Université P. et M. Curie (Paris VI) date de mise à jour: 22/02/2011
Deuxième semestre 2010/2011

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales

Deuxième fascicule : 09/02/2011

2 Corps finis

Références :
M. Mignotte, *Algèbre concrète*, Cours et exercices ; Chap. III : Les corps finis. Ellipses, 2003, 206p.
M. Demazure [2], Chap. 8.
S. Lang [7], Chap. 5 § 5.
D.S. Dummit & R.M. Foote [3], § 14.3.
R. Lidl & H. Niederreiter [8].
V. Shoup [10], Chap. 20.
M. Waldschmidt, *Course on finite fields*, CIMPA Research school on number theory in cryptography and its applications. School of Science, Kathmandu University, Dhulikhel, Népal.
`http://www.math.jussieu.fr/~miw/articles/pdf/FiniteFieldsKathmanduCIMPA2010.pdf`.
Wikipedia : Corps fini
`http://fr.wikipedia.org/wiki/Corps_fini`

2.1 Structure des corps finis

Un corps fini est appelé en anglais *Gauss Field*. On connaît déjà les corps finis avec p éléments quand p est un nombre premier : c'est le quotient $\mathbf{Z}/p\mathbf{Z}$. Étant donnés deux corps finis F et F' ayant tous deux p éléments avec p premier, il y a un unique isomorphisme $F \to F'$. Pour p premier, on notera $\mathbf{F}_p$ l'unique corps ayant p éléments.

La caractéristique d'un corps fini F est un nombre premier p, donc son sous–corps premier est $\mathbf{F}_p$. Comme F est un espace vectoriel de dimension finie sur $\mathbf{F}_p$, son nombre d'éléments est une puissance de p ; plus précisément, si s est le degré de F comme $\mathbf{F}_p$–espace vectoriel, $[F : \mathbf{F}_p] = s$, alors F a p^s éléments. Ainsi le nombre d'éléments d'un corps fini est une puissance d'un nombre premier, et ce nombre premier est la caractéristique du corps.

`Exemple le plus simple d'un corps fini qui n'est pas un corps premier`.

Soit $\mathbf{F}_4$ un corps ayant 4 éléments. Les deux éléments autres que 0 et 1 jouent exactement le même rôle. L'application qui les permute et qui laisse fixes 0 et 1 est un automorphisme de $\mathbf{F}_4$, c'est le Frobenius Frob_2. Notons α un des deux éléments de $\mathbf{F}_4$ qui n'est ni 0 ni 1. L'autre doit être à la fois α^2 et $\alpha + 1$, donc $\alpha^2 = \alpha + 1$. Alors $\mathbf{F}_4 = \{0, 1, \alpha, \alpha^2\}$ et α est un générateur du groupe multiplicatif $\mathbf{F}_4^\times = \{1, \alpha, \alpha^2\}$. Le polynôme $X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur le corps fini $\mathbf{F}_2$ à deux éléments, ce corps possède donc une unique extension quadratique $\mathbf{F}_4$, à isomorphisme près.

Voici les tables d'addition et de multiplication de ce corps $\mathbf{F}_4$:

$(\mathbf{F}_4,+)$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$(\mathbf{F}_4,\times)$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Les éléments de ce groupe additif d'ordre 4 sont d'ordre 1 ou 2 ; en particulier le groupe additif de $\mathbf{F}_4$ n'est pas cyclique, donc pas isomorphe au groupe additif de l'anneau $\mathbf{Z}/4\mathbf{Z}$. Les éléments inversible de l'anneau $\mathbf{Z}/4\mathbf{Z}$ sont les classes de 1 et 3, il y en a 2, ils forment donc un groupe cyclique d'ordre 2, alors que les éléments du groupe multiplicatif $\mathbf{F}_4^\times$ sont tous inversibles et forment un groupe cyclique d'ordre 3.

Pour un corps fini F, le groupe multiplicatif $F^\times$ est fini, donc tout élément est de torsion, ce qui signifie que tous les éléments non nuls de F sont des racines de l'unité. C'est pourquoi les polynômes cyclotomiques jouent un rôle si important dans l'étude des corps finis.

Soit K un corps de caractéristique finie p et soit m un entier positif. Écrivons $m = p^s n$ avec $s \geq 0$ et $\mathrm{pgcd}(p,n) = 1$. Dans $K[X]$ on a

$$X^m - 1 = (X^n - 1)^{p^s}. \tag{2.1}$$

Soit maintenant K un corps fini ayant q éléments. Le groupe multiplicatif de K est d'ordre $q-1$, tout élément de $K^\times$ vérifie $x^{q-1} = 1$, par conséquent tout élément de K vérifie $x^q = x$. Le nombre de racines d'un polynôme dans un corps étant majoré par le degré, on en déduit que $K^\times$ est l'ensemble des racines du polynôme $X^{q-1} - 1$, tandis que K est l'ensemble des racines du polynôme $X^q - X$:

$$X^{q-1} - 1 = \prod_{x \in K^\times} (X - x), \qquad X^q - X = \prod_{x \in K} (X - x). \tag{2.2}$$

Exercice. Montrer que si F est un corps fini avec q éléments, alors le polynôme $X^q - X + 1$ n'a pas de racine dans F. En déduire que F n'est pas algébriquement clos.

Les relations (2.2) ont pour conséquence :

Proposition 2.3. *Toute extension finie de corps finis est normale et séparable.*

Démonstration. Soient K/F une extension finie de corps finis, q le nombre d'éléments de K, $\mathbf{F}_p$ le sous–corps premier. Le corps K est le corps de décomposition sur $\mathbf{F}_p$ (donc sur F) du polynôme $X^q - X$, par conséquent l'extension $K/\mathbf{F}_p$ est normale, et donc K/F aussi. Si α est un élément de K, il est algébrique sur F, son polynôme irréductible sur F divise $X^q - X$, il est totalement décomposé sur K, sans racine multiple (noter que p ne divise pas $q-1$), donc il est séparable. □

Voici plusieurs variantes de la solution d'un exercice proposé au début du § 1.7.

Proposition 2.4. *Si K est un corps et G un sous-groupe fini du groupe multiplicatif $K^\times$, alors G est cyclique. Si n est l'ordre de G, alors G est l'ensemble des racines du polynôme $X^n - 1$ qui est donc totalement décomposé dans K.*

On en déduit que l'ordre d'un sous-groupe fini du groupe multiplicatif $K^\times$ est premier avec p.

Première démonstration. La suite $(\Phi_n)_{n\geq 0}$ des polynômes cyclotomiques peut être définie par récurrence sur n par les relations $\Phi_0 = 1$, $\Phi_1(X) = X - 1$ et

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

(cf. (1.23)). Les racines du polynôme $X^n - 1$ dans K sont les racines n-ièmes de l'unité dans K, les racines du polynôme $\Phi_n(X)$ dans K sont les racines primitives n-ièmes de l'unité dans K, c'est–à–dire les éléments d'ordre n dans le groupe multiplicatif $K^\times$. Maintenant soit G un sous-groupe de $K^\times$ d'ordre n. Tout élément x de G vérifie $x^n = 1$, donc d'après (1.23) est racine d'un des Φ_d pour d divisant n. Notons a_d le nombre de racines de $\Phi_d(X)$ dans K. On vient de montrer $n \leq \sum_{d|n} a_d$. Mais Φ_d est un polynôme de degré $\varphi(d)$, et n'a donc pas plus de $\varphi(d)$ racines dans le corps K. Les degrés des deux membres de (1.23) donnent

$$\sum_{d|n} \varphi(d) = n. \tag{2.5}$$

Ainsi

$$n \leq \sum_{d|n} a_d \leq \sum_{d|n} \varphi(d) = n.$$

Il en résulte que $a_d = \varphi(d)$ pour tout $d|n$, en particulier pour $d = n$, donc $a_n \geq 1$ et il existe dans G au moins un élément d'ordre n. Ceci montre que G est cyclique, que G est l'unique sous-groupe de $K^\times$ d'ordre n (il est constitué des racines du polynôme $X^n - 1$) et que le polynôme $X^n - 1$ est complètement décomposé dans K sans racine multiple. Les générateurs du groupe cyclique G sont les $\varphi(n)$ racines de Φ_n.

□

Deuxième démonstration. Tout élément de G est racine de $X^n - 1$, donc G est l'ensemble des racines de ce polynôme, et les polynômes cyclotomiques Φ_d avec d divisant n ont toutes leurs racines dans G. C'est le cas de Φ_n. Or la proposition 1.28 affirme que toute racine de Φ_n est d'ordre n, donc G est cyclique engendré par toute racine de Φ_n.

□

Troisième démonstration. Désignons par e l'exposant de G : c'est le ppcm des ordres des éléments de G, c'est donc le plus petit entier tel que $x^e = 1$ pour tout x dans G. Comme G est abélien il existe un élément x_0 d'ordre e dans G.

D'après le théorème de Lagrange, e divise n. Tout x dans G est racine du polynôme $X^e - 1$. Comme G est d'ordre n, il y a n racines dans K de ce polynôme $X^e - 1$ de degré $e \leq n$. Donc $e = n$ et x_0 est un générateur de G.

□

Par exemple, quand p est un nombre premier, le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $\varphi(p-1)$. Un entier est appelé *racine primitive modulo* p s'il est premier avec p et si sa classe modulo p est un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$. Par conséquent, un entier a est racine primitive modulo p si et seulement si

$$a^{(p-1)/q} \not\equiv 1 \bmod p$$

pour tout diviseur premier q de $p-1$.

Si a et n sont premiers entre eux, l'*ordre de a modulo n* est l'ordre de la classe de a dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$. Autrement dit, c'est le plus petit entier ℓ tel que a^ℓ est congruent à 1 modulo n.

Exercice. Soient p un nombre premier, Φ_p le polynôme cyclotomique d'indice p :

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1},$$

n un entier ≥ 1, q un diviseur premier du nombre $\Phi_p(np)$.
a) Vérifier $q \neq p$, $\mathrm{pgcd}(q, n) = 1$, $np \not\equiv 1 \pmod q$, $(np)^p \equiv 1 \pmod q$.
b) Quel est l'ordre de np modulo q ?
c) En déduire que q est congru à 1 modulo p.
d) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo p.

Soit K un corps et soit m un entier positif. Le groupe multiplicatif $K^\times$ possède un sous-groupe fini d'ordre m si et seulement si le polynôme $X^m - 1$ est complètement décomposé dans $K[X]$ avec m racines distinctes dans K. C'est aussi équivalent de dire que le polynôme cyclotomique $\Phi_m(X)$ est complètement décomposé dans $K[X]$ avec $\varphi(m)$ racines distinctes dans K. Dans ce cas, ce sous-groupe de $K^\times$ d'ordre m est unique, il est composé des racines du polynôme $X^m - 1$ qui sont les racines m–ièmes de l'unité, tandis que les racines du polynôme cyclotomique $\Phi_m(X)$ sont les racines primitives m–ièmes de l'unité, qui ne sont autres que les générateurs de l'unique sous–groupe d'ordre m de $K^\times$, et m n'est pas divisible par p.

En passant nous pouvons compléter la démonstration du corollaire 1.21 :

Proposition 2.6. *Si F est un corps fini et K une extension finie de F, alors l'extension K/F est monogène.*

Démonstration de la proposition 2.6. Soit q le nombre d'éléments de K ; le groupe multiplicatif $K^\times$ est cyclique : soit α un générateur de ce groupe. Alors

$$K = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\right\} = \mathbf{F}_p(\alpha),$$

et à plus forte raison $K = F(\alpha)$.

□

Lemme 2.7. *Soit A un anneau de caractéristique p avec p premier. Pour x et y dans A, on a $(x+y)^p = x^p + y^p$.*

Démonstration. Si n est un entier dans l'intervalle $1 \leq n < p$, le coefficient du binôme

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

est divisible par p. □

Le lemme 1.27 résulte de l'énoncé suivant, qui interviendra plusieurs fois dans la suite.

Lemme 2.8. *Soient F un corps fini à q éléments, K une extension de F et f un élément de $K[X]$. Alors $f \in F[X]$ si et seulement si $f(X)^q = f(X^q)$.*

Démonstration. Nous avons vu que, pour a dans K, on a $a^q = a$ si et seulement si $a \in F$. Comme q est une puissance de la caractéristique p de K, si on écrit

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

on a

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}$$

et par récurrence

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}$$

Par conséquent $f(X)^q = f(X^q)$ si et seulement si $a_i^q = a_i$ pour tout $i = 0, 1, \ldots, n$.

□

Proposition 2.9. *Soit K un corps de caractéristique p. Alors l'application*

$$\begin{array}{rccc} \mathrm{Frob}_p : & K & \to & K \\ & x & \mapsto & x^p \end{array}$$

est un endomorphisme de K. On l'appelle le Frobenius *de K sur $\mathbf{F}_p$.*

Démonstration. Cette application est un morphisme de corps, puisque, pour x et y dans K, on a trivialement,

$$\mathrm{Frob}_p(xy) = \mathrm{Frob}_p(x)\mathrm{Frob}_p(y),$$

tandis que le lemme 2.7 montre que

$$\mathrm{Frob}_p(x+y) = \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y).$$

□

Comme tout homomorphisme de corps, Frob_p est injectif (on peut aussi noter que la condition $x^p = 0$ implique $x = 0$. Quand le corps K est fini, le Frobenius Frob_p est surjectif car il est injectif et qu'il envoie l'ensemble fini K dans lui–même. Quand le corps K est algébriquement clos, le Frobenius Frob_p est encore surjectif, puisque tout élément de K est une puissance p–ième dans K. Mais, par exemple, quand K est le corps $\mathbf{F}_p(X)$ des fractions rationnelles sur $\mathbf{F}_p$, l'image du Frobenius est le sous–corps $\mathbf{F}_p(X^p)$, qui est un sous–corps strict de $\mathbf{F}_p(X)$, bien qu'il lui soit isomorphe.

Si s est un entier ≥ 0, on désigne par Frob_p^s l'endomorphisme itéré, que l'on note aussi Frob_{p^s} :

$$\mathrm{Frob}_p^0 = I, \quad \mathrm{Frob}_{p^s} = \mathrm{Frob}_{p^{s-1}} \circ \mathrm{Frob}_p \qquad (s \geq 1),$$

de sorte que $\mathrm{Frob}_{p^s}(x) = x^{p^s}$ pour $x \in K$. Si K contient un sous–corps F ayant $q = p^s$ éléments (auquel cas ce sous–corps est unique), alors, d'après (2.2), l'ensemble des éléments de K fixés par Frob_{p^s} est F :

$$F = \left\{ x \in K \ ; \ \mathrm{Frob}_{p^s}(x) = x \right\},$$

et donc Frob_{p^s} est un F–endomorphisme de K appelé *Frobenius de K sur F.*

Proposition 2.10. *Soit K/F une extension finie de corps finis de degré d. Alors le groupe* $\mathrm{Aut}_F K$ *des F–automorphismes de K est cyclique d'ordre d engendré par le Frobenius* Frob_q *de K sur F :*

$$\mathrm{Aut}_F K = \{\mathrm{Frob}_{q^\ell} \ ; \ \ell = 0, 1, \ldots, d-1\}.$$

Démonstration. Soit $q = p^r$ le nombre d'éléments de K et soit α un générateur du groupe cyclique $K^\times$, c'est–à–dire un élément d'ordre $p^r - 1$:

$$K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^r-2}\}.$$

Pour $1 \le \ell < r$ on a $1 \le p^\ell - 1 < p^r - 1 = q - 1$, donc $\alpha^{p^\ell - 1} \ne 1$ et $\mathrm{Frob}_{p^\ell}(\alpha) \ne \alpha$. Il en résulte que les éléments $\mathrm{Frob}_{p^\ell}(\alpha) \ ; \ \ell = 0, 1, \ldots, r-1$ sont r conjugués distincts de α sur $\mathbf{F}_p$, et comme $K = \mathbf{F}_p(\alpha)$ avec $[K : \mathbf{F}_p] = r$, on en déduit que ce sont tous les conjugués de α. Un automorphisme de K est entièrement déterminé par sa valeur en α. Par conséquent le groupe des automorphismes de K (qui sont évidemment les $\mathbf{F}_p$–automorphismes de K) est cyclique engendré par Frob_p :

$$\mathrm{Aut} K = \{\mathrm{Frob}_{p^\ell} \ ; \ \ell = 0, 1, \ldots, r-1\}.$$

Notons maintenant $s = [F : \mathbf{F}_p]$ de sorte que $r = ds$. Un élément Frob_{p^ℓ} de $\mathrm{Aut} K$ est un F–automorphisme de K si et seulement si ℓ est multiple de s, donc si et seulement si p^ℓ est une puissance de p^s. Il en résulte que, dans le groupe $\mathrm{Aut}_F K$, Frob_q est d'ordre d et il engendre le sous-groupe $\mathrm{Aut}_F K$. □

2.2 Construction des corps finis et théorie de Galois

Théorème 2.11. *Soient p un nombre premier et s un entier positif. On pose $q = p^s$. Il existe un corps ayant q éléments. Deux corps ayant q éléments sont isomorphes. Si Ω est un corps algébriquement clos de caractéristique p, alors Ω contient un unique sous-corps fini ayant q éléments,*

Démonstration. Soit K un corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. Alors K est l'ensemble des racines de ce polynôme et donc a q éléments.

Inversement, si K est un corps avec q éléments, alors K est l'ensemble des racines du polynôme $X^q - X$.

Par conséquent si Ω est un corps algébriquement clos de caractéristique p, alors le seul sous-corps de Ω ayant q éléments est l'ensemble des racines du polynôme $X^q - X$.

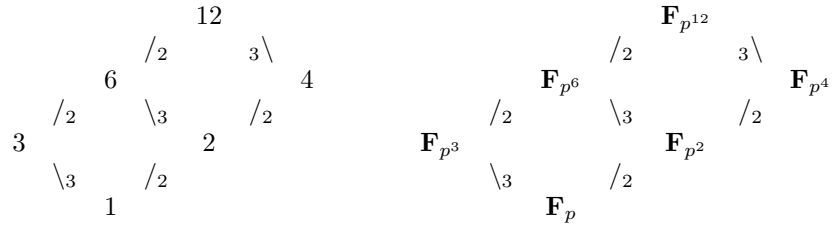
□

Notons $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. Pour chaque entier $s \ge 1$, il existe un unique sous-corps fini de $\overline{\mathbf{F}}_p$ ayant p^s éléments : c'est l'ensemble des racines du polynôme $X^{p^s} - X$. On le note $\mathbf{F}_{p^s}$. Pour n et m entiers positifs, on a l'équivalence

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divise } m. \tag{2.12}$$

Étant donné un entier $n \ge 2$, un groupe G cyclique d'ordre n et un corps fini F ayant p^n éléments, il y a des bijections naturelles entre
• l'ensemble des diviseurs de n,
• l'ensemble des sous–groupes de G,
• l'ensemble des sous–corps de F.

Pour illustrer ce fait, voici les graphes des diviseurs de 12 et des sous–corps du corps $\mathbf{F}_{p^{12}}$ pour p premier :



D'après le théorème 1.19, pour une extension finie K/F de degré n, les conditions suivantes sont équivalentes :
(i) Le groupe des F–automorphismes de K a n éléments.
(ii) L'extension K/F est normale et séparable.
Une telle extension est appelée *Galoisienne* et le groupe $\mathrm{Aut}_F K$ des F–automorphismes de K est appelé le *groupe de Galois de l'extension*. On le note $\mathrm{Gal}(K/F)$. La théorie de Galois établit alors une bijection entre les sous-groupes H de $G := \mathrm{Gal}(K/F)$ et les sous–corps E de K contenant F :
• À tout sous-groupe H de G, on associe le sous–corps $E = K^H$ de K invariant par H :

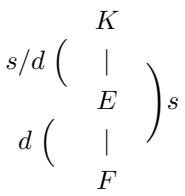
$$K^H := \{x \in K \ ; \ \sigma(x) = x \ \text{ pour tout } \ \sigma \in H\}$$

• À tout sous-corps E de K contenant F, on associe le groupe de Galois $H = \mathrm{Gal}(K/E)$ de K sur E, qui est un sous–groupe de G :

$$\begin{array}{ccc} G & & K \\ \bigcup & & \bigcup \\ H & \longmapsto & K^H \end{array} \qquad\qquad \begin{array}{ccc} K & & G \\ \bigcup & & \bigcup \\ E & \longmapsto & \mathrm{Gal}(K/E) \end{array}$$

Pour les corps finis, l'énoncé est le suivant, il résulte de ce que nous avons démontré :

Théorème 2.13 (Théorie de Galois pour les corps finis)**.** *Soit F un corps fini ayant q éléments et soit K une extension finie de F de degré s. Il y a une bijection entre l'ensemble des sous–corps E de K contenant F et les diviseurs d de s.*



• *Si E est un sous–corps de K contenant F, alors le nombre d'éléments de E est de la forme q^d où d divise s.*
• *Inversement, si d divise s, alors K a un unique sous corps E ayant q^d éléments, c'est le corps fixé par* Frob_{q^d} *:*

$$E = \{\alpha \in K \ ; \ \mathrm{Frob}_{q^d}(\alpha) = \alpha\}.$$

et ce corps E contient F.

Le théorème qui suit donne une recette pour déterminer le polynôme irréductible d'un élément algébrique sur un corps fini : on considère les images de cet élément sous l'action du Frobenius itéré.

Théorème 2.14. *Soient F un corps fini à q éléments, K une extension de F et α un élément non nul de K algébrique sur F. Il existe des entiers $\ell \geq 1$ tels que $\alpha^{q^\ell} = \alpha$. Notons r le plus petit :*

$$r = \min\{\ell \geq 1 \,;\, \mathrm{Frob}_q^\ell(\alpha) = \alpha\}.$$

Alors le corps $F(\alpha)$ a q^r éléments et le polynôme irréductible de α sur F est

$$\prod_{\ell=0}^{r-1} \big(X - \mathrm{Frob}_q^\ell(\alpha)\big) = \prod_{\ell=0}^{r-1} (X - \alpha^{q^\ell}). \tag{2.15}$$

Démonstration. La démonstration reprend les arguments de celle de la proposition 2.10. Soit $s = [F(\alpha) : F]$. L'extension $F(\alpha)/F$ est galoisienne de groupe de Galois le groupe cyclique d'ordre s engendré par Frob_q. Les conjugués de α sur F sont les images de α par ces automorphismes. Comme Frob_q^s est l'identité sur $F(\alpha)$ on a $\mathrm{Frob}_q^s(\alpha) = \alpha$. Si $\mathrm{Frob}_q^h(\alpha) = \mathrm{Frob}_q^\ell(\alpha)$, alors $\mathrm{Frob}_q^{h-\ell}(\alpha) = \alpha$. Il en résulte que si r est le plus petit entier positif tel que $\mathrm{Frob}_q^r(\alpha) = \alpha$, alors, pour $\ell \in \mathbf{Z}$, si j est le reste de la division Euclidienne de ℓ par r on a $\mathrm{Frob}_q^\ell(\alpha) = \mathrm{Frob}_q^j(\alpha)$. Ceci montre que l'ensemble des conjugués de α est $\{\alpha, \mathrm{Frob}_q(\alpha), \mathrm{Frob}_q^2(\alpha), \ldots, \mathrm{Frob}_q^{r-1}(\alpha)\}$. Donc $r = s$. Le théorème 2.14 en résulte.

□

Soit F un corps fini ayant q éléments et soit E est une extension finie de degré s de F. Pour $\alpha \in E$, la *norme de α de E sur F* est (voir § 3.2) le produit des conjugués de α sur F, tandis que la *trace de α de E sur F* est la somme de ces conjugués

$$\mathrm{N}_{E/F}(\alpha) = \prod_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \alpha^{(q^s-1)/(q-1)}, \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}$$

Pour $\alpha \in F$ on a $\mathrm{N}_{E/F}(\alpha) = \alpha^s$ et $\mathrm{Tr}_{E/F}(\alpha) = s\alpha$. La norme $\mathrm{N}_{E/F}$ induit un homomorphisme surjectif du groupe $E^\times$ sur $F^\times$. La trace $\mathrm{Tr}_{E/F}$ est une application F–linéaire surjective de E sur F, dont le noyau est formé des racines dans E du polynôme $X + X^q + \cdots + X^{q^{s-1}}$.

Soit p un nombre premier. Désignons par $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. L'extension $\overline{\mathbf{F}}_p/\mathbf{F}_p$ est algébrique infinie, normale et séparable : c'est une extension *galoisienne infinie*. Son *groupe de Galois* $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est le groupe des automorphismes de $\mathbf{F}_p$. On le décrit comme la limite projective des groupes de Galois des extensions finies de $\mathbf{F}_p$ contenues dans $\overline{\mathbf{F}}_p/\mathbf{F}_p$:

$$\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) = \varprojlim_{[L:\mathbf{F}_p]<\infty} \mathrm{Gal}(L/\mathbf{F}_p).$$

Ainsi $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est le groupe

$$\hat{\mathbf{Z}} := \varprojlim_{n\to\infty} \mathbf{Z}/n\mathbf{Z}.$$

Cette limite projective est l'ensemble des $(a_n)_{n\geq 1}$ dans le produit Cartésien $\prod_{n\geq 1}\mathbf{Z}/n\mathbf{Z}$ qui vérifient $s_{nm}(a_n) = a_m$ pour tout couple d'entiers positifs (n,m) où m divise n, en désignant par

$$s_{n,m} : \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z}$$

la surjection canonique.

On a aussi

$$\hat{\mathbf{Z}} := \prod_p \mathbf{Z}_p \quad \text{avec} \quad \mathbf{Z}_p = \varprojlim_{r\to\infty} \mathbf{Z}/p^r\mathbf{Z}.$$

Voir par exemple [3] exercice 19 p. 635 et [6] Appendice p. 288.

2.3 Décomposition des polynômes cyclotomiques en facteurs irréductibles

L'exercice suivant explique pourquoi, quand on étudie la décomposition d'un polynôme cyclotomique Φ_n en facteurs irréductibles sur un corps fini, on suppose l'indice n premier à la caractéristique.

Exercice. Soit K un corps de caractéristique p. Vérifier, pour $r \geq 1$ et $m \geq 1$,

$$\Phi_{mp^r}(X) = \Phi_m(X)^{p^{r-1}(p-1)}.$$

`Indication:` *On peut utiliser* (2.1) *et démontrer le résultat par récurrence.*

La démonstration de la proposition 2.16 utilisera le résultat de l'exercice suivant :

Exercice. Soient K un corps, m et n deux entiers ≥ 1, a et b deux entiers ≥ 2. Vérifier que les conditions suivantes sont équivalentes.
(i) n divise m
(ii) Dans $K[X]$ le polynôme $X^n - 1$ divise $X^m - 1$
(iii) $a^n - 1$ divise $a^m - 1$
(ii') Dans $K[X]$ le polynôme $X^{a^n} - X$ divise $X^{a^m} - X$
(iii') $b^{a^n} - b$ divise $b^{a^m} - b$.

`Indication.` *Si r est le reste de la division de m par n, alors $a^r - 1$ est le reste de la division de $a^m - 1$ par $a^n - 1$.*

Proposition 2.16. *Soient F un corps fini à q éléments et r un entier positif. Le polynôme $X^{q^r} - X$ est le produit de tous les polynômes unitaires irréductibles de $F[X]$ dont le degré divise r :*

$$X^{q^r} - X = \prod_{d|r} \prod_{f\in E_q(d)} f(X)$$

où $E_q(d)$ est l'ensemble des polynômes unitaires irréductibles de $\mathbf{F}_q[X]$ de degré d.

Démonstration. Soit $f \in F[X]$ un polynôme irréductible de degré d. Notons $K = F[X]/(f)$ son corps de rupture sur K : c'est une extension de degré d de F, il a donc q^d éléments, la classe α de X vérifie $\alpha^{q^d} = \alpha$, donc le polynôme $X^{q^d} - X$ est multiple de f.

Si d divise r, alors le polynôme $X^{q^r} - X$ est multiple de $X^{q^d} - X$, donc multiple de f. Ceci montre que $X^{q^r} - X$ est multiple de tous les polynômes irréductibles de degré divisant r. Comme sa dérivée est -1, il n'a pas de facteur multiple.

Réciproquement si le polynôme $X^{q^r} - X$ est multiple de f, on a $\alpha^{q^r} = \alpha$ dans K, l'ensemble des $\alpha \in K$ qui vérifient $\alpha^{q^r} = \alpha$ est K lui-même et tout générateur γ du groupe multiplicatif $K^\times$, qui est d'ordre $q^d - 1$, satisfait $\gamma^{q^r-1} = 1$. Il en résulte que $q^d - 1$ divise $q^r - 1$, donc d divise r. □

Par définition, une *fonction arithmétique* est une application définie sur les entiers > 0. Une fonction arithmétique est dite *multiplicative* si elle est à valeurs entières et vérifie $f(ab) = f(a)f(b)$ quand a et b sont des entiers positifs premiers entre eux. Un exemple de fonction multiplicative est *l'indicatrice d'Euler* $\varphi(n)$ qui compte le nombre d'entiers k dans l'intervalle $1 \le k \le n$ avec $\mathrm{pgcd}(k, n) = 1$) (c'est le degré du polynôme cyclotomique Φ_n). Une fonction multiplicative est déterminée par ses valeurs aux entiers qui sont puissances d'un nombre premier.

La *fonction de Möbius* μ (voir par exemple [5], Chap. XVI, ou [10] § 2.9) est la fonction arithmétique multiplicative, à valeurs dans $\{0, 1, -1\}$ caractérisée par les propriétés $\mu(1) = 1$, $\mu(p) = -1$ pour p premier et $\mu(p^m) = 0$ pour p premier et $m \ge 2$. Ainsi $\mu(a) = 0$ si et seulement si a a des diviseurs carrés. Un entier positif a sans facteur carré (*quadratfrei* en allemand et *squarefree* en anglais) est produit de nombres premiers deux-à-deux distincts, et si s est le nombre de ces facteurs, alors $\mu(a) = (-1)^s$:

$$\mu(p_1 \cdots p_s) = (-1)^s.$$

Il y a plusieurs variantes de la *formule d'inversion de Möbius* ([7] Chap. II Ex. 12.c et Chap. V, Ex. 21 ; [5] § 16.4). La plus classique énonce que si f et g sont deux fonctions arithmétiques à valeurs dans un groupe additif, alors les deux conditions suivantes sont équivalentes :
(i) *pour tout entier* $n \ge 1$,

$$g(n) = \sum_{d|n} f(d).$$

(ii) *Pour tout entier* $n \ge 1$,

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Par exemple la relation (2.5) est équivalente à

$$\varphi(n) = \sum_{d|n} \mu(n/d) d \quad \text{for all } n \ge 1.$$

Exercice. a) Vérifier

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \ge 2. \end{cases}$$

b) Pour tout nombre complexe s la fonction f définie par $f(n) = n^s$ est multiplicative.
On définit une loi multiplicative $\star$ sur l'ensemble des fonctions arithmétiques, le *produit de convolution de Dirichlet*, par la condition

$$f \star g(n) = \sum_{d|n} f(d) g(n/d) = \sum_{dd'=n} f(d) g(d').$$

On note $\mathbf{1}$ la fonction arithmétique définie par $\mathbf{1}(n) = 1$ pour tout $n \ge 1$. Vérifier

$$g = f \star \mathbf{1} \iff f = g \star \mu.$$

On peut énoncer la formule d'inversion de Möbius sous forme multiplicative équivalente en considérant deux fonctions arithmétiques f, g à valeurs dans un groupe multiplicatif ; alors les conditions suivantes sont équivalentes :
(i) *Pour tout entier $n \geq 1$,*

$$g(n) = \prod_{d|n} f(d).$$

(ii) *Pour tout entier $n \geq 1$,*

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

Une troisième variante de cette formule concerne deux fonctions F et G de $[1, +\infty)$ dans $\mathbf{C}$. Les deux conditions suivantes sont équivalentes :
(i) *Pour tout nombre réel $x \geq 1$,*

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) *Pour tout nombre réel $x \geq 1$,*

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

Si on prend par exemple $F(x) = 1$ et $G(x) = \lfloor x \rfloor$ (*partie entière* de x) pour tout $x \in [1, +\infty)$, alors

$$\sum_{n \leq x} \mu(n) \lfloor x/n \rfloor = 1$$

Grâce à la formule d'inversion de Möbius sous la seconde forme (multiplicative), on déduit de la relation (1.23) :

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

L'exercice suivant concerne la fonction arithmétique que nous noterons $\Psi_q(n)$ qui, pour q puissance d'un nombre premier et n entier positif, compte le nombre de polynômes unitaires irréductibles de degré n dans $\mathbf{F}_q[X]$.

Exercice. Soit F un corps fini à q éléments.
a) Vérifier

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

b) En déduire

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

c) Donner les valeurs de $\Psi_2(n)$ pour $1 \leq n \leq 6$.
Quand ℓ est un nombre premier différent de la caractéristique p de $\mathbf{F}_q$, vérifier

$$N_q(\ell) = \frac{q^\ell - q}{\ell}. \tag{2.17}$$

d) Vérifier

$$\frac{q^n}{2n} \le \Psi_q(n) \le \frac{q^n}{n}.$$

e) Soient p la caractéristique de F et $\mathbf{F}_p$ le sous-corps premier de F. Montrer que plus de la moitié des éléments α de F vérifient $F = \mathbf{F}_p(\alpha)$.

Exercice. Soient F un corps fini, E une extension de F et α, β deux éléments de E algébriques sur F de degrés respectivement a et b. On suppose a et b premiers entre eux. Vérifier

$$F(\alpha, \beta) = F(\alpha + \beta).$$

Suivant (2.2), étant donné $q = p^r$, l'unique sous–corps de $\overline{\mathbf{F}}_p$ ayant q est l'ensemble $\mathbf{F}_q$ des racines de $X^q - X$ dans $\overline{\mathbf{F}}_p$. L'ensemble $\{X - x \ ; \ x \in \mathbf{F}_q\}$ est l'ensemble des polynômes de degré 1 à coefficients dans $\mathbf{F}_q$. Donc (2.2) est le cas particulier $n = q - 1$ (donc $d = 1$) de l'énoncé suivant.

Théorème 2.18. *Soient $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q. On désigne par d l'ordre de q modulo n. Alors tous les facteurs irréductibles du polynôme Φ_n dans $\mathbf{F}_q[X]$ sont de degré d.*

Démonstration. Dans un corps de décomposition K du polynôme Φ_n sur $\mathbf{F}_q$, soit α une racine de Φ_n. Nous avons vu que α était d'ordre n dans $K^\times$. Le degré de α sur $\mathbf{F}_q$ est donné par le théorème 2.14 : c'est le plus petit des entiers $s \ge 1$ tels que $\alpha^{q^s-1} = 1$. C'est donc le plus petit des entiers $s \ge 1$ tels que n divise $q^s - 1$, qui n'est autre que l'ordre de l'image de q dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Comme un élément $\zeta \in \overline{\mathbf{F}}_p^\times$ est d'ordre n dans le groupe multiplicatif $\overline{\mathbf{F}}_p^\times$ si et seulement si ζ est racine de Φ_n, un énoncé équivalent au théorème 2.18 est le suivant :

Corollaire 2.19. *Si $\zeta \in \overline{\mathbf{F}}_p^\times$ est d'ordre n dans le groupe multiplicatif $\overline{\mathbf{F}}_p^\times$, alors son degré $d = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ sur $\mathbf{F}_q$ est l'ordre de q modulo n.*

Pour $d = 1$ cela signifie :

Corollaire 2.20. *Si $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q, le polynôme cyclotomique Φ_n est complètement décomposé dans $\mathbf{F}_q$ si et seulement si $q \equiv 1 \pmod{n}$.*

On le voit aussi directement, puisque $\mathbf{F}_q^\times$ est cyclique d'ordre $q - 1$.
L'autre cas extrême est $d = \varphi(n)$:

Corollaire 2.21. *Soient $\mathbf{F}_q$ un corps fini et n un entier premier avec q. Les conditions suivantes sont équivalentes :*
(i) Le polynôme Φ_n est irréductible sur $\mathbf{F}_q$.
(ii) La classe de q modulo n est d'ordre $\varphi(n)$.
(iii) La classe de q modulo n est un générateur de $(\mathbf{Z}/n\mathbf{Z})^\times$.

Bien entendu cela ne peut arriver que si le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique : le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique si et seulement si n est soit 2, 4, ℓ^s ou ℓ^{2s}, avec ℓ premier impair et $s \ge 1$.

`Remarque:` *Pour $s \ge 2$, $(\mathbf{Z}/2^s\mathbf{Z})^\times$ est le produit d'un groupe cyclique d'ordre 2 par un groupe cyclique d'ordre 2^{s-2}, donc quand $s \ge 3$, il n'est pas cyclique.*

Voici un troisième exemple d'application du théorème 2.18 :

Corollaire 2.22. *Soient $\mathbf{F}_q$ un corps fini, m un entier positif et $n = q^m - 1$. Le polynôme Φ_n se décompose en produit de polynômes irréductibles sur $\mathbf{F}_q$ qui sont tous de degré m.*

On peut noter que le nombre de facteurs dans cette décomposition est $\varphi(q^m-1)/m$, il en résulte donc que m divise $\varphi(q^m-1)/m$.

Exercice. 1) Soient a et m deux entiers ≥ 2. On pose $n = (a^m-1)/(a-1)$. Vérifier que a est d'ordre m modulo n
2) Soient p un nombre premier et m un entier ≥ 2. On suppose que $p^m - 1$ n'est pas premier. Montrer qu'il existe un entier $n \neq p^m - 1$ tel que p soit d'ordre m modulo n.
`Indication:` *Pour traiter le cas $p = 2$, on pourra vérifier que si m est premier et n est un diviseur de $2^m - 1$, alors 2 est d'ordre m modulo n. Si m possède un diviseur strict d, alors 2 est d'ordre m modulo n pour $n = (2^m - 1)/(2^d - 1)$.*

Exemples numériques

On fixe une clôture algébrique $\overline{\mathbf{F}}_p$ du corps premier $\mathbf{F}_p$, et pour q puissance de p on désigne par $\mathbf{F}_q$ l'unique sous–corps de $\overline{\mathbf{F}}_p$ ayant q éléments. Évidemment, $\overline{\mathbf{F}}_p$ est aussi une clôture algébrique de $\mathbf{F}_q$.

Exemple 6. Considérons l'extension quadratique $\mathbf{F}_4/\mathbf{F}_2$ déjà étudiée au début de cette section. Il y a un unique polynôme irréductible de degré 2 sur $\mathbf{F}_2$, c'est $\Phi_3 = X^2 + X + 1$. On désigne par ζ une de ses racines dans $\mathbf{F}_4$. L'autre racine est ζ^2 avec $\zeta^2 = \zeta + 1$ et

$$\mathbf{F}_4 = \{0,\ 1,\ \zeta,\ \zeta^2\}.$$

Si on pose $\eta = \zeta^2$, alors les deux racines de Φ_3 sont η et η^2, avec $\eta^2 = \eta + 1$ et

$$\mathbf{F}_4 = \{0,\ 1,\ \eta,\ \eta^2\}.$$

On ne peut pas distinguer ces deux racines, elles jouent le même rôle. C'est un phénomène analogue à la situation des deux racines $\pm i$ de $X^2 + 1$ dans $\mathbf{C}$.

Exemple 7. On considère l'extension cubique $\mathbf{F}_8/\mathbf{F}_2$. Il y a 6 éléments dans $\mathbf{F}_8$ qui ne sont pas dans $\mathbf{F}_2$, chacun d'eux est de degré 3 sur $\mathbf{F}_2$, donc il a deux polynômes irréductibles de degré 3 sur $\mathbf{F}_2[X]$. Effectivement, de (2.17), on déduit $\Psi_2(3) = 2$. Les deux facteurs irréductibles de Φ_7 sur $\mathbf{F}_2$ sont les seuls polynômes irréductibles de degré 3 sur $\mathbf{F}_2$:

$$X^8-X = X(X+1)\Phi_7(X), \quad \Phi_7(X) = Q_1(X)Q_2(X), \quad Q_1(X) = X^3+X+1, \quad Q_2(X) = X^3+X^2+1.$$

Les $6 = \varphi(7)$ éléments de $\mathbf{F}_8^\times$ de degré 3 sont les six racines de Φ_7, donc ce sont des éléments d'ordre 7. Si ζ est l'un quelconque d'entre eux, on a

$$\mathbf{F}_8 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6\}.$$

Si ζ est une racine de Q_1, alors les deux autres racines de ce polynôme sont ζ^2 et ζ^4, tandis que les racines de Q_2 sont ζ^3, ζ^5 et ζ^6. Noter que $\zeta^6 = \zeta^{-1}$ et $Q_2(X) = X^3 Q_1(1/X)$. Posons $\eta = \zeta^{-1}$. Alors

$$\mathbf{F}_8 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6\}$$

et

$$Q_1(X) = (X-\zeta)(X-\zeta^2)(X-\zeta^4), \quad Q_2(X) = (X-\eta)(X-\eta^2)(X-\eta^4).$$

L'application $x \mapsto x+1$ est donnée par

$$\zeta+1=\zeta^3,\ \zeta^2+1=\zeta^6,\ \zeta^3+1=\zeta,\ \zeta^4+1=\zeta^5,\ \zeta^5+1=\zeta^4,\ \zeta^6+1=\zeta^2$$

et par

$$\eta+1=\eta^5,\ \eta^2+1=\eta^3,\ \eta^3+1=\eta^2,\ \eta^4+1=\eta^6,\ \eta^5+1=\eta,\ \eta^6+1=\eta^4.$$

Exemple 8. On considère l'extension quadratique $\mathbf{F}_9/\mathbf{F}_3$. Sur $\mathbf{F}_3$,

$$X^9 - X = X(X-1)(X+1)(X^2+1)\Phi_8(X), \quad \Phi_8(X) = (X^2+X-1)(X^2-X-1).$$

Dans $\mathbf{F}_9^\times$, il y a $4 = \varphi(8)$ éléments d'ordre 8 (les 4 racines de Φ_8) et ce sont des éléments de degré 2 sur $\mathbf{F}_3$. Il y a deux éléments d'ordre 4, ce sont les racines de $\Phi_4(X) = X^2+1$; ce sont aussi les carrés des éléments d'ordre 8 et ils sont de degré 2 sur $\mathbf{F}_3$, leur carré est -1. Il y a un élément d'ordre 2, c'est -1, et il y a un élément d'ordre 1, c'est 1. De (2.17), on déduit $\Psi_3(2) = 3$: les trois polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3$ sont Φ_4 et les deux facteurs irréductibles de Φ_8.

Soit ζ une racine de X^2+X-1 et soit $\eta = \zeta^{-1}$. Alors $\eta = \zeta^7$, $\eta^3 = \zeta^5$ et

$$X^2+X-1 = (X-\zeta)(X-\zeta^3), \quad X^2-X-1 = (X-\eta)(X-\eta^3).$$

On a

$$\mathbf{F}_9 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6,\ \zeta^7\}$$

et aussi

$$\mathbf{F}_9 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6,\ \eta^7\}.$$

L'élément $\zeta^4 = \eta^4 = -1$ est l'élément d'ordre 2 et de degré 1, les deux éléments d'ordre 4 (qui sont de degré 2), racines de X^2+1, sont $\zeta^2 = \eta^6$ et $\zeta^6 = \eta^2$.

Exercice. Vérifier que 3 est d'ordre 5 modulo 11 et que

$$X^{11}-1 = (X-1)(X^5-X^3+X^2-X-1)(X^5+X^4-X^3+X^2-1)$$

est la décomposition de $X^{11}-1$ en facteurs irréductibles sur $\mathbf{F}_3$.

Exercice. Vérifier que 2 est d'ordre 11 modulo 23 et que $X^{23}-1$ sur $\mathbf{F}_2$ est le produit de trois polynômes irréductibles unitaires, qui sont $X-1$,

$$X^{11}+X^{10}+X^6+X^5+X^4+X^2+1 \quad \text{et} \quad X^{11}+X^9+X^7+X^6+X^5+X+1.$$

Exemple 9. Supposons q impair et considérons le polynôme $\Phi_4(X) = X^2+1$.
- Si $q \equiv 1 \bmod 4$, alors X^2+1 a deux racines dans $\mathbf{F}_q$.
- Si $q \equiv -1 \bmod 4$, alors X^2+1 est irréductible sur $\mathbf{F}_q$.

Exemple 10. On suppose de nouveau q impair et on considère le polynôme $\Phi_8(X) = X^4+1$.
- Si $q \equiv 1 \bmod 8$, alors X^4+1 a quatre racines dans $\mathbf{F}_q$.
- Sinon, X^4+1 est produit de 2 facteurs irréductibles de degré 2 dans $\mathbf{F}_q[X]$.

En particulier le polynôme X^4+1 n'est jamais irréductible sur un corps fini (alors qu'il est irréductible dans $\mathbf{Z}[X]$).

L'exemple 8 donne sur $\mathbf{F}_3$

$$X^4+1=(X^2+X-1)(X^2-X-1).$$

En utilisant l'exemple 9, on en déduit que dans la décomposition de X^8-1 sur $\mathbf{F}_q$, il y a

8 facteurs de degré 1 si $q\equiv 1 \bmod 8$,
4 facteurs de degré 1 et 2 facteurs de degré 2 si $q\equiv 5 \bmod 8$,
2 facteurs de degré 1 et 3 facteurs de degré 2 si $q\equiv -1 \bmod 4$.

Exemple 11. Le groupe $(\mathbf{Z}/5\mathbf{Z})^\times$ est cyclique d'ordre 4, il y a $\varphi(4)=2$ éléments qui sont générateurs, ce sont les classes de 2 et de 3. La classe de 4 modulo 5 est d'ordre 2 et la classe de 1 est d'ordre 1. Donc

- Si $q\equiv 2$ ou 3 mod 5, alors Φ_5 est irréductible dans $\mathbf{F}_q[X]$,
- Si $q\equiv -1 \bmod 5$, alors Φ_5 se décompose en un produit de 2 polynômes irréductibles de degré 2 dans $\mathbf{F}_q[X]$,
- Si $q\equiv 1 \bmod 5$, alors Φ_5 est totalement décomposé sur $\mathbf{F}_q$,
- Si q est une puissance de 5, alors $\Phi_5=(X-1)^4$ dans $\mathbf{F}_q[X]$.

Décomposition de Φ_n en facteurs irréductibles sur $\mathbf{F}_q$

Comme d'habitude, on suppose $\mathrm{pgcd}(n,q)=1$. Le théorème 2.18 entraîne que Φ_n est un produit de polynômes irréductibles sur $\mathbf{F}_q$, tous du même degré d. Soit G le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$. Alors d est l'ordre de q dans G. Soit H le sous–groupe de G engendré par q :

$$H=\{1,q,q^2,\dots,q^{d-1}\}.$$

Soit ζ une racine quelconque de Φ_n (dans une clôture algébrique de $\mathbf{F}_q$, ou si on préfère dans le corps de décomposition de $\Phi_n(X)$ sur $\mathbf{F}_q$). Alors les conjugués de ζ sur $\mathbf{F}_q$ sont les images sous le Frobenius itéré Frob_q qui envoie x sur x^q. Donc le polynôme minimal de ζ sur $\mathbf{F}_q$ est

$$P_H(X)=\prod_{i=0}^{d-1}(X-\zeta^{q^i})=\prod_{h\in H}(X-\zeta^h).$$

Ceci est vrai pour n'importe quelle racine ζ de Φ_n. Maintenant on en fixe une. Alors les autres sont ζ^m où $\mathrm{pgcd}(m,n)=1$. Le polynôme minimal de ζ^m est donc

$$\prod_{i=0}^{d-1}(X-\zeta^{mq^i}).$$

On peut écrire ce polynôme

$$P_{mH}(X)=\prod_{h\in mH}(X-\zeta^h)$$

où mH est la classe $\{mq^i\ ;\ 0\le i\le d-1\}$ de m modulo H dans G. Il y a $\varphi(n)/d$ classes de G modulo H, et la décomposition de $\Phi_n(X)$ en facteurs irréductibles sur $\mathbf{F}_q$ est

$$\Phi_n(X)=\prod_{mH\in G/H}P_{mH}(X).$$

Facteurs de $X^n - 1$ dans $\mathbf{F}_q[X]$
On suppose comme toujours $\mathrm{pgcd}(n, q) = 1$. Nous venons d'étudier la décomposition sur $\mathbf{F}_q$ des polynômes cyclotomiques, et $X^n - 1$ est le produit des $\Phi_d(X)$ pour d divisant n. On peut ainsi décomposer le polynôme $X^n - 1$ en facteurs irréductibles sur $\mathbf{F}_q[X]$. La proposition 2.23 ci–dessous en résulte, mais on peut aussi l'établir directement.

Soit ζ une racine primitive n-ème de l'unité dans une extension F de $\mathbf{F}_q$. Rappelons que pour j dans $\mathbf{Z}$, ζ^j ne dépend que de la classe de j modulo n. On peut donc noter encore ζ^i quand i est un élément de $\mathbf{Z}/n\mathbf{Z}$:

$$X^n - 1 = \prod_{i \in \mathbf{Z}/n\mathbf{Z}} (X - \zeta^i).$$

Pour chaque sous–ensemble I de $\mathbf{Z}/n\mathbf{Z}$, on pose

$$Q_I(X) = \prod_{i \in I} (X - \zeta^i).$$

Pour I décrivant les 2^n sous–ensembles de $\mathbf{Z}/n\mathbf{Z}$, on obtient ainsi tous les diviseurs unitaires de $X^n - 1$ dans $F[X]$. Le lemme 2.8 implique que Q_I appartient à $\mathbf{F}_q[X]$ si et seulement si $Q_I(X^q) = Q_I(X)^q$.

Comme q et n sont premiers entre eux, la multiplication par q, que nous noterons $[q]$, définit une permutation du groupe cyclique $\mathbf{Z}/n\mathbf{Z}$:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}/n\mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z}/n\mathbf{Z} \\ x & \longmapsto & qx. \end{array}$$

La condition $Q_I(X^q) = Q_I(X)^q$ équivaut à dire $[q](I) = I$, ce qui signifie que la multiplication par q induit une permutation de I. On dira qu'un sous–ensemble I de $\mathbf{Z}/n\mathbf{Z}$ ayant cette propriété est *stable sous la multiplication par q*. Par conséquent :

Proposition 2.23. *L'application $I \mapsto Q_I$ est une bijection entre les sous–ensembles I de $\mathbf{Z}/n\mathbf{Z}$ qui sont stables sous la multiplication par q d'une part, et les diviseurs unitaires de $X^n - 1$ dans $\mathbf{F}_q[X]$ d'autre part.*

Un facteur irréductible de $X^n - 1$ sur $\mathbf{F}_q$ est un facteur Q dont aucun diviseur propre Q n'a ses coefficients dans $\mathbf{F}_q$. Donc :

Corollaire 2.24. *Sous cette bijection $I \mapsto Q_I$, les facteurs irréductibles de $X^n - 1$ correspondent aux sous–ensembles non vides minimaux I de $\mathbf{Z}/n\mathbf{Z}$ qui sont stables sous la multiplication par q.*

Voici quelques exemples :
- Pour $I = \emptyset$, on a $Q_\emptyset = 1$.
- Pour $I = \mathbf{Z}/n\mathbf{Z}$, on a $Q_{\mathbf{Z}/n\mathbf{Z}} = X^n - 1$.
- Pour $I = \{0\}$, on a $Q_0(X) = X - 1$.
- Si n est pair (auquel cas q est impair, bien entendu), alors pour $I = \{n/2\}$, on a $Q_{n/2}(X) = X + 1$.

– Soit d un diviseur de n. Il y a un unique sous–groupe C_d d'ordre d dans le groupe cyclique $\mathbf{Z}/n\mathbf{Z}$. Ce sous–groupe est engendré par la classe de n/d, c'est l'ensemble des $k \in \mathbf{Z}/n\mathbf{Z}$ tels que $dk = 0$, il est stable sous la multiplication par tout élément premier avec n. Alors $Q_{C_d}(X) = X^d - 1$.
– Soit encore d un diviseur de n et soit E_d l'ensemble des générateurs de C_d : cet ensemble a $\varphi(d)$ éléments qui sont les éléments d'ordre d dans le groupe cyclique $\mathbf{Z}/n\mathbf{Z}$. De nouveau, ce sous–ensemble de $\mathbf{Z}/n\mathbf{Z}$ est stable sous la multiplication par tout élément premier avec n. Alors Q_{E_d} est le polynôme cyclotomique Φ_d de degré $\varphi(d)$.

Exemple 12. Prenons $n = 15$, $q = 2$. En divisant $(X^{15} - 1)/(X^5 - 1) = X^{10} + X^5 + 1$ par $\Phi_3(X) = X^2 + X + 1$, on obtient dans $\mathbf{Z}[X]$:

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Les sous–ensembles minimaux de $\mathbf{Z}/15\mathbf{Z}$ qui sont stables sous la multiplication par 2 modulo 15 sont les classes de

$$\{0\},\ \{5, 10\},\ \{3, 6, 9, 12\},\ \{1, 2, 4, 8\},\ \{7, 11, 13, 14\}.$$

On retrouve le fait que dans la décomposition

$$X^{15} - 1 = \Phi_1(X)\Phi_3(X)\Phi_5(X)\Phi_{15}(X)$$

sur $\mathbf{F}_2$, le facteur Φ_1 est irréductible de degré 1, les facteurs Φ_3 et Φ_5 sont irréductibles de degré 2 et 4 respectivement, tandis que Φ_{15} se décompose en 2 facteurs de degré 4 (on le vérifie en utilisant le fait que 2 est d'ordre 2 modulo 3, d'ordre 4 modulo 5 est aussi d'ordre 4 modulo 15).

Il y a 3 polynômes irréductibles de degré 4 sur $\mathbf{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad \Phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

Dans $\mathbf{F}_2[X]$,

$$\Phi_{15}(X) = (X^4 + X^3 + 1)(X^4 + X + 1).$$

Soit ζ une racine primitive 15-ème de l'unité (c'est–à–dire une racine de Φ_{15}). Alors $\zeta^{15} = 1$ est la racine de Φ_1, ζ^5 et ζ^{10} sont les racines de Φ_3 (ce sont les racines primitives cubiques de l'unité, elles appartiennent à $\mathbf{F}_4$), tandis que $\zeta^3, \zeta^6, \zeta^9, \zeta^{12}$ sont les racines de Φ_5 (ce sont les racines primitives 5-èmes de l'unité). Un des deux facteurs irréductibles de Φ_{15} a pour racines $\zeta, \zeta^2, \zeta^4, \zeta^8$, l'autre a pour racines $\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}$. On a aussi

$$\{\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}\} = \{\zeta^{-1}, \zeta^{-2}, \zeta^{-4}, \zeta^{-8}\}.$$

Le corps de décomposition sur $\mathbf{F}_2$ de l'un quelconque des trois facteurs irréductibles de degré 4 de $X^{15} - 1$ est le corps F_{16} à 2^4 éléments, mais pour l'un d'eux (à savoir Φ_5) les 4 racines sont d'ordre 5 dans $F_{16}^\times$, tandis que pour les deux autres les racines sont d'ordre 15.

On a ainsi vérifié que dans $\mathbf{F}_{16}^\times$, il y a
– 1 élément d'ordre 1 et de degré 1 sur $\mathbf{F}_2$, à savoir $\{1\} \subset \mathbf{F}_2$,
– 2 éléments d'ordre 3 et de degré 2 sur $\mathbf{F}_2$, à savoir $\{\zeta^5,\ \zeta^{10}\} \subset \mathbf{F}_4$,
– 4 éléments d'ordre 5 et de degré 4 sur $\mathbf{F}_2$, à savoir $\{\zeta^3,\ \zeta^6,\ \zeta^9,\ \zeta^{12}\}$,
– 8 éléments d'ordre 15 et de degré 4 sur $\mathbf{F}_2$.

2.4 Loi de réciprocité quadratique

Soit p un nombre premier. Étudions les extensions quadratiques du corps $\mathbf{F}_p$ à p éléments. Dans une extension algébriquement close de $\mathbf{F}_p$ il y en a une et une seule. Pour l'expliciter on est amené à étudier les polynômes unitaires irréductibles de degré 2 sur $\mathbf{F}_p$. Pour $p = 2$ il y en a un et un seul, $X^2 + X + 1$ (nous l'avons vu en considérant le corps à 4 éléments).

Supposons dorénavant p impair. Dans K on peut diviser par 2 : on écrit $X^2 + aX + b = (X + a/2)^2 + b - a^2/4$. Il reste à déterminer quels sont les carrés dans $\mathbf{F}_p$.

Un élément α du corps $\mathbf{F}_p$ est appelé *résidu quadratique* si l'équation $X^2 - \alpha$ a une racine dans $\mathbf{F}_p$, on dit qu'il est *non–résidu quadratique* sinon, c'est-à-dire si ce polynôme $X^2 - \alpha$ est irréductible sur $\mathbf{F}_p$. On dit qu'un entier $a \in \mathbf{Z}$ est *résidu quadratique modulo* p si sa classe $\alpha \in \mathbf{Z}/p\mathbf{Z}$ modulo p l'est, *non–résidu modulo* p dans le cas contraire. En notant α la classe de a modulo p on définit le *symbole de Legendre* par

$$\left(\frac{\alpha}{p}\right) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } \alpha = 0 \\ 1 & \text{si } \alpha \text{ est résidu quadratique} \\ -1 & \text{si } \alpha \text{ est non–résidu quadratique.} \end{cases}$$

On a supposé p impair. L'application $x \mapsto x^2$ est un endomorphisme du groupe $\mathbf{F}_p^\times$, de noyau $\{-1, +1\}$. L'image de cette application a donc $(p-1)/2$ éléments, ce qui veut dire qu'il y a $(p-1)/2$ éléments dans $\mathbf{F}_p^\times$ qui sont des résidus quadratiques non nuls dans $\mathbf{F}_p$ et il y en a autant qui ne sont pas résidus quadratiques. On en déduit

$$\sum_{\alpha \in \mathbf{F}_p} \left(\frac{\alpha}{p}\right) = 0. \tag{2.25}$$

Comme p est impair, on a

$$X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1),$$

et les carrés sont racines du polynôme $(X^{(p-1)/2} - 1)$. Il en résulte que les $(p-1)/2$ résidus quadratiques dans $\mathbf{F}_p^\times$ sont les racines du polynôme $X^{(p-1)/2} - 1$, et que les non–résidus sont les racines du polynôme $X^{(p-1)/2} + 1$. Par conséquent pour $\alpha \in \mathbf{F}_p$ on a

$$\left(\frac{\alpha}{p}\right) = \alpha^{(p-1)/2}. \tag{2.26}$$

Par exemple

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv \ \ 1 \pmod 4 \\ -1 & \text{si } p \equiv -1 \pmod 4. \end{cases} \tag{2.27}$$

Si $\zeta \in \mathbf{F}_p$ est une *racine primitive modulo* p (c'est-à-dire un générateur de $\mathbf{F}_p^\times$, ou encore une racine primitive $p-1$-ième de l'unité), alors les résidus quadratiques modulo p sont les éléments ζ^k de $\mathbf{F}_p^\times$ avec $0 \le k \le p-3$ et k pair, tandis que les non–résidus quadratiques sont les ζ^k avec $1 \le k \le p-2$ et k impair. En particulier

$$\left(\frac{\zeta}{p}\right) = -1$$

et (*théorème de Wilson*)

$$(p-1)! \equiv \prod_{k=1}^{p-1} \zeta^k \equiv \zeta^{p(p-1)/2} \equiv \zeta^{(p-1)/2} \equiv \left(\frac{\zeta}{p}\right) \equiv -1 \pmod{p}.$$

Lemme 2.28. *Pour α et β dans $\mathbf{F}_p$ on a*

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right).$$

De plus

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & si\ p \equiv \pm 1 \pmod 8 \\ -1 & si\ p \equiv \pm 3 \pmod 8). \end{cases}$$

Démonstration. La relation (2.26) montre que l'application

$$\alpha \longmapsto \left(\frac{\alpha}{p}\right)$$

est un homomorphisme du groupe multiplicatif $\mathbf{F}_p^\times$ sur le groupe à deux éléments $\{-1,+1\}$. Le noyau est constitué des résidus quadratiques dans $\mathbf{F}_p^\times$.

Pour savoir si 2 est résidu quadratique modulo p, on doit déterminer si le polynôme X^2-2 est réductible ou non dans $\mathbf{F}_p[X]$.

Dans le corps des nombres complexes, une des racines primitives 8èmes de l'unité est

$$\zeta_8 = e^{2i\pi/8} = \frac{(1+i)\sqrt{2}}{2}.$$

Elle vérifie $\zeta_8^2 = i$ et $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$. On vérifie aussi

$$\zeta_8^n + \zeta_8^{-n} = \begin{cases} \sqrt{2} & \text{si } n \equiv 1 \text{ ou } 7 \pmod 8, \\ -\sqrt{2} & \text{si } n \equiv 3 \text{ ou } 5 \pmod 8). \end{cases}$$

Ces calculs complexes (et faciles) vont motiver ceux que nous allons faire en caractéristique finie p.

Soit $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$ et soit $\mathbf{F}_{p^2}$ le sous-corps de $\overline{\mathbf{F}}_p$ ayant p^2 éléments. Comme p^2-1 est multiple de 8 il existe une racine primitive 8-ième de l'unité $\alpha \in \mathbf{F}_{p^2}$. Posons $\beta = \alpha + \alpha^{-1}$. On a $\alpha^4 = -1$ et $\alpha^2 = -\alpha^{-2}$, donc

$$\beta^2 = (\alpha+\alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2.$$

Il s'agit maintenant de savoir si β est ou non dans $\mathbf{F}_p^\times$, c'est-à dire si β^p est égal à β ou à $-\beta$.

Si $p \equiv \pm 1 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{\alpha, \alpha^{-1}\}$, donc $\beta^p = \beta$ et $\beta \in \mathbf{F}_p$, ce qui donne

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

Si $p \equiv \pm 3 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{-\alpha, -\alpha^{-1}\}$, donc $\beta^p = -\beta$ et $\beta \notin \mathbf{F}_p$, d'où on conclut

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

□

Exercice. Donner une nouvelle démonstration du fait (cf. exemple 10) que le polynôme X^4+1 est réductible sur $\mathbf{F}_p$ pour tout nombre premier p. Vérifier qu'il est irréductible sur $\mathbf{Q}$.

Voici l'énoncé de la loi de réciprocité quadratique :

Théorème 2.29. *Soient p et ℓ des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{2.30}$$

Il existe un grand nombre de démonstrations de cet énoncé, les premières ayant été données par C.F. Gauss. En voici une qui repose sur l'utilisation des *sommes de Gauss* qui sont définies de la façon suivante : soit K un corps contenant une racine primitive p-ième de l'unité ζ, c'est-à-dire un élément d'ordre p dans le groupe multiplicatif $K^{\times}$ [2]. On pose

$$S = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$

Cette formule associe l'application

$$a \longmapsto \left(\frac{a}{p}\right)$$

qui est un homomorphisme de groupes multiplicatifs de $\mathbf{F}_p^{\times}$ dans $\{-1,\ +1\}$ (ce qu'on appelle un *caractère multiplicatif* – cf. Lemme 2.28) avec l'application

$$a \longmapsto \zeta^a$$

qui est un homomorphisme du groupe additif $\mathbf{F}_p$ dans le groupe multiplicatif $K^{\times}$ (*caractère additif*).

Démonstration du théorème 2.29. Comme ζ^a ne dépend que de la classe de a modulo p, qu'il en est de même du symbole de Legendre $\left(\frac{a}{p}\right)$ et que ce dernier est nul pour $a=0$, on peut écrire

$$S = \sum_{\alpha\in\mathbf{F}_p^{\times}} \left(\frac{\alpha}{p}\right) \zeta^{\alpha}.$$

Soit $\alpha \in \mathbf{F}_p^{\times}$. L'application $\beta \mapsto \alpha\beta$ est une bijection du groupe $\mathbf{F}_p^{\times}$ sur lui même, donc

$$S = \sum_{\beta\in\mathbf{F}_p^{\times}} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta}.$$

Comme

$$\left(\frac{\alpha}{p}\right)\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha^2\beta}{p}\right) = \left(\frac{\beta}{p}\right)$$

2. Par exemple on peut prendre $K=\mathbf{C}$ et $\zeta = e^{2i\pi/p}$. Mais on ne peut pas prendre un corps de caractéristique p bien sûr !

on obtient

$$S^2 = \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^\alpha \sum_{\beta\in\mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta} = \sum_{\beta\in\mathbf{F}_p^\times} \left(\frac{\beta}{p}\right) \sum_{\alpha\in\mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)}.$$

Comme la somme des racines du polynôme $X^p - 1$ est nulle, on a

$$\sum_{\gamma\in\mathbf{F}_p} \zeta^\gamma = 0, \qquad \text{donc} \qquad \sum_{\gamma\in\mathbf{F}_p^\times} \zeta^\gamma = -1.$$

Ainsi

$$\sum_{\alpha\in\mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)} = \begin{cases} p-1 & \text{si } \beta = -1 \\ -1 & \text{si } \beta \neq -1. \end{cases}$$

En utilisant (2.25) et (2.27) on en déduit

$$S^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{\substack{\beta\in\mathbf{F}_p^\times \\ \beta\neq -1}} \left(\frac{\beta}{p}\right) = p\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} p.$$

Ces calculs sont valables dans tout corps K contenant une racine primitive p-ième de l'unité ζ. Choisissons maintenant pour K une clôture algébrique $\overline{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$. On a dans $\overline{\mathbf{F}}_\ell$

$$S^\ell = \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\ell\alpha}{p}\right) \zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) S,$$

donc

$$S^{\ell-1} = \left(\frac{\ell}{p}\right).$$

Alors, toujours dans $\overline{\mathbf{F}}_\ell$, on a

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

Ceci démontre la relation (2.30).

□