Exercices de théorie des corps finis

Exercice 1. — *1) Donner tous les polynômes irréductibles de degré inférieur à* 4 *sur* $\mathbf{F}_2$.

2) Quelle est la factorisation sur $\mathbb{F}_4$ *d'un polynôme de* $\mathbb{F}_2[X]$ *irréductible de degré* 4 *?*

3) Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 *sur* $\mathbf{F}_4$.

4) Expliciter les polynômes irréductibles de degré 2 *sur* $\mathbb{F}_4$.

Exercice 2. — *1) Le nombre* 2 *est-il un carré dans* $\mathbf{F}_5$ *? Montrer que* $X^2 + X + 1$ *est irréductible sur* $\mathbf{F}_5$.

2) Soit $P(X) \in \mathbf{F}_5[X]$ *un polynôme unitaire irréductible de degré deux . Montrer que le quotient*

$$\frac{\mathbf{F}_5[X]}{(P(X))}$$

est isomorphe au corps $\mathbf{F}_{25}$ *et que* P *a deux racines dans* $\mathbf{F}_{25}$.

3) On note α *une racine de* $X^2 + X + 1$ *dans* $\mathbf{F}_{25}$. *Montrer que tout* $\beta \in \mathbf{F}_{25}$ *peut s'écrire* $a\alpha + b$ *avec* a *et* b *dans* $\mathbf{F}_5$.

4) Soit $P = X^5 - X + 1$. *Montrer que pour tout* $\beta \in \mathbf{F}_{25}$, *on a* $P(\beta) \neq 0$. *En déduire que* P *est irréductible sur* $\mathbf{F}_5$. P *est-il irréductible sur* $\mathbf{Q}$ *?*

Exercice 3. — *On considère le polynôme* $Q(X) = X^9 - X + 1$ *sur* $\mathbf{F}_3$.

1) Montrer que le polynôme Q *n'a pas de racines dans* $\mathbb{F}_3, \mathbb{F}_9$.

2) Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3 - X - 1)}$.

3) Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ *du polynôme* $X^3 - X - 1$ *est une racine du polynôme* Q.

4) Déterminer toutes le racines de Q *dans* $\mathbb{F}_{27}$.

5) Factoriser le polynôme Q *sur le corps* $\mathbb{F}_3$.

Exercice 4. — *A quelle condition un polynôme* P *à coefficients dans* $\mathbf{F}_p$ *de degré* n *est-il irréductible sur* $\mathbf{F}_{p^m}$ *? Dans le cas où* P *est irréductible sur* $\mathbf{F}_p$, *on donnera des précisions sur les degrés des facteurs irréductibles de* P *sur* $\mathbf{F}_{p^m}$. *En particulier pour* $n = 5$, *donner* m *minimal tel que tout polynôme de degré* 5 *à coefficients dans* $\mathbf{F}_p$ *soit totalement décomposé (resp. possède une racine) sur* $\mathbf{F}_{p^m}$.

Exercice 5. — *Théorie de Galois des corps finis et version faible du théorème de Dirichlet Soit* p *un nombre premier et* n *un entier premier avec* p. *On pose* $q = p^r$.

1) Décrire le groupe de Galois de l'extension $\mathbb{F}_{q^n} : \mathbb{F}_q$ *et expliciter la théorie de Galois, i.e. montrer que l'application qui à un sous-groupe* H *de* $gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *associe le sous-corps de* $\mathbb{F}_{q^n}$ *des éléments fixés par tous les éléments de* H, *est une bijection entre les sous-groupes du groupe de Galois et les extensions intermédiaires* $\mathbb{F}_q \subset \mathbf{K} \subset \mathbb{F}_{q^n}$.

2) Soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$. *Montrer que* $\mathrm{Gal}(L/\mathbb{F}_p)$ *est isomorphe au sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$ *engendré par l'image de* p. *Montrer que le* n*-ième polynôme cyclotomique* $\Phi_n(X)$ *se décompose sur* $\mathbb{F}_p$ *en un produit de* $\phi(n)/k$ *facteurs irréductibles distincts, tous de degré* k. *Quel est cet entier* k *? En déduire une version faible du théorème de progression arithmétique, i.e. :*
pour tout entier n *il existe une infinité de nombres premiers* p *congrus à* 1 *modulo* n.

Exercice 6. — *1) Montrer que* X^4+1 *est irréductible sur* $\mathbb{Z}$ *et réductible modulo tout nombre premier* p. *(Indication : montrer que pour tout nombre premier impair* p, *le polynôme* $X^4 + 1$ *a une racine dans le corps* $\mathbb{F}_{p^2}$.

2) Soit n *un entier ne s'écrivant pas sous la forme* p^α *ou* $2p^\alpha$ *avec* p *premier impair. On sait que le* n*-ième polynôme cyclotomique* Φ_n *est irréductible sur* $\mathbb{Z}$. *Montrer en utilisant la question (ii) de l'exercice sur la théorie de Galois des corps finis, que* Φ_n *est réductible modulo tout nombre premier.*

Exercice 7. — *Soit* $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$

1) Décomposer P *en facteurs irréductibles modulo 2,3,5.*

2) Montrer que P *est irréductible sur* $\mathbb{Q}$.

Exercice 8. — *Soit* $K = \mathbb{F}_3[X]/(X^3 + 2X + 1)$ *; montrez que* K *est un corps de cardinal* 27 *et que* X *est un générateur du groupe multiplicatif. Trouvez* i *tel que* $X^2 + X = X^i$.

1 1) Les polynômes irréductibles de degré 1 sont X et $X-1$; ceux de degré 2 sont tels que $X^4 - X = X(X-1)P$ ce qui donne $X^2 + X + 1$. Pour ceux de degré 3, on a $X^8 - X = X(X-1)P_1P_2$ et on trouve $X^3 + X + 1$ et $X^3 + X^2 + 1$. Enfin pour ceux de degré 4, on a $X^16 - X = (X^4 - X)Q_1Q_2Q_3$ et on trouve $X^4 + X + 1$, $X^4 + X^3 + X^2 + X + 1$ et $X^4 + X^3 + 1$. En effet ceux-ci sont irréductibles car un élément j de $\mathbb{F}_4$ qui n'est pas dans $\mathbb{F}_2$ vérifie $j^3 = 1$ de sorte qu'il ne peut être racine des polynômes en question.

2) Tout polynôme de $\mathbb{F}_2[X]$ de degré 4, irréductible sur $\mathbb{F}_2$, possède une racine dans $\mathbb{F}_{2^4}$ qui est une extension de degré 2 de $\mathbb{F}_4$; on en déduit donc que sur $\mathbb{F}_4$ il se factorise en un produit de 2 polynômes irréductibles de degré 2.

3) Les 3 polynômes de degré 4, irréductibles dans $\mathbb{F}_2[X]$ fournissent 6 polynômes de $\mathbb{F}_4[X]$ irréductibles de degré 2 ; ceux-ci sont distincts deux à deux car les 3 polynômes de degré 4 du départ sont premiers deux à deux dans $\mathbb{F}_2$ et donc dans $\mathbb{F}_4$.

Par ailleurs étant donné un polynôme de $\mathbb{F}_4[X]$ irréductible de degré 2, en le multipliant par son conjugué par l'unique élément non trivial du groupe de Galois de $\mathbb{F}_4 : \mathbb{F}_2$, qui échange j et j^2 avec les notations précédentes, on obtient un polynôme de degré 4 à coefficient dans $\mathbb{F}_2$, car les coefficients sont invariants par le groupe de Galois, et irréductible.

4) On note $0, 1, j, j^2$ les éléments de $\mathbb{F}_4$ avec $1 + j + j^2 = 0$. Les polynômes de degré 1 sont $X, X-1, X-j, X-j^2$ de produit $X^4 - X$. En ce qui concerne le degré 2, $X^4 + X + 1$, $X^4 + X^3 + X^2 + X + 1$ et $X^4 + X^3 + 1$ doivent s'écrire comme le produit de 2 polynôme irréductible de degré sur $\mathbb{F}_4$. On trouve alors $X^4 + X + 1 = (X^2 + X + j)(X^2 + X + j^2)$, $X^4 + X^3 + 1 = (X^2 + jX + j)(X^2 + j^2X + j^2)$ et $X^4 + X^3 + X^2 + X + 1 = (X^2 + jX + 1)(X^2 + j^2X + 1)$.

2 1) On écrit la table des carrés de $\mathbb{F}_5$, soit

x	0	1	2	-2	-1
x^2	0	1	-1	-1	1

et on remarque que 2 n'est pas un carré dans $\mathbb{F}_5$. On vérifie rapidement que pour $P(x) := X^2 + X + 1$, $P(0)$, $P(\pm 1)$ et $P(\pm 2)$ ne sont pas nuls de sorte que P n'a pas de racine dans $\mathbb{F}_5$, étant de degré 2 il y est donc irréductible.

2) Le corps $\mathbb{F}_5[X]/(P(X))$ est de cardinal 25 et donc isomorphe à $\mathbb{F}_{25}$ qui est un corps de décomposition de $X^{25} - X$. Par ailleurs la classe x de X dans $\mathbb{F}_5[X]/(P(X))$ vérifie $P(x) = 0$ de sorte que x est une racine de P qui étant de degré 2, y est alors totalement décomposé. On en déduit alors que P admet deux racines dans $\mathbb{F}_{25}$.

3) Un isomorphisme $f : \mathbb{F}_5[X]/(X^2 + X + 1) \simeq \mathbb{F}_{25}$ étant fixée, l'image $\alpha \in \mathbb{F}_{25}$ de X par f vérifie alors $\alpha^2 + \alpha + 1 = 0$ et est donc une racine de $X^2 + X + 1$. Le sous-espace vectoriel sur $\mathbb{F}_5$ de $\mathbb{F}_{25}$ engendré par 1 et α est de dimension 2 car $\alpha \notin \mathbb{F}_5$ et est donc égal à $\mathbb{F}_{25}$ de sorte que tout élément $\beta \in \mathbb{F}_{25}$ s'écrit sous la forme $a\alpha + b$ avec $a, b \in \mathbb{F}_5$.

4) On vérifie rapidement que P n'a pas de racine dans $\mathbb{F}_5$. Soit alors $\beta = a\alpha + b \in \mathbb{F}_{25}$; on a $\beta^5 = a^5\alpha^5 + b^5 = a\alpha^5 + b$. Or on a $\alpha^2 = -\alpha - 1$ soit $\alpha^4 = \alpha^2 + 2\alpha + 1 = \alpha$ et donc $\alpha^5 = \alpha^2 = -\alpha - 1$. Ainsi $\beta^5 - \beta + 1 = \alpha(-a - a) + (b - b - a + 1) \neq 0$ car $\alpha \notin \mathbb{F}_5$ soit P n'a pas de racine dans $\mathbb{F}_{25}$ de sorte qu'il est irréductible sur $\mathbb{F}_5$.

Par ailleurs, P en tant que polynôme de $\mathbb{Z}[X]$ unitaire, y est irréductible. En effet une factorisation $P = QR$ dans $\mathbb{Z}[X]$ induit par réduction modulo 5 une factorisation $\bar{P} = \bar{Q}\bar{R}$ dans $\mathbb{F}_5[X]$. Comme P est unitaire, Q et R le sont aussi, de sorte que $\deg Q = \deg \bar{Q}$ et $\deg R = \deg \bar{R}$; $\bar{P}$ étant irréductible, on en déduit que $\bar{Q}$, ou $\bar{R}$, est un polynôme constant

donc, étant unitaire, égal à $\bar{1}$ et donc Q, ou R, est le polynôme constant égal à 1. Ainsi P est irréductible sur $\mathbb{Z}$ et donc irréductible sur $\mathbb{Q}$ d'après le lemme de Gauss.

3 1) On vérifie rapidement que Q n'a pas de racine dans $\mathbb{F}_3$. On cherche alors ses racines dans $\mathbb{F}_9$. Pour $a \in \mathbb{F}_9$, on a $a^9 = a$ de sorte que $a^9 - a + 1 = 1$ et donc Q n'a pas de racine dans $\mathbb{F}_9$.

2) Afin de calculer dans $\mathbb{F}_{27}$, on commence par le décrire concrètement : on vérifie aisément que $X^3 - X - 1$ n'a pas de racines dans $\mathbb{F}_3$ et est donc irréductible sur $\mathbb{F}_3$ et $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(X^3 - X - 1)$.

3) Soit alors $\alpha \in \mathbb{F}_{27}$ tel que $\alpha^3 = \alpha + 1$. On a alors $\alpha^9 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$ et donc finalement α est une racine de Q dans $\mathbb{F}_{27}$ de sorte que Q possède un facteur irréductible de degré 3 sur $\mathbb{F}_3$, à savoir $X^3 - X - 1$, soit $X^9 - X + 1 = (X^3 - X - 1)(X^6 + X^4 + X^3 + X^2 - X - 1)$.

4) Cherchons de manière générale toutes les racines dans $\mathbb{F}_{27}$; un élément quelconque s'écrit sous la forme $x = a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbb{F}_3$. On a alors $x^9 = a\alpha^{18} + b\alpha^9 + c$ avec $\alpha^9 = \alpha - 1$ et donc $\alpha^{18} = \alpha^2 + \alpha + 1$ de sorte que $x^9 - x + 1 = a\alpha + a - b + 1$ ce qui impose $a = 0$ et $b = 1$ soit $x = \alpha, \alpha + 1, \alpha - 1$.

5) On en déduit alors que $X^6 + X^4 + X^3 + X^2 - X - 1$ n'a pas de racines dans $\mathbb{F}_{27}$ comme il n'en avait pas non plus dans $\mathbb{F}_9$, il est donc irréductible.

4 Si P est réductible sur $\mathbb{F}_p$, il l'est sur toute extension $\mathbb{F}_{p^m}$. Supposons donc P irréductible sur $\mathbb{F}_p$ de sorte que toutes les racines de P, vues dans $\bar{\mathbb{F}}_p$, sont dans $\mathbb{F}_{p^n}$ et aucune n'appartient à un sous-corps strict. On regarde alors P comme un polynôme dans $\mathbb{F}_{p^m}[X]$ dont on se demande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines dans $\mathbb{F}_{p^{mr}}$ pour $r \leq n/2$ et donc si $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{mr}}$, soit n divise mr ce qui est possible si et seulement si n et m ne sont pas premiers entre eux. En outre en notant $d = n \wedge m$, les facteurs irréductibles sont alors de degré r un multiple de n/d.

Pour $n = 5$, la décomposition en facteur irréductible donne en prenant les degrés les décompositions suivantes de $5 : 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$. Si on veut être sur d'avoir toutes les racines (resp. au moins une racine) il faut donc se placer dans $\mathbb{F}_{p^{60}}$ (resp. $\mathbb{F}_{p^{10}}$) avec $60 = 5.4.3$ (resp. $10 + 5.2$).

5 1) On considère le morphisme de Frobenius

$$\mathrm{Fr}_q : x \in \mathbb{F}_{q^n} \longmapsto x^q \in \mathbb{F}_{q^n}$$

dont on vérifie aisément que c'est un morphisme de corps car $\mathrm{Fr}_q(x + y) = (x + y)^q = x^q + y^q$ et $\mathrm{Fr}_q(xy) = x^q y^q$, qui laisse le corps $\mathbb{F}_q$ invariant car pour tout $x \in \mathbb{F}_q$ on a $x^q = x$. En outre il est immédiat que le groupe engendré par Fr_q est d'ordre n de sorte que $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est de cardinal supérieur ou égal à n. Pour montrer l'inégalité inverse, soit χ un générateur de $\mathbb{F}_{q^n}^\times$ et soit μ_χ son polynôme minimal unitaire sur $\mathbb{F}_q$; on a alors $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(\mu_\chi(X))$ de sorte que μ_χ est irréductible de degré n. Ainsi tout élément $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est déterminée par $\sigma(\chi)$ qui doit être une racine de μ_χ ce qui donne au plus n choix. On en déduit ainsi $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) =< \mathrm{Fr}_q > \simeq \mathbb{Z}/n\mathbb{Z}$.

Un sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $\mathbb{Z}/r\mathbb{Z}$ pour r un diviseur de n, un générateur étant n/r. On considère alors le sous-groupe de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ engendré par $\mathrm{Fr}_q^{n/r}$; le sous-corps fixé est alors l'ensemble des éléments x de $\mathbb{F}_{q^n}$ tels que $x^{q^{n/r}} = x$ ce qui correspond au corps $\mathbb{F}_{q^{n/r}} \subset \mathbb{F}_{q^n}$. D'après l'exercice précédent, l'application de la théorie de Galois est bien une bijection.

2) Le corps L est isomorphe à $\mathbb{F}_{p^r}$ pour un certain r et $\mathrm{Gal}(L/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par Fr_p. En outre on a $L = \mathbb{F}_p[\chi]$ pour $\chi \in L$ une racine primitive n-ième de l'unité. Ainsi un élément $\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ est déterminé par $\sigma(\chi)$ qui doit être une racine primitive n-ième de

l'unité et donc de la forme χ^k pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient ainsi une application injective naturelle

$$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p) \longmapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$$

l'image étant le groupe engendré par la classe de p. Ainsi r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Soit $\bar{\Phi}_n(X) = P_1 \cdots P_s$ la décomposition en irréductibles de la réduction modulo p de Φ_n. Soit χ une racine de P_1 de sorte que $L = \mathbb{F}_p[\chi]$ et donc P_1 est le polynôme minimal de χ sur $\mathbb{F}_p$ et donc $\deg P_1 = [L : \mathbb{F}_p]$. En conclusion tous les P_i sont de même degré $[L : \mathbb{F}_p]$ et donc $s = \frac{\psi(n)}{[L:\mathbb{F}_p]}$ où l'on rappelle que $[L : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ainsi $p \equiv 1 \mod n$ est équivalent à demander que $\bar{\Phi}_n$ est totalement décomposé sur $\mathbb{F}_p$ ce qui on vient de le voir, est équivalent à demander que $\bar{\Phi}_n$ a une racine dans $\mathbb{F}_p$. Soit donc p premier divisant $\Phi_n(N!) \equiv 1 \mod N!$ soit $p > N$ et $p \equiv 1 \mod n$ car $\bar{\Phi}_n$ a pour racine $\bar{N!}$. On vient donc de montrer une version faible du théorème de progression arithmétique dont l'énoncé fort est que pour tout a premier avec n, il existe une infinité de premiers congrus à a modulo n, ceux-ci se répartissant de manière uniforme en un sens que l'on ne précise pas ici, sur les $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

6 1) Le polynôme $X^4 + 1$ est le huitième polynôme cyclotomique Φ_8 qui est irréductible. On peut aussi le voir directement en considérant $\Phi_8(X + 1)$ qui est un polynôme d'Eisenstein pour 2.

Modulo 2, on a $X^4 + 1 = (X + 1)^4$ et pour $p \neq 2$, $\mathbb{F}_{p^2}^\times$ est cyclique d'ordre $p^2 - 1$ qui est divisible par 8. Soit alors $x \in \mathbb{F}_{p^2}^\times$ d'ordre 8, on a $x^8 = (x^4)^2 = 1$ et $x^4 \neq 1$ soit $x^4 = -1$ de sorte que Φ_8 a une racine dans $\mathbb{F}_{p^2}$ et donc Φ_8 est réductible modulo p.

2) Avec les hypothèses de l'énoncé $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique. D'après loc. cit., la réduction modulo p de ψ_n est un produit de polynômes irréductibles qui ont tous le même degré à savoir l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi ψ_n est irréductible modulo p si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ ce qui ne se peut pas si ce dernier groupe n'est pas cyclique.
Remarque : On a ainsi une famille d'exemples de polynômes irréductibles sur $\mathbb{Z}$ et réductible modulo tout premier p.

7 1) modulo 2, on a $\bar{P} = X^4 + X^2 + 1 = (X^2 + X + 1)^2$, modulo 3, $\bar{P} = X^4 + 2X^3 + 2X + 2 = (X^2+1)(X^2+2X+2)$ et modulo 5, $\bar{P} = X^4 + X^2 + 1$ qui n'a pas de racine dans $\mathbb{F}_5$; regardons dans $\mathbb{F}_{25}$. Comme $\mathbb{F}_{25}^\times \simeq \mathbb{Z}/24\mathbb{Z}$, soit x un élément d'ordre 6 : $x^6 = 1$ avec $x^2 \neq 1$ et $x^3 \neq 1$. Soit $y = x^2$ de sorte que $y^3 - 1 = (y - 1)(y^2 + y + 1) = 0$ et $y \neq 1$ soit $y^2 + y + 1 = 0$ et donc x est une racine de $\bar{P} = (X^2 + X + 1)(X^2 + 4X + 1)$.

2) Sur $\mathbb{Z}$, P n'a pas de racine car sinon il en aurait modulo 2 ce qui n'est pas. Si P était réductible, on aurait alors $P(X) = (X^2 + aX + b)(X^2 + cX + d)$ et donc

$$\begin{cases} a + c = 10 \\ b + d + ac = 21 \\ ad + bc = -10 \\ bd = 11 \end{cases}$$

Ainsi on obtient soit $\{b, d\} = \{1, 11\}$ et donc $ac = 9$ et $\{a, c\} = \{-1, -9\}$ car $a + c = -10$, et $ad + bc \neq -10$; soit $\{b, d\} = \{-1, -11\}$ et $ac = 33$ et $a + c \neq -10$. Ainsi P est irréductible sur $\mathbb{Z}$.

8 Le polynôme X^3+2X+1 n'a pas de racines dans $\mathbb{F}_3$, il y est donc irréductible. L'ordre de X est soit $1, 2, 13, 26$; les cas 1 et 2 sont clairement exclus calculons alors $X^{13} = X^9.X^3.X$. On a

$X^3 = X - 1$ puis $X^9 = X^3 - 1 = X + 1$ et donc $X^{13} = -1$. On vérifie aussi que $X^{10} = X^2 + X$ et donc $i = 10$