Factorisation des polynômes

Solution de l'exercice (??) les polynômes irréductibles de degré 1 sont X et $X-1$; ceux de degré 2 sont tels que $X^4-X=X(X-1)P$ (corollaire **??**), 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. Ces polynômes sont irréductibles sur $\mathbf{F_2}$ car un élément j de $\mathbf{F_4}$ qui n'est pas dans $\mathbf{F_2}$ vérifie $j^3=1$ de sorte qu'il ne peut être racine des polynômes en question.

Solution de l'exercice (??) Pour la première question, il suffit de recopier la démonstration de la remarque **??**, 4.
Pour la seconde, on a $X^{16}-X=(X^4-X)Q_1Q_2Q_3$ (exercice **??**), avec $Q_1=X^4+X+1$, $Q_2=X^4+X^3+X^2+X+1, Q_3=X^4+X^3+1$.

Notons $0,1,j,j^2$ les éléments de $\mathbf{F_4}$ 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, on voit en appliquant la question 1. que X^4+X+1, $X^4+X^3+X^2+X+1$ et X^4+X^3+1 doivent s'écrire chacun comme le produit de deux polynômes irréductibles de degré deux sur $\mathbf{F_4}$. 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 $X^4+X^3+X^2+X+1=(X^2+jX+1)(X^2+j^2X+1)$.

Solution de l'exercice (??) (a) On note $(1,-1,0)$ les éléments du corps $\mathbf{F_3}$. On vérifie rapidement que $Q(0)$, $Q(1)$ et $Q(-1)$ ne sont pas nuls de sorte que Q n'a pas de racine dans $\mathbf{F}_3$. On cherche alors ses racines dans $\mathbf{F}_9$. Pour $a\in\mathbf{F}_9$, on a $a^9=a$ de sorte que $a^9-a+1=1$ et donc Q n'a pas de racine dans $\mathbf{F}_9$.

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

(c) Soit alors $\alpha\in\mathbf{F}_{27}$ 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 $\mathbf{F}_{27}$ de sorte que Q est divisible par X^3-X-1, polynôme minimal de α sur $\mathbf{F_3}$. Cela donne $X^9-X+1=(X^3-X-1)(X^6+X^4+X^3+X^2-X-1)$.

(d) Cherchons de manière générale toutes les racines de Q dans $\mathbf{F}_{27}$,; d'après (b), un élément quelconque s'écrit sous la forme $x=a\alpha^2+b\alpha+c$ avec $a,b,c\in\mathbf{F}_3$. 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 $x=\alpha,\alpha+1,\alpha-1$.

(e) On en déduit alors que $X^6+X^4+X^3+X^2-X-1$ n'a pas de racines dans $\mathbf{F}_{27}$; ceci implique qu'il est irréductible sur $\mathbf{F_3}$, car sinon il aurait un facteur irréductible de degré b1,2 ou 3 et donc une racine dans $\mathbf{F_3}$, $\mathbf{F_9}$ ou $\mathbf{F_{27}}$.

Solution de l'exercice (??)

Solution de l'exercice (??) si P est réductible sur $\mathbf{F}_p$, il l'est sur toute extension $\mathbf{F}_{p^m}$. Supposons donc P irréductible sur $\mathbf{F}_p$ de sorte que toutes les racines de P, vues dans $\bar{\mathbf{F}}_p$, sont dans $\mathbf{F}_{p^n}$ et aucune n'appartient à un sous-corps strict (remarque **??**). On regarde alors P comme un polynôme dans $\mathbf{F}_{p^m}[X]$ dont on se demande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines dans $\mathbf{F}_{p^{mr}}$ pour $r \leq n/2$ (exercice **??**) et donc si $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{mr}}$; ceci signifie que 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.

La décomposition en facteurs irréductibles d'un polynôme de degré 5 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 $\mathbf{F}_{p^{60}}$ (resp. $\mathbf{F}_{p^{10}}$) avec $60 = 5.4.3$ (resp. $10 = 5.2$).

Solution de l'exercice (??) le polynôme $P = X^4 + 1$ est irréductible sur $\mathbf{Q}$ (donc sur $\mathbf{Z}$) car sa décomposition en facteurs irréductibles unitaires sur $\mathbf{R}$ n'est pas à coefficients dans $\mathbf{Q}$ ($X^4+1 = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$).

Modulo 2, on a $X^4 + 1 = (X + 1)^4$ et pour $p \neq 2$,

On a ainsi un exemple d'un polynôme irréductible sur $\mathbf{Z}$ et réductible modulo tout nombre premier p.

Solution de l'exercice (??) (a) - Modulo 2, on a $\bar{P} = X^4 + X^2 + 1$ que l'on factorise facilement en $(X^2 + X + 1)^2$.

- Modulo 3, on a $\bar{P} = X^4 - X^3 - X - 1$ qui n'a pas de racine dans $\mathbf{F}_3$. On regarde alors dans $\mathbf{F}_9$, qui en remarquant que $X^2 + 1$ n'a pas de racines dans $\mathbf{F}_3$, est alors isomorphe à $\mathbf{F}_3[X]/(X^2+1)$. Notons i l'image de X dans $\mathbf{F}_9$ par l'isomorphisme $\mathbf{F}_3[X](X^2 + 1) \longrightarrow \mathbf{F}_9$. On a alors $i^4 = 1$ et $i^3 = -i$ de sorte que $\bar{P}(i) = 0$. On en déduit alors que $\bar{P}$ est divisible par $X^2 + 1$ et on calcule le quotient $X^2 - X - 1$ qui, ne possédant pas de racine sur $\mathbf{F}_3$, est irréductible sur $\mathbf{F}_3$, d'où la factorisation $\bar{P} = (X^2 + 1)(X^2 - X - 1)$.

(b) Sur $\mathbf{Z}$, 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 $\mathbf{Z}$.

Corps finis

Solution de l'exercice (??) (a) Le groupe multiplicatif $\mathbf{F}_{23}^*$ est cyclique, (proposition **??**), et donc isomorphe à $(\mathbf{Z}/22\mathbf{Z},+)$, de sorte que l'ordre d'un élément distinct de 1 est 2, 11 ou 22.

(b) On a $5^2\equiv 2 \mod 23$ de sorte que 5 n'est pas d'ordre 2. Pour calculer 5^{11}, on propose d'écrire 11 en base 2, *i.e.* $11=2^3+2^1+2^0$ et de calculer 5^{2^i} pour $i\leq 3$ de sorte que $5^{11}=5^{2^3}5^{2^1}5^{2^0}$, ce qui donne : $5^{2^4}=(5^2)^2\equiv 2^2 \mod 23$ et $5^{2^3}\equiv 4^2 \mod 23$. On obtient alors $5^{11}\equiv 16.2.5 \mod 23$ soit $5^{11}\equiv -1 \mod 23$.

(c) On déduit de (b) que 5 est d'ordre 22 et engendre donc $\mathbf{F}_{23}^*$.

Solution de l'exercice (??) (a) - De manière évidente $P_1(X_1,\cdots,X_s)=X_1$.

- De l'égalité $\sum_{i=1}^s \alpha_i^2=(\sum_{i=1}^s \alpha_i)^2-2\sum_{1\leq i<j\leq s}\alpha_i\alpha_j$, on en déduit que $P_2(X_1,\cdots,X_s)=X_1^2-2X_2$.

- On calcule de même $\sum_{i=1}^s \alpha_i^3=(\sum_{i=1}^s \alpha_i)^3-3\sum_{1\leq i\neq j\leq s}\alpha_i^2\alpha_j)$ ce qui donne $P_3(X_1,\cdots,X_s)=X_1^3-3(X_1X_2-3X_3)$.

(b) On rappelle que les $x\in\mathbf{F}_q$ sont les racines du polynôme X^q-X de sorte que $\sigma_1=\cdots=\sigma_{q-2}=\sigma_q=0$ et $(-1)^{q-1}\sigma_{q-1}=-1$ dans $\mathbf{F}_p$. Pour i divisible par $q-1$, on a $x^i=1$ pour tout $x\in\mathbf{F}_q^*$ puisque $x^{q-1}=1$, d'où $\psi(i)=0+(q-1).1=-1$ dans $\mathbf{F}_q$. De manière générale, le même argument montre que $\psi(i)=\psi(r)$ où r est le reste de la division euclidienne de i par $q-1$. Par ailleurs, pour $1\leq r\leq q$, $\psi(r)$ est un polynôme en les σ_k pour $1\leq k\leq i$ de sorte que $\psi(i)=0$ si i n'est pas congru à 0 modulo $q-1$.

Solution de l'exercice (??)

(a) Le sous-anneau de $\mathbf{F}_{p^n}$ engendré par a est un sous-corps isomorphe à $\mathbf{F}[X]/(q_a(X))$ qui est isomorphe à $\mathbf{F}_{p^{\deg q_a}}$ de sorte que $\deg q_a$ divise n.

(b) L'application de Frobenius $Fr : x \mapsto x^p$ est un automorphisme du corps $\mathbf{F}_{p^n}$ qui laisse stable le sous-corps $\mathbf{F}_p$. On applique alors le Fr à l'égalité $q_a(a) = 0$ ce qui donne $q_a(a^p) = 0$, car q_a étant à coefficients dans $\mathbf{F}_p$ est invariant par Fr. On en déduit alors que a^p est une racine de q_a ; ce dernier étant irréductible, c'est le polynôme minimal de a^p.

(c) Le lemme **??** implique immédiatement que n est le plus petit entier s tel que $a^{p^s} = a$. On en déduit donc que pour tout $0 \leq i \neq j \leq n-1$, $a^{p^i} \neq a^{p^j}$ de sorte que les q_a admet les n racines: $a, a^p, \cdots, a^{p^{n-1}}$. Or q_a étant de degré n, ce sont exactement toutes ses racines.

Solution de l'exercice (??)

Solution de l'exercice (??)

Solution de l'exercice (??) (i) On vérifie rapidement que X^2+X+1 n'a pas de racines dans $\mathbf{F}_2$; étant de degré 2 il est alors irréductible de sorte que $\mathbf{F}_2[X]/(X^2+X+1)$ est un corps, une extension de degré 2 de $\mathbf{F}_2$ et donc isomorphe à $\mathbf{F}_4$.

(ii) De même, on vérifie que X^3+X+1 n'a pas de racines dans $\mathbf{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbf{F}_2$ de sorte que $\mathbf{F}_2[X]/(X^3+X+1)$ est un corps de cardinal 8 et donc isomorphe à $\mathbf{F}_8$. Comme $\mathbf{F}_8^* \simeq \mathbf{Z}/7\mathbf{Z}$ tout élément autre que 1 est un générateur du groupe des inversibles, par exemple x (x désigne la classe de X dans $\mathbf{F}_2[X]/(X^3+X+1)$).

(iii) A nouveau X^2+X-1 n'a pas de racines dans $\mathbf{F}_3$, il y est donc irréductible et $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$. En outre $\mathbf{F}_9^* \simeq \mathbf{Z}/8\mathbf{Z}$ de sorte qu'il y a $\varphi(8) = 4$ générateurs. On a $X^4 = (X-1)^2 = X^2 - 2X + 1 = -3X + 2 = -1$ et X est un générateur de $\mathbf{F}_9^*$.

Solution de l'exercice (??)

Problèmes

Solution du problème (??)

(1) On écrit la table des carrés de $\mathbf{F}_5$, soit $\begin{array}{cccccc} x & 0 & 1 & 2 & -2 & -1 \\ x^2 & 0 & 1 & -1 & -1 & 1 \end{array}$ et on remarque que 2 n'est pas un carré dans $\mathbf{F}_5$.

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 $\mathbf{F}_5$, étant de degré 2 il y est donc irréductible.

(3) Le corps $\mathbf{F}_5[X]/(P(X))$ est de cardinal 25 et donc isomorphe à $\mathbf{F}_{25}$ qui est un corps de décomposition de $X^{25}-X$ Par ailleurs la classe x de X dans $\mathbf{F}_5[X]/(P(X))$ 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 $\mathbf{F}_{25}$.

(3) Un isomorphisme $f : \mathbf{F}_5[X]/(X^2+X+1) \simeq \mathbf{F}_{25}$ étant fixé, l'image $\alpha \in \mathbf{F}_{25}$ 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 $\mathbf{F}_5$ de $\mathbf{F}_{25}$ engendré par 1 et α est de dimension 2 car $\alpha \notin \mathbf{F}_5$ et est donc égal à $\mathbf{F}_{25}$ de sorte que tout élément $\beta \in \mathbf{F}_{25}$ s'écrit sous la forme $a\alpha+b$ avec $a,b \in \mathbf{F}_5$.

(4) On vérifie rapidement que P n'a pas de racine dans $\mathbf{F}_5$. Soit alors $\beta = a\alpha+b \in \mathbf{F}_{25}$; 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 $\alpha \notin \mathbf{F}_5$ soit P n'a pas de racine dans $\mathbf{F}_{25}$ de sorte qu'il est irréductible sur $\mathbf{F}_5$.

Par ailleurs, P en tant que polynôme de $\mathbf{Z}[X]$ unitaire, y est irréductible. En effet une factorisation $P=QR$ dans $\mathbf{Z}[X]$ induit par réduction modulo 5 une factorisation $\bar{P}=\bar{Q}\bar{R}$ dans $\mathbf{F}_5[X]$. 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 $\mathbf{Z}$ et donc irréductible sur $\mathbf{Q}$ d'après le lemme de Gauss (*cf.* la proposition (**??**)).

Solution du problème (??)

(a) On pose donc $y=xz$ de sorte que $\left(\frac{xy}{q}\right) = \left(\frac{x}{q}\right)^2\left(\frac{z}{q}\right) = \left(\frac{z}{q}\right)$. On obtient alors

$$\tau^2 = \sum_{z\in(\mathbf{Z}/q\mathbf{Z})^\times}\left(\frac{z}{q}\right)\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} w^{x(1+z)}$$

En outre on a $\sum_{x=1}^{q-1} w^x = 0$ de sorte que si $z\neq -1$, $\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} w^{x(1+z)} = -1$ ce qui permet d'écrire

$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{z\in(\mathbf{Z}/q\mathbf{Z})^* \\ z\neq -1}} -\left(\frac{z}{q}\right)$$

(b) Comme il y a autant de carrés que de non carrés dans $(\mathbf{Z}/q\mathbf{Z})^*$, on en déduit que $\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^*}\left(\frac{x}{q}\right)=0$ d'où le résultat.

(c) Ainsi $\left(\frac{-1}{q}\right) q$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si τ appartient à $\mathbf{Z}/p\mathbf{Z}$, soit si et seulement si $\tau^p = \tau$. En effet on rappelle que $\mathbf{Z}/p\mathbf{Z} \subset K$ est l'ensemble des racines de l'équation $X^p - X$. On peut aussi utiliser la théorie de Galois en disant que $\tau \in K$ appartient à $\mathbf{Z}/p\mathbf{Z}$ si et seulement si il est invariant par tous les éléments du groupe de Galois de l'extension $K : \mathbf{Z}/p\mathbf{Z}$ la propriété découle alors du fait que ce groupe est cyclique engendré par le Frobenius $x \mapsto x^p$.

(d) On calcule alors

$$\begin{aligned} \tau^p &= \textstyle\sum_{x \in (\mathbf{Z}/q\mathbf{Z})^\times} \left(\frac{x}{q}\right) w^{px} \\ &= \left(\frac{p}{q}\right)^{-1} \textstyle\sum_{y \in (\mathbf{Z}/q\mathbf{Z})^\times} \left(\frac{y}{q}\right) w^y = \left(\frac{p}{q}\right) \tau \end{aligned}$$

Ainsi $\left(\frac{-1}{q}\right) q$ est un carré si et seulement si $\left(\frac{p}{q}\right) = 1$ *i.e.* p est un résidu quadratique modulo p. On a alors

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{(-1)^{(q-1)/2}}{p}\right) \left(\frac{q}{p}\right) \\ &= \left(\frac{-1}{q}\right)^{(q-1)/2} \left(\frac{q}{p}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{(p-1)(q-1)}{2}} \end{aligned}$$

Solution du problème (??)

(1) Prenons par exemple le mouvement élémentaire de la figure (**??**). Dans le plateau de gauche on a $\alpha = j^{x_0+y_0}(1+j)$ (resp. $\beta = j^{x_0-y_0}(1+j)$) alors que dans le plateau de droite on a $\alpha = j^{x_0+y_0}.j^2$ (resp. $\beta = j^{x_0-y_0}j^2$), avec $(x_0, y_0) = (-2, -1)$. Le résultat découle alors de l'égalité $1 + j = j^2$ dans $\mathbf{F}_4$ (on rappelle que dans $\mathbf{F}_4$, on a $1 = -1$). Les autres mouvements élémentaires se traitent de manière strictement identique.

(2) Commençons par calculer (α, β) pour la configuration où tous les réceptacles contiennent une bille. La configuration étant invariante par la réflexion d'axe (Oy), on a $\alpha = \beta$, calculons donc α. Pour cela on propose de sommer sur les droites $x + y$ constantes, de sorte que ne contribuent que les droites où il y a un nombre impair de billes, ce qui donne $\alpha = j^0 + j^2 + j^{-2} = 0$, comme on le voit sur la figure suivante.

Notons alors avec un indice *tot* (resp. $\mathcal{C}_0$, resp. 0) ce qui fait référence à la configuration où tous les réceptacles sont remplis (resp. tous sauf en (x_0, y_0), resp aucun sauf en (x_0, y_0)). On a ainsi $(\alpha_{tot}, \beta_{tot}) = (\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) + (\alpha_0, \beta_0) = (0, 0)$ de sorte que $(\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) = (\alpha_0, \beta_0)$.

(3) On calcule comme précédemment les invariant (α, β) ce qui donne $(0, 0)$ qui ne peut pas être de la forme $(j^{x_0+y_0}, j^{x_0-y_0})$.