abla.
2 - Mermoul Roqiya.

Dirigé par :
– Mr. Bouguebina Mounir.

Année universitaire 2011-2012

Corps Finis et Leur Application en Théorie des Codes

Mermoul Roqiya et Barkat Abla

Remerciements

Nous remercions nos trés chers parents, frères, soeurs, collègues et amis respectifs qui nous ont encouragés, soutenu durant tout notre parcours.

Nous présentons notre grand remerciement à professeur : Bouguebina Mounir sur tous ce qu'il nous a présenté comme conseils et orientations durant la réalisation de notre mémoire.

Nous remercions aussi tout éducateur, maitre et professeur qui nous appris un mot ou un cours, et orienté sur le chemin de la connaissance et du savoir depuis le cycle primaire, jusqu'au cycle universitaire.

Nous souhaitons la réussite à tous les étudiants des sections Mathématique et Informatique.

Enfin, nous remercions, tous ceux et celles qui nous ont aidées à faire ce mémoire.

Introduction

Les corps finis, comme leur nom l'indique, sont des corps ayant un nombre fini d'éléments. Ils sont tous de caractéristique un nombre premier, ce qui les différencie des corps comme $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Leur structure est telle qu'ils se prêtent trés bien à l'étude des questions arithmétiques ou algébriques. Mais on les trouve aussi dans d'autres branches des mathématiques comme la Géométrie Algébrique et la Géométrie Arithmétique. Le but de ce mémoire est de présenter de nouvelles applications des corps finis apparues récemment avec le developpement de l'informatique et notamment dans la théorie des codes correcteurs d'erreurs.

Ce mémoire est constitué de trois chapitres et est organisé de la manière suivante : dans le premier chapitre, on présente brièvement les notions classiques de groupe, d'anneau et de corps qui vont nous servir tout le long de ce travail. On y aborde aussi de façon concise les extensions de corps et la théorie de Galois. Dans le deuxième chapitre, on commence l'étude des corps finis. On y montre notamment que à isomorphisme prés, un corps fini est entièrement déterminé par son cardinal qui est toujours la puissance d'un nombre premier. Plus exactement pour tout nombre premier p et pour tout entier naturel n non nul, il existe un corps de cardinal $q = p^n$, qui se présente comme l'unique extension de degré n du corps premier $\mathbb{F}_p$. Dans le troisième chapitre, on définit les codes linéaires basés sur l'alphabet des éléments d'un corps fini et on explique comment ces codes permettent de détecter et de corriger les erreurs commises lors du transfert de l'information. Enfin, on présente l'exemple célèbre des codes de Reed-Solomon qui sont encore souvent utilisés dans le monde informatique.

Table des matières

Chapitre 1

Anneaux et Corps

Dans ce chapitre, on passe rapidement en revue les outils dont nous aurons besoin par la suite : les groupes, les anneaux et les corps. La notion d'extension de corps est à la base de la théorie de Galois que nous rappelons à la fin du chapitre et qui nous servira dans l'étude de la structure des corps finis.

1.1 Groupes, anneaux et corps

Soit G un ensemble muni d'une loi de composition interne $*$.

Définition 1 *: $(G, *)$ est un groupe si :*

- *$*$ est associative : pour tous x, y, z dans G on a :*

$$x * (y * z) = (x * y) * z$$

- *$*$ admet un élément neutre $e \in G$: pour tout $x \in G$ on a :*

$$x * e = e * x = x$$

- *tout élément x de G admet un symétrique $x^{'}$ pour $*$:*

$$x * x^{'} = x^{'} * x = e$$

Si $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou abélien.
Exemple :
1) les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ munis de l'addition sont des groupes commutatifs. l'élément neutre est 0 et le symétrique de x est $-x$.

2) les ensembles $(\mathbb{Q}-\{0\}), (\mathbb{R}-\{0\})$ et $(\mathbb{C}-\{0\})$ munis des produit sont des groupes commutatifs. l'élément neutre est 1 et le symétrique de x est x^{-1}.

Définition 2 *: soit H une partie de G. H est un sous-groupe de G si H est stable pour $*$ $(x, y \in H \Rightarrow x * y \in H)$ et si H est lui-même un groupe pour la loi $*$.*

On peut montrer facilement que H est un sous-groupe de G si et seulement si $x * y^{'} \in H$ pour tous $x, y \in H$. En particulier $e_G = e_H$.
Exemple :
1) Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. En effet $n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement soit H un sous-groupe de $\mathbb{Z}$. Soit n le plus petit élément positif non nul de H. Si $x \in H$, la division euclidienne de x par n donne $x = kn + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < n$. Comme H est un sous-groupe, on doit avoir $x - kn = r \in H$. Par définition de n, on doit avoir $r = 0$ et $x = kn$. Donc $H = n\mathbb{Z}$
2) Soit G un groupe. Alors $H = \{e_G\}$ est un sous-groupe de G appelé le sous-groupe trivial.

Définition 3 *: Soient $(G, *)$ et $(H, \perp)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :*

$$f(x * y) = f(x) \perp f(y)$$

$\forall x, y \in G$.

Autrement dit f préserve les structures de groupes de G et H. Si f est bijective, on dit que c'est un isomorphisme. Si $G = H$ et $* = \perp$, on parle d'endomorphisme et d'automorphisme. Noter que $f(e_G) = e_H$. Le noyau du morphisme f est :

$$Kerf = \{x \in G : f(x) = e_H\} = f^{-1}(e_H).$$

C'est un sous-groupe de G. Le noyau est utile pour detecter si f est injective ou non. En effet on a : f injective $\Leftrightarrow Kerf = \{e_G\}$. Par exemple le morphisme $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ donné par $f(x) = 3x$ est injectif puisque $Kerf = \{0\}$ (la loi de groupe est l'addition).

Soit $(G, *)$ un groupe abélien et soit H un sous-groupe de G. On définit une relation sur G par :

$$x \Re y \Leftrightarrow x * y^{'} \in H.$$

On vérifie facilement que $\Re$ est une relation d'équivalence. On a donc l'ensemble quotient, ensemble des classes d'équivalence :

$$\frac{G}{\Re} = \frac{G}{H} = \{\overline{x}, x \in G\}$$

Définissons $\overline{*}$ par $\overline{x} \,\overline{*}\, \overline{y} = \overline{x * y}$. On a donc une loi $\overline{*}$ sur $\frac{G}{H}$ qui devient ainsi un groupe abélien appelé le groupe quotient de G par H. En effet :

- l'associativité de $\overline{*}$ découle de celle de $*$ par définition.
- l'élément neutre de $\overline{*}$ est $\overline{e}$ avec e l'élément neutre de $*$.
- le symétrique de $\overline{x}$ est $\overline{x^{'}}$ avec $x^{'}$ le symétrique de x.

On a automatiquement un morphisme surjectif canonique de groupes :

$$\phi : G \longrightarrow \frac{G}{H}$$

qui à x associe $\overline{x}$, de noyau $Ker\phi = H$.
Exemple : On prend $(G, *) = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. On a $x\Re y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x \equiv y \; mod(n)$ et :

$$\frac{G}{H} = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Convention : Dans la suite un groupe $(G, *)$ sera noté multiplicativement : $* = .$ et $e_G = 1$. Le symétrique $x^{'}$ de x sera noté x^{-1}. Si la loi est commutative, on le notera additivement : $* = +$, $e_G = 0$ et le symétrique $x^{'}$ de x sera noté $-x$.

Définition 4 *: Soit A un ensemble possédant deux lois internes que l'on note, par analogie avec $\mathbb{Z}$, $+$ et $.$. On dit que le triplet $(A, +, .)$ posséde une structure d'anneau si :*

- *$(A, +)$ a une structure de groupe abélien d'élément neutre 0_A.*
- *La loi $.$ est distributive à gauche et à droite par rapport a la loi $+$: $\forall x, y, z \in A$, on a :*

$$x.(y + z) = x.y + x.z$$

$$(x + y).z = x.z + y.z$$

- *La loi $.$ est associative : $\forall x, y, z \in A$, on a :*

$$x.(y.z) = (x.y).z$$

Si de plus, il existe un élément neutre 1_A dans A pour la loi . (qu'on appelle élément unité de l'anneau) alors l'anneau A sera dit unitaire.
Si l'élément x de A posséde un inverse pour la loi ., on dira que x est un élément inversible et on notera x^{-1} son inverse. Enfin si la loi . est commutative, l'anneau sera dit commutatif.

Définition 5 *: Soit $(A, +, .)$ un anneau soit B une partie de A contenant 1_A et stable pour les lois $+$ et .. On dit que B est un sous-anneau de A si muni de ces deux lois B est lui-même un anneau.*

Remarquer que la condition $1_A \in B$ est nécessaire. Par exemple $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1. Par contre $B = \{a+b\sqrt{2}, a, b \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Q}, +, .)$. Dans la pratique pour montrer que B est un sous-anneau de A, il suffit de vérifier que $1_A \in B$ et que $\forall x, y \in B$, on a $x - y$ et $x.y \in B$.

Définition 6 *: Une partie I d'un anneau A est appelé idéal à gauche (respectivement à droite) si :*
- *I est un sous-groupe de $(A, +)$.*
- *$\forall a \in A, \forall x \in I : a.x \in I$ (respectivement $x.a \in I$).*

Si I est un idéal à gauche et à droite à la fois de A, on dit que c'est un idéal bilatère de A.

Remarque :
1) Si A est commutatif, les idéaux à gauche et à droite coincident.
2) $\{0_A\}$ et A sont des idéaux de A. Ils sont appelés idéaux triviaux. Les autre idéaux de A sont dits propres.
3) Un idéal de A n'est pas forcément un sous-anneau de A, car il ne contient pas en général 1_A. Plus précisément on a :

$$1_A \in I \Leftrightarrow I = A$$

4) Dans la suite, on va considérer uniquement des anneaux commutatifs. On dira donc anneau pour anneau commutatif.
Exemple :
1) Soit A un anneau et soit $a \in A$. Alors l'ensemble $I = aA = \{a.x, x \in A\}$ est un idéal de A. On l'appelle l'idéal principal engendré par a. L'anneau A sera dit principal si tous ses idéaux sont principaux.

2) $(\mathbb{Z}, +, .)$ est un anneau principal. En effet, on a vu que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$ et ce sont donc les seuls idéaux de $\mathbb{Z}$.
3) L'intersection d'un nombre quelconque idéaux est un idéal. Plus généralement l'intersection de tous les idéaux contenant une partie G de A est un idéal appelé l'idéal engendré par la partie G. Ses éléments sont les sommes finies $\sum_{k=1}^{n} a_k x_k$ avec $a_k \in A$ et $x_k \in G$.
4) la somme de deux idéaux I_1 et I_2 est l'ideal $I_1 + I_2 = \{x+y, x \in I_1, y \in I_2\}$. On peut aussi le définir comme étant l'idéal engendré par$I_1 \cup I_2$. En particulier il contient I_1 et I_2 De manière plus générale la somme $\sum_\lambda I_\lambda$ d'une famille d'idéaux I_λ est le plus petit idéal de A contenat chacun des I_λ.
5) Le produit de deux idéaux I et J est l'idéal IJ engendré par les produits $x.y$ avec $x \in I$ et $y \in J$. Concrètement ses éléments sont les sommes finies $\sum x_i.y_i$ avec $x_i \in I$ et $y_i \in J$.

Soient $a, b \in A$. On dit que a divise b ou que b est un multiple de a s'il existe $c \in A$ avec $b = ac$. L'idéal $I = aA$ est donc l'ensemble des multiples de a. Remarquer que a divise b si et seulement si $bA \subset aA$. Un élément a est une unité s'il a un inverse a^{-1} pour la multiplication. a est dit premier ou irréductible si $a = bc$ implique que b ou c est une unité. $a \neq 0$ est un diviseur de 0 s'il existe $b \neq 0$ tel que $a.b = 0$. Les anneaux qui n'ont pas de diviseurs de zéro sont appelés des anneaux intègres. Par exemple dans $\mathbb{Z}$, les éléments premiers sont (au signe prés) les nombres premiers p. L'equation $a.b = 0$ n'a pas de solution non nulle dans $\mathbb{Z}$ qui est donc un anneau intègre.

Définition 7 *: Un idéal propre I d'un anneau A est dit premier si $ab \in I$ implique $a \in I$ ou $b \in I$. I est dit maximal s'il n'est contenu dans aucun autre idéal propre de A.*

Proposition 1 *: Un idéal maximal est premier. Les idéaux premiers de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier et ils sont tous maximaux.*

Preuve : Soit I un idéal maximal. Soient $a, b \in A$ avec $ab \in I$. Supposons que $a \notin I$. Alors l'idéal $I + aA$ est égal à A, car I est maximal. Il existe alors $d \in I$ et $x \in A$ avec $d + a.x = 1$ et donc $d.b + a.b.x = b \in I$ (rappelons que A est commutatif). Ceci montre que I est premier. Tout idéal propre de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \neq 0 \in \mathbb{N}$. Supposons que $n\mathbb{Z}$ premier. $ab \in n\mathbb{Z}$ implique $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$ s'écrit n divise ab implique n divise a ou n divise b, ce qui par le lemme de gauss veut dire que $n = p$ un nombre premier. Enfin $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. Ceci montre que tout idéal premier de $\mathbb{Z}$ est maximal.

Une application $f : A \longrightarrow B$ entre deux anneaux est un morphisme si :

$$f(x+y) = f(x) + f(y)$$

$$f(x.y) = f(x).f(y)$$

$$f(1_A) = 1_B$$

pour tous $x, y \in A$. Autrement dit f préserve les opérations d'anneau. Si f est de plus bijective, on dit que c'est un isomorphisme entre A et B. Si $A = B$, on parle d'endomorphisme et d'automorphismes, respectivement. Le noyau d'un morphisme f est :

$$Kerf = \{x \in A : f(x) = 0_B\} = f^{-1}(0_B).$$

C'est un idéal de A. L'image de f est :

$$Imf = \{f(x), x \in A\} = f(A).$$

C'est un sous-anneau de B.

Soit A un anneau et soit I un idéal de A. On définit une relation $\Re$ sur A par :

$$x \Re y \Leftrightarrow x - y \in I.$$

On verifie facilement que $\Re$ est une relation d'equivalence sur A. Sur l'ensemble quotient

$$\frac{A}{\Re} = \frac{A}{I} = \{\overline{x}, x \in A\},$$

on définit deux opérations $\overline{+}$ et $\overline{\cdot}$ en posant : $\overline{x} \ \overline{+} \ \overline{y} = \overline{x+y}$ et $\overline{x} \ \overline{\cdot} \ \overline{y} = \overline{x.y}$. Ces deux opérations sont bien définies et font de $\frac{A}{I}$ un anneau. C'est l'anneau quotient de A par I. Remarquer que $\overline{x} = x + I$. En particulier $\overline{0} = I$ est l'élément neutre de $\overline{+}$.

On a un morphisme canonique surjectif d'anneaux :

$$\phi : A \longrightarrow \frac{A}{I}$$

qui à x associe sa classe modulo I, $\overline{x} = x + I$ et de noyau $Ker\phi = I$. De plus il y a une correspondance bijective entre les idéaux J de A qui contiennent I et les idéaux $\overline{J}$ de $\frac{A}{I}$ donnée par $J = \phi^{-1}(\overline{J})$.

Exemple : On prend $A = \mathbb{Z}$ et $I = n\mathbb{Z}$. On a alors $x - y \in n\mathbb{Z} \Longleftrightarrow x \equiv y$

$mod(n)$. L'ensemble quotient est donc l'ensemble des classes de congruence modulo n :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et les opérations d'anneau sont celles bien connues de l'addition et de la multiplication des congruences.

Proposition 2 *: L'idéal I est premier si et seulement si l'anneau quotient $\frac{A}{I}$ est intègre.*

Preuve : Un anneau est intègre s'il n'a pas de diviseurs de 0. Supposons I premier et soient $\overline{a}$ et $\overline{b}$ tels que $\overline{a}.\overline{b} = \overline{0}$. donc $a.b \in I$. Comme I est premier, cela veut dire que $a \in I$ ou $b \in I$, c'est à dire que $\overline{a} = \overline{0}$ ou que $\overline{b} = \overline{0}$ et donc que l'anneau quotient est intègre. Inversement supposons l'anneau quotient intègre et soient $a, b \in A$ avec $a.b \in I$. Donc $\overline{a}.\overline{b} = \overline{0}$ et donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, c'est à dire que $a \in I$ ou $b \in I$. Ceci montre que I est premier.

Définition 8 *: Un corps K est un anneau non nul dans lequel tout élément différent de 0 a un inverse pour la multiplication.*

Ainsi $K^* = K - \{0\}$ muni de la loi de multiplication devient un groupe qu'on appelle groupe multiplicatif de K. Par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sont des corps.
Un sous corps de K est une partie L de K stable pour les lois + et . et qui est, pour ces lois, elle-même un corps. Par exemple $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$.
Un corps K est automatiquement intègre. En effet soit $a.b = 0$ et supposons $a \neq 0$. On a alors $a^{-1}.a.b = b = 0$.
Remarque : Un corps K n'a pas d'idéal propre. Autrement dit les seuls idéaux de K sont $\{0\}$ et K lui-même. En effet soit I un idéal de K non nul et soit $x \neq 0 \in I$, alors $x^{-1}.x = 1 \in I$ et donc $I = K$. En particulier tout morphisme non nul $f : K \longrightarrow L$ entre deux corps est injectif puisque, $Kerf$ etant un idéal, il doit-être égal à $\{0\}$.

Proposition 3 *: Un idéal I d'un anneau A est maximal si et seulement si l'anneau quotient $\frac{A}{I}$ est un corps.*

Preuve : Supposons I maximal et soit $\overline{x} \neq \overline{0} \in \frac{A}{I}$. Nous devons montrer que $\overline{x}$ a un inverse pour la multiplication. Comme $\overline{x} \neq \overline{0}$, $x \notin I$. L'idéal $I + xA$ doit donc être égal à A car I est maximal. Il existe donc $a \in A$ et $b \in I$

avec $b + x.a = 1$ ou encore $x.a = 1 - b \in 1 + I = \overline{1}$. Ce qui veut dire que $\overline{x}.\overline{a} = \overline{1}$ et donc $\overline{x}$ a un inverse. Inversement supposons que $\frac{A}{I}$ est un corps. Pour montrer que I est maximal, il suffit de montrer que pour tout $x \notin I$, l'idéal $I + xA$ doit être égal à A. Pour cela il faut montrer que $1 \in I + xA$. Or $x \notin I$ équivaut à $\overline{x} \neq 0$ et donc $\overline{x}$ a un inverse $\overline{y}$: $\overline{x}.\overline{y} = \overline{1}$. Donc $xy \in 1 + I$ et $1 \in I + xA$.
Exemple : On a vu que les idéaux maximaux de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier. Donc pour tout nombre premier p, les congruences modulo p :

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

forment un corps qu'on appelle le corps premier à p éléments et qu'on note $\mathbb{F}_p$.

1.2 Anneau des polynômes sur un corps

Soit K un corps.

Définition 9 *: Un polynôme en la variable X à coefficient dans le corps K est une expression de la forme*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

avec $a_i \in K$.

Si $a_n \neq 0$ l'entier n est appelé le degré du polynôme. Un polynoôme de degré n est dit unitaire si $a_n = 1$. Le polynôme nul est le polynôme dont tous les coefficients sont nuls. Notons $K[X]$ l'ensemble des polynômes à coefficients dans K. On peut définir une addition et une multiplication dans $K[X]$ par les formules

$$(\sum_i a_i X^i) + (\sum_i b_i X^i) = \sum_i (a_i + b_i) X^i$$

et

$$(\sum_i a_i X^i).(\sum_j b_j X^j) = \sum_k (\sum_{i+j=k} a_i b_j) X^k$$

On vérifie facilement que ces deux opérations font de $K[X]$ un anneau commutatif. L'élément neutre pour l'addition est le polynôme nul et l'élément

neutre pour la multiplication est $P(X) = 1$. On peut aussi multiplier un polynôme P par un scalaire $\lambda \in K$

$$(\lambda P)(X) = \lambda P(X) = \sum_i \lambda a_i X^i.$$

Ceci permet de regarder $K[X]$ comme un K-espace vectoriel de dimension infinie et de base $\{1, X, X^2, \ldots\}$.

L'anneau $K[X]$ a des propriétés trés similaires à celles de l'anneau $\mathbb{Z}$ des entiers relatifs et notamment en ce qui concerne la divisibilité. On dira qu'un polynôme Q divise un polynôme P s'il existe un autre polynôme R tel que

$$P = Q.R$$

Un polynôme sera dit irréductible si ses seuls diviseurs sont 1 et lui-même.

1.3 Extensions de corps et théorie de Galois

Définition 10 *: Si un corps L contient un autre corps K comme sous-corps, on dit que L/K est une extension de corps.*

On peut regarder L comme un K-espace vectoriel. La dimension $dim_K(L)$ est alors appelée le degré de l'extension. On le note $[L : K]$. L'extension est finie si $[L : K] = n < \infty$ et il existe alors une base finie $\{\alpha_1, \ldots, \alpha_n\}$ de L sur K. Tout élément $\gamma \in L$ s'écrit : $\gamma = \sum_{i=1}^{n} a_i \alpha_i$ avec $a_i \in K$. On vérifie facilement que si L/K et M/L sont deux extensions finies, alors :

$$[M : K] = [M : L].[L : K]$$

Définition 11 *: Un élément $\alpha \in L$ est dit algébrique sur K s'il existe un polynôme non nul $f(X) \in K[X]$ avec $f(\alpha) = 0$.*

Parmi tous les polynômes qui annulent α, il en existe un de plus petit degré et unitaire et donc irréductible. On l'appelle le polynôme minimal de α sur K. L'extension de corps L/K est dite algébrique si tous les éléments de L sont algébriques sur K.

Soient $\gamma_1, \ldots, \gamma_r \in L$. Le plus petit sous-corps de L contenant K et les γ_i (on dit aussi le sous-corps de L engendré par les γ_i sur K) est noté $K(\gamma_1, \ldots, \gamma_r)$. L'extension $K(\gamma_1, \ldots, \gamma_r)/K$ est finie si et seulement si tous

les γ_i sont algébriques sur K. En particulier $\alpha \in L$ est algébrique sur K si et seulement si $[K(\alpha) : K] < \infty$. Si $p(X)$ est le polynôme minimal de α sur K et si $r = deg(p(X))$, alors $[K(\alpha) : K] = r$ et les éléments $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ forment une base de $(K(\alpha)/K)$.

Soient L_1/K et L_2/K deux extensions de K. Un morphisme de corps (nécéssaiement injectif car un corps ne contient pas d'idéal propre) $\sigma : L_1 \longrightarrow L_2$ est appelé un K-morphisme si $\sigma(a) = a$ pour tout $a \in K$. σ définit alors un plongement $\sigma(L_1) \subseteq L_2$ de L_1 dans L_2 sur K. Un K-isomorphisme est un K-morphisme surjectif (et donc bijectif).

Si K est un corps et si $f(X) \in K[X]$ est un polynôme non constant, alors il existe une extension algébrique $L = K(\alpha)$ de K avec $f(\alpha) = 0$: c'est l'extension obtenue par l'adjonction de la racine α de f sur K. L'extension de K obtenue par l'adjonction de toutes les racines de f est appelée le corps de décomposition du polynôme f.

Définition 12 *: Un corps M est dit algébriquement clos si tout polynôme $f(X) \in M[X]$ de degré ≥ 1 a au moins une racine dans M.*

Pour tout corps K, la clôture algébrique de K est le plus petit corps (au sens de l'inclusion) algébriquement clos contenant K. On le note $\overline{K}$. Intuitivement il est obtenu par l'adjonction des racines de tous les polynômes sur K. Si L/K est une extension algébrique, qu'on peut supposer pour simplifier simple i.e $L = K(\alpha)$, alors toute racine α_i du polynôme minimal $p(X)$ de α définit un plongement :

$$\sigma_i : L \longrightarrow \overline{K}$$

qui consiste à envoyer α vers α_i. Le nombre de tels plongements est donc égal au nombre de racines distinctes de $p(X)$ et il est donc au plus égal à $[L : K]$.

Soit K un corps et soit 1 son élément neutre pour la multiplication. Pour tout entier $m > 0$, posons :

$$m.1 = 1 + 1 + \ldots + 1 \in K$$

Si $m.1 \neq 0$ pour tout m, on dit que K est de caractéristique 0 : $car(K) = 0$. Sinon, il existe un unique nombre premier p tel que $p.1 = 0$ et on dit que K est de caractéristique p : $car(K) = p$. Dans le premier cas K contient le corps des rationnels $\mathbb{Q}$ et dans le second, il contient le corps fini $\mathbb{F}_p$. Les corps $\mathbb{Q}$ et $\mathbb{F}_p$ sont appelés des corps premiers car ce sont les plus petits corps

de caractéristique respectivement 0 et p. Remarquer que dans un corps de caractéristique p, on a toujours :

$$(a+b)^q = a^q + b^q$$

pour tous $a, b \in K$ et pour tout $q = p^j, j \geq 0$.

Soit $f(X) \in K[X]$ un polynôme unitaire de degré $d \geq 1$. Dans une certaine extension L de K (par exemple dans son corps de décomposition), le polynôme f s'écrit comme produit de facteurs linéaires :

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i)$$

Définition 13 *: Le polynôme f est dit séparable si $\alpha_i \neq \alpha_j$ pour tout $i \neq j$. Sinon il est dit inséparable.*

Autrement dit, un polynôme est séparable s'il na pas de racines multiples. On peut caractériser la séparabilité en utilisant la derivée $f^{'}(X) = \sum i a_i X^{i-1}$ de $f(X) = \sum a_i X^i$. En effet une racine α de f est multiple si et seulement si c'est une racine commune de f et $f^{'}$. On montre alors facilement qu'un polynôme irréductible f est séparable si et seulement si $f^{'}(X) \neq 0$ (si $f^{'}(X) = 0$, alors toute racine de f est aussi racine de $f^{'}$ et est donc multiple. Inversement soit $f^{'} \neq 0$ et supposons que f n'est pas séparable. Il a donc au moins une racine commune avec $f^{'}$. Ceci veut dire que le plus grand commun diviseur D de f et $f^{'}$ dans $K[X]$ est de degré ≥ 1 ce qui contredit le fait que f est irréductible). Ainsi, en caractéristique 0, tout polynôme irréductible est séparable et en caracétristique p, le polynôme irréductible f est séparable si et seulement si $a_i \neq 0$ pour un certain i non congru à 0 modulo p.

Si L/K est une extension algébrique, un élément $\alpha \in L$ est dit séparable sur K si son polynôme minimal $p(X) \in K[X]$ est séparable. L'extension elle même est dite séparable si tout élément de L est séparable sur K. En caractéristique 0, toute extension algébrique est séparable. Une extension simple $K(\alpha)/K$ est donc séparable si et seulement si il existe r plongements :

$$\sigma_1, \ldots, \sigma_r : K(\alpha) \longrightarrow \overline{K}$$

avec $r = [K(\alpha) : K]$ ou dit autrement si et seulement les racines du polynôme minimal $p(X)$ de α sont toutes distinctes i.e si et seulement si $p(X)$ est séparable.

Pour une extension L/K le groupe des K-automorphismes de L sera noté $Aut(L/K)$. Si l'extension est finie, on a vu (dans le cas simple $L = K(\alpha)$) qu'on a toujours :

$$\#Aut(L/K) \leq [L : K].$$

Définition 14 *: L'extension finie L/K est dite galoisienne si $\#Aut(L/K) = [L : K]$.*

Dans ce cas $Aut(L/K)$ est appelé le groupe de Galois de l'extension. On le note $Gal(L/K)$:

$$Aut(L/K) = Gal(L/K)$$

Par définition une extension finie L/K est galoisienne si le nombre de K-automorphismes de L est égal au degré de l'extension. Si on reprend l'exemple de l'extension simple $L = K(\alpha)$ cela veut dire que toutes les racines du polynôme minimal de α sont distinctes (l'extension est séparable) et qu'elles sont toutes dans $K(\alpha)$. Cette deuxième condition a aussi un nom :

Définition 15 *: L'extension L de K est dite normale si elle est algébrique et si pour tout $\alpha \in L$ le polynôme minimal $p(X)$ de α a toutes ses racines dans L.*

Ainsi une extension est galoisienne si et seulement si elle est normale et séparable.

Soit L/K une extension galoisienne de groupe de Galois $G = Gal(L/K)$. La théorie de Galois établit une correspondance bijective entre l'ensemble des sous-groupes de G et l'ensemble des corps intermédiaires $K \subseteq N \subseteq L$. Au corps N, on associe le groupe $Gal(L/N)$ et au sous-groupe H de G, on associe le corps intermédiaire :

$$N = L^H = \{c \in L/\sigma(c) = c, \forall \sigma \in H\}$$

De plus si le groupe de Galois est abélien alors toute extension intermédiaire est galoisienne et on a :

$$Gal(L^H/K) = \frac{G}{H}$$

Chapitre 2

Structure des corps finis

Dans ce chapitre, on présente quelques résultats fondamentaux sur les corps finis. On commence dans la première section par démontrer l'existence et l'unicité des corps finis et une caractérisation simple du groupe multiplicatif de leurs éléments non nuls. Dans la deuxième section on introduit la notion de conjugués d'un élément d'un corps fini et on calcule ces conjugués grâce à l'automorphisme de Frobenius. La relation entre les conjugués et les polynômes irréductibles est à la base d'une application intéressante de cette notion : combien y a-t-il de polynômes irréductibles unitaire sur le corps fini $\mathbb{F}_q$ de degré donné n ? Dans la troisième section, on s'interesse aux applications Norme et Trace entre extensions de corps finis.

2.1 Structure des corps finis

Soit p un nombre premier. On sait que l'anneau des congruences de Gauss modulo p, $\mathbb{Z}/p\mathbb{Z}$ est un corps. On le note $\mathbb{F}_p$:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}.$$

C'est un corps qui contient un nombre fini d'éléments (p éléments exactement). $\mathbb{F}_p$ est un corps premier dans le sens qu'il ne contient pas de sous-corps. C'est le corps premier de caractéristique p. Tout autre corps de caractéristique p contient (une copie de) $\mathbb{F}_p$. Les $\mathbb{F}_p$, pour $p = 2, 3, 5, \ldots$ un nombre premier sont nos premiers exemples de corps finis.

Définition 16 *: Un corps fini est un corps qui contient un nombre fini d'éléments.*

Soit K un corps fini ayant q éléments. On peut déja dégager quelques informations sur K.

Proposition 4 *: Soit K un corps fini ayant q élément. Alors :*

1. *Il existe un nombre premier p tel que $\mathbb{F}_p \subseteq K$.*
2. *$q = p^n$ pour un certain entier $n \geq 1$.*
3. *$\alpha^q = \alpha$, $\forall \alpha \in K$.*

Preuve :
1) Comme K est un corps fini, sa caractéristique doit être un nombre premier p (sinon si caractéristique $K = 0$ alors $\mathbb{Q} \subseteq K$ et K ne serait plus fini). Ainsi K contient le sous-corps premier $\mathbb{F}_p$
2) On regarde K comme espace vectoriel sur $\mathbb{F}_p$. Comme $card(K) < \infty$, on a $n = dim_{F_p}(K) < \infty$. Soit $\{\alpha_1, \ldots, \alpha_n\}$ une base de K sur $\mathbb{F}_p$. Tout élément $\alpha \in K$ s'écrit d'une manière unique

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$$

avec $a_1, \ldots, a_n \in \mathbb{F}_p$. Donc $q = card(K) = p^n$.
3) Si $\alpha = 0$, on a clairement $\alpha^q = 0 = \alpha$, sinon si $\alpha \neq 0$ alors $\alpha \in K^*$ et on sait que K^*, le groupe multiplicatif de K, est d'ordre $q-1$ et donc $\alpha^{q-1} = 1$. On a aussi

$$\alpha^q = \alpha.\alpha^{q-1} = \alpha.1 = \alpha.$$

En utilisant ces quelques informations on peut démontrer le résultat principal sur les corps finis, leur existence et leur unicité.

Théorème 1 *: Pour tout nombre premier p et pour tout entier $n \geq 1$, il existe un corps fini ayant p^n éléments. Tout corps fini ayant $q = p^n$ éléments est isomorphe on corps de décomposition du polynôme $x^q - x$ sur $\mathbb{F}_p$.*

Preuve :
(Existence) : Soit $\overline{\mathbb{F}}_p$ la clôture algébrique de $\mathbb{F}_p$ et soit $K \subseteq \overline{\mathbb{F}}_p$ le corps de décomposition du polynôme $x^{p^n} - x$ sur $\mathbb{F}_p$. Soit R l'ensemble des solutions de $x^{p^n} - x$ dans K. R a exactement p^n éléments. En effet la dérivée de $x^{p^n} - x$ est $p^n x^{p^n-1} - 1 = -1$ et donc $x^{p^n} - x$ n'a pas de racines multiples. De plus

R contient $\mathbb{F}_p$ (tout élément de $\mathbb{F}_p$ vérifie $x^p = x$ et donc $x^{p^n} = x, \forall n \geq 1$) et est un sous-corps de $\mathbb{F}_p$ (En effet $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}, \forall \alpha, \beta \in \overline{\mathbb{F}}_p$). Donc R est un corps qui contient les p^n racines de $x^{p^n} - x$ et qui contient $\mathbb{F}_p$. Donc $R = K =$ corps de décomposition de $x^{p^n} - x$ et c'est donc un corps fini à $q = p^n$ éléments.
(Unicité) : Soit $K \subseteq \overline{\mathbb{F}}_p$ un corps fini à q éléments. Par la proposition précédente tous les éléments de K sont racines du polynôme $x^q - x$. Donc K est le corps de décomposition du polynôme $x^q - x$ sur $\mathbb{F}_p$.

D'aprés le théorème pour toute puissance $q = p^n$ du nombre premier p il existe un corps fini et un seul ayant q éléments (dans une cloture $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$). Ce corps est noté $\mathbb{F}_q$ et est appelé le corps fini à q éléments.

Proposition 5 *: Le groupe de Galois $Gal(\mathbb{F}_q/\mathbb{F}_p)$ (avec $q = p^n$) est cyclique d'ordre n engendré par $\sigma : \alpha \longrightarrow \alpha^p$.*

Preuve : $\sigma : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ donné par $\alpha \longmapsto \alpha^p$ est bien un automorphisme élément de $Gal(\mathbb{F}_q/\mathbb{F}_p)$. Si $m \geq 1$ est tel que $\sigma^m = Id_{\mathbb{F}_q}$ alors $\sigma^m(\alpha) = \alpha, \forall \alpha \in \mathbb{F}_q$, donc $\alpha^{p^m} - \alpha = 0, \forall \alpha \in \mathbb{F}_q$. Ceci veut dire que le polynôme $x^{p^m} - x$ a au moins $q = p^n$ racines et donc $p^m \geq p^n$ et $m \geq n$. Comme l'ordre du groupe de Galois est égal à n, on doit aussi avoir l'ordre de $\sigma = n$ et :

$$Gal(\mathbb{F}_q/\mathbb{F}_p) =< \sigma > .$$

Comme conséquence on obtient le résultat suivant qui caractérise les sous-corps de $\mathbb{F}_q$ avec $q = p^n$.

Proposition 6 *: Le corps fini $\mathbb{F}_{p^m}$ est un sous-corps de $\mathbb{F}_{p^n}$ si et seulement si m divise n.*

Preuve : Si m divise n, alors il ya un sous-groupe H de $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ d'ordre n/m puisque $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est cyclique d'ordre n. Soit K le sous-corps de $\mathbb{F}_{p^n}/\mathbb{F}_p$ fixé par H. Alors par la théorie de Galois on a $[K : \mathbb{F}_p] = m$ et donc $K = \mathbb{F}_{p^m}$, par l'unicité des corps finis. Inversement supposons que $\mathbb{F}_{p^m}$ est un sous-corps de $\mathbb{F}_{p^n}$. Alors $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$ divise le degré $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$.
Remarque : En adaptant un peu les preuves des deux dernières proposition, on arrive facilemment au faits suivants : Soit $q = p^s$ une puissence d'un nombre premier. Alors :
1) $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{q^n}$ pour tout $n \geq 1$.
2) $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est cyclique d'ordre n engendré par $\sigma : \alpha \longrightarrow \alpha^q$.
3) $\mathbb{F}_{q^m}$ est un sous-corps de $\mathbb{F}_{q^n}$ si et seulement si m divise n.

Terminons cette section par une étude rapide du groupe multiplicatif $\mathbb{F}_q^*$ du corps fini $\mathbb{F}_q$ à $q = p^n$ éléments.

Proposition 7 *: Le groupe multiplicatif $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ est cyclique (d'ordre $q-1$).*

Preuve : Soit $t \leq q-1$ le plus grand ordre des éléments du groupe $\mathbb{F}_q^*$. Par le théorème de structure des groupes abéliens finis, l'ordre de tout élément de $\mathbb{F}_q^*$ est racine du polynôme $x^t - 1$. Comme l'ordre de $\mathbb{F}_q^*$ est $q-1$ on doit avoir $t \geq q-1$. Comme $t \leq q-1$, on a $t = q-1$. Il existe donc un élément d'ordre $q-1$ qui engendre $\mathbb{F}_q^*$.

Définition 17 *: Un générateur de $\mathbb{F}_q^*$ est appelé un élément primitif de $\mathbb{F}_q$.*

On peut se demander quel est le nombre des éléments primitifs de $\mathbb{F}_q$:

Proposition 8 *: Il y a exactement $\phi(q-1)$ élément primitifs de $\mathbb{F}_q$ avec ϕ la fonction d'Euler :*

$$\phi(n) = \#\{m/pgcd(n,m) = 1\}.$$

Preuve : Si γ est un générateur de $\mathbb{F}_q^*$, alors γ^n est aussi un générateur si et seulement si $pgcd(n, q-1) = 1$.

2.2 Eléments conjugués

Soit $\overline{\mathbb{F}}_q$ la clôture algébrique de $\mathbb{F}_q$. Si p est la caractéristique de $\mathbb{F}_q$, il est clair que l'on a :

$$\overline{\mathbb{F}}_q = \overline{\mathbb{F}}_p$$

et on peut mieux identifier $\overline{\mathbb{F}}_q$:

Proposition 9 *: La clôture algébrique de $\mathbb{F}_q$ est :*

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

Preuve : Posons $K = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$. On vérifie facilement que K est un corps. De plus $K \subseteq \overline{\mathbb{F}}_q$ (car $\mathbb{F}_{q^n} \subset \overline{\mathbb{F}}_q$ pour tout n). Il reste à montrer l'inclusion inverse. Soit $f(X) = \sum_{i=0}^{s} a_i X^i$ un polynôme non constant à coefficients dans

K. Pour tout $0 \leq i \leq s$, on a $a_i \in \mathbb{F}_{q^{m_j}}$ pour un certain $m_j \geq 1$. Donc f est un polynôme à coefficients dans $\mathbb{F}_{q^m}$ avec $m = \prod_{i=0}^{s} m_i$. Soit α une racine de f. Alors $\mathbb{F}_{q^m}(\alpha)$ est une extension algébrique finie de $\mathbb{F}_{q^m}$. Donc $\mathbb{F}_{q^m}(\alpha)$ est aussi un corps fini contenant $\mathbb{F}_q$. Si r le degré de $\mathbb{F}_{q^m}(\alpha)$ sur $\mathbb{F}_{q^m}$, alors $\mathbb{F}_{q^m}(\alpha)$ contient exactement q^{rm} éléments. Autrement dit on a $\mathbb{F}_{q^m}(\alpha) = \mathbb{F}_{q^{rm}}$ et $\alpha \in K$.

Soit $\alpha \in \overline{\mathbb{F}}_q$ et soit $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Définition 18 *: L'élément $\sigma(\alpha)$ est appelé le conjugué de α par rapport à $\mathbb{F}_q$.*

Soit le morphisme :

$$\pi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$$

donné par $x \longmapsto \pi(x) = x^q$. π est un $\mathbb{F}_q$-automorphisme de $\overline{\mathbb{F}}_q$ et c'est donc un élément de $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. On l'appelle l'automorphisme de Frobenius. La proposition suivante montre son utilité.

Proposition 10 *: L'ensemble des conjugués d'un élément $\alpha \in \overline{\mathbb{F}}_q$ par rapport à $\mathbb{F}_q$ est égal à l'ensemble :*

$$\{\pi^i(\alpha), i = 0, 1, 2, \ldots\}$$

avec $\pi \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ l'automorphisme de Frobenius.

Preuve : On sait que :

$$\overline{\mathbb{F}}_q = \bigcup_{m \geq 1} \mathbb{F}_{q^m}$$

Si $\alpha \in \overline{\mathbb{F}}_q$, alors il existe $m \geq 1$ tel que $\alpha \in \mathbb{F}_{q^m}$. Soit $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Alors $\sigma_{|\mathbb{F}_{q^m}}$ et $\pi_{|\mathbb{F}_{q^m}}$ sont des éléments de $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ et on sait que

$$\pi_{|\mathbb{F}_{q^m}} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$$

qui envoie α vers α^q, est un générateur de Gal $(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Donc

$$\sigma_{|\mathbb{F}_{q^m}} = (\pi_{|\mathbb{F}_{q^m}})^i.$$

pour un certain $i \geq 0$, et donc

$$\sigma(\alpha) = \sigma_{|\mathbb{F}_{q^m}}(\alpha) = (\pi_{|\mathbb{F}_{q^m}})^i(\alpha) = \pi^i(\alpha).$$

On peut encore être plus precis :

Proposition 11 *: Tous les conjugués de $\alpha \in \overline{\mathbb{F}}_q$ par rapport à $\mathbb{F}_q$ sont*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

où m est le plut petit entier tel que $\mathbb{F}_{q^m}$ contienne α i.e $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Preuve : La restriction $\pi_{|\mathbb{F}_{q^m}}$ de π à $\mathbb{F}_{q^m}$ est d'ordre m puisque c'est un générateur de $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Donc $\pi^m(\alpha) = (\pi_{|\mathbb{F}_{q^m}})^m(\alpha) = \alpha$ donc $\alpha, \pi(\alpha), \ldots$ et $\pi^{m-1}(\alpha)$ sont tous les conjugués de α. Il reste à montrer qu'ils sont tous distincts. Supposons $\pi^n(\alpha) = \alpha$, pour un $n \geq 1$. Alors $\pi^n(\beta) = \beta$, pour tout $\beta \in \mathbb{F}_q(\alpha)$ i.e $\beta^{q^n} - \beta = 0, \forall \beta \in \mathbb{F}_{q^m}$. Ainsi le polynôme $x^{q^n} - x$ a au moins q^m racines et donc $n \geq m$. Ceci prouve que $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$ sont tous distincts. On finit en remarquant que $\pi(\alpha) = \alpha^q$.

Comme application de ce dernier résultat essayons de déterminer le nombre de polynômes irréductibls unitaires sur $\mathbb{F}_q$ de degré donné n. Le lieu entre les éléments coujugués et les polynômes irréductubles est donné par la :

Proposition 12 *: Soit f un polynôme irréductible sur $\mathbb{F}_q$ de degré m et soit $\alpha \in \overline{\mathbb{F}}_q$ une racine de f. Alors $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ sont toutes les racines (distinctes) de f. De plus $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.*

Preuve : Remarquer que f n'a pas de racines dans $\mathbb{F}_q$ puisqu'il est irréductible sur $\mathbb{F}_q$. La preuve repose sur la remarque suivante : Si α est une racine de f alors $\sigma(\alpha)$ est aussi une racine de f, pour tout $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. En effet si $f(x) = a_0 + a_1(x) + \ldots + a_m(x^m)$ avec $a_0, a_1, \ldots, a_m \in \mathbb{F}_q$ et si $f(\alpha) = 0$, alors $a_0 + a_1\sigma(\alpha) + \ldots + a_m\sigma(\alpha)^m = \sigma(a_0 + a_1\alpha + \ldots + a_m\alpha^m) = \sigma(0) = 0$. Comme f a exactement m racines dans $\overline{\mathbb{F}}_q$ et que les conjugués de α sont au nombre de m, on obtient le résultat.
Remarque : Toutes les racines d'un polynôme irréductible f sur $\mathbb{F}_q$ sont donc distinctes et $\mathbb{F}_{q^m}$ est le corps de décomposition de f avec $m = degf$.

On aura aussi besoin du résultat suivant :

Proposition 13 *: Un polynôme irréductible unitaire de degér m sur $\mathbb{F}_q$ divise le polynôme $x^{q^n} - x$ si et seulement si m divise n.*

preuve : Soit $\alpha \in \overline{\mathbb{F}}_q$ une racine de f. On a donc $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$. Si m divise n alors $\mathbb{F}_{q^m}$ est un sous-corps de $\mathbb{F}_{q^n}$. Donc $\beta^{q^n} - \beta = 0$, $\forall \beta \in \mathbb{F}_{q^n}$ et donc $\alpha^{q^n} - \alpha = 0$. Comme f est le polynôme de plus petit degré qui anulle α, on obtient que f divise $x^{q^n} - x$.

Inversement si f divise $x^{q^n} - x$ alors $\alpha^{q^n} - \alpha = 0$ donc $\alpha \in \mathbb{F}_{q^n}$. Mais $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, donc m divise n.

Comme $x^{q^n} - x$ n'a pas de racines multiples, ce dernier résultat montre que le produit de tous les polynômes irréductibles unitaires sur $\mathbb{F}_q$ dont le degré divise n est egal à $x^{q^n} - x$. Cette remarque est suffisante pour démontrer le :

Théorème 2 *: Soit $I_q(n)$ le nombre de polynômes unitaires irréductibles sur $\mathbb{F}_q$ de degré $n \geq 1$. Alors on a :*

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

avec μ la fonction de Moebius définie sur $\mathbb{N}$ par :

$$\mu(d) = \begin{cases} 1 & \textit{si } d = 1. \\ (-1)^n & \textit{si } d = \textit{produit de } n \textit{ nombres premies distiucts.} \\ 0 & \textit{sinon.} \end{cases}$$

Preuve : Par la remarque précédente et en comparant les degrés des polynômes, on a :

$$q^n = \sum_{d|n} d I_q(d).$$

On obtient le résultat en appliquant la formule d'inversion de Moebius (si $g(n)$ et $f(n)$ sont des fonctions arithmétiques et si $g(n) = \sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} \mu(d) g(n/d)$)

2.3 Trace et Norme

On va étudier ici deux applications de $\mathbb{F}_{q^m}$ vers $\mathbb{F}_q$: la trace et la norme.

Définition 19 *: L'application Trace de $\mathbb{F}_{q^m}$ vers $\mathbb{F}_q$ est l'application :*

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$

définie par

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$$

avec $G = Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Si les corps $\mathbb{F}_{q^m}$ et $\mathbb{F}_q$ sont fixés, on la note tout simplement Tr. Pour tout élément $\tau \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$, on a :

$$\tau(Tr(\alpha)) = \tau(\sum_{\sigma \in G} \sigma(\alpha)) = \sum_{\sigma \in G} (\tau o \sigma)(\alpha)$$

$$= \sum_{\sigma \in G} \sigma(\alpha) = Tr(\alpha).$$

Ceci montre bien que Tr est une application de $\mathbb{F}_{q^m}$ vers $\mathbb{F}_q$. L'application Trace a quelques propriétés simples :
1) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta), \forall \alpha, \beta \in \mathbb{F}_{q^m}$
2) $Tr(a\alpha) = aTr(\alpha), \forall \alpha \in \mathbb{F}_{q^m}, \forall a \in \mathbb{F}_q$
3) $Tr(\sigma(\alpha)) = Tr(\alpha), \forall \sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ et $\forall \alpha \in \mathbb{F}_{q^m}$. En particulier

$$Tr(\pi(\alpha)) = Tr(\alpha^q) = Tr(\alpha)$$

avec $\pi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ le Frobenius.

Ces propriétés découlent directement de la définition de l'application Trace. Elles nous informent en particulier que Tr est une application linéaire quand on regarde $\mathbb{F}_{q^m}$ et $\mathbb{F}_q$ comme des espaces vectoriels $((1) + (2))$

On sait que le Frobenius π est un générateur de $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ puisqu'il est d'ordre m. Donc

$$Tr(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) = \sum_{i=0}^{m-1} \pi^i(\alpha) = \sum_{i=0}^{m-1} \alpha^i$$

Autrement dit la trace de α est la somme des conjugués de α.

Le résultat suivant étudie Tr en tant qu'application linéaire :

Proposition 14 *:*
1) $Tr : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ *est surjective. Son noyau* $Ker(Tr)$ *est donc un sous-espace de* $\mathbb{F}_{q^m}$ *de dimension* $m-1$ *sur* $\mathbb{F}_q$*.*
2) $\alpha \in \mathbb{F}_{q^m}$ *vérifie* $Tr(\alpha) = 0$ *si et seulement si* $\alpha = \pi(\beta) - \beta = \beta^q - \beta$ *pour un certain* $\beta \in \mathbb{F}_{q^m}$*.*

Preuve :
1) $\alpha \in \mathbb{F}_{q^m}$ est dans le noyau de Tr si et seulement si il est racine du polynôme $x + x^q + \ldots + x^{q^{m-1}}$ qui est de degré q^{m-1}. Donc le noyau de Tr contient au plus q^{m-1} éléments et il y a au moins $\frac{q^m}{q^{m-1}} = q$ éléments dans

l'image de Tr qui est un sous-ensemble de $\mathbb{F}_q$. L'image de Tr est donc égale à $\mathbb{F}_q$ et Tr est surjective. Comme $dim_{\mathbb{F}_q}\mathbb{F}_{q^m} = m$ et $dim_{\mathbb{F}_q}\mathbb{F}_q = 1$, on a $dim_{\mathbb{F}_q}Ker(Tr) = m - 1$.
2) Soit l'appplication $\mathbb{F}_q$-linéaire $\phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ donnée par $\gamma \longmapsto \pi(\gamma) - \gamma$. Par la proposition précédente $Im(\phi) \subseteq Ker(Tr)$. D'autre part $\phi(\gamma) = 0 \Leftrightarrow \pi(\gamma) = \gamma \Leftrightarrow \gamma \in \mathbb{F}_q$. Ainsi $Ker(\phi) = \mathbb{F}_q$. Donc $Im(\phi)$ contient $\frac{q^m}{q} = q^{m-1}$ éléments et donc $Im(\phi) = Ker(Tr)$ i.e $Tr(\alpha) = 0 \Leftrightarrow \alpha \in Im\phi \Leftrightarrow \exists \beta \in \mathbb{F}_{q^m}$ tel que $\alpha = \phi(\beta) = \pi(\beta) - \beta = \beta^q - \beta$.

Définition 20 *: L'application Norme de $\mathbb{F}_{q^m}$ vers $\mathbb{F}_q$ est l'application :*

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$

donnée par $\alpha \longmapsto \prod_{\sigma \in G} \sigma(\alpha)$, avec toujours $G = Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

On la note N si les corps $\mathbb{F}_{q^m}$ et $\mathbb{F}_q$ sont fixés. Pour $\tau \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ et $\alpha \in \mathbb{F}_{q^m}$, on a :

$$\tau(N(\alpha)) = \tau(\prod_{\sigma \in G} \sigma(\alpha)) = \prod_{\sigma \in G} (\tau \circ \sigma)(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = N(\alpha)$$

ce qui montre que N est bien une application de $\mathbb{F}_{q^m}$ vers $\mathbb{F}_q$. Comme pour la trace, l'application norme a des propriétés simples :
1) $N(\alpha.\beta) = N(\alpha).N(\beta), \forall \alpha, \beta \in \mathbb{F}_{q^m}$.
2) $N(a\alpha) = a^m N(\alpha), \forall \alpha \in \mathbb{F}_{q^m}, \forall a \in \mathbb{F}_q$.
3) $N(\sigma(\alpha)) = N(\alpha), \forall \sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ et $\alpha \in \mathbb{F}_{q^m}$. En particulier $N(\pi(\alpha)) = N(\alpha^q) = N(\alpha)$ avec π le Frobenius.
Ces propriétés découlent directement de la définition de la norme. Elles montrent en particulier que :

$$N : \mathbb{F}_{q^m}^* \longrightarrow \mathbb{F}_q^*,$$

est un morphiseme de groups multiplicatifs. Comme π est un générateur de $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$, on a :

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=0}^{q^{m-1}} \pi^i(\alpha)$$

Autrement dit la norme de α est le produit des conjugués de α. On finit avec la :

Proposition 15 *:*
1) $N : \mathbb{F}_{q^m}^* \longrightarrow \mathbb{F}_q^*$ *est surjective de noyau un groupe cyclique d'ordre* $\frac{q^m-1}{q-1}$.
2) $N_m(\alpha) = 1$ *pour* $\alpha \in \mathbb{F}_{q^m} \Leftrightarrow \alpha = \frac{\pi(\beta)}{\beta} = \beta^{q-1}$ *pour un certain* $\beta \in \mathbb{F}_q^*$.

Preuve : On utilise les mêmes arguments que pour la trace.

Chapitre 3

Codes correcteurs d'erreurs

Avec l'avènement de l'informatique et des nouvelles technologies, la transmission de l'information de manière sûre et fiable (sans altération et sans erreurs) est devenue d'une importance capitale. Les codes correcteurs d'erreurs ont été inventés justement pour permettre cela. Dans ce chapitre, on explique brièvement comment les corps finis interviennent dans la fabrication de ces codes. Il est organisé de la manière suivante : dans la première section, on définit les codes linéaires basés sur l'alphabet $\mathbb{F}_q$, le corps fini à q éléments. Dans la seconde section, on explique comment ces codes détectent et corrigent les erreurs qui peuvent survenir au cours du transfert de données informatiques. Enfin dans la troisième et dernière section, on illustre tout cela avec l'exemple important des codes de Reed-Solomon qui sont largement utilisés dans l'industrie informatique.

3.1 Codes linéaires

Soit $\mathbb{F}_q$ le corps fini à q éléments et soit

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n)/a_i \in \mathbb{F}_q, i = 1, \ldots, n\}.$$

le $\mathbb{F}_q$-espace vectoriel de dimension n.

Définition 21 *: Un code (linéaire) C (sur l'alphabet $\mathbb{F}_q$) est un sous-espace vectoriel $C \subseteq \mathbb{F}_q^n$. Les éléments de C sont appelés des mots de code, n est la longueur du code et $k = dim_{\mathbb{F}_q}(C)$ est sa dimension. On dit que C est un $[n, k]$ code.*

Si $a = (a_1, \ldots, a_n)$ et $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, la distance de Hamming entre a et b est :

$$d(a, b) = \#\{i/a_i \neq b_i\}$$

Autrement dit c'est le nombre de coordonnées en lesquelles a et b diffèrent. On l'appelle distance car elle définit une vraie distance sur $\mathbb{F}_q^n$ i.e une application :

$$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{R}_+$$

telle que :

1. $d(a, b) = 0 \Longleftrightarrow a = b$.
2. $d(a, b) = d(b, a)$.
3. $d(a, c) \leq d(a, b) + d(b, c)$.

pour tous $a, b, c \in \mathbb{F}_q^n$. Le poids d'un élément $a \in \mathbb{F}_q^n$ est défini par :

$$w(a) = d(a, 0) = \#\{i/a_i \neq 0\}$$

La distance minimum $d(C)$ d'un code $C \neq 0$ est :

$$d(C) = min\{d(a, b)/a, b \in C, a \neq b\}$$

Comme $d(a, b) = d(a - b, 0) = w(a - b)$, elle est aussi donneé par :

$$d(C) = min\{w(c)/0 \neq c \in C\}$$

Un $[n, k]$ code de distance minimum d est appelé un $[n, k, d]$ code.

La manière la plus simple pour décrire un code C est de donner une base $\{v_1, v_2, \ldots, v_k\}$ de C. Si $v_i = (v_{i1}, \ldots, v_{in}), i = 1, \ldots, k$, alors l'application

$$E : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

Donnée par

$$E(a_1, \ldots, a_k) = \sum_{i=1}^{k} a_i v_i = (\sum_{i=1}^{k} a_i v_{i1}, \ldots, \sum_{i=1}^{k} a_i v_{in}).$$

peut-être vue comme un moyen d'encoder des mots dans $\mathbb{F}_q^k$ (qui est ainsi identifié à l'ensemble des mots d'un langage naturel). Appliquer E à un élément de $\mathbb{F}_q^k$ (un mot), c'est le coder et le transformer en un mot de code

$E(a) \in C \subset \mathbb{F}_q^n$. La matrice $G = (v_{ij})_{i,j}$ est appelée la matrice génératrice du code C. Ses lignes sont les vecteurs $v_1, \ldots, v_k$ de la base de C.

L'idée du codage est donc la suivante : l'application de codage E envoie un mot (élément) m de $\mathbb{F}_q^k$ vers $\mathbb{F}_q^n$. Si $E(m) \in C$, on dit que le mot a eté envoyé sans erreurs. Si $E(m) \notin C$ alors le mot a été envoyé avec des erreurs. Corriger ces erreurs revient à trouver l'élément de C le plus proche (pour la distance de Hamming). L'application de codage E envoie un vecteur de k coordonnées vers un vecteur de n coordonnées. Comme $k \leq n$, l'information contenue dans un mot de code $c \in C$ dépend de k de ses coordonnées. Le reste est de l'information redondante utilisée pour contrôler si $c \in C$ ou non.

Définition 22 *: Le niveau d'information d'un $[n, k]$ code C est $i(C) = \frac{k}{n}$.*

$i(C)$ mesure le quotient entre le nombre de coordonnées du mot de départ et le nombre total de coordonnées reçues aprés l'encodage.

Une autre manière pour décrire un code C est à travers ce qu'on appelle sa matrice de parité ou sa matrice de contrôle. Définissons le produit scalaire canonique sur $\mathbb{F}_q^n$ par

$$< a, b >= \sum_{i=1}^{n} a_i b_i.$$

si $a = (a_1, \ldots, a_n)$ et $b = (b_1, \ldots, b_n)$.

Définition 23 *: Si $C \subseteq \mathbb{F}_q^n$ est un code, son dual est*

$$C^{\perp} = \{u \in \mathbb{F}_q^n / < u, c >= 0, \forall c \in C\}$$

Comme $C^{\perp}$ est un sous-espace de $\mathbb{F}_q^n$, c'est aussi un code linéaire. C est auto-dual (respectivement auto-orthogonal) si $C = C^{\perp}$ (respectivement $C \subseteq C^{\perp}$). Par le cours d'algebre linéaire, le dual d'un $[n, k]$ code est un $[n, n-k]$ code et $(C^{\perp})^{\perp} = C$.
La matrice de contrôle de C est la matrice génératrice H de $C^{\perp}$. Si C est un $[n, k]$ code, H est une matrice $(n-k) \times n$ et on a :

$$C = \{u \in \mathbb{F}_q^n / H.u^t = 0\}$$

avec u^t le transposé de u. Autrement dit H contrôle si $u \in C$ ou non. La matrice H définit une application linéaire

$$H : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$$

et $c = (c_1, \ldots, c_n) \in C \iff H(c_1, \ldots, c_n) = 0$. Le terme matrice de parité vient de léxemple suivant :
Exemple : Soit $C \subseteq \mathbb{F}_2^{n+1}$ donné par

$$C = \{(x_1, \ldots, x_n, x_1 + \ldots + x_n)/(x_1, \ldots, x_n) \in \mathbb{F}_2^n\}.$$

En utilisant le fait que $a+a = 0$ dans $\mathbb{F}_2$, on obtient une autre caractérisation de C :

$$C = \{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{F}_2^{n+1} / \sum_{i=1}^{n+1} x_i = 0\}.$$

C'est donc le noyau de la forme linéaire :

$$\begin{array}{rcl} \mathbb{F}_2^{n+1} & \longrightarrow & \mathbb{F}_2 \\ (x_1, \ldots, x_{n+1}) & \longmapsto & \sum_{i=1}^{n+1} x_i \end{array}$$

C'est donc un hyperplan de $\mathbb{F}_2^{n+1}$ et $dim_{\mathbb{F}_2}(C) = n$. C'est un $[n+1, n]$ code. La matrice de parité de C est la matrice H de la forme linéaire plus haut. Donc

$$H = (1, 1, \ldots, 1).$$

Et on a ainsi

$$C = \{u \in \mathbb{F}_2^{n+1} / H.u^t = 0\}.$$

Dans cet exemple $c \in C$ si et seulement si c a un nombre pair de coordonnées non nulles et c'est pour cela que H est appelée la matrice de parité de C.

3.2 Correction et détection des erreurs

Un bon code est un code dans lequel deux mots de code sont trés différents l'un dans l'autre et donc trés eloigués l'un de l'autre pour la distance de Hamming. Ainsi si on recoit un mot avec des erreurs, il serait facile de le corriger en le remplacant par le mot de code le plus proche.

Définition 24 *: Un code C corrige t erreurs si pour tout $y \in \mathbb{F}_q^n$ il existe au plus un mot de code $c \in C$ tel que $d(c, y) \leq t$.*

Autrement dit si on reçoit un mot y avec au plus t erreurs, i.e y differè d'un mot de code $c \in C$ en au plus t coordonneés et si c est l'unique élément de C le plus proche de y, on code alors y en c. Dans ce sens on a la :

Proposition 16 *: Soit C un code de distance minimum $d = d(C)$. Alors C corrige $t = [\frac{d(C)-1}{2}]$ erreurs. ($[x]$ est la partie entière d'un nombre réel x ie $x = [x] + \epsilon$ avec $[x] \in \mathbb{Z}$ et $0 \leq \epsilon < 1$).*

Preuve : Soit $t = [\frac{d(C)-1}{2}]$. Supposons que C ne corrige pas t erreurs i.e qu'il existe $y \in \mathbb{F}_q^n$ et $c_1, c_2 \in C$ avec $c_1 \neq c_2$ et $d(c_i, y) \leq t, i = 1, 2$. Donc

$$d(c_1, c_2) \leq d(c_1, y) + d(y, c_2) \leq 2t.$$

Comme $c_1 \neq c_2$ et par définition de $d(C)$, on a aussi :

$$d(c_1, c_2) \geq 2t + 1,$$

contradiction. Donc si $y \in \mathbb{F}_q^n$ et si $c \in C$ vérifie $d(y, c) \leq t$ alors c est le seul mot de code qui vérifie $d(y, c) \leq t$.
Ainsi plus la distance minimum $d(C)$ d'un code C est grande et plus le code est bon dans le sens qu'il corrige beaucoup d'erreurs.
Remarque : On a déja introduit la notion de niveau d'information $i(C) = \frac{k}{n}$ d'un code avec $k = dim_{F_q}(C)$ et n la longueur du code. Plus $i(C)$ est grand i.e plus k est grand par rapport à n, plus le code rend beaucoup d'information. En combinant cela avec le résultat précédent, on arrive à la conclusion intéressante suivante : un bon code est un code dont la dimension k et la distance minimum d sont larges par rapport à sa longueur n. Malheureusement il y a des restrictions sur les valeurs que peuvent prendre k et d par rapport à n.

Proposition 17 *: Soit C un $[n, k, d]$ code sur l'alphabet $\mathbb{F}_q$. Alors on a toujours*

$$k + d \leq n + 1$$

Preuve : Soit $W \subseteq \mathbb{F}_q^n$ le sous-espace défini par : $W = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n / a_i = 0 \text{ pour } i \geq d\}$. Pour tout $a \in W$, on a $w(a) \leq d - 1$ et donc $W \cap C = \{0\}$. Comme $dim(W) = d - 1$, on a :

$$k + (d - 1) = dim(C) + dim(W) = dim(C + W) + dim(C \cap W)$$

$$= dim(C + W) \leq n$$

Ainsi les codes qui vérifient $k + d = n + 1$ sont les meilleurs possibles. On les appele des codes MDS (maximum distance separable).

Soit C un $[n, k]$ code donné par sa matrice de parité H i.e comme noyau de l'application :

$$H : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$$

Définition 25 *: Si $x \in \mathbb{F}_q^n$, son syndrome est $H(x)$.*

Pour tout $v \in \mathbb{F}_q^{n-k}$, choisissons un $e_v \in \mathbb{F}_q^n$ tel que $H(e_v) = v$ et tel que $w(e_v)$ soit minimal dans $H^{-1}(v)$ (ie e_v de poids minimum). e_v est appelé le coset leader de $H^{-1}(v)$. Il peut ne pas être unique, mais on en fait un choix une fois pour toute.
Voici comment on utilise les syndromes et les coset leader pour décoder un mot y i.e pour retrouver le vrai mot envoyé $c \in C$. On calcule le syndrome de y, $H(y) = v$. Si e_v est le coset leader correspondant, on corrige en posant

$$c = y - e_v$$

et on a bien :

$$H(c) = H(y - e_v) = H(y) - H(e_v) = v - v = 0.$$

et donc $c \in C$. Remarquer aussi que $d(c, y) = w(e_v)$ (par déffinition de e_v) et donc c et le mot de code le plus proche de y. Si donc C corrige t erreurs, le processus de décodage va nous redonner le vrai mot envoyé au depart (i.e les erreurs auront été corrigées) pourvu que le mot envoyé y ait pour syndrome v tel que $w(e_v) \leq t$.

3.3 Les codes de Reed-Solomon

Les codes de Reed-Solomon forment une classe importante en théorie des codes. Nous les présentons ici comme exemple illustrant toute la théorie.

Posons $n = q - 1$ et soit $\beta \in \mathbb{F}_q$ un élément primitif i.e un générateur du groupe multiplicatif $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$:

$$\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^n = 1\}$$

Pour tout entier $1 \leq k \leq n$, on considère l'espace vectoriel sur $\mathbb{F}_q$:

$$L_k = \{f \in \mathbb{F}_q[X] / deg(f) \leq k - 1\}$$

La dimension de L_k est k. En effet $\{1, X, \ldots, X^{k-1}\}$ est une base de L_k. On considère aussi l'application :

$$g : L_k \longrightarrow \mathbb{F}_q^n$$

donnée par :

$$g(f) = (f(\beta), \ldots, f(\beta^n)) \in \mathbb{F}_q^n$$

g est donc l'application évaluation de f en $\beta, \beta^2, \ldots, \beta^n$.

Proposition 18 *: g est $\mathbb{F}_q$-linéaire et est injective.*

Preuve : g est evidemment linéaire. Qu'elle soit injective résulte du fait que tout polynôme non nul $f \in \mathbb{F}_q[X]$ de degré plus petit que n a moins de n racines.
Comme conséquence, on obtient que :

$$C_k = \{g(f), f \in L_k\} = \{f(\beta), \ldots, f(\beta^n, f \in L_k)\}$$

est un sous-espace vectoriel de $\mathbb{F}_q^n$ (comme image de L_k par g) et C_k est donc un code linéaire sur $\mathbb{F}_q$ de dimension k et de longueur n i.e un $[n, k]$ code.

Définition 26 *: Les codes C_k sont appelés des codes de Reed-Solomon ou des codes RS.*

Les codes de Reed-Solomon sont de bons codes comme le montre le :

Théorème 3 *: Les codes de Reed-Solomon sont des codes MDS.*

Preuve : Le poids d'un mot de code $0 \neq c = g(f) \in C_k$ est donné par :

$$w(c) = n - \mid \{i \in \{1, \ldots, n\}/f(\beta^i = 0\} \mid$$

$$\geq n - deg(f) \geq n - (k - 1)$$

Ainsi la distance minimum d de C_k vérifie :

$$d \geq n + 1 - k$$

D'autre part comme démontré précedemment on a toujours :

$$d \leq n + 1 - k$$

Donc $d = n + 1 - k$.

Bibliographie

[1] J.Calais, Extensions de Corps, Mathématiques à l'Université, Ellipses, 2006.

[2] I.Stewart, Galois Theory, Third Edition, Chapman & Hall, 2006.

[3] Lidl. Rudolf, Introduction to Finite Fields and Their Applications, University of Tasmania, Habart, Australia, 1986.

[4] Jim Carlson, Error Correcting Codes, An Introduction Through Problems, November 19, 1999.

[5] I. El Hage, Théorie de Galois, 2001.