Corps finis

Table des matières

Références

[BMP05] Vincent Beck, Jérôme Malick, and Gabriel Peyré. *Objectif agrégation*. H&K, 2005.

[CG13] Philippe Caldero and Jérôme Germoni. *Histoires hédonistes de groupes et de géométries*. Calvage & Mounet, 2013.

[Dem09] Michel Demazure. *Cours d'algèbre*. Cassini, 2009.

[Hin08] Marc Hindry. *Arithmétique*. Calvage & Mounet, 2008.

[NQ92] Patrice Naudin and Claude Quitté. *Algorithmique algébrique*. Masson, 1992.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique*. puf, 1970.

[Zém00] Gilles Zémor. *Cours de cryptographie*. Cassini, 2000.

Sauf mention expresse du contraire, tous les anneaux considérés seront supposés commutatifs et unitaires. Par la suite, un corps désignera une algèbre à division commutative et unitaire.

1 Généralité [Ser70]

1.1 Quelques propriétés relatives aux corps

Proposition 1.1 - Caractéristique d'un anneau - Sous-corps premier.
Pour un anneau A, on appelle *caractéristique* de A, notée $\operatorname{car} A$, l'unique entier naturel n tel que le noyau de l'unique morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow A$ soit l'idéal (n).

Si A est intègre, $\operatorname{car} A$ est égal à 0 ou à un nombre premier p. Si A est un corps, on appelle alors *sous-corps premier* de A le corps de fractions de l'image de φ, qui est isomorphe à $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$) si $\operatorname{car} A = 0$ (resp. p).

Si $\operatorname{car} A = p$, alors l'application $x \longmapsto x^p$ est un endomorphisme de A, appelé *morphisme de Frobenius*.

Démonstration. La première assertion résulte de ce que $\mathbb{Z}$ est un groupe monogène et un anneau principal.

Si A est un anneau intègre de caractéristique non nulle n, alors $\operatorname{im}\varphi \simeq \mathbb{Z}/n\mathbb{Z}$ est un sous-anneau de A. Or $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

La seule propriété non triviale de l'endomorphisme de Frobenius est son additivité, qui résulte de la formule du binôme de Newton et du lemme suivant :

Lemme 1.2 Si p est un nombre premier, alors $p \mid \binom{p}{k}$, pour $1 \leqslant k \leqslant p-1$.

Pour $1 \leqslant k \leqslant p-1$, $k\binom{p}{k} = p\binom{p-1}{k-1}$ et p est premier à k, d'où le résultat par le lemme de Gauß.

QED

Remarque 1.3 $\operatorname{car} A$ est le plus petit entier naturel n tel que $n \cdot 1_A = 0_A$ et le sous-corps premier d'un corps k est le plus petit sous-corps de ce dernier. En outre, si K/k est une extension de corps, k et K ont le même sous-corps premier et la même caractéristique.

Proposition 1.4 Un anneau intègre fini est un corps.

Démonstration. Soit A un tel anneau. Pour $a \in A \setminus \{0\}$, $x \longmapsto ax$ est une injection, puisque a est régulier, donc une bijection.

QED

Exemple 1.5 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier.

Dans l'énoncés suivant, les anneaux ne sont plus supposés commutatifs.

Théorème 1.6 - Wedderburn. Une algèbre à division finie est un corps (*i.e.* nécessairement commutatif).

Démonstration.[Per96, Chap. III, § 4, th 4.9] Soit k une algèbre à division finie. Son centre Z est un corps de cardinal $q \geqslant 2$; k est alors un Z-espace vectoriel et on a $|k| = q^n$. Supposons par l'absurde que k n'est pas commutative, *i.e.* $n > 1$.

k^* opère sur lui-même par conjugaison. Pour $x \in k^*$, $k_x = k_x^* \cup \{0\}$ est une sous-algèbre à divison de k qui contient Z, ainsi, comme précedemment, $|k_x| = q^d$ et $d \mid n$, car k_x^* est un sous-groupe de k^* (cf. lemme 1.9). On a donc, pour le cardinal de l'orbite de x, $|k^*.x| = \frac{|k^*|}{|k_x^*|} = \frac{q^n-1}{q^d-1}$ et l'équation aux classes donne

$$q^n - 1 = |k^*| = |Z^*| + \sum_{x \notin Z} |k_x^*| = q - 1 + \sum \frac{q^n-1}{q^d-1},$$

où la somme porte sur un certain nombre de diviseurs d stricts de n ($d = n$ signifie que $x \in Z$).

Or, de la relation $X^n - 1 = \prod_{m|n} \Phi_m$ dans $\mathbb{Z}[X]$, on déduit que, pour $d \mid n$, $\frac{q^n-1}{q^d-1} = \prod_{m|n \text{ et } m\nmid d} \Phi_m(q)$, ainsi $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$, pour $d \neq n$.

Finalement, on a donc $\Phi_n(q) \mid q-1$ et, en particulier, $|\Phi_n(q)| \leqslant q-1$. Or $\Phi_n(q) = (q-\zeta_1)\dots(q-\zeta_{\varphi(n)})$, où les ζ_i sont les racines primitives $n^{\text{èmes}}$ de l'unité dans $\mathbb{C}$ et $|q-\zeta_i| > |q-1|$ (faire un dessin !), ainsi $|\Phi_n(q)| > (q-1)^{\varphi(n)} \geqslant q-1$, d'où une contradiction.

QED

1.2 Existence et unicité des corps finis

Théorème 1.7

(i) Le cardinal d'un corps fini k est une puissance d'un nombre premier. Précisément, $|k| = p^{[k:\mathbb{F}_p]}$, où p est la caractéristique de k.

(ii) Soit p un nombre premier, $q = p^d$, avec $d \in \mathbb{N}_*$, et Ω un corps algébriquement clos de caractéristique p. Il existe un unique sous-corps à q éléments de Ω, noté $\mathbb{F}_q$; c'est l'ensemble des racines du polynôme $X^q - X$.

(iii) Tout corps fini à $q = p^d$ éléments est $\mathbb{F}_p$-isomorphe à $\mathbb{F}_q$.

Démonstration. (i) Le sous-corps premier de k ne saurait être $\mathbb{Q}$, k est donc un espace vectoriel de dimension finie sur son sous-corps premier $\mathbb{F}_p$.

(ii) Puisque Ω est algébriquement clos, $f : x \longmapsto x^q$ est un automorphisme de Ω (puissance $d^{\text{ème}}$du Frobenius). Les éléments de Ω invariants par f forment un sous-corps $\mathbb{F}_q$ de Ω qui a q éléments. En effet il s'agit des racines du polynôme $X^q - X$ qui est séparable sur $\mathbb{F}_p$ et scindé dans Ω algébriquement clos. En outre, si k est un sous-corps de Ω à q éléments, le groupe multiplicatif de k est d'ordre $q-1$, ainsi $x^{q-1} = 1$, pour $x \in k^\star$ (th. de Lagrange), d'où $x^q = x$ pour tout $x \in k$. Ainsi $k \subset \mathbb{F}_q$ et l'égalité par égalité des cardinaux.

(iii) $\mathbb{F}_q$ n'est rien d'autre qu'un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

QED

Remarque 1.8 D'après le point (iii), il n'y a essentiellement qu'un corps fini à q éléments. Toutefois, il n'y a pas unicité d'un isomorphisme entre deux tels corps (cf. les sections 2.3 et 2.5), d'où un certain danger de la notation $\mathbb{F}_q$. À ce sujet, on pourra consulter la remarque de la section 9.3.3 de [Dem09, p. 223].

Il est alors naturel de se demander quels sont les sous-corps de $\mathbb{F}_q$? La réponse découle essentiellement du lemme préliminaire suivant.

Lemme 1.9 Soit a un entier supérieur à 2 et d et n deux entiers naturels. $a^d - 1 \,|\, a^n - 1 \iff d \,|\, n$.

Démonstration. Si $n = db$, alors

$$a^n - 1 = (a^d)^b - 1 = (a^d - 1)((a^d)^{b-1} + \dots + 1) = (a^d - 1)N.$$

Réciproquement, écrivons la division euclidienne de n par d : $n = bd + r$. Modulo $a^d - 1$, on a $a^d \equiv 1$, donc $a^{db} \equiv 1$, or $a^n \equiv 1$, ainsi $a^r \equiv 1$, ce qui impose $r = 0$, puisque $r < d$.

QED

Proposition 1.10 - Sous-corps de $\mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}$ possède un sous-corps de cardinal p^d si et seulement si $d \mid n$. Le cas échéant un tel sous-corps est unique, formé de l'ensemble des racines de $X^{p^d} - X$.

Démonstration. Si $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_{p^n}$, alors en particulier $\mathbb{F}_{p^d}^*$ est un sous-groupe de $\mathbb{F}_{p^n}^*$. Par conséquent $p^d - 1 | p^n - 1$ et $d|n$, d'après le lemme. Réciproquement, si $n = kd$, alors, avec les notations de la démonstration du lemme, on a

$$X^{p^n} - X = X\left(X^{(p^d-1)N} - 1\right) = X\left(X^{p^d-1} - 1\right)\left(\left(X^{p^d-1}\right)^{N-1} + \cdots + 1\right) = \left(X^{p^d} - X\right)Q,$$

ce qui montre que $\mathbb{F}_{p^n}$ contient un corps de décomposition de $X^{p^d} - X$, *i.e.* une unique réalisation de $\mathbb{F}_{p^d}$ (cf. théorème 1.7.(iii)).

QED

Remarque 1.11 Il y a ainsi un isomorphisme entre le treillis * des diviseurs de n et celui des sous-corps de $\mathbb{F}_{p^n}$.

Exemple 1.12 Les sous-corps stricts de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$ et $\mathbb{F}_4$. Notamment $\mathbb{F}_{16}$ n'a pas de sous-corps à 8 éléments !

1.3 Groupe multiplicatif d'un corps fini

Soit p un nombre premier et $q = p^d$, avec $d \in \mathbb{N}_*$.

Théorème 1.13 $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q - 1$.

Corollaire 1.14 Toute extension finie d'un corps fini est monogène.

Remarque 1.15 Attention toutefois, si $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, α n'est pas nécessairement un générateur du groupe cyclique $\mathbb{F}_q^*$. Penser par exemple à $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$, où la classe de X est un élément d'ordre 5 !

Lemme 1.16 Soit n un entier naturel non nul, $n = \sum_{d|n} \varphi(d)$.

Démonstration. $\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \{\text{générateurs de l'unique sous-groupe (cyclique) d'ordre } d \text{ de } \mathbb{Z}/n\mathbb{Z}\}$.

QED

Lemme 1.17 Soit G un groupe fini d'ordre n. On suppose que, pour tout diviseur d de n, l'ensemble des $x \in G$ tels que $x^d = 1$ a au plus d éléments. G est alors cyclique.

Démonstration. Soit d un diviseur de n. S'il existe dans G un élément x d'ordre d, alors $\langle x \rangle$ est un sous-groupe cyclique d'ordre d de G et tout élément $y \in G$ tel que $y^d = 1$ appartient à $\langle x \rangle$, vu l'hypothèse. Ainsi le nombre d'éléments d'ordre d dans G est 0 ou $\varphi(d)$. Le lemme 1.16 exclu alors le premier cas et G possède nécessairement un élément d'ordre n.

∗. Un treillis est un ensemble partiellement ordonné dans lequel chaque couple d'éléments admet une borne supérieure et une borne inférieure. Pour deux entiers m et n il s'agit de leurs ppcm et pgcd. Pour deux sous-corps il s'agit de leur extension composée et de leur intersection.

QED

Le théorème résulte alors simplement du lemme 1.17, puisqu'il est clair que l'équation $x^d = 1$ a au plus d solutions dans $\mathbb{F}_q$.

Remarque 1.18 Ce qui précède montre plus généralement que tout sous-groupe fini du groupe multiplicatif d'un corps K est cyclique. L'hypothèses de commutativité du corps K est indispensable. Par exemple le sous-groupe quaternionique $\mathbf{H}_8$ de l'algèbre à division des quaternions $\mathbb{H}$ n'est pas cyclique (il est d'ordre 8 et non abélien.

Corollaire 1.19 Les extensions de corps finis K/k sont monogènes, *i.e.* il existe $\alpha \in K$ tel que $K = k(\alpha)$. Toutefois, attention, si $K = k(\alpha)$, α n'est pas nécessairement un générateur de K^* !

Remarque 1.20 Pour le corollaire précédent, il suffit de prendre pour α un générateur de K^*.

Remarque 1.21 Finalement les structures additive et multiplicative de $\mathbb{F}_q$, avec $q = p^n$, sont aisées à décrire (cf. aussi l'exercice 4.3) :

— $(\mathbb{F}_q, +)$ est isomorphe au groupe abélien $(\mathbb{Z}/p\mathbb{Z})^n$;

— $(\mathbb{F}_q^*, \times)$ est isomorphe au groupe cyclique $\mathbb{Z}/(q-1)\mathbb{Z}$.

En revanche, c'est le lien entre ces deux structures qui est moins évident a priori. Il va être précisé au cours de la section suivante, où l'on va apprendre à construire explicitement le corps $\mathbb{F}_q$ et calculer explicitement dans de petits corps finis.

2 Polynômes sur les corps finis et leurs racines [Dem09]

2.1 Clôture algébrique d'un corps fini

Commençons par observer que, pour un corps fini k, le polynôme $1 + \prod_{\alpha \in k} (X - \alpha)$ est sans racine dans k. Ainsi un corps fini ne saurait être algébriquement clos.

Proposition 2.1 $\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de tout corps fini de caractéristique p.

Démonstration. Posons $\Omega = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$. Ω est une union croissante de corps qui est donc naturellement munie d'une structure de corps et qui admet comme sous-corps n'importe quel corps fini de caractéristique p (cf. proposition 1.10). Soit $P \in \Omega[X]$ irréductible, il existe $n \in \mathbb{N}$ tel que $P \in \mathbb{F}_{p^{n!}}[X]$. P admet donc une racine dans $\mathbb{F}_{p^{n! \deg P}}$ (corps de rupture) et donc dans Ω. Ainsi Ω est algébriquement clos. Par définition de Ω, ses éléments sont tous algébriques sur $\mathbb{F}_p$ et Ω est donc une extension algébrique de n'importe quel corps fini de caractéristique p.

QED

2.2 Polynômes irréductibles

Fixons un entier $q = p^r$, avec p premier et $r \in \mathbb{N}_*$. On note $I(n,q)$ l'ensemble des polynômes irréductibles et unitaires de degré n sur $\mathbb{F}_q$ et $m(n,q)$ le cardinal de cet ensemble.

Commençons par un lemme qui caractérise les facteurs irréductibles du polynôme $X^{q^n} - X$.

Lemme 2.2 Soit $P \in I(d,q)$, $P \mid X^{q^n} - X$ si et seulement si $d \mid n$.

Démonstration. Soit $P \in I(d,q)$ un diviseur de $X^{q^n} - X$. $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$, dans lequel P est donc scindé. Soit α une racine de P dans $\mathbb{F}_{q^n}$, on a alors $d = \deg P = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ qui divise $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Réciproquement, considérons α une racine de P dans une clôture algébrique de $\mathbb{F}_{q^n}$, alors $\alpha \in \mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, puisque $d \mid n$. Ainsi, α est une racine de $X^{q^n} - X$ et $P = \pi_{\alpha,\mathbb{F}_q} \mid X^{q^n} - X$.

QED

Corollaire 2.3 Sur un corps fini, les notions de corps de rupture et de corps de décomposition coïncident.

Démonstration. Soit $P \in I(n,q)$, son corps de rupture est $\mathbb{F}_{q^n}$, qui est, d'après le th. 1.7, le corps de décomposition de $X^{q^n} - X$. Or $P \mid X^{q^n} - X$ et P est donc scindé dans $\mathbb{F}_{q^n}$.

QED

Proposition 2.4 Pour $n \in \mathbb{N}_*$, on a l'égalité suivante dans $\mathbb{F}_q[X]$: $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P$.

Démonstration. Du fait du lemme précédent, les deux polynômes considérés étant unitaires, il suffit de remarquer que $X^{q^n} - X$ est séparable.

QED

À partir de ce résultat, il est possible de dénombrer précisément le nombre de polynômes irréductibles de degré donné sur $\mathbb{F}_q$.

Corollaire 2.5 Pour $n \in \mathbb{N}_*$, $q^n = \sum_{d|n} d\, m(d,q)$.

On déduit de cette formule l'encadrement $\frac{q^n - 2q^{n/2}}{n} \leqslant m(n,q) \leqslant \frac{q^n}{n}$. Il existe donc des polynômes irréductibles de tout degré sur $\mathbb{F}_q$ [†]. En outre, un polynôme unitaire de grand degré n choisi au hasard a environ une chance sur n d'être irréductible.

Remarque 2.6 La fonction de Möbius μ permet de donner une expression exacte pour $m(n,q)$ [‡] :

$$m(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Corollaire 2.7 - Test de Rabin, 1979. Soit $P \in \mathbb{F}_q[X]$ de degré $n \in \mathbb{N}_*$. P est irréductible sur $\mathbb{F}_q$ si et seulement si P divise $X^{q^n} - X$ et si, pour tout facteur premier r de n, P est premier à $X^{q^{n/r}} - X$.

†. Ce résulat s'obtient plus simplement de la façon suivante : $\mathbb{F}_{q^n}^*$ est cyclique, soit donc α un générateur de ce groupe, alors $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ et $\pi_{\alpha,\mathbb{F}_q}$, qui est irréductible, est de degré n.

‡. Formule d'inversion de Möbius : si $f(n) = \sum_{d|n} g(d)$, alors $g(n) = \sum_{d|n} \mu(d) f(n/d)$, pour $f, g : \mathbb{N}_* \longrightarrow G$, avec G un groupe abélien. Rappelons que $\mu : \mathbb{N}_* \longrightarrow \{0, \pm 1\}$ est définie par $\mu(d) = \begin{cases} 1 & \text{si } d = 1\,; \\ (-1)^k & \text{si } d \text{ est libre de carré et de la forme } p_1 \dots p_k\,; \\ 0 & \text{sinon.} \end{cases}$

Remarque 2.8 Le corollaire précédent fournit (modulo la capacité de déterminer les facteurs premiers d'un entier) un test algorithmique (basé sur des calculs de pgcd) pour l'irréductibilité d'un polynôme sur un corps fini.

Application 2.9 $X^p - X - a$, avec $a \in \mathbb{F}_p^\star$, est irréductible sur $\mathbb{F}_p$.
(*Indication : établir par récurrence sur i que $X^{p^i} \equiv X + ia \mod X^p - X - a$.*)

Pour terminer cette section, rappelons le résultat utile suivant qui caractérise l'irréductibilité d'un polynôme par l'absence de racine dans certaines extensions.

Proposition 2.10 Soit k un corps et $P \in k[X]$ de degré n. P est irréductible sur k si et seulement si P n'a pas de racine dans les extensions de k de degré $\leqslant n/2$.

Démonstration. Si P est irréductible, le degré d'une plus petite extension de k qui contient une racine de P est le degré d'un corps de rupture de P sur k, *i.e.* n. Réciproquement, raisonnons par contraposition en supposant que P est réductible sur k. Alors P a un facteur irréductible $Q \in k[X]$ de degré $d \leqslant n/2$ et ce dernier, et donc P également, a une racine dans l'extension $k[X]/(Q)$ de degré d sur k (corps de rupture de Q sur k).

QED

Application 2.11 Montrer que $\Phi_8 = X^4 + 1$ est réductible sur $\mathbb{F}_p$, pour tout nombre premier p.

Le cas $p = 2$ est clair. On peut donc supposer dorénavant que p est impair. D'après la proposition 2.10, $X^4 + 1$ est réductible sur $\mathbb{F}_p$ si et seulement s'il a une racine dans $\mathbb{F}_{p^2}$. Or les racines de $X^4 + 1$ dans un corps de décomposition sont les racines primitives $8^{\text{ème}}$ de l'unité, ainsi sa réductibilité sur $\mathbb{F}_p$ équivaut à ce que $8 \mid |\mathbb{F}_{p^2}^*| = p^2 - 1$ et cette dernière assertion est toujours vraie.

Remarque 2.12 La question en suspend est finalement de factoriser les polynômes sur les corps finis en leurs facteurs irréductibles. Une réponse est apportée par l'algorithme de Berlekamp, exposé par exemple dans [BMP05, 5.3.2] ou [Dem09, 9.6.2].

2.3 Construction et calculs explicites dans les corps finis

Il est important de savoir construire explicitement les corps finis de petit cardinal et calculer dans ces derniers. Nous allons illustrer cela avec les corps $\mathbb{F}_4$ et $\mathbb{F}_{16}$.

$\mathbb{F}_4$ **:** c'est une extension de degré 2 de $\mathbb{F}_2$, il s'agit donc de déterminer un polynôme irréductible unitaire de degré 2 sur $\mathbb{F}_2$. Autrement dit $X^2 + aX + b \in \mathbb{F}_2[X]$ doit être sans racine dans $\mathbb{F}_2$, ce qui impose $a = b = 1$ [§]. Ainsi $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ est une réalisation du corps à 4 éléments. Si j désigne la classe de X modulo $X^2 + X + 1$, j est une racine primitive troisième de l'unité et $\mathbb{F}_4 = \mathbb{F}_2[j] = \{0, 1, j, j + 1\} = \{0, 1, j, j^2\}$, avec $j(j + 1) = j^2 + j = 1$.

§. Ainsi il existe un unique polynôme irréductible unitaire de degré 2 sur $\mathbb{F}_2$.

$\mathbb{F}_{16}$ **:** au choix, on peut construire $\mathbb{F}_{16}$ comme une extension de degré 4 de $\mathbb{F}_2$ ou de degré 2 de $\mathbb{F}_4$. Choisissons la première possibilité et cherchons les polynômes irréductibles unitaires de degré 4 sur $\mathbb{F}_2$ [¶]. D'après la proposition 2.10, ce sont les polynômes $X^4+aX^3+bX^2+cX+d \in \mathbb{F}_2[X]$ sans racine dans $\mathbb{F}_4$, ce qui mène aux conditions :

$$\left\{\begin{array}{rcl} d & \neq & 0 \\ a+b+c+d+1 & \neq & 0 \\ (b+c+1)j+a+b+d & \neq & 0 \\ (b+c+1)j+a+c+d+1 & \neq & 0 \end{array}\right. \iff \left\{\begin{array}{rcl} d & = & 1 \\ a+b+c & = & 1 \\ aj+a+b+1 & \neq & 0 \\ aj+a+c & \neq & 0 \end{array}\right. \iff \left| \begin{array}{c} a=d=1 \text{ et } b=c \\ d=1, a=b=0 \text{ et } c=1 \end{array}\right. ,$$

soit les trois polynômes $f_1 = X^4+X^3+1$, $f_2 = X^4+X+1$ et $f_3 = X^4+X^3+X^2+X+1$, qui donnent trois constructions de $\mathbb{F}_{16}$: $k_i = \mathbb{F}_2[X]/(f_i) = \mathbb{F}_2[\alpha_i]$.

Ces trois corps sont évidemment isomorphes et il est utile de savoir expliciter de tels isomorphismes [‖]. Illustrons cela avec k_1 et k_2. Un morphisme injectif (et donc bijectif pour des raisons de cardinalité) de corps entre k_1 et k_2 s'obtient via la donnée d'un morphisme d'anneaux $\varphi : \mathbb{F}_2[T] \longrightarrow k_2$ tel que $\ker\varphi = (f_1)$ (1^{er} th. d'isomorphisme), *i.e.* pour lequel T est envoyé sur une racine de f_1 dans k_2. Dans le cas présent, on peut remarquer que f_1 est le polynôme réciproque de f_2, soit l'isomorphisme suivant

$$\widetilde{\varphi} : \left| \begin{array}{ccc} k_1 & \xrightarrow{\sim} & k_2 \\ \alpha_1 & \longmapsto & \frac{1}{\alpha_2} \end{array}\right. .$$

2.4 Racines de l'unité dans les corps finis

Cf. le cours sur la cyclotomie.

2.5 Groupe de Galois

Proposition 2.13 Si $P \in \mathbb{F}_q[X]$ est irréductible de degré n, alors P a une racine α dans $\mathbb{F}_{q^n}$. En outre, toutes les racines de P sont simples et données par $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$.

Démonstration. $\mathbb{F}_{q^n}$ est un corps de rupture de P. L'automorphsime $\varphi : x \longmapsto x^q$ de $\mathbb{F}_{q^n}$ laisse fixe $\mathbb{F}_q$, ainsi, pour $\beta \in \mathbb{F}_{q^n}$, $P(\beta^q) = \varphi(P)(\varphi(\beta)) = \varphi(P(\beta)) = P(\beta)^q$. Il ne reste donc plus qu'à montrer que $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ sont distincts. Par l'absurde, si $\alpha^{q^i} = \alpha^{q^j}$, pour $0 \leqslant i < j \leqslant n-1$, il vient, en multipliant par $\alpha^{q^{n-j}}$, $\alpha^{q^{n+i-j}} = \alpha$. Or ceci n'est possible que si $n \mid n+i-j$, d'où une contradiction.

QED

Remarque 2.14 Ainsi, pour α de degré n sur $\mathbb{F}_q$, $\pi_{\alpha,\mathbb{F}_q} = \prod_{i=0}^{n-1}(X-\alpha^{q^i}) = \prod_{i=0}^{n-1}(X-\varphi^i(\alpha))$.

On a donc établit que tout polyôme irréductible sur un corps fini est séparable. Ainsi les extensions finies de corps finis sont séparables.

Exercice 2.15 Déterminer les polynômes minimaux sur $\mathbb{F}_2$ des éléments de $\mathbb{F}_{16}$.

Théorème 2.16 Les automorphismes de corps de $\mathbb{F}_{q^n}$ identique sur $\mathbb{F}_q$ sont exactement les puissances de l'automorphisme de Frobenius $\varphi : x \longmapsto x^q$. Autrement dit, $\mathrm{Gal}\,(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$.

Démonstration. Soit $\psi \in \mathrm{Gal}\,(\mathbb{F}_{q^n}/\mathbb{F}_q)$ et $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. $\psi(\alpha)$ doit être une racine de $\pi_{\alpha,\mathbb{F}_q}$, *i.e.* un α^{q^i}, pour $0 \leqslant i < n$, d'après la proposition précédente. Mais puisque ψ est $\mathbb{F}_q$-linéaire, $\psi = \varphi^i$.

QED

¶. D'après le corollaire 2.5, $m(4,2)$ vérifie $2^4 = m(1,2) + 2m(2,2) + 4m(4,2)$, soit $m(4,2) = (16-2-2)/4 = 3$.

‖. Typiquement pour comparer deux résultats de calculs effectués dans deux constructions distinctes d'un même corps fini (ce qui doit arriver couramment au sein d'un logiciel de calcul formel !).

3 Carrés modulo p [Hin08, Ser70]

3.1 Carrés de $\mathbb{F}_q$

Soit q une puissance d'un nombre premier p.

Théorème 3.1 Selon la parité de p, on a l'alternative suivante :

(i) si $p = 2$, tout élément de $\mathbb{F}_q$ est un carré ;

(ii) si $p \neq 2$, les carrés de $\mathbb{F}_q^*$ forment un sous-groupe d'indice 2 de $\mathbb{F}_q^*$, noyau du morphisme de groupes

$$\left|\begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \{\pm 1\} \\ x & \longmapsto & x^{(q-1)/2} \end{array}\right. .$$

Démonstration.

(i) Pour $p = 2$ le morphisme de Frobenius $x \longmapsto x^2$ est un automorphisme de $\mathbb{F}_q$.

(ii) Soit l'endomorphisme de groupes $f : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*, x \longmapsto x^2$; $\ker f = \{\pm 1\}$, ainsi $\mathbb{F}_q^{*2} = \operatorname{im} f \simeq \mathbb{F}_q^*/(\ker f)$ est donc un sous-groupe d'indice 2 de $\mathbb{F}_q^*$. En outre, si x est un carré de $\mathbb{F}_q^*$, alors il existe $y \in \mathbb{F}_q^*$ tel que $x = y^2$, donc, d'après le théorème de Lagrange, $x^{(q-1)/2} = y^{q-1} = 1$, ce qui achève la démonstration, vu le nombre maximal de racines de $X^{(q-1)/2} - 1$ dans $\mathbb{F}_q$.

QED

Remarque 3.2 Pour $p \neq 2$, d'après le point (ii) du théorème, le produit de deux éléments non carrés de $\mathbb{F}_q$ est un carré de $\mathbb{F}_q$.

Application 3.3 Une forme quadratique de rang 2 sur $\mathbb{F}_q$ représente tout élément de $\mathbb{F}_q$.

En effet soit ax^2+by^2, $a, b \in \mathbb{F}_q^*$, une telle forme et $c \in \mathbb{F}_q$, on peut supposer q impair (le cas pair étant trivial). $A = \{ax^2 \ / \ x \in \mathbb{F}_q\}$ et $B = \{c-by^2 \ / \ y \in \mathbb{F}_q\}$ sont en bijection avec $\mathbb{F}_q^2$, ainsi $|A|+|B| = \frac{q+1}{2} + \frac{q+1}{2} = q+1 > |\mathbb{F}_q|$ et $A \cap B \neq \emptyset$. Il existe donc $x, y \in \mathbb{F}_q$ tel que $ax^2 = c - by^2$.

Application 3.4 - Classification des formes quadratiques non-dégénérées sur $\mathbb{F}_q$, $p \neq 2$.

Théorème 3.5 Soit E un $\mathbb{F}_q$-espace vectoriel de dimension n et $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E, de matrices

$$Q_1 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \quad \text{ou} \quad Q_2 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \alpha \end{pmatrix}.$$

Une forme est de l'un ou l'autre type suivant que son discriminant est ou non un carré dans $\mathbb{F}_q^*$.

Démonstration. Notons déjà que Q_1 et Q_2 ne sont pas équivalentes car leurs discriminants ne sont pas égaux modulo $\mathbb{F}_q^{*2}$. Soit Q une forme quadratique sur E. Le cas $n = 1$ est trivial. Pour $n \geqslant 2$, on procède par récurrence.

Pour $n = 2$, on choisit une base orthogonale pour Q dans laquelle on a $Q(x, y) = ax^2 + by^2$. De l'application 3.3, on déduit l'existence de $e_1 \in E$ tel que $Q(e_1) = 1$. Soit alors $e_2 \in \langle e_1 \rangle^\perp$, en vertu du théorème 3.1, on a l'alternative $Q(e_2) = \lambda^2$ ou $Q(e_2) = \lambda^2\alpha$. La base $(e_1, \frac{1}{\lambda}e_2)$ convient.

Pour $n > 2$, on considère une base orthogonale $(\varepsilon_1, \ldots, \varepsilon_n)$ et l'application 3.3 montre qu'il existe $e_1 \in \langle \varepsilon_1, \varepsilon_2 \rangle$ tel que $Q(e_1) = 1$. On applique alors l'hypothèse de récurrence à l'hyperplan $\langle e_1 \rangle^\perp$.

QED

D'après le point (i) du théorème 3.1, il est naturel, pour étudier les carrés, de se placer sous l'hypothèse p impair, ce que nous faisons dans la suite.

3.2 Symboles de Legendre et de Jacobi

Soit p un nombre premier impair.

Définition 3.6 On appelle **symbole de Legendre** de $a \in \mathbb{Z}$ l'entier

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } p \nmid a \text{ et } a \text{ est un carré modulo } p \\ -1 & \text{sinon} \end{cases}$$

Lorsque $\left(\frac{a}{p}\right) = 0$ ou 1 (resp. -1), on dit que a est un **résidu quadratique** (resp. **non-résidu quadratique**) modulo p.

Remarques 3.7 $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p, on s'autorisera donc à utiliser ce symbole pour $a \in \mathbb{F}_p$.

Théorème 3.8 Pour $a \in \mathbb{Z}$,

(i) $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$ (formule d'Euler) ;

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ et $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;

(iv) si q est un nombre premier impair $\neq p$, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ (loi de réciprocité quadratique).

Démonstration. (i) et (ii) résultent aisément du point (ii) du théorème 3.1.

Pour (iii) la première égalité découle simplement de (i). Pour la seconde, considérons ζ une racine primitive $8^{\text{ème}}$ de l'unité dans une extension de $\mathbb{F}_p$ ($\mathbb{F}_{p^2}$ en l'occurrence, puisque $8 \mid p^2-1$), *i.e.* une racine de $\Phi_8 = X^4+1$, et posons $\alpha = \zeta + \zeta^{-1}$. Alors $\alpha^2 = \zeta^2 + \zeta^{-2} + 2 = \zeta^{-2}(\zeta^4+1) + 2 = 2$. Ainsi 2 est un carré dans $\mathbb{F}_p$ si et seulement si $\alpha \in \mathbb{F}_p$, ce qui équivaut à $\alpha^p = \alpha$. Or $\alpha^p = \zeta^p + \zeta^{-p} = \alpha$ si $p \equiv \pm 1 \mod 8$ et $\alpha^p = -\alpha$ si $p \equiv \pm 3 \mod 8$.

(iv) sera démontré à la section 3.4. Une démonstration alternative est proposée à l'exercice 4.13.

QED

Remarques 3.9

1. L'introduction de $\alpha = \zeta + \zeta^{-1}$ comme « $\sqrt{2}$ » dans $\mathbb{F}_{p^2}$ s'explique par l'observation suivante : si $\zeta = e^{2i\pi/8} \in \mathbb{C}$, alors ζ est une racine primitive $8^{\text{ème}}$ de l'unité et $\zeta = \frac{\sqrt{2}}{2}(1+i)$, ainsi $\zeta + \zeta^{-1} = \zeta + \overline{\zeta} = \sqrt{2}$.
2. -1 est un carré mod $p \Leftrightarrow p \equiv 1 \mod 4$ et 2 est un carré mod $p \Leftrightarrow p \equiv \pm 1 \mod 8$.
3. La loi de réciprocité énonce :
   - p est un carré mod $q \Leftrightarrow q$ est un carré mod p, lorsque p ou $q \equiv 1 \mod 4$;
   - p est un carré mod $q \Leftrightarrow q$ n'est pas un carré mod p, lorsque p et $q \equiv -1 \mod 4$.
4. Le symbole de Legendre est l'unique morphisme de groupes non trivial entre $\mathbb{F}_p^*$ et $\{\pm 1\}$ (cf. théorème 3.1) ; cette assertion constitue une des étapes d'une démonstration du théorème de Frobenius-Zolotarev (cf. exercice 4.12).

Introduisons maintenant une généralisation du symbole précédent pour $N = p_1^{\alpha_1} \dots p_r^{\alpha_r} \in \mathbb{Z}$ impair.

Définition 3.10 On appelle **symbole de Jacobi** de l'entier relatif a l'entier

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Théorème 3.11 Le symbole de Jacobi vérifie, *mutatis mutandis*, les mêmes propriétés que celles du symbole de Legendre énoncées au théorème 3.8, à l'exception de la formule d'Euler au point (i) **.

Démonstration. $\varepsilon : (\mathbb{Z}/4\mathbb{Z})^\star \longrightarrow \mathbb{Z}/2\mathbb{Z}, n \longmapsto \frac{n-1}{2} \mod 2$ et $\omega : (\mathbb{Z}/8\mathbb{Z})^\star \longrightarrow \mathbb{Z}/2\mathbb{Z}, n \longmapsto \frac{n^2-1}{8} \mod 2$ sont des morphismes de groupes.

QED

**. Cette mise en défaut de la formule d'Euler pour le symbole de Jacobi est à la base du test de primalité de Solovay-Strassen (cf. cours sur la cryptographie).

Remarques 3.12

1. Les propriétés du symbole de Jacobi fournissent un algorithme pour le calcul de ce dernier par réductions successives, selon un *modus operandi* analogue à l'algorithme d'Euclide (cf. exemple ci-après) et qui, notamment, ne nécessite pas de connaître la factorisation de N.
2. Contrairement au symbole de Legendre, le symbole de Jacobi ne caractérise pas les carrés modulo N. Précisément, si $\left(\frac{a}{N}\right) = -1$ alors a ne peut être un carré modulo N, mais $\left(\frac{a}{N}\right) = 1$ n'implique pas que a est un carré modulo N. En effet, si $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$, pour p et q premiers distincts, alors $\left(\frac{a}{pq}\right) = 1$, or a ne saurait être un carré modulo pq.

3.3 Quelques applications

38 est-il un carré modulo 71 ?

$$\left(\frac{38}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{19}{71}\right) = -\left(\frac{14}{19}\right) = -(-1)(-1)\left(\frac{5}{7}\right) = -\left(\frac{2}{5}\right) = 1.$$

Pour quel nombre premier p 3 est-il un résidu quadratique ?

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \mod 3 \text{ et } p \equiv 1 \mod 4 \\ -1 & \text{si } p \equiv 1 \mod 3 \text{ et } p \equiv -1 \mod 4 \\ -1 & \text{si } p \equiv -1 \mod 3 \text{ et } p \equiv 1 \mod 4 \\ 1 & \text{si } p \equiv -1 \mod 3 \text{ et } p \equiv -1 \mod 4 \\ 0 & \text{si } p = 3 \end{cases}$$

Finalement 3 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1 \mod 12$ ou $p = 3$.

Exercice 3.13 Dans quels corps finis 3 est-il un carré ?

Étude des irréductibles des anneaux $\mathbb{Z}[\sqrt{d}]$: l'irréductibilité de $p \in \mathbb{Z}$ dans $\mathbb{Z}[\sqrt{d}]$, lorsque cet anneau est factoriel, est liée à l'intégrité de l'anneau quotient $\mathbb{Z}[\sqrt{d}]/(p) \simeq \mathbb{F}_p[X]/(X^2 - d)$, *i.e.* au fait que d soit ou non un carré modulo p.

Quel nombre premier p s'écrit $p = x^2 - 6y^2$, avec $x, y \in \mathbb{Z}$? Pour un tel nombre, $\left(\frac{6}{p}\right) = 1$, soit $1 = (-1)^{(p^2-1)/8}(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$, ce qui équivaut à $\left|\begin{array}{ccc} p \equiv 1 \text{ ou } 3 \mod 8 & \text{et} & p \equiv 1 \mod 3 \\ p \equiv -1 \text{ ou } -3 \mod 8 & \text{et} & p \equiv -1 \mod 3 \end{array}\right.$, soit, par le lemme Chinois, $p \equiv 1, 5, 19 \text{ ou } 23 \mod 24$. L'obtention d'une condition suffisante est plus délicat !

Il existe une infinité de nombre premier congru à 1 modulo 4 : soit p un facteur premier de $n!^2 + 1$, alors $p > n$, puisqu'il ne peut diviser $n!$, et $-1 \equiv n!^2 \mod p$, *i.e.* -1 est un carré modulo p et p est donc congru à 1 modulo 4.

Proposition 3.14 - Carrés de $\mathbb{Z}$ vs. carrés modulo p. Si un entier n est un résidu quadratique modulo presque tout nombre premier p, alors n est un carré dans $\mathbb{Z}$.

Démonstration. Raisonnons par l'absurde en considérant un entier n, qui peut être supposé sans perte de généralité sans facteur carré, résidu quadratique modulo presque tout p et qui n'est pas un carré dans $\mathbb{Z}$. On note $q_1, \ldots, q_s$ les premiers pour lesquels n est non-résidu quadratique et, pour aboutir à une contradiction, il suffit alors de montrer qu'il existe un entier impair $m \geqslant 3$ et premier à $q_1, \ldots, q_s$ tel que $\left(\frac{n}{m}\right) = -1$. D'après le point (iii) du théorème 3.8, $n \in \{-1, \pm 2\}$ est exclu ; écrivons alors $n = p_0 \ldots p_r$, avec $p_0 \in \{\pm 1, \pm 2\}$, p_i

premiers impairs distincts et $r \geqslant 1$, et considérons un entier impair m, dont l'existence est assurée par le théorème Chinois, défini par $m \equiv 1 \mod 8p_1 \dots p_{r-1}q_1 \dots q_s$ et $m \equiv u \mod p_r$, pour un entier u tel que $\left(\frac{u}{p_r}\right) = -1$. Alors $\left(\frac{p_0}{m}\right) = 1$ et $\left(\frac{p_i}{m}\right) = \left(\frac{m}{p_i}\right)$, puisque $m \equiv 1 \mod 8$, or $\left(\frac{m}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$, pour $1 \leqslant i \leqslant r-1$ et $\left(\frac{m}{p_r}\right) = \left(\frac{u}{p_r}\right) = -1$, d'où $\left(\frac{n}{m}\right) = -1$ et la contradiction recherchée.

QED

Théorème de Frobenius-Zolotarev : cf. exercice 4.12.

3.4 Sommes de Gauss (cf. [NQ92, (61) p.314])

Soit p et q deux nombres premiers distincts et ζ une racine primitive $p^{\text{ème}}$ de l'unité dans une extension de $\mathbb{F}_q$ (savoir pourquoi un tel élément existe !). Remarquons déjà que ζ^x ne dépend que de $x \mod p$ et garde donc un sens pour $x \in \mathbb{F}_p$. Considérons alors la *somme de Gauss* dans $\mathbb{F}_q(\zeta)$:

$$\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \zeta^x$$

Remarque 3.15 il s'agit de l'analogue, en caractéristique finie, de la somme de Gauss

$$\tau = \sum_{x \in \mathbb{F}_p} \exp\left(\frac{2ix^2}{p}\right) = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \exp\left(\frac{2ix}{p}\right).$$

La démonstration donnée ici de la loi de réciprocité quadratique repose sur la construction d'une racine carrée modulo q de $\left(\frac{-1}{p}\right) p$, obtenue grâce à τ comme l'affirme le lemme suivant :

Lemme 3.16 $\tau^2 = \left(\frac{-1}{p}\right) p$.

Démonstration.

$$\tau^2 = \sum_{x,y \in \mathbb{F}_p} \left(\frac{xy}{p}\right) \zeta^{x+y} = \sum_{u \in \mathbb{F}_p} S(u)\zeta^u, \quad \text{avec } S(u) = \sum_{x+y=u} \left(\frac{xy}{p}\right) = \sum_{x \in \mathbb{F}_p} \left(\frac{x(u-x)}{p}\right)$$

Pour $u = 0$, on a $S(u) = \sum_{x \in \mathbb{F}_p} \left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right)(p-1)$ et, pour $u \in \mathbb{F}_p^*$, la somme $S(u)$ vaut

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x(u-x)}{p}\right) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{-x^2(1-ux^{-1})}{p}\right) = \left(\frac{-1}{p}\right) \sum_{x \in \mathbb{F}_p^*} \left(\frac{1-ux^{-1}}{p}\right) = \left(\frac{-1}{p}\right) \left[\sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right) - 1\right],$$

en effet $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p \setminus \{1\}, x \longmapsto 1 - ux^{-1}$ est une bijection. Or, $\sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right) = 0$, d'après th.3.1.ii), soit $S(u) = -\left(\frac{-1}{p}\right)$. Finalement,

$$\tau^2 = \left(\frac{-1}{p}\right)\left(p - 1 - \sum_{u=1}^{p-1} \zeta^u\right) = \left(\frac{-1}{p}\right) p,$$

puisque ζ est une racine $p^{\text{ème}}$ de l'unité.

QED

Démonstration.[Loi de réciprocité quadratique, point (iv) du théorème 3.8] Pour p et q premiers impairs distincts, d'après le lemme précédent, $\left(\frac{-1}{p}\right)p$ est un carré modulo q si et seulement si $\tau \in \mathbb{F}_q$, *i.e.* $\tau^q = \tau$. Or

$$\tau^q = \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)^q \zeta^{qx} = \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)\zeta^{qx} = \left(\frac{q}{p}\right)\sum_{x\in\mathbb{F}_p}\left(\frac{qx}{p}\right)\zeta^{qx} = \left(\frac{q}{p}\right)\tau$$

Autrement dit, on a établit que

$$\left(\frac{q}{p}\right) = \left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

QED

Remarque 3.17 Les démonstrations de la loi de réciprocité quadratique sont innombrables [††]. On en trouvera une basée sur le résultant à l'exercice 4.13 et une autre basée sur les formes quadratiques dans [CG13, C.5 p. 185].

3.5 Extractions de racines carrées modulo p

Soit p un nombre premier et $q = p^n$. Une fois établi que $a \in \mathbb{F}_q$ est un carré, se pose la question d'expliciter une racine carrée de a.

Si $p = 2$: l'inverse de l'automorphisme de Frobenius $f : x \longmapsto x^2$ est son $n-1^{\text{ème}}$ itéré $f^{n-1} : x \longmapsto x^{2^{n-1}}$. Ainsi, l'unique racine carrée de a est obtenue comme $a^{2^{n-1}}$.

Un cas facile : si $q \equiv 3 \mod 4$, alors $\left(a^{(q+1)/4}\right)^2 = a^{(q+1)/2} = a^{(q-1)/2}a = a$ et $a^{(q+1)/4}$ est donc une racine carrée de a.

Remarque 3.18 On peut observer que ces deux premiers cas découlent du fait général suivant (avec $G = \mathbb{F}_q^{*2}$).

Dans un groupe G d'ordre m impair, pour tout $a \in G$, l'équation $y^2 = a$ admet $y = a^{(m+1)/2}$ pour solution.

Algorithme de Cipolla (1903) : pour le cas général avec p impair (le cas $q \equiv 1 \mod 4$ reste à traiter), nous présentons l'algorithme de Cipolla.

Soit $u \in \mathbb{F}_q$ tel que $u^2 - a \notin \mathbb{F}_q^2$ (on admettra que la probabilité qu'un tel $u \in \mathbb{F}_q$ convienne est d'environ $1/2$), alors $P = X^2 - 2uX + a$ est irréductible sur $\mathbb{F}_q$ (calculer le discriminant de P...). Soit ω la classe de X dans $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^2}$, on a $\omega\omega^q = P(0) = a$ (action du Frobenius). Ainsi $\pm\omega^{(q+1)/2}$ sont les deux racines carrées de a dans $\mathbb{F}_q$.

Remarque 3.19

1. Notons qu'on obtient systématiquement un algorithme polynomial en $O(\log_2 q)$ opérations dans $\mathbb{F}_q$, basé sur l'exponentiation rapide.
2. Un algorithme alternatif pour le calcul d'une racine carrée est celui de Shanks [Dem09, §5.1.3 p. 115].
3. La détermination d'une racine carrée de a se ramène aussi à la factorisation d'un polynôme, qui est un problème algorithmique facile sur les corps finis. En effet, dire que a est un carré de $\mathbb{F}_q$ équivaut à ce que $X^2 - a$ soit scindé sur $\mathbb{F}_q$ et expliciter les racines carrées de a revient à déterminer les racines de $X^2 - a$, *i.e.* ses facteurs linéaires.
4. Notons que l'extraction de racine carrée dans $\mathbb{Z}/n\mathbb{Z}$, pour n composé, est en revanche un problème difficile, équivalent notamment à celui de la factorisation de n (cf. [Zém00, §4.4.1]).

††. Voir la vertigineuse liste compilée par Franz Lemmermeyer à l'adresse http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html.

4 Exercices

Les exercices affublés d'une * sont ceux qu'il est indispensable de savoir faire, si l'on souhaite parler de corps finis et/ou de symbole de Legendre lors d'un oral de l'agrégation.

Exercice 4.1 * Donner la liste des sous-corps de $\mathbb{F}_{4096}$ ainsi que leurs inclusions respectives.

Exercice 4.2 * Soit $K = \mathbb{F}_2[X]/(X^4+X^3+X^2+X+1)$ et $L = \mathbb{F}_2[Y]/(Y^4+Y+1)$.

1. Montrer que $\overline{X}$ n'engendre pas $K^\star$. Trouver un générateur de $L^\star$.
2. Montrer que K et L sont des corps isomorphes et expliciter un isomorphisme.
3. Déterminer les polynômes minimaux sur $\mathbb{F}_2$ des éléments de K.

Exercice 4.3 - Facteurs invariants d'un corps fini. Soit p un nombre premier, $n \in \mathbb{N}_\star$ et $q = p^n$. Quels sont les facteurs invariants des deux groupes abéliens $(\mathbb{F}_q, +)$ et $(\mathbb{F}_q^\star, \times)$?

Exercice 4.4 Montrer que $\left| \begin{array}{ccc} \mathbb{F}_{p^n}^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^{1+p+\cdots+p^{n-1}} \end{array} \right.$ est un homomorphisme de groupes surjectif.

Exercice 4.5 * Soit α un élément primitif pour l'extension $\mathbb{F}_q/\mathbb{F}_p$, *i.e.* $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. α est-il un générateur de $\mathbb{F}_q^*$? Donner des exemples.

Exercice 4.6 Déterminer le corps $\mathbb{F}_3(\alpha)$, où α est une racine primitive $7^{\text{ème}}$ de l'unité.

Exercice 4.7 * Calculer les symboles de Legendre suivants :

1. $\left(\frac{-1}{17}\right)$, $\left(\frac{2}{29}\right)$, $\left(\frac{13}{17}\right)$, $\left(\frac{7}{19}\right)$, $\left(\frac{-8}{23}\right)$.
2. $\left(\frac{x}{p}\right)$ lorsque x est un générateur de $\mathbb{F}_p^*$.

Exercice 4.8 * Résoudre sur $\mathbb{F}_{101}$ et sur $\mathbb{F}_{109}$ l'équation $x^2+5x+3=0$.

Exercice 4.9 Montrer que tout entier a est un carré modulo une infinité de nombre premier.
(Indication : on pourra considérer, pour $n \geqslant a$, l'entier $b_n = \frac{n!^2}{a} - 1$).

Exercice 4.10 - Racines de l'unité. Soit p un nombre premier, $n \in \mathbb{N}_*$ et $q = p^n$.

1. Montrer que X^2+X+1 est irréductible sur $\mathbb{F}_q$ si et seulement si $q \equiv -1 \mod 3$.
   (Indication : on pourra distinguer les cas $p=3$ et $p \neq 3$ et remarquer que $(X^2+X+1)(X-1) = X^3-1$.)
2. Montrer que X^2+1 est irréductible sur $\mathbb{F}_q$ si et seulement si $q \equiv -1 \mod 4$
   (Indication : on pourra distinguer les cas $p=2$ et $p \neq 2$ et remarquer que $(X^2+1)(X^2-1) = X^4-1$.)
3. En déduire que si $q \equiv -1 \mod 12$, alors $\mathbb{F}_q[X]/(X^2+X+1)$ et $\mathbb{F}_q[X]/(X^2+1)$ sont isomorphes et décrire un isomorphisme explicite entre ces deux corps.

Exercice 4.11 - Fonctions polynomiales sur un corps fini. Soit k un corps et

$$\varphi : \left| \begin{array}{ccc} k[X_1, \dots, X_n] & \longrightarrow & \mathcal{F}(k^n, k) \\ P & \longmapsto & \widetilde{P} \end{array} \right. , \text{ où } \widetilde{P} \text{ désigne la fonction polynomiale associée à } P.$$

1. Montrer que φ est un morphisme de k-algèbres.
2. Montrer que cette application est injective lorsque k est infini.
3. On suppose désormais que k est un corps fini à q éléments.
   Montrer que le noyau de φ est l'idéal $(X_1^q - X_1, \dots, X_n^q - X_n)$ et que φ est surjective (on pourra s'intéresser aux fonctions associées aux polynômes $1 - (X - a)^{q-1}$ pour construire les indicatrices des points de k).

Exercice 4.12 - Théorème de Frobenius-Zolotarev, [BMP05, 5.4 p. 251].

1. Soit k un corps et M un groupe abélien. Montrer que si $k \neq \mathbb{F}_2$ ou $n \neq 2$, alors tout morphisme de groupes $f : \mathrm{GL}_n(k) \longrightarrow M$ se factorise de manière unique à travers le déterminant , *i.e.* il existe un unique morphisme de groupes $\delta : k^\star \longrightarrow M$, tel que $f = \delta \circ \det$.
2. Soit p premier impair. Montrer que le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.
3. En déduire le théorème de Frobenius-Zolotarev : soit p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie, alors, pour tout $u \in \mathrm{GL}(V)$,
$$\varepsilon(u) = \left(\frac{\det u}{p}\right).$$
   (Indication : on pourra considérer le $\mathbb{F}_p$-endomorphisme u de $\mathbb{F}_{p^n}$ défini par $u(x) = gx$, pour g un générateur de $\mathbb{F}_{p^n}^*$).
4. Application : la signature de l'automorphisme de Frobenius $F : x \longmapsto x^p$ sur $\mathbb{F}_{p^n}$, pour p premier impair, est $\varepsilon(F) = (-1)^{(p-1)(n+1)/2}$.

Exercice 4.13 - Une autre démonstration de la loi de réciprocité quadratique, cf. [Hin08, 7.14 p. 70].

Soit $P = \prod_{i=1}^r (X - \alpha_i)$ et $Q = \prod_{i=1}^s (X - \beta_i)$ deux polynômes dans $A[X]$, on définit leur résultant par la formule

$$\mathrm{Res}\,(P, Q) = \prod_{i=1}^{r} \prod_{j=1}^{s} (\alpha_i - \beta_j).$$

On introduit enfin, pour $n \geqslant 3$, les polynômes unitaires Φ_n^+ définis par $(\Phi_n^+)^2 = \prod_{\zeta \in \mu_n^\star(\mathbb{C})} (X - \zeta - \zeta^{-1})$.

1. Montrer que $\mathrm{Res}\,(Q, P) = (-1)^{rs} \mathrm{Res}\,(P, Q)$.
2. On suppose désormais $P, Q \in \mathbb{Z}[X]$ et, pour q premier impair, on note $\widetilde{P}$ et $\widetilde{Q}$ leur réduction modulo q. Établir que $\mathrm{Res}\,(P, Q) \equiv \mathrm{Res}\left(\widetilde{P}, \widetilde{Q}\right) \mod q$.
3. Montrer que $\deg \Phi_n^+ = \varphi(n)/2$, $\Phi_n(X) = X^{\varphi(n)/2} \Phi_n^+(X + X^{-1})$ et $\Phi_n^+ \in \mathbb{Z}[X]$. En déduire, en particulier, que $\Phi_p^+(2) = \Phi_p(1) = p$.
4. Montrer que $\widetilde{\Phi}_q^+ = (X - 2)^{(q-1)/2}$ dans $\mathbb{F}_q[X]$.
5. Déduire de ce qui précède que $\mathrm{Res}\left(\widetilde{\Phi}_q^+, \widetilde{\Phi}_p^+\right) \equiv p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \mod q$.
6. Montrer que $\mathrm{Res}\left(\Phi_q^+, \Phi_p^+\right) = \prod_{\eta \in \mu_q^\star(\mathbb{C})} \eta^{-(p-1)/2} \Phi_p(\eta)$ et en déduire que $\mathrm{Res}\left(\Phi_q^+, \Phi_p^+\right) \in \{\pm 1\}$.
7. Démontrer la formule $\mathrm{Res}\left(\Phi_q^+, \Phi_p^+\right) = \left(\frac{p}{q}\right)$ et en déduire une preuve de la loi de réciprocité quadratique.