

Introduction aux corps finis et aux sommes de Gauss et de Jacobi

Jean-Pierre Cherdieu

► **To cite this version:**

Jean-Pierre Cherdieu. Introduction aux corps finis et aux sommes de Gauss et de Jacobi. 3rd cycle. La Havane (Cuba), 2000, pp.18. cel-00374738

HAL Id: cel-00374738

<https://cel.archives-ouvertes.fr/cel-00374738>

Submitted on 9 Apr 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Introduction aux corps finis et aux sommes de Gauss et de Jacobi

Ecole du CIMPA-UNSA-ICTP-UNESCO-ICIMAF,
Algebraic Geometry and its Applications
to Cryptography and Error Correcting Codes
La Havane (Cuba), 20 Novembre 2000 - 01 Décembre 2000

Jean-Pierre Cherdieu.*

*Département de Mathématiques et Informatique. Université des Antilles et de la Guyane. Campus de Fouillole, F97159 Pointe-à-Pitre CEDEX. e-mail : jpcherdi@univ-ag.fr

Table des matières

1	Quelques rappels en théorie des corps	3
2	Propriétés des corps finis	3
2.1	les sous-corps de \mathbb{F}_q	5
3	Construction des corps finis	5
4	Automorphisme de Frobenius, Norme et Trace	6
4.1	Groupe de Galois d'une extension finie, Trace et Norme	6
5	Les sommes exponentielles	7
5.1	Caractères additifs et multiplicatifs d'un corps fini	7
5.1.1	les caractères additifs de \mathbb{F}_q	8
5.1.2	les caractères multiplicatifs de \mathbb{F}_q	8
5.2	la relation d'orthogonalité	9
6	les sommes de Gauss	9
6.1	Définition et premières propriétés	9
7	les sommes de Jacobi	10
7.1	Définition et premières propriétés	10
7.2	le théorème de Stickelberger	12
7.2.1	le symbole de résidu m -ique	12
7.2.2	Quand l'anneau $\mathbb{Z}[\zeta]$ est principal	14
8	Applications des sommes exponentielles	15
8.1	Avec les caractères additifs	15
8.2	Avec les caractères multiplicatifs	15
8.2.1	Nombre de solutions de l'équation $\alpha_1 x_1^{k_1-1} + \dots + \alpha_n x_n^{k_n-1} =$ α dans \mathbb{F}_q^n	15

1 Quelques rappels en théorie des corps

Soient $(K, +, \times)$ un corps et k un sous-ensemble de K . Si $(k, +, \times)$ est lui aussi un corps, on dira que K est une extension de k , et on note K/k . On dit aussi que k est un sous-corps de K . Si le seul sous-corps de K est K lui-même, on dira que K est un corps *simple*.

Comme l'intersection de deux sous-corps de K est encore un sous-corps de K , on en déduit que l'intersection de tous les sous-corps de K est encore un sous-corps de K (le plus petit) et on l'appellera le *sous-corps premier* de K . Ce sous-corps premier est bien sur un corps simple. On établit alors que :

Théorème 1.1 *Les seuls corps simples sont \mathbb{Q} et les $\mathbb{F}_p = GF(p) = \mathbb{Z}/p\mathbb{Z}$, avec p premier.*

Les corps dont le sous-corps premier est \mathbb{Q} sont dits de *caractéristique 0*, et ceux dont le sous-corps est \mathbb{F}_p de *caractéristique p* .

Si $\alpha \in K$ et $\alpha \notin k$, le sous-corps de K engendré par k et α est $k(\alpha) = \{f(\alpha)/g(\alpha) \mid f, g \in k[X], g(\alpha) \neq 0\}$. On dit que $k(\alpha)$ est une extension simple ou monogène de k . En particulier si α est racine d'un polynôme irréductible à coefficients dans k , on dit que $k(\alpha)$ est une extension algébrique de k . Ce corps $k(\alpha)$ est un *corps de rupture* pour g , mais toutes les racines de g ne sont pas nécessairement dans $k(\alpha)$. Si l'on veut une extension minimale contenant toutes les racines de g , on introduit la notion de *corps de décomposition* de g sur k ;

Définition 1.1 *Soient K une extension de k , $g(X) \in k[X]$ et $\deg(g) = n$. On dit que K est un corps de décomposition de g sur k si :*

1. $\exists a \in K$ et $\alpha_1, \dots, \alpha_n \in K$ tels que $g(x) = a(X - \alpha_1) \dots (X - \alpha_n)$,
2. $K = k(\alpha_1, \dots, \alpha_n)$.

Pour un $g(X)$ donné, un tel corps existe toujours ; De plus deux corps de décomposition pour g sont isomorphes ; Ainsi on parlera du corps de décomposition de g (à isomorphisme près).

2 Propriétés des corps finis

Concentrons nous maintenant sur les corps finis, c'est à dire ceux qui ont un nombre fini d'éléments. Notons tout d'abord que , selon un théorème de Wedderburn, **tout corps fini est commutatif**. On a alors :

Proposition 2.1 *Soit K un corps fini à q éléments, alors $q = p^n$ où p est un nombre premier et $n \in \mathbb{N}$.*

Preuve : Comme K est un corps fini, il a comme caractéristique un nombre premier p . Notons \mathbb{F}_p ce sous-corps premier de K . Ce dernier peut être vu comme un \mathbb{F}_p -espace vectoriel de dimension finie n . Ainsi tout élément $v \in K$ s'écrit de manière unique

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n,$$

où les $(v_i)_i$ forment une base de K et les $(\alpha_i)_i$ sont dans K . Donc

$$\#K = p^n.$$

■

Cette proposition, si elle donne la taille des corps finis, n'en prouve pas pour autant l'existence. De même elle ne dit pas s'il existe plusieurs types de corps finis à q éléments. C'est le but de la proposition suivante.

Théorème 2.1 *Pour tout nombre premier p et tout entier $n \in \mathbb{N}$, il existe un unique corps fini à $q = p^n$ éléments, c'est le corps de décomposition de $X^q - X$.*

Preuve : Prouvons tout d'abord l'existence d'un tel corps. Soit F le corps de décomposition de $X^q - X$ sur \mathbb{F}_p et $S = \{\alpha \in F \mid \alpha^q = \alpha\}$. On a, d'une part $S \subset F$.

D'autre part, puisque $(\alpha_i \alpha_j)^q = \alpha_i^q \alpha_j^q$ et $(\alpha_i + \alpha_j)^q = \alpha_i^q + \alpha_j^q$, on peut déduire que S est un corps. Comme F est le plus petit corps sur lequel $P(X) = X^q - X$ se factorise, on en déduit que $F = S$.

De plus comme $P'(X) = -1 \neq 0$, les racines de $P(X)$ sont toutes distinctes. On a alors $\text{Card}(F) = \text{Card}(S) = q$.

L'unicité, quant à elle, est une conséquence directe de l'unicité du corps de décomposition d'un polynôme. ■

Pour bien décrire le corps fini à q éléments le résultat suivant est important.

Théorème 2.2 *Le groupe \mathbb{F}_q^\times est cyclique.*

Preuve : Si r est l'annulateur de \mathbb{F}_q^\times ¹ alors $x^r = 1$ pour tout $x \in \mathbb{F}_q^\times$. On en déduit que \mathbb{F}_q^\times est un sous-groupe du groupe cyclique des racines r -ièmes de l'unité, donc cyclique lui-même. ■

¹L'annulateur de \mathbb{F}_q^\times est le plus petit entier r tel que $x^r = 1$.

Un élément générateur de \mathbb{F}_q^\times s'appelle *un élément primitif* de \mathbb{F}_q .

Exemple : Le corps $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ avec $\alpha^2 + \alpha + 1 = 0$.

2.1 les sous-corps de \mathbb{F}_q

Pour les trouver on utilise le résultat suivant :

Lemme 2.1 *Soient m et n deux entiers positifs. Alors*

$$(X^m - 1) \mid (X^n - 1) \iff m \mid n.$$

Preuve : Si $n = bm + r$, alors,

$$X^n - 1 = X^r \left(\sum_{i=0}^{b-1} X^{im} \right) (X^m - 1) + X^r - 1.$$

il s'ensuit que $(X^m - 1) \mid (X^n - 1)$ ssi $X^r - 1 = 0$ i.e. $r = 0$. Autrement dit ssi $m \mid n$. ■

Conséquence :

Théorème 2.3 *Le corps \mathbb{F}_{p^m} est un sous-corps de \mathbb{F}_{p^n} si et seulement si $m \mid n$.*

3 Construction des corps finis

Le théorème clef pour la construction d'un corps fini à $q = p^n$ éléments est le suivant :

Théorème 3.1 *Soit $\theta \in F/K$ et soit g le polynôme minimal de θ sur K . Alors :*

1. $K(\theta)$ est isomorphe à $K[X]/(g)$.
2. Une base de $K(\theta)$ sur K est $\{1, \theta, \theta^2, \dots, \theta^{\deg(g)-1}\}$.

Exemple : On prend $g(x) = x^2 + x + 1$. C'est un polynôme unitaire et irréductible sur \mathbb{F}_2 . On note α une de ses racines et on a :

$$\mathbb{F}_2(\alpha) \sim \mathbb{F}_2[X]/(g),$$

et $\{1, \alpha\}$ est une base de $\mathbb{F}_2(\alpha)$.

On a

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1 = \alpha^2\}.$$

4 Automorphisme de Frobenius, Norme et Trace

4.1 Groupe de Galois d'une extension finie, Trace et Norme

La théorie de Galois pour les corps finis donne le résultat suivant :

Proposition 4.1 *Le groupe de Galois $G = Gal(\mathbb{F}_{q^s}/\mathbb{F}_q)$ de l'extension $\mathbb{F}_{q^s}/\mathbb{F}_q$ est cyclique et d'ordre s . Il est engendré par l'endomorphisme de Frobenius de \mathbb{F}_q , noté F , défini par $F(x) = x^q$. De plus il est isomorphe à $\mathbb{Z}/s\mathbb{Z}$.*

Remarque : L'homomorphisme de Frobenius est en fait un automorphisme. Les conjugués de x sont les x^{q^j} pour $j = 1, \dots, s-1$. On définit alors l'application *Trace*, $Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q} : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_q$ et l'application *Norme*, $N_{\mathbb{F}_{q^s}/\mathbb{F}_q} : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_q$ d'un élément de \mathbb{F}_{q^s} en posant :

$$Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) = x + x^q + \dots + x^{q^{s-1}},$$

et

$$N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) = x \cdot x^q \cdot \dots \cdot x^{q^{s-1}}.$$

Les principales propriétés de ces deux applications sont énumérées dans les propositions qui suivent.

Proposition 4.2 *Soient x et y deux éléments de \mathbb{F}_{q^s} et $c \in \mathbb{F}_q$, alors :*

1. $Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) \in \mathbb{F}_q$.
2. $Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x + y) = Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) + Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(y)$.
3. $Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(cx) = cTr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x)$.

Proposition 4.3 *L'application $Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q} : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_q$ est surjective, et*

$$Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) = 0 \iff \exists y \in \mathbb{F}_{q^s}, \text{ tel que } x = y^q - y.$$

Enfin, si r, s sont deux entiers, tels que $r \mid s$ (Il s'en suit que $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$), on a :

$$Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q} = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q} \circ Tr_{\mathbb{F}_{q^s}/\mathbb{F}_{q^r}}.$$

De même on a :

Proposition 4.4 Soient x et y deux éléments de \mathbb{F}_{q^s} et $c \in \mathbb{F}_q$, alors :

1. $N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) \in \mathbb{F}_q$.
2. $N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(xy) = N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) \cdot N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(y)$.
3. $N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(cx) = c^s N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x)$.

Théorème 4.1 (Théorème 90 de Hilbert) L'application $N_{\mathbb{F}_{q^s}/\mathbb{F}_q} : \mathbb{F}_{q^s}^\times \longrightarrow \mathbb{F}_q^\times$ est surjective, et

$$N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(x) = 1 \iff \exists y \in \mathbb{F}_{q^s}^\times, \text{ tel que } x = y^{q-1}.$$

Si r, s sont deux entiers, tels que $r \mid s$ on a :

$$N_{\mathbb{F}_{q^s}/\mathbb{F}_q} = N_{\mathbb{F}_{q^r}/\mathbb{F}_q} \circ N_{\mathbb{F}_{q^s}/\mathbb{F}_{q^r}}.$$

5 Les sommes exponentielles

5.1 Caractères additifs et multiplicatifs d'un corps fini

Soient (G, \cdot) un groupe, et \mathcal{U} l'ensemble des nombres complexes de module 1. On appelle *caractère* de G tout homomorphisme f de G dans \mathcal{U} . En particulier

- si $(G, \cdot) = (\mathbb{F}_q, +)$, les caractères vérifient $\chi(x+y) = \chi(x)\chi(y)$, on les appelle *les caractères additifs* de \mathbb{F}_q .
- Si $(G, \cdot) = (\mathbb{F}_q^\times, \cdot)$, les caractères vérifient $\lambda(xy) = \lambda(x)\lambda(y)$ et sont appelés *les caractères multiplicatifs* de \mathbb{F}_q^\times .

L'ensemble des caractères de G se note \widehat{G} . Si on le munit de la multiplication $(\chi_1 \cdot \chi_2)(x) = \chi_1(x) \cdot \chi_2(x)$ il forme un groupe, appelé *dual* de G dont l'élément neutre est le caractère trivial ε défini par $\varepsilon(x) = 1 \forall x \in G$, et l'inverse de χ est $\chi^{-1}(x) = \overline{\chi(x)}$. En particulier dans le cas de \mathbb{F}_q , pour les caractères additifs $\chi^{-1}(x) = \chi(-x)$, et pour les caractères multiplicatifs $\lambda^{-1}(x) = \lambda(x^{-1})$.

5.1.1 les caractères additifs de \mathbb{F}_q

En fait on sait décrire tous les caractères additifs de \mathbb{F}_q . Il est facile de vérifier que l'application $\chi(x) = \exp\left(\frac{2i\pi \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}{p}\right)$ est un caractère additif de \mathbb{F}_q . On a

Proposition 5.1 (cf. [7] pro. 1 p.37) Soit χ un caractère additif non trivial et, pour tout x et tout y dans \mathbb{F}_q posons

$$\chi_y(x) = \chi(yx).$$

Alors l'application $y \longrightarrow \chi_y$ est un isomorphisme de k sur le groupe des caractères additifs.

Preuve : Il suffit de montrer que cette application est injective. Mais si $y_1 \neq y_2$ le caractère $\chi_{y_1 y_2^{-1}} \neq \varepsilon$. Donc il existe $x \in \mathbb{F}_q$ telque $\chi_{y_1 y_2^{-1}}(x) \neq 1$. ■

Remarque : La proposition précédente dit que les caractères additifs de \mathbb{F}_{q^s} sont de la forme :

$$\chi_y^{(s)}(x) = \exp\left(2i\pi \frac{\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(yx)}{p}\right).$$

Mais vu que

$$\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p} = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \circ \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q},$$

on a,

$$\chi^{(s)} = \chi \circ \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}.$$

5.1.2 les caractères multiplicatifs de \mathbb{F}_q

Soit g est un élément générateur du groupe multiplicatif \mathbb{F}_q^\times , alors pour tout $x \in \mathbb{F}_q^\times$ il existe $k \in \mathbb{N}$ tel que $x = g^k$. On pose alors

$$\lambda(x) = \exp\left(2i\pi \frac{k}{q-1}\right).$$

C'est un caractère multiplicatif d'ordre $q-1$. L'application $h \longrightarrow \lambda^h$ est un isomorphisme de $\mathbb{Z}/(q-1)\mathbb{Z}$ sur le groupe des caractères multiplicatifs de \mathbb{F}_q .

Remarque : On obtient des caractères multiplicatifs de \mathbb{F}_{q^s} en posant :

$$\lambda^{(s)} = \lambda \circ N_{\mathbb{F}_{q^s}/\mathbb{F}_q}.$$

5.2 la relation d'orthogonalité

Pour calculer avec les caractères d'un groupe, l'on dispose de la relation suivante.

Théorème 5.1 *Soit χ un caractère du groupe G , alors :*

1.

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & \text{si } \chi \neq \epsilon, \\ \text{card}(G) & \text{si } \chi = \epsilon, \end{cases}$$

2.

$$\sum_{x \in \widehat{G}} \chi(x) = \begin{cases} 0 & \text{si } x \neq 0, \\ \text{card}(\widehat{G}) & \text{si } x = 0. \end{cases}$$

6 les sommes de Gauss

6.1 Définition et premières propriétés

Dans cette partie χ désignera un caractère additif de \mathbb{F}_q et λ un caractère multiplicatif. On suit ici l'exposé de Joly [7]. On rappelle que λ est défini sur \mathbb{F}_q^\times . On convient de l'étendre à \mathbb{F}_q tout entier en posant $\lambda(0) = 1$ si λ est le caractère trivial et $\lambda(0) = 0$ sinon. On pose alors :

Définition 6.1 *La somme de Gauss, notée $G(\chi, \lambda)$, associée à χ et à λ est la quantité*

$$G(\chi, \lambda) = \sum_{x \in \mathbb{F}_q} \chi(x)\lambda(x).$$

Il n'y a pas de formule générale donnant la valeur d'une somme de Gauss. On dispose cependant de certaines informations.

1. Si λ est trivial, mais non χ , on a : $G(\chi, \lambda) = -1$.
2. Si χ est trivial, mais non λ , on a : $G(\chi, \lambda) = 0$.
3. Si χ et λ sont triviaux, alors $G(\chi, \lambda) = q - 1$.

Mais on a toujours,

Proposition 6.1 *Si $\lambda \neq \varepsilon$,*

$$G(\chi, \lambda)G(\chi, \bar{\lambda}) = q\lambda(-1).$$

On a aussi,

Proposition 6.2 *Si $\lambda \neq \varepsilon$, alors $|G(\chi, \lambda)| = \sqrt{q}$.*

7 les sommes de Jacobi

7.1 Définition et premières propriétés

Dans cette partie on ne présentera que les sommes de Jacobi à deux caractères. Pour une généralisation à plusieurs caractères on consultera cf. [6], [7] ou encore [11] et [1]. On note $\mathbb{X} = \mathbb{X}(\mathbb{F}_q^\times)$ le groupe des caractères multiplicatifs de \mathbb{F}_q^\times .

Définition 7.1 *La somme de Jacobi associée au couple $(\psi, \lambda) \in \mathbb{X}$ est*

$$j(\psi, \lambda) = \sum_{x+y=1} \psi(x)\lambda(y),$$

où x et y sont dans \mathbb{F}_q^\times . L'ordre de la somme de Jacobi est le ppcm des ordres de ψ et λ . Une somme de Jacobi d'ordre m est un entier du corps cyclotomique $\mathbb{Q}(\zeta_m)$ avec $\zeta_m = \exp(2i\pi/m)$.

La détermination des sommes de Jacobi est aussi un problème ouvert. Pour un état de l'art on consultera le livre de Berndt, Evans et Williams, la "bible" en la matière, cf. [1]. Toutefois on dispose des résultats suivants :

1. Si ψ et λ sont triviaux alors $j(\psi, \lambda) = q$.
2. Si $\psi = \varepsilon$ et $\lambda \neq \varepsilon$, alors $j(\psi, \lambda) = 0$.
3. Si ψ et λ sont non triviaux, mais que $\psi\lambda$ l'est, alors $j(\psi, \lambda) = -\psi(-1)$.

Proposition 7.1 *Si $\psi\lambda$ n'est pas trivial, alors*

1.

$$j(\psi, \lambda) = \frac{G(\psi)G(\lambda)}{G(\psi\lambda)},$$

2. Si de plus ψ, λ , ne sont pas triviaux,

$$|j(\psi, \lambda)| = q^{\frac{1}{2}}.$$

Remarque : Cette deuxième égalité n'est autre qu'un système d'équations Diophantiennes dont les inconnues sont les coordonnées de $j(\psi, \lambda)$ dans une base de $\mathbb{Z}[\zeta_{ppcm(ord(\psi), ord(\lambda))}]$. D'autres indications sur ces coefficients nous sont données par les théorèmes suivants :

Théorème 7.1 Soient λ_1 et λ_2 deux caractères multiplicatifs d'ordre respectifs k_1 et k_2 ($k_1 \neq k_2$), et soit $\zeta_j = \exp(2i\pi/k_j)$, alors

$$j(\lambda_1, \lambda_2) \equiv -q \pmod{(1 - \zeta_1)(1 - \zeta_2)}.$$

Preuve : On a d'une part

$$A := \sum_{u+v=1} (1 - \lambda_1(u))(1 - \lambda_2(v)) \equiv 0 \pmod{(1 - \zeta_1)(1 - \zeta_2)},$$

et d'autre part

$$A := \sum_{u+v=1} 1 - \sum_{u+v=1} \lambda_1(u) - \sum_{u+v=1} \lambda_2(v) + \sum_{u+v=1} \lambda_1(u)\lambda_2(v) = q + \sum_{u+v=1} \lambda_1(u)\lambda_2(v).$$

■

Théorème 7.2 Soient λ_1 et λ_2 deux caractères multiplicatifs d'ordre $k > 2$ et $\zeta_k = \exp(2i\pi/k)$, alors

$$j(\lambda_1, \lambda_2) \equiv -1 \pmod{(1 - \zeta)^2}.$$

Remarque : Si k est un nombre premier supérieur à 3 l'exposant 2 est remplacé par 3 cf. [4] et [5].

On a aussi souvent besoin de la décomposition en produit d'idéaux premiers de l'idéal engendré par $j(\lambda_1, \lambda_2)$. C'est le but du théorème de stickelberger.

7.2 le théorème de Stickelberger

7.2.1 le symbole de résidu m -ique

Soient m un entier positif et $\mathbb{Q}[\zeta_m]$ le m -ième corps cyclotomique. on a :

Théorème 7.3 *Soit p un nombre premier $p \nmid m$. Soit f le plus petit entier tel que $p^f \equiv 1 \pmod{m}$, alors*

$$(p) = \mathfrak{p}_1 \dots \mathfrak{p}_g,$$

avec $g = \varphi(m)/f$ (φ est la fonction d'Euler).

Preuve : on consultera [6] p.196. ■

Remarque : Pour une approche algorithmique de la détermination de \mathfrak{p} on consultera le livre de H. Cohen cf. [2] p. 193.

Si vous disposez de Maple taper :

$$\text{Factor}(f(x)) \pmod{p};$$

où $f(x)$ est le polynôme qui définit l'extension $\mathbb{Q}[\zeta_m]/\mathbb{Q}$.

Si \mathfrak{p} un idéal premier de $\mathbb{Z}[\zeta_m]$ au dessus de p et ne contenant pas m . On sait que $\mathbb{Z}[\zeta_m]/\mathfrak{p}$ est un corps (puisque $\mathbb{Z}[\zeta_m]$ est un anneau de Dedekin), et on a

$$N(\mathfrak{p}) = \#(\mathbb{Z}[\zeta_m]/\mathfrak{p}) = q = p^f.$$

L'entier f s'appelle le *degré* de \mathfrak{p} .

Exemple : Si l'on prend $m = 10$ et $p = 11$, alors $f(x) = \Phi_{10}(x)$ le 10-ième polynôme cyclotomique, $p \equiv 1 \pmod{10}$ et $f = 1$. Dans $\mathbb{Z}[\zeta_{10}]$ on a alors la décomposition suivante :

$$(11) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4,$$

où

$$\begin{aligned} \mathfrak{p}_1 &= (11, \zeta_{10} + 4) & \mathfrak{p}_2 &= (11, \zeta_{10} + 3), \\ \mathfrak{p}_3 &= (11, \zeta_{10} + 5) & \mathfrak{p}_4 &= (11, \zeta_{10} + 9). \end{aligned}$$

De plus $\mathbb{Z}[\zeta_{10}]/\mathfrak{p} \sim \mathbb{F}_{11}$.

Proposition 7.2 *Soient p un nombre premier tel que $p \nmid m$, et \mathfrak{p} un idéal premier de $\mathbb{Z}[\zeta_m]$ au dessus de p . Alors $1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}$, sont tous distincts $\pmod{\mathfrak{p}}$.*

Preuve : On a

$$x^m - 1 = \prod_{i=0}^{m-1} (x - \zeta_m^i),$$

et donc

$$1 + x + \dots + x^{m-1} = \prod_{i=1}^{m-1} (x - \zeta_m^i).$$

Si l'on fait $x = 1$ dans la dernière égalité on obtient successivement $m = \prod_{i=0}^{m-1} (1 - \zeta_m^i)$, et $\overline{m} \prod_{i=0}^{m-1} \overline{(1 - \zeta_m^i)}$, où \overline{T} représente la classe de T dans $\mathbb{Z}[\zeta_m]/\mathfrak{p}$. Comme $p \nmid m$ alors $\overline{m} \neq \overline{0}$ et donc $\overline{\zeta_m^i} \neq 1$ pour tout $1 \leq i \leq m-1$.

Proposition 7.3 *Soit $\alpha \in \mathbb{Z}[\zeta_m]$ et $\alpha \notin \mathfrak{p}$. Il existe un unique entier i tel que*

$$\alpha^{(q-1)/m} \equiv \zeta_m^i, \quad \text{mod } \mathfrak{p}.$$

Preuve : Le groupe multiplicatif de $\mathbb{Z}[\zeta_m]/\mathfrak{p}$ a $q-1$ éléments donc $\alpha^{q-1} \equiv 1 \pmod{\mathfrak{p}}$. Donc

$$\prod_{i=1}^{m-1} (\alpha^{(q-1)/m} - \zeta_m^i) \equiv 0 \pmod{\mathfrak{p}}.$$

Mais \mathfrak{p} est un idéal premier, d'où l'existence. L'unicité vient de la proposition précédente. ■

Définition 7.2 *Soit $\alpha \in \mathbb{Z}[\zeta_m]$ et $\alpha \notin \mathfrak{p}$, on définit*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \begin{cases} 0 & \text{si } \alpha \in \mathfrak{p}, \\ \text{l'unique racine } m\text{-ième de l'unité } \equiv \alpha^{(q-1)/m} \pmod{\mathfrak{p}} & \text{sinon.} \end{cases}$$

Soit x un élément de \mathbb{F}_q , et notons encore x son image de x dans $\mathbb{Z}[\zeta_m]/\mathfrak{p}$. il existe $X \in \mathbb{Z}[\zeta_m]$ tel que x soit la classe de X dans $\mathbb{Z}[\zeta_m]/\mathfrak{p}$. On définit $\psi_{\mathfrak{p}}$ en posant :

$$\psi_{\mathfrak{p}}(x) := \left(\frac{X}{\mathfrak{p}}\right)_m \equiv x^{\frac{q-1}{m}} \pmod{\mathfrak{p}}.$$

C'est un caractère multiplicatif de $k = \mathbb{F}_q$ et un générateur du groupe $\mathbb{X} = \mathbb{X}(k^\times)$. On l'appelle *symbole de résidu m -ique* par rapport à \mathfrak{p} .

Exemple : Si l'on prend $m = 3$ et $p = 7$ dans $\mathbb{Z}[\zeta_3]$ ($\zeta_3 = j$), on a :

$$(7) = \mathfrak{p}_1 \mathfrak{p}_2,$$

avec, $\mathfrak{p}_1 = 7\mathbb{Z}[\zeta_3] + (\zeta_3 + 5)\mathbb{Z}[\zeta_3]$ et $\mathfrak{p}_2 = 7\mathbb{Z}[\zeta_3] + (\zeta_3 + 3)\mathbb{Z}[\zeta_3]$. Alors,

$$\left(\frac{2}{\mathfrak{p}_1}\right)_3 \equiv 4 \pmod{\mathfrak{p}_1}.$$

Mais comme $4 - \zeta_3^2 = 4 - (-\zeta_3 - 1) = 5 + \zeta_3 \equiv 0 \pmod{\mathfrak{p}_1}$, on en déduit alors que :

$$\left(\frac{2}{\mathfrak{p}_1}\right)_3 = \zeta_3^2.$$

Si a et b sont deux entiers naturels, on pose :

$$j_{\mathfrak{p}}(\psi_{\mathfrak{p}}^a, \psi_{\mathfrak{p}}^b) = \sum_{x+y=1} \psi_{\mathfrak{p}}^a(x) \psi_{\mathfrak{p}}^b(y).$$

On a alors le résultat suivant.

Proposition 7.4 (Relation de Stickelberger cf. [10] thm. IV.11, p.98)
Soient p un nombre premier tel que $p \equiv 1 \pmod{m}$, et $\mathfrak{p}|p$. Si a et b sont deux entiers naturels tels que $ab(a+b) \not\equiv 0 \pmod{p}$, alors,

$$(j_{\mathfrak{p}}(\psi_{\mathfrak{p}}^a, \psi_{\mathfrak{p}}^b)) = \mathfrak{p}^{\theta(a,b)},$$

où

$$\theta(a,b) = \sum_{n \in (\mathbb{Z}/m\mathbb{Z})^*} \left(\left[\frac{(a+b)n}{m} \right] - \left[\frac{an}{m} \right] - \left[\frac{bn}{m} \right] \right) \sigma_j^{-1}(n),$$

(où σ_j désigne l'application qui à $j \in (\mathbb{Z}/m\mathbb{Z})^*$ associe ζ_m^j dans le groupe des racines m -ième de l'unité).

On trouvera un exemple d'application de ces théorèmes dans [9].

7.2.2 Quand l'anneau $\mathbb{Z}[\zeta]$ est principal

Si l'anneau $\mathbb{Z}[\zeta]$ est principal et si l'on note β un générateur de \mathfrak{p} , le théorème précédent se réécrit :

$$(j_{\mathfrak{p}}(\psi_{\mathfrak{p}}^a, \psi_{\mathfrak{p}}^b)) = (\beta)^{\theta(a,b)}.$$

Mais on a de plus les résultats suivants :

Lemme 7.1 *Si tous les conjugués algébriques d'un entier algébrique α sur \mathbb{Q} sont de module 1, alors α est une racine de l'unité.*

Et aussi,

Lemme 7.2 (cf. [1] p.64 thm. 2.1.13) *Soit $K = \mathbb{Q}(\beta)$, où $\beta = \exp(2i\pi/k)$. Les seuls éléments de norme 1 dans O_K , l'anneau des entiers de K , sont les $\pm\beta^j$, $0 \leq j < k$. En particulier les seules racines de l'unité dans O_K sont les $\pm\beta^j$.*

Ce qui, pour les sommes de Jacobi, entraîne qu'il existe une racine de l'unité $\pm\zeta_m^j$ telle que :

$$j_p(\psi_p^a, \psi_p^b) = \pm\zeta_m^j \beta^{\theta(a,b)}.$$

On consultera Berndt, Evans et Williams cf.[1] p.65, voir aussi Koblitz et Buhler cf.[8].

8 Applications des sommes exponentielles

8.1 Avec les caractères additifs

Le résultat suivant est très utilisé cf. [7] p.38 prop. 3.

Proposition 8.1 *Soit F un polynôme à coefficients dans $k = \mathbb{F}_q$. Si β désigne un caractère additif non trivial de k , le nombre N de solutions dans k^* de l'équation $F = 0$ est donné par :*

$$N = q^{-1} \sum_{y,x} \beta(yF(x_1, \dots, x_n)),$$

la sommation portant sur tous les $(y, x_1, \dots, x_n) \in k^{n+1}$.

8.2 Avec les caractères multiplicatifs

8.2.1 Nombre de solutions de l'équation $\alpha_1 x_1^{k-1} + \dots + \alpha_n x_n^{k-1} = \alpha$ dans \mathbb{F}_q^n

C'est une application des plus classiques. On consultera par exemple cf. [1] ch.10 ou [7] chapitres 4,5 et 6 et aussi cf [13] et [14]. Établissons tout d'abord le résultat suivant :

Proposition 8.2 Soit $a \in \mathbb{F}_q$ et $n \in \mathbb{N}$. Soit λ un caractère multiplicatif de \mathbb{F}_q et d'ordre $d = (n, q-1)$, alors le nombre de solutions dans \mathbb{F}_q de l'équation $x^n = a$ est :

$$N(x^n = a) = \sum_{j=0}^{d-1} \lambda^j(a).$$

On établit que

Théorème 8.1 (cf. [1] p.304 thm. 10.4.2) Soient k_1, k_2, \dots, k_n des entiers naturels. soient $\alpha_1, \dots, \alpha_n$ des éléments de \mathbb{F}_q^\times et λ_i des caractères multiplicatifs d'ordre $d_i = (k_i, q-1)$. Si l'on pose

$$j(\lambda_1^{j_1}, \dots, \lambda_n^{j_n}) = \sum_{u_1 + \dots + u_n = 1} \lambda_1^{j_1}(u_1) \dots \lambda_n^{j_n}(u_n),$$

où $u_i \in \mathbb{F}_q$, alors le nombre de solutions de l'équation $\alpha_1 x_1^{k_1} + \dots + \alpha_n x_n^{k_n} = \alpha$ est :

$$N = q^{n-1} + \sum_{j_1=1}^{d_1-1} \dots \sum_{j_n=1}^{d_n-1} \lambda_1(\alpha \alpha_1^{-1}) \dots \lambda_n(\alpha \alpha_n^{-1}) j(\lambda_1^{j_1}, \dots, \lambda_n^{j_n}),$$

si $\alpha \neq 0$.

Preuve : La démonstration est classique cf. [13] ou [1] p.304. Pour $\alpha \neq 0$ on a :

$$\begin{aligned} N &= \sum_{u_1 + \dots + u_n = \alpha} = N(\alpha_1 x_1^{k_1} = u_1) \dots N(\alpha_n x_n^{k_n} = u_n) \\ &= \sum_{u_1 + \dots + u_n = \alpha} N(x_1^{k_1} = \alpha_1^{-1} u_1) \dots N(x_n^{k_n} = \alpha_n^{-1} u_n) \\ &= \sum_{u_1 + \dots + u_n = \alpha} \left(\sum_{j_1=0}^{d_1-1} \lambda_1^{j_1}(\alpha_1^{-1} u_1) \right) \dots \left(\sum_{j_n=0}^{d_n-1} \lambda_n^{j_n}(\alpha_n^{-1} u_n) \right) \\ &= \sum_{j_1=0}^{d_1-1} \dots \sum_{j_n=0}^{d_n-1} \lambda_1^{j_1}(\alpha_1^{-1}) \dots \lambda_n^{j_n}(\alpha_n^{-1}) \left(\sum_{u_1 + \dots + u_n = \alpha} \lambda_1^{j_1}(u_1) \dots \lambda_n^{j_n}(u_n) \right) \\ &= \sum_{j_1=0}^{d_1-1} \dots \sum_{j_n=0}^{d_n-1} \lambda_1^{j_1}(\alpha \alpha_1^{-1}) \dots \lambda_n^{j_n}(\alpha \alpha_n^{-1}) j(\lambda_1^{j_1}, \dots, \lambda_n^{j_n}) \\ &= q^{n-1} + \sum_{j_1=1}^{d_1-1} \dots \sum_{j_n=1}^{d_n-1} \lambda_1^{j_1}(\alpha \alpha_1^{-1}) \dots \lambda_n^{j_n}(\alpha \alpha_n^{-1}) j(\lambda_1^{j_1}, \dots, \lambda_n^{j_n}). \quad \square \end{aligned}$$

Références

- [1] **BERNDT B. C., EVANS R.J., WILLIAMS K.S.** *Gauss and Jacobi Sums*. Canadian Math. Society, Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publication, (1997).
- [2] **COHEN, H.** *A Course in Computational Number Theory*. Graduate Texts in Math., vol. 138, Springer, New-York,(1993).
- [3] **ESCOFIER J-P.**, *Théorie de Galois*, Collection Enseignement des Mathématiques, Masson, Paris, (1997).
- [4] **IHARA Y.**, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. **123**, p. 43-106, (1986).
- [5] **IWASAWA K.**, *A note on Jacobi sums*, Istituto Nazionale di Acta Mathematica, symposia Mathematica, vol. 15, Academic Press, pp. 447-459 London, (1975).
- [6] **IRELAND K., ROSEN M.** *A classical introduction to modern number theory*, Graduate Texts in Math., vol. 84, Springer, New-York,(1982).
- [7] **JOLY, J.R.**, *Equations et variétés algébriques sur un corps fini*. Enseignement Mathématiques, 19, , pp. 1-117, (1973).
- [8] **BUHLER, J.KOBLITZ, N.**, *Lattices basis reduction, Jacobi sums and hyperelliptic cryptosystems*. Bull. Australian Math. Soc., Vol. 58, pp.147-154,(1998).
- [9] **LACHAUD G.**, *Courbes diagonales et courbes de Picard*. Preprint Institut de Mathématiques de Luminy, CNRS, Marseille, (1998).
- [10] **LANG S.**, *Algebraic Number Theory*, Graduate Texts in Math., vol. 110, Springer, New-York, (1991).
- [11] **LIDL, R., NIEDERREITER H.**, *Finite fields*. Volume 20 of Encyclopedia of Mathematics and its applications. Cambridge University Press, (1983).
- [12] **MILNE, J.S.**, *Algebraic Number Theory*. Math 676, <http://www.jmilne.org/math/>, (1996).

- [13] **WEIL A.**, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949) 497-508 ; =œuvres Scientifiques[1949b], vol. I, pp. 399-410.
- [14] **WEIL A.**, *Jacobi sums as "Größencharaktere"*, Bull. Amer. Math. Soc., VI. 73, pp.487-495 ; =œuvres Scientifiques[1952d], vol. II, pp. 63-71.