MAT4111

Premier semestre — 2020–2021

Fiche 6: Corps finis

1. Soient $\mathbb{F}_q$ un corps à q éléments et $\mathbb{F}_{q^n}$ une extension de degré n de $\mathbb{F}_q$. Montrer qu'il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

Solution. On sait que $\mathbb{F}_{q^n}^*$ est un groupe cyclique, puisque tout sous-groupe fini du groupe d'éléments non nuls d'un corps est cyclique. Soit $\alpha \in \mathbb{F}_{q^n}^*$ un générateur. Par conséquent, tout élément de $\mathbb{F}_{q^n}^*$ est une puissance de α, ce qui implique en particulier que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

2. (*a*) Déterminer tous les polynômes irréductibles unitaires de degré 2 de $\mathbb{F}_3[X]$.

(*b*) Montrer que $\mathbb{F}_3[X]/(X^2-X-1)$ et $\mathbb{F}_3[Y]/(Y^2+1)$ sont deux corps isomorphes.

(*c*) On note α, resp. β, la classe de X, resp. Y , dans le quotient. Déterminer l'ordre de α et β dans le groupe multiplicatif $\mathbb{F}_{3^2}^*$.

(*d*) Expliciter un isomorphisme et sa réciproque entre $\mathbb{F}_3(\alpha) \simeq \mathbb{F}_3[X]/(X^2-X-1)$ et $\mathbb{F}_3(\beta) \simeq \mathbb{F}_3[Y]/(Y^2+1)$.

(*e*) Déterminer tous les générateurs de $\mathbb{F}_3(\alpha)^*$ et de $\mathbb{F}_3(\beta)^*$.

Solution.

(*a*) On laisse à la lectrice/au lecteur la vérification immédiate du fait que X^2+1, X^2+X-1 et X^2-X-1 sont les seuls polynômes unitaires de degré 2 de $\mathbb{F}_3[X]$ sans aucune racine dans $\mathbb{F}_3$. Cette dernière propriété équivaut à être irréductible, puisque les polynômes ont degré 2.

(*b*) Le résultat suit du fait que $\mathbb{F}_3[X]/(X^2-X-1)$ et $\mathbb{F}_3[Y]/(Y^2+1)$ ont dimension 2 sur $\mathbb{F}_3$, vu qu'il existe un seul corps d'ordre p^n pour tout $p \in \mathbb{N}$ premier et $n \in \mathbb{N}^*$, à isomorphisme près.

(*c*) L'ordre de α est 8 et celui de β est 4.

(*d*) Soit $\phi : \mathbb{F}_3[X] \to \mathbb{F}_3[Y]/(Y^2+1)$ le morphisme surjectif d'anneaux donné par $P(X) \mapsto [P(Y-1)]$, où les crochets dénotent la classe d'un élément dans $\mathbb{F}_3[Y]/(Y^2+1)$. C'est clair que $\phi(X^2-X-1) = [Y^2+1] = 0$, ce qui donne un morphisme surjectif d'anneaux $\bar{\phi} : \mathbb{F}_3[X]/(X^2-X-1) \to \mathbb{F}_3[Y]/(Y^2+1)$. Comme $\mathbb{F}_3[X]/(X^2-X-1)$ et $\mathbb{F}_3[Y]/(Y^2+1)$ ont dimension 2 sur $\mathbb{F}_3$, $\bar{\phi}$ es un isomorphisme. La réciproque est le morphisme d'anneaux $\bar{\psi} : \mathbb{F}_3[Y]/(Y^2+1) \to \mathbb{F}_3[X]/(X^2-X-1)$ induit par le morphisme surjectif d'anneaux $\psi : \mathbb{F}_3[Y] \to \mathbb{F}_3[X]/(X^2-X-1)$ donné par $P(Y) \mapsto [P(X+1)]$.

(*e*) Les générateurs de $\mathbb{F}_3(\alpha)^*$ sont donnés par α^d avec $d \in \{1, \dots, 7\}$ premiers avec 8, *i.e.* $\{\alpha, \alpha^3, \alpha^5, \alpha^7\}$. Un calcul élémentaire donne $\{\pm X, \pm(1-X)\}$, où l'on a omis la barre pour dénoter la classe d'équivalence. Si l'on applique l'isomorphisme $\bar{\phi}$ on trouve que les générateurs de $\mathbb{F}_3(\beta)^*$ sont $\{\pm(Y-1), \pm(Y+1)\}$.

3. (*a*) Donner un exemple de construction d'un corps k à 4 éléments, d'un corps K à 8 éléments, d'un corps L à 16 éléments.

(b) Existe-t-il un plongement du corps k dans le corps L ? Si oui, en donner un.

(c) Existe-t-il un plongement du corps K dans le corps L ? Si oui, en donner un.

(d) Combien existe-il de tels plongements ?

(e) Combien le corps L contient-il de sous-corps à 4 éléments ?

(f) Soit γ le morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{F}_2[X]$ défini par

$$\gamma\Big(\sum_{i=0}^{m} a_i X^i\Big) = \sum_{i=0}^{m} \bar{a}_i X^i.$$

(i) Quelle est la décomposition de $\gamma(\Phi_{15})$ en produit d'éléments irréductibles de $\mathbb{F}_2[X]$?

(ii) Combien le polynôme $\gamma(\Phi_{15})$ possède-t-il de racines dans L ?

(iii) Montrer que les générateurs du groupe L^* sont exactement les racines de $\gamma(\Phi_{15})$ dans L.

Solution.

(a) On rappelle que, étant donné un corps $\Bbbk$, si $P \in \Bbbk[X]$ a degré $d \in \mathbb{N}$, alors $\Bbbk[X]/(P)$ a dimension d sur $\Bbbk$. En plus, si $\Bbbk$ est un corps à m éléments et V est un espace vectoriel sur $\Bbbk$ de dimension d, alors $\#(V) = m^d$. On voit bien que les polynômes $P = X^2 + X + 1 \in \mathbb{F}_2[X]$ et $Q = X^3 + X + 1 \in \mathbb{F}_2[X]$ sont irréductibles, car ils ont degré inférieur ou égal à 3 et ils n'ont pas de racines dans $\mathbb{F}_2$. En conséquence, $k = \mathbb{F}_2[X]/(P)$ et $K = \mathbb{F}_2[X]/(Q)$ sont des corps à 4 et à 8 éléments, respectivement.

Par ailleurs on peut vérifier que le polynôme $R = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ est irréductible. En effet, si l'on suppose que $R = R_1R_2$, avec $R_1, R_2 \in \mathbb{F}_2[X]$ unitaires, on note d'abord que $\deg(R_1), \deg(R_2) > 1$, car R n'a pas de racines dans $\mathbb{F}_2$. Cela nous dit que $\deg(R_1) = \deg(R_2) = 2$. Si l'on écrit $R_1 = X^2 + aX + b$ et $R_2 = X^2 + cX + d$, $R = R_1R_2$ nous dit que $bd = 1$, ce qui implique $b = d = 1$. Si l'on regarde les coefficients des puissances positives de X dans $R = R_1R_2$, on trouve en plus $a + c = 1$, $ac = 0$ et $a + c = 0$, ce qui est absurde. En conséquence, $R = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ est irréductible. On conclut que $L = \mathbb{F}_2[X]/(R)$ est un corps à 16 éléments. On observe que le même argument montre aussi que $S = X^4 + X + 1 \in \mathbb{F}_2[X]$ est irréductible et que $L' = \mathbb{F}_2[X]/(S)$ est un corps à 16 éléments. Comme il existe un seul corps d'ordre p^n pour tout $p \in \mathbb{N}$ premier et $n \in \mathbb{N}^*$, à isomorphisme près, $L = \mathbb{F}_2[X]/(R)$ et $L' = \mathbb{F}_2[X]/(S)$ sont isomorphes. Par exemple, c'est facile à vérifier que le seul morphisme d'anneaux $\rho : \mathbb{F}_2[X] \to \mathbb{F}_2[X]/(R)$ qui associe à X le polynôme X^2+X+1 induit un morphisme d'anneaux $\bar{\rho} : \mathbb{F}_2[X]/(S) \to \mathbb{F}_2[X]/(R)$, qui est injectif donc bijectif, car les deux corps ont le même cardinal.

(b) Oui. Soit $T = aX^3 + bX^2 + cX + d \in \mathbb{F}_2[X]$. On considère le seul morphisme d'anneaux $\phi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]/(R)$ qui associe à X la classe de $T \in \mathbb{F}_2[X]$ dans $\mathbb{F}_2[X]/(R)$. On voit bien que

$$\phi(P) = \phi(X^2 + X + 1) = T^2 + T + 1 = bX^3 + (a + b + c)X^2 + (a + c)X + (a + b + 1),$$

ce qui nous dit que $\phi(P) = 0$ si et seulement si $a = c = 1$ et $b = 0$. En conséquence, ϕ induit un morphisme d'anneaux $\bar{\phi} : \mathbb{F}_2[X]/(P) \to \mathbb{F}_2[X]/(R)$ si et seulement si $a = c = 1$ et $b = 0$, *i.e.* $T = X^3+X+d$, avec $d \in \mathbb{F}_2$. Comme tout morphisme d'anneaux entre corps est injectif, on conclut que $\bar{\phi} : k \to L$ est injectif. On remarque en plus que pour tout morphisme d'anneaux $\bar{\psi} : \mathbb{F}_2[X]/(P) \to \mathbb{F}_2[X]/(R)$ est le morphisme induit par le morphisme d'anneaux $\psi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]/(R)$ donné par la composition de la projection canonique $\mathbb{F}_2[X] \to \mathbb{F}_2[X]/(P)$ et de $\bar{\psi}$. En conséquence, on a trouvé tous les morphismes d'anneaux $k \to L$.

(*c*) Non. S'il existe un plongement de K dans L, alors L est un espace vectoriel sur K. Si l'on applique le résultat rappelé dans le premier item au corps K et au espace vectoriel L, on trouve un absurde, car le cardinal de L devrait être une puissance du cardinal de K.

(*d*) On l'a déjà fait dans les items précédents.

(*e*) Il existe un seul sous-corps à 4 éléments dans L, car ce sous-corps est de l'ensemble de racines du polynôme $X^4 - X$ dans L.

(*f*) On laisse à la lectrice/au lecteur la vérification du fait élémentaire que

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \in \mathbb{Z}[X]$$

(voir l'exercice **12**).

(i) On voit bien que

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

dans $\mathbb{F}_2[X]$. En plus, on a montré dans le premier item que les polynômes X^4+X+1 et $X^4 + X^3 + 1$ sont irréductibles dans $\mathbb{F}_2[X]$.

(ii) On remarque que si $\alpha \in L$ (resp., $\beta \in L$) est une racine de $R = X^4 + X^3 + 1$ (resp., $S = X^4 + X + 1$), alors α^2 est aussi des racine de R (resp., S) dans L

$$R(\alpha^2) = \alpha^8 + \alpha^6 + 1 = (\alpha^3 + 1)^2 + \alpha^6 + 1 = 0$$

$$\left(\text{resp., } S(\beta^2) = \beta^8 + \beta^2 + 1 = (\beta + 1)^2 + \beta^2 + 1 = \beta^2 + 1 + \beta^2 + 1 = 0\right).$$

En particulier, α^{2^n} (resp., β^{2^n}) est aussi une racine de $R = X^4 + X^3 + 1$ (resp., $S = X^4 + X + 1$) pour tout $n \in \mathbb{N}^*$. Par exemple, si $\alpha \in L$ (resp., $\beta \in L$) est une racine de $R = X^4+X^3+1$ (resp., $S = X^4+X+1$), alors $\alpha^4 = \alpha^3+1$ (resp., $\beta^4 = \beta+1$) est aussi une racine de $R = X^4+X^3+1$ (resp., $S = X^4+X+1$). On remarque que, si $\alpha \in L$ est une racine de R, le cardinal de l'ensemble $\{\alpha, \alpha^2, \alpha^3+1, \alpha^3+\alpha^2+\alpha\} \subseteq L$ de racines de R est 4, car sinon α serait la racine d'un polynôme dans $\mathbb{F}_2[X]$ de degré inférieur à 4, ce qui est absurde, car α est une racine du polynôme irréductible R sur $\mathbb{F}_2$. De façon analogue, si $\beta \in L$ est une racine de S, le cardinal de l'ensemble $\{\beta, \beta+1, \beta^2, \beta^2+1\} \subseteq L$ de racines de S est 4, car sinon β serait la racine d'un polynôme dans $\mathbb{F}_2[X]$ de degré inférieur à 4, ce qui est absurde, car β est une racine du polynôme irréductible S sur $\mathbb{F}_2$.

Soit $\beta' \in L'$ la classe de X dans $L' = \mathbb{F}_2[X]/(S)$ et α la classe de de X dans $L = \mathbb{F}_2[X]/(R)$. C'est clair que α est une racine de R dans L. En conséquence, on trouve que les 4 racines de R dans L, donc *a fortiori* des racines de $\gamma(\Phi_{15})$ dans L, sont données par

$$\{\alpha, \alpha^2, \alpha^3 + 1, \alpha^3 + \alpha^2 + \alpha\}. \tag{1}$$

Par ailleurs, c'est aussi clair que β' est une racine de S dans L', ce qui implique que $\beta = \bar{\rho}(\beta') = \alpha^2+\alpha+1$ est une racine de S dans L. En conséquence, on trouve que les 4 racines de S dans L, donc *a fortiori* des racines de $\gamma(\Phi_{15})$ dans L, sont données par

$$\{\beta, \beta^2, \beta + 1, \beta^2 + 1\} = \{\alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^2 + \alpha, \alpha^3 + \alpha^2\}. \tag{2}$$

La réunion des ensembles (disjoints) donnés dans (1) et (2) nous donne les racines de $\gamma(\Phi_{15})$ dans L.

(iii) Soit $\delta \in L^*$. Comme le cardinal du groupe L^* est 15, on a $\delta^{15} = 1$, *i.e.* δ est une racine de $X^{15} - 1$. Le groupe L^* étant cyclique, $\delta \in L^*$ est un générateur si et seulement si l'ordre de δ est 15, *i.e.* son ordre n'est pas un diviseur propre de 15. Autrement dit, $\delta \in L^*$ est un générateur si et seulement si δ n'est pas une racine de $X^3 - 1 = (X-1)\gamma(\Phi_3)$ et δ n'est pas une racine de $X^5 - 1 = (X-1)\gamma(\Phi_5)$. Comme $X^{15} - 1 = (X-1)\gamma(\Phi_3)\gamma(\Phi_5)\gamma(\Phi_{15})$ est un polynôme séparable, vu que sa dérivée X^{14} admet seulement la racine nulle, les polynômes $(X-1)\gamma(\Phi_3)\gamma(\Phi_5)$ et $\gamma(\Phi_{15})$ sont premiers entre eux. En conséquence, $\delta \in L^*$ est un générateur si et seulement si δ est une racine de $\gamma(\Phi_{15})$, comme on voulait démontrer.

4. (a) Quel est le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$? de degré 4 sur $\mathbb{F}_3$?

(b) Donner une construction du corps $\mathbb{F}_{5^2}$.

(c) Donner un élément d'ordre 8 dans $\mathbb{F}_{5^2}^*$.

(d) Quel est le corps de décomposition de $X^4 + 1$ sur $\mathbb{F}_5$?

(e) Quel est le corps de décomposition de $X^3 - 2$ sur $\mathbb{F}_5$? $\mathbb{F}_7$?

(f) Le polynôme $X^4 - 2$ est-il irréductible sur $\mathbb{F}_5$? sur $\mathbb{F}_{5^2}$?

Solution.

(a) On dénote $M_n(q)$ le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$. D'ailleurs, on note que le nombre de polynômes unitaires de degré n dans $\mathbb{F}_q[X]$ est q^n.

On va d'abord calculer $M_2(q)$, où $q \in \mathbb{N}^*$ est de la forme p^k, avec $p \in \mathbb{N}^*$ premier et $k \in \mathbb{N}^*$. En outre, un polynôme $P \in \mathbb{F}_q[X]$ de degré 2 n'est pas irréductible sur $\mathbb{F}_q$ si et seulement s'il admet une racine dans $\mathbb{F}_q$, si et seulement si $P = (X-a)(X-b)$, avec $a, b \in \mathbb{F}_q$. En conséquence, on voit bien que le nombre de polynômes $P \in \mathbb{F}_q[X]$ de degré 2 qui ne sont pas irréductibles sur $\mathbb{F}_q$ est

$$q + \binom{q}{2} = \frac{q(q+1)}{2}, \tag{3}$$

car q est le nombre de polynômes de la forme $(X-a)^2$ avec $a \in \mathbb{F}_q$ et $q!/(2!(q-2)!)$ est le nombre de polynômes de la forme $(X-a)(X-b)$ avec $a, b \in \mathbb{F}_q$ différents. En conséquence,

$$M_2(q) = q^2 - \left(q + \binom{q}{2}\right) = q^2 - \frac{q(q+1)}{2} = \frac{q(q-1)}{2}, \tag{4}$$

En particulier, $M_2(3) = 3$ et $M_2(7) = 21$.

On va maintenant calculer $M_3(q)$, avec $q \geq 3$. Pour le faire, on remarque d'abord qu'un polynôme unitaire $P \in \mathbb{F}_q[X]$ de degré 3 non irréductible sur $\mathbb{F}_q$ est de la forme

(C.1) $P = (X-a)(X-b)(X-c)$, avec $a, b, c \in \mathbb{F}_q$;

(C.2) $P = (X-a)Q$, avec $a \in \mathbb{F}_q$ et $Q \in \mathbb{F}_q[X]$ unitaire de degré 2 irréductible sur $\mathbb{F}_q$.

Dans le cas (C.1) on a trois possibilités disjointes :

(C.1.i) $\{a, b, c\}$ a cardinal 3, *i.e.* $a, b, c \in \mathbb{F}_q$ sont différents ;

(C.1.ii) $\{a, b, c\}$ a cardinal 2, *i.e.* P admet une racine double dans $\mathbb{F}_q$ et une racine simple ;

(C.1.iii) $\{a, b, c\}$ a cardinal 2, *i.e.* P admet une racine triple dans $\mathbb{F}_q$.

Cela implique que le nombre de polynômes dans le cas (C.1) est

$$\binom{q}{3} + q.(q-1) + q = \frac{q(q^2-3q+2)}{6}.$$

En outre, c'est clair que le nombre de polynômes dans le cas (C.2) est

$$q.M_2(q) = \frac{q^2(q-1)}{2}.$$

En conséquence,

$$M_3(q) = q^3 - \left(\frac{q(q^2+3q+2)}{6} + \frac{q^2(q-1)}{2}\right) = \frac{q(q^2-1)}{3}.$$

Cela nous dit que $M_3(3) = 8$ et

$$M_3(7) = \frac{7.48}{3} = 112.$$

On va finalement calculer $M_4(3)$. Pour le faire, on remarque d'abord qu'un polynôme unitaire $P \in \mathbb{F}_q[X]$ de degré 4 non irréductible sur $\mathbb{F}_q$ est de la forme

(D.1) $P = (X-a)(X-b)(X-c)(X-d)$, avec $a, b, c, d \in \mathbb{F}_q$;

(D.2) $P = (X-a)Q$, avec $a \in \mathbb{F}_q$ et $Q \in \mathbb{F}_q[X]$ unitaire de degré 3 irréductible sur $\mathbb{F}_q$;

(D.3) $P = (X-a)(X-b).Q$, avec $Q \in \mathbb{F}_q[X]$ unitaire de degré 2 irréductible sur $\mathbb{F}_q$;

(D.4) $P = R.S$, avec $R, S \in \mathbb{F}_q[X]$ unitaires de degré 2 irréductibles sur $\mathbb{F}_q$;

On fixe désormais $q = 3$. Dans le cas (D.1) on a quatre possibilités disjointes :

(D.1.i) $\{a, b, c, d\}$ a cardinal 3, *i.e.* P admet une racine double dans $\mathbb{F}_3$ et deux racine simples dans $\mathbb{F}_q$;

(D.1.ii) P admet une racine triple dans $\mathbb{F}_q$ et une racine simple ;

(D.1.iii) P admet deux racines doubles différentes dans $\mathbb{F}_q$.

(D.1.iv) $\{a, b, c, d\}$ a cardinal 1, *i.e.* P admet une racine d'ordre 4 dans $\mathbb{F}_3$.

On note que $\{a, b, c, d\}$ a cardinal 2 dans les cas (D.1.ii) et (D.1.iii). Cela implique que le nombre de polynômes dans le cas (D.1) est

$$3 + 3.2 + 3 + 3 = 15.$$

Par ailleurs, le nombre de polynômes dans le cas (D.2) est

$$3.M_3(3) = 3.8 = 24.$$

En outre, le nombre de polynômes dans le cas (D.3) est

$$\left(3 + \binom{3}{2}\right).M_2(3) = 6.3 = 18.$$

Finalement, le nombre de polynômes dans le cas (D.4) est

$$\left(3 + \binom{3}{2}\right) = 6,$$

vu que le nombre de polynômes unitaire de degré 2 irréductibles sur $\mathbb{F}_3$ est 3. En conséquence,

$$M_4(3) = 3^4 - \left(15 + 24 + 18 + 6\right) = 18.$$

Pour un point de vue plus général, voir l'exercice **11**, item (b).

(b) C'est facile à vérifier que le polynôme $X^2-2 \in \mathbb{F}_5[X]$ est irréductible, puisqu'il n'a pas de racines dans $\mathbb{F}_5$. Le même argument nous dit que $X^2+2 \in \mathbb{F}_5[X]$ est irréductible. Par conséquent, $\mathbb{F}_5[X]/(X^2-2)$ est un corps à 25 éléments. Par unicité à isomorphisme près des corps finis, $\mathbb{F}_5[X]/(X^2-2) = \mathbb{F}_{5^2}$.

(c) La classe $[X]$ de X dans $\mathbb{F}_5[X]/(X^2-2)$ a ordre 8. En effet, $[X]^2 = 2$, $[X]^4 = 4 = -1$ et $[X]^8 = (-1)^2 = 1$.

(d) C'est clair que $X^4+1 = (X^2+2)(X^2-2)$ est une décomposition en facteurs irréductibles dans $\mathbb{F}_5[X]$. Le corps de décomposition de X^2-2 est $\mathbb{F}_5[X]/(X^2-2) \simeq \mathbb{F}_{5^2}$, car si $\alpha \in \mathbb{F}_{5^2}$ est une racine de X^2-2, alors $-\alpha \in \mathbb{F}_{5^2}$ est l'autre racine. Le même argument nous dit que le corps de décomposition de X^2+2 est $\mathbb{F}_5[X]/(X^2+2) \simeq \mathbb{F}_{5^2}$. Par la propriété d'unicité de corps finis, il existe un isomorphisme d'anneaux $\phi : \mathbb{F}_5[X]/(X^2+2) \to \mathbb{F}_5[X]/(X^2-2)$. Soit $\beta' \in \mathbb{F}_5[X]/(X^2+2)$ la classe de X. En particulier, β' est une racine de X^2+2, ce qui nous dit que $\beta = \phi(\beta')$ et $-\beta$ sont les racines de X^2+2 dans $\mathbb{F}_5[X]/(X^2-2)$. Comme $\{\pm\alpha, \pm\beta\} \subseteq \mathbb{F}_5[X]/(X^2-2)$, on conclut que $\mathbb{F}_{5^2}$ est le corps de décomposition de X^4+1.

(e) On remarque d'abord que $X^3-2 = (X+2)(X^2-2X-1)$ dans $\mathbb{F}_5[X]$. Comme (X^2-2X-1) est irréductible sur $\mathbb{F}_5$, vu que ce polynôme n'a pas de racines dans $\mathbb{F}_5$, le corps de décomposition de X^3-2 coïncide avec celui de (X^2-2X-1), *i.e.* $\mathbb{F}_5[X]/(X^2-2X-1) \simeq \mathbb{F}_{5^2}$, vu que le corps de décomposition d'un polynôme irréductible de degré 2 coïncide avec le corps de rupture.

Par ailleurs, X^3-2 est irréductible sur $\mathbb{F}_7$, vu que ce polynôme n'a pas de racines dans $\mathbb{F}_7$. Soit $\gamma \in \mathbb{F}_7/(X^3-2)$ la classe de X. Cela nous dit que γ est une racine de X^3-2 dans $\mathbb{F}_7/(X^3-2)$. On voit que $X^3-2 = (X-\gamma)(X-2\gamma)(X+3\gamma)$ dans $\mathbb{F}_7[X]/(X^3-2)$. Cela implique que le corps de décomposition de $X^3-2 \in \mathbb{F}_7[X]$ est $\mathbb{F}_7[X]/(X^3-2) \simeq \mathbb{F}_{7^3}$.

(f) C'est clair que X^4-2 n'a aucune racine dans $\mathbb{F}_5$. Cela implique, si X^4-2 est réductible, la seule factorisation possible (en polynômes unitaires) dans $\mathbb{F}_5[X]$ est de la forme

$$X^4-2 = (X^2+aX+b)(X^2+cX+d),$$

avec $a, b, c, d \in \mathbb{F}_5$. L'égalité précédente équivaut à $a+c=0$, $ac+b+d=0$, $ad+bc=0$ et $bd=-2$. Si l'on remplace c par $-a$, on trouve alors $b+d=a^2$, $a(d-b)=0$ et $bd=-2$. La deuxième condition implique que $a=0$ ou $b=d$. Si $a=0$, alors $b+d=0$, ce qui nous dit que $b^2=-bd=2$. Comme le carré de tout élément de $\mathbb{F}_5$ est dans $\{0, \pm1\}$, $b^2=2$ est impossible. Si $b=d$, on trouve que $b^2=bd=-2$, ce qui est aussi impossible. Par conséquent, $X^4-2 \in \mathbb{F}_5[X]$ est irréductible.

Par contre, X^4-2 est réductible sur $\mathbb{F}_{5^2}$, puisque, si $a \in \bar{\mathbb{F}}_5$ est une racine de X^2-2 (*i.e.* $a \in \mathbb{F}_5[X]/(X^2-2) \simeq \mathbb{F}_{5^2}$), alors $X^4-2 = (X^2-a)(X^2+a)$.

5. Soit p un nombre premier et soit $m, n \in \mathbb{N}^*$. On note $q = p^m$.

(a) Montrer que p^m-1 divise $p^{mn}-1$. En déduire que $X^{p^m-1}-1$ divise $X^{p^{mn}-1}-1$.

(b) En déduire que le corps fini $\mathbb{F}_{p^{mn}}$ admet un unique sous-corps à p^m éléments et que $[\mathbb{F}_{p^{mn}} : \mathbb{F}_{p^m}] = n$.

(c) En déduire que tout corps intermédiaire $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ est un corps à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d.

(d) Donner tous les sous-corps de $\mathbb{F}_{2^3}$ et $\mathbb{F}_{2^6}$.

Solution.

(a) Étant donnés a et b dans un anneau commutatif A et $N \in \mathbb{N}^*$, c'est clair que $a-b$ divise $a^N - b^N$, puisque

$$a^N - b^N = (a-b)\Big(\sum_{i=0}^{N-1} a^{N-i-1}b^i\Big).$$

En particulier, $p^m - 1$ divise $(p^m)^n - 1^n = p^{mn} - 1$. Si l'on écrit $p^{mn} - 1 = k(p^m - 1)$, avec $k \in \mathbb{N}^*$, alors $X^{p^m-1} - 1$ divise $(X^{p^m-1})^k - 1^k = X^{p^{mn}-1} - 1$.

(b) Si l'on fixe $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, on sait que l'unique sous-corps $\mathbb{F}_{p^N}$ de $\bar{\mathbb{F}}_p$ à p^N éléments est l'ensemble de racines de $X^{p^N} - X = X(X^{p^N-1} - 1)$ dans $\bar{\mathbb{F}}_p$. Comme $X^{p^m-1} - 1$ divise $X^{p^{mn}-1} - 1$, on conclut que toutes les racines de $X^{p^m} - X$ dans $\bar{\mathbb{F}}_p$ sont aussi des racines de $X^{p^{mn}} - X$ dans $\bar{\mathbb{F}}_p$. On trouve ainsi un unique sous-corps de $\mathbb{F}_{p^{mn}}$ à p^m éléments. C'est clair que le cardinal d'un $\mathbb{F}_{p^m}$-espace vectoriel de dimension n est $(p^m)^n = p^{mn}$, ce qui nous dit que $[\mathbb{F}_{p^{mn}} : \mathbb{F}_{p^m}] = n$.

(c) L'item précédent nous dit que, si $d|n$, alors un existe un unique corps $K = \mathbb{F}_{p^{dm}}$ à $p^{dm} = q^d$ éléments, formé par les racines de $X^{p^{dm}} - X = X^{q^d} - X$. C'est clair que $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$, puisque $X^q - X$ divise $X^{q^d} - X$, qui divise $X^{q^n} - X$. Réciproquement, soit K un corps tel que $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$. Soit $d = [K : \mathbb{F}_q]$. Comme $\mathbb{F}_q$ a q éléments et K est un $\mathbb{F}_q$-espace vectoriel de dimension d, le cardinal de K est q^d. Finalement, comme $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$, $d = [K : \mathbb{F}_q]$ divise n.

(d) Les sous-corps de $\mathbb{F}_{2^3}$ sont $\mathbb{F}_{2^i}$, avec $i \in \{1,3\}$, tandis que les sous-corps de $\mathbb{F}_{2^6}$ sont $\mathbb{F}_{2^i}$, avec $i \in \{1,2,3,6\}$.

6. Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On considère un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré e.

(a) Montrer qu'un corps de rupture de P sur $\mathbb{F}_q$ est aussi un corps de décomposition de P sur $\mathbb{F}_q$.

(b) Soit $N \in \mathbb{N}^*$. Démontrer que $P|(X^{q^N} - X)$ dans $\mathbb{F}_q$ si et seulement si $e|N$.

(c) Soit $\alpha \in \bar{\mathbb{F}}_p$ une racine de P. Montrer que l'ensemble de racines de P est $\{\alpha^{q^\ell} : \ell \in \{0,\dots,e-1\}\}$, de cardinalité e. Retrouver le résultat du premier item.

Solution.

(a) On trouvera ce résultat comme conséquence du dernier item.

(b) Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré e et soit $N \in \mathbb{N}^*$. On suppose d'abord que $e|N$. Or, $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^e}$, ce qui dit que tout élément de ce corps est une racine du polynôme $X^{q^e} - X$. Si $\alpha \in \mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^e}$ est la classe de X, on voit bien que α est une racine de P mais aussi une racine de $X^{q^e} - X$, par définition de $\mathbb{F}_{q^e}$. Cela implique que $P|X^{q^e} - X$, car P est le polynôme minimal de α. Comme $e|N$, $X^{q^e} - X$ divise $X^{q^N} - X$ et par conséquent $P|(X^{q^N} - X)$ dans $\mathbb{F}_q$. Réciproquement, si $P|(X^{q^N} - X)$ dans $\mathbb{F}_q$, alors P est scindé dans $\mathbb{F}_{q^N}$. Soit $\alpha \in \mathbb{F}_{q^N}$ une racine de P. Alors $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^e} \subseteq \mathbb{F}_{q^N}$ ce qui dit que $e = \deg(P)$ divise $N = [\mathbb{F}_{q^N} : \mathbb{F}_q] = [\mathbb{F}_{q^N} : \mathbb{F}_{q^e}][\mathbb{F}_{q^e} : \mathbb{F}_q] = [\mathbb{F}_{q^N} : \mathbb{F}_{q^e}]e$.

(c) Noter que $\alpha^{q^\ell} = \bar{\sigma}^\ell(\alpha)$, où $\bar{\sigma} : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q$ est l'automorphisme $x \mapsto x^q$. C'est clair que

$$P(\alpha^{q^\ell}) = P(\sigma^\ell(\alpha)) = \sigma^\ell(P(\alpha)) = P(\alpha)^{q^\ell} = 0,$$

ce qui nous dit que tout élément de la forme α^{q^ℓ}, avec $\ell \in \mathbb{N}$, est une racine de P. En outre, soient $\ell', \ell \in \{0, \dots, e-1\}$. Sans perte de généralité, on suppose que $\ell \leq \ell'$. Soit $r = \ell' - \ell$. Alors, $\alpha^{q^\ell} = \alpha^{q^{\ell'}} = (\alpha^{q^r})^{q^\ell}$ équivaut à $(\alpha^{q^r} - \alpha)^{q^\ell} = 0$, *i.e.* $\alpha^{q^r} - \alpha = 0$. Cette dernière égalité est équivalente à $P|(X^{q^r} - X)$ dans $\mathbb{F}_q$, ce qui équivaut à $e|r$ par la propriété démontrée dans l'item précédent, *i.e.* $e|(\ell' - \ell)$. Cela nous dit que les éléments de l'ensemble $\{\alpha^{q^\ell} : \ell \in \{0, \dots, e-1\}\}$ sont tous différents, comme on voulait démontrer. La dernière partie de l'item est une conséquence immédiate.

7. Soit $p \in \mathbb{N}^*$ premier et $n \in \mathbb{N}^*$.

(a) Démontrer que l'ordre du morphisme de Frobenius σ de $\mathbb{F}_{p^n}$ est n.

(b) En utilisant que l'extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ est monogène, montrer que son degré est majoré par n.

(c) En déduire que le groupe des automorphismes de $\mathbb{F}_{p^n}$ est cyclique d'ordre n, engendré par le morphisme de Frobenius σ.

Solution.

(a) C'est clair que $\sigma^n(x) = x^{p^n} = x$, pour tout $x \in \mathbb{F}_{p^n}$. Soit $d \in \mathbb{N}^*$ une période de σ, *i.e.* $\sigma^d(x) = x^{p^d} = x$ pour tout $x \in \mathbb{F}_{p^n}$. Alors le polynôme $X^{p^d} - X$ a au plus p^d racines, ce qui nous dit $d \geq n$.

(b) Il suffit de montrer que $\mathbb{F}_{p^n}$ a au plus n automorphismes de corps. Or, on sait qu'il existe $P \in \mathbb{F}_p[X]$ irréductible de degré n tel que, $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$. Comme tout automorphisme de corps ϕ de $\mathbb{F}_p[X]/(P)$ est l'identité sur $\mathbb{F}_p$ et il préserve l'ensemble de racines de P (dans une clôture algébrique de $\mathbb{F}_p$), un endomorphisme de corps de $\mathbb{F}_p[X]/(P)$ est déterminé de façon unique par l'image de la classe $[X]$ de X dans $\mathbb{F}_p[X]/(P)$. Comme $\phi([X])$ est aussi une racine de P, on voit que $\mathbb{F}_{p^n}$ a au plus n automorphismes de corps.

(c) Le dernier item est une conséquence directe.

8. Soient p un nombre premier et $n, m \in \mathbb{N}^*$. On note $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ l'automorphisme de Frobenius $x \mapsto x^p$.

(a) Montrer que tout polynôme irréductible de $\mathbb{F}_{p^n}[X]$ est à racines simples dans son corps de décomposition.

(b) Montrer qu'il y a soit zéro, soit n morphismes de corps de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^m}$.

(c) Montrer que l'ensemble des éléments de $\mathbb{F}_{p^n}$ laissés fixes par l'automorphisme σ^ℓ (avec $\ell \in \mathbb{N}^*$) est le sous-corps de $\mathbb{F}_{p^n}$ à p^d éléments avec $d = \mathsf{PGCD}(n, \ell)$.

Solution.

(a) Il s'agit d'une conséquence du dernier item de l'exercice **6**.

(b) S'il existe au moins un morphisme de corps φ de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^m}$, alors son image est le seul sous-corps F de $\mathbb{F}_{p^m}$ à p^n éléments. Comme φ est injectif, il induit un isomorphisme entre $\mathbb{F}_{p^n}$ et F. On affirme que l'application

$$\mathsf{Aut}_{\text{corps}}(\mathbb{F}_{p^n}) \to \mathsf{Mor}_{\text{corps}}(\mathbb{F}_{p^n}, \mathbb{F}_{p^m})$$

donnée par $\psi \mapsto \varphi \circ \psi$ est une bijection. Elle est clairement injective, puisque φ est injectif. En outre, si φ' est un morphisme de corps de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^m}$, on voit que $\mathsf{Img}(\varphi') = F = \mathsf{Img}(\varphi)$, le seul sous-corps F de $\mathbb{F}_{p^m}$ à p^n éléments, et $\psi = \varphi^{-1} \circ \varphi'$ est un automorphisme de $\mathbb{F}_{p^n}$ tel que $\varphi' = \varphi \circ \psi$. Le résultat est alors une conséquence du résultat du cours qui dit que la cardinalité de $\mathsf{Aut}_{\text{corps}}(\mathbb{F}_{p^n})$ est n. Ce dernier résultat est aussi une conséquence de l'exercice **7**.

(c) C'est clair que l'ensemble d'éléments laissés fixes par un automorphisme de corps est un sous-corps. On note F le sous-corps de $\mathbb{F}_{p^n}$ laissé fixe par l'automorphisme σ^ℓ. On remarque que l'égalité $x^{p^n} = x$ pour tout $x \in \mathbb{F}_{p^n}$ nous dit que $x^{p^{cn}} = x$, pour tout $c \in \mathbb{Z}$. De même, comme $x^{p^\ell} = x$ pour tout $x \in F$, alors $x^{p^{c\ell}} = x$, pour tout $c \in \mathbb{Z}$. Soit $d = \mathsf{PGCD}(n, \ell)$. On peut écrire $d = an + b\ell$, avec $a, b \in \mathbb{Z}$, ce qui nous dit que

$$x^{p^d} = (x^{p^{an}})^{p^{b\ell}} = x^{p^{b\ell}} = x,$$

pour tout $x \in F$. En conséquence, $F \subseteq \mathbb{F}_{p^d}$. Par ailleurs, soit $x \in \mathbb{F}_{p^d}$, $x^{p^d} = x$. Si $\ell' = \ell/d \in \mathbb{N}^*$, on voit que $\sigma^\ell(x) = (\sigma^d)^{\ell'}(x) = x$, ce qui nous dit que $x \in F$ et en conséquence $\mathbb{F}_{p^d} \subseteq F$.

9. Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On considère un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré $n > 1$.

(a) Soit $d > 1$ un diviseur de n. Montrer que $\mathbb{F}_{q^n}$ est un corps de décomposition de P sur $\mathbb{F}_{q^d}$. En déduire que P n'est pas irréductible sur $\mathbb{F}_{q^d}$.

(b) Soit Q un facteur irréductible de P dans $\mathbb{F}_{q^d}[X]$. Montrer qu'un corps de rupture de Q sur $\mathbb{F}_{q^d}$ est un corps de décomposition de P sur $\mathbb{F}_q$. En déduire que P est un produit de d facteurs irréductibles de degré n/d dans $\mathbb{F}_{q^d}[X]$.

(c) Soit $\ell \in \mathbb{N}^*$. Montrer que P est irréductible sur $\mathbb{F}_{q^\ell}$ si et seulement si ℓ et n sont premiers entre eux.

Solution.

(a) La première partie de l'item est une conséquence immédiate de l'exercice **6**, puisque si P est un polynôme irréductible de degré n, $\mathbb{F}_{q^n}$ est en fait un corps de décomposition de P sur $\mathbb{F}_q$. La deuxième partie est immédiate. En effet, si P est irréductible sur $\mathbb{F}_{q^d}$, alors $\mathbb{F}_{q^d}[X]/(P)$ est un corps de rupture de P, et il est donc inclus dans $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^n}$. Par ailleurs, $\mathbb{F}_{q^d}[X]/(P)$ a cardinal $q^{dn} > q^n$, ce qui est absurde.

(b) La première partie de l'item est une conséquence du résultat dans le deuxième item de l'exercice **6**. En effet, si $Q \in \mathbb{F}_{q^d}[X]$ est un facteur irréductible de P, un corps de rupture de Q sur $\mathbb{F}_{q^d}$ est donné par $\mathbb{F}_{q^d}(\alpha)$, avec $\alpha \in \mathbb{F}_{q^n}$ racine de Q, et donc *a fortiori* racine de P. Le résultat suit de

$$\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^d}(\alpha) \subseteq \mathbb{F}_{q^n}.$$

Cela nous dit que $[\mathbb{F}_{q^n} : \mathbb{F}_{q^d}] = \deg Q$. Par conséquent,

$$\deg P = n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^d}][\mathbb{F}_{q^d} : \mathbb{F}_q] = d \deg Q.$$

(c) Soit $d = \mathsf{PGCD}(n, \ell)$. On a déjà démontré que si $d > 1$, P est réductible sur $\mathbb{F}_{q^d}$, donc *a fortiori* sur $\mathbb{F}_{q^\ell} \supseteq \mathbb{F}_{q^d}$. Il reste à montrer que $d = 1$, P est irréductible sur $\mathbb{F}_{q^\ell}$. Or, P est irréductible sur $\mathbb{F}_q$. Si $\alpha \in \mathbb{F}_{q^n}$ est une racine de P, alors $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Le compositum

$E = \mathbb{F}_{q^n}.\mathbb{F}_{q^\ell} = \mathbb{F}_{q^\ell}(\alpha)$ (dans une clôture algébrique $\bar{\mathbb{F}}_q$) satisfait alors que $[E : \mathbb{F}_q]$ est divisible par $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ et par $[\mathbb{F}_{q^\ell} : \mathbb{F}_q] = \ell$. Comme ℓ et n sont premiers entre eux, $[E : \mathbb{F}_q]$ est divisible par $n\ell$. En outre, comme le degré de P est n et α est une racine de P, $[E : \mathbb{F}_{q^\ell}] \leq n$. On conclut alors que $[E : \mathbb{F}_q] = n\ell$, et en conséquence $[E : \mathbb{F}_{q^\ell}] = n$. Cela implique que P est le polynôme minimal de α sur $\mathbb{F}_{q^\ell}$ et en particulier il P est irréductible sur $\mathbb{F}_{q^\ell}$.

10. Soit $p \in \mathbb{N}^*$ un nombre premier. Pour tout $i \in \mathbb{N}^*$, on choisit un morphisme de corps $f_i : \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{(i+1)!}}$. On pose alors $K = \cup_{i \in \mathbb{N}^*} \mathbb{F}_{p^{i!}}$ où chaque $\mathbb{F}_{p^{i!}}$ s'identifie à son image par $f_{j-1} \circ \cdots \circ f_i$ dans $\mathbb{F}_{p^{j!}}$ pour tout $j > i$. Montrer que K est une clôture algébrique de $\mathbb{F}_p$.

Solution. Soit $P \in K[X]$. Alors, il existe $i \in \mathbb{N}^*$ tel que $P \in \mathbb{F}_{p^{i!}}[X]$. On sait que le corps de décomposition L de P sur $\mathbb{F}_{p^{i!}}$ est une extension finie de $\mathbb{F}_{p^{i!}}$, et donc un corps fini. On suppose que $L = \mathbb{F}_{p^N}$. Cela nous dit que, à isomorphisme près, on peut considérer, que $L \subseteq \mathbb{F}_{p^{(N+i)!}} \subseteq K$. En conséquence, toutes les racines de P appartiennent à K, ce qui implique que K est algébriquement clos. En outre, comme f_i est une extension algébrique et la composition d'extensions algébriques est algébrique, on voit que $K \supseteq \mathbb{F}_p$ est algébrique.

⋆ **11.** On note $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ la fonction de Möbius, définie de la façon suivante :

(i) $\mu(n) = 0$ s'il existe un premier $p \in \mathbb{N}^*$ tel que $p^2 | n$,

(ii) $\mu(n) = (-1)^\ell$ si $n = \prod_{i=1}^{\ell} p_i$, avec $\ell \in \mathbb{N}$ et premiers $p_i \in \mathbb{N}^*$ tels que $p_i \neq p_j$ si $i \neq j$.

Noter que $\mu(1) = 1$.

Soit $M(\mathbb{N}^*, \mathbb{C})$ l'ensemble des applications de $\mathbb{N}^*$ dans $\mathbb{C}$. On définit la somme $(f + g)(n) = f(n) + g(n)$ et le produit

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d),$$

pour tout $n \in \mathbb{N}^*$. Vérifier que $M(\mathbb{N}^*, \mathbb{C})$ est une anneau commutatif dont l'unité est l'application $\delta : \mathbb{N}^* \to \mathbb{C}$ donnée par $\delta(n) = 0$ si $n \neq 1$ et $\delta(1) = 1$. On admettra l'identité suivante, appelée **formule d'inversion de Möbius** : $\mu * \phi_1 = \delta$, où $\phi_1 \in M(\mathbb{N}^*, \mathbb{C})$ est l'application constante de valeur 1.

(*a*) Soit $\exp_q \in M(\mathbb{N}^*, \mathbb{C})$ l'application $n \mapsto q^n$. Montrer que le nombre de polynômes irréductibles unitaires de degré n dans $\mathbb{F}_q[X]$ est égal à $(\mu * \exp_q)(n)/n$

(*b*) Retrouver ainsi le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$ et de degré 4 sur $\mathbb{F}_3$.

Solution.

(*a*) On remarque d'abord que

$$X^{q^n} - X = \prod_{P \in \mathscr{P}_n} P \tag{5}$$

où $\mathscr{P}_n$ est l'ensemble fini formé de tous les polynômes unitaires irréductibles dans $\mathbb{F}_q[X]$ de degré d avec $d|n$. En effet, on a montré dans le premier item de l'exercice **6** que, si P est un polynôme unitaire irréductible dans $\mathbb{F}_q[X]$ de degré d, P divise $X^{q^n} - X$ si et seulement si $d|n$. On définit

$$M_d(q) = \#\{P \in \mathbb{F}_q[X] : \ P \text{ unitaires irréductibles de degré } d\ \}.$$

Alors, si l'on regarde le degré des polynômes dans (5) on trouve que

$$q^n = \sum_{d|n} d M_d(q). \tag{6}$$

Soit $P_q \in M(\mathbb{N}^*, \mathbb{C})$ défini par $d \mapsto d M_d(q)$. Alors, (6) nous dit que $\mathsf{exp}_q = \phi_1 * P_q$. La formule d'inversion de Möbius implique alors que $P_q = \mu * \mathsf{exp}_q$, et en particulier

$$M_n(q) = \frac{(\mu * \mathsf{exp}_q)(n)}{n} = \frac{\sum_{d|n} q^{n/d} \mu(d)}{n},$$

pour tout $n \in \mathbb{N}^*$.

(b) La formule précédente nous dit que $M_4(3) = 18$ et $M_3(7) = 112$.

12. (a) Calculer les polynômes cyclotomiques Φ_{14} et Φ_{15}.

(b) Soient p un nombre premier et α un entier naturel non nul. Calculer Φ_p et montrer que $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$.

Solution.

(a) On sait que pour tout p premier positif, $\Phi_p(X) = \sum_{\ell=0}^{p-1} X^\ell$, $\Phi_{2n}(X) = \Phi_n(-X)$ si $n > 1$ est impair, et $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ si $n \in \mathbb{N}^*$ n'est pas divisible par le premier p. On remarque que $p = 2$ est possible pour la dernière égalité. En plus, on note que $\Phi_{2n}(X) = \Phi_n(-X)$ n'est pas vérifié si $n = 1$, car $\Phi_2(X) = X + 1 \neq -X - 1 = \Phi_1(-X)$. On va prouver l'identité $\Phi_p(X) = \sum_{\ell=0}^{p-1} X^\ell$ dans l'item suivant, mais on va démontrer les autres égalités dans cet item.

On rappelle que les polynômes cyclotomiques sont définis (par récurrence) à partir de

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(X)},$$

pour tout $n \in \mathbb{N}^*$ tel que $n > 1$, et $\Phi_1(X) = X - 1$. Par rapport à la preuve de la propriété $\Phi_{2n}(X) = \Phi_n(-X)$ si $n > 1$ est impair, on procède par récurrence. D'abord, par définition on a que

$$\begin{aligned} \Phi_6(X) &= \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = \frac{X^6 - 1}{(X^2-1)(X^2+X+1)} \\ &= \frac{X^4 + X^2 + 1}{X^2 + X + 1} = X^2 - X + 1, \end{aligned}$$

ce qui implique que $\Phi_6(X) = X^2 - X + 1 = (-X)^2 + (-X) + 1 = \Phi_3(-X)$, comme on voulait démontrer. Soit $n > 3$ impair. On suppose que $\Phi_{2m}(X) = \Phi_m(-X)$, pour tout

$1 < m < n$ impair. On va démontrer que $\Phi_{2n}(X) = \Phi_n(-X)$ est vérifié. Or, on voit bien que

$$\{d \in \mathbb{N}^* | d \text{ divise } 2n\} = \{\ell \in \mathbb{N}^* | \ell \text{ divise } n\} \cup \{2\ell | \ell \in \mathbb{N}^* \text{ et } \ell \text{ divise } n\}.$$

Soient $A = \{\ell \in \mathbb{N}^* | \ell \text{ divise } n\}$, $A' = A \setminus \{n\}$ et $A'' = A' \setminus \{1\}$. Alors,

$$\begin{aligned}\Phi_{2n}(X) &= \frac{X^{2n}-1}{\prod_{\ell\in A}\Phi_\ell(X)\prod_{\ell'\in A'}\Phi_{2\ell'}(X)} = \frac{(X^n-1)(X^n+1)}{\prod_{\ell\in A}\Phi_\ell(X)\prod_{\ell'\in A'}\Phi_{2\ell'}(X)}\\ &= \frac{(X^n+1)}{\prod_{\ell'\in A'}\Phi_{2\ell'}(X)} = \frac{-((-X)^n-1)}{-((-X)-1)\prod_{\ell'\in A''}\Phi_{\ell'}(-X)}\\ &= \frac{((-X)^n-1)}{((-X)-1)\prod_{\ell'\in A''}\Phi_{\ell'}(-X)} = \Phi_n(-X),\end{aligned}$$

où l'on a utilisé dans la troisième égalité que $X^n - 1 = \prod_{\ell\in A}\Phi_d(X)$, par définition des polynômes cyclotomiques, et la récurrence dans la quatrième égalité.

Pour démontrer que $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ si $n \in \mathbb{N}^*$ n'est pas divisible par le premier p, on va procéder par récurrence aussi. L'argument est presque identique. L'égalité est vérifiée pour $n = 1$, car $\Phi_p(X) = (X^p - 1)/(X - 1) = \Phi_1(X^p)/\Phi_1(X)$. On suppose que $\Phi_{pm}(X) = \Phi_m(X^p)/\Phi_m(X)$, pour tout m tel que $1 \leq m < n$ et m ne soit pas divisible par p. On va démontrer que $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ est vérifié. Comme dans le cas précédent, on voit bien que

$$\{d \in \mathbb{N}^* | d \text{ divise } pn\} = \{\ell \in \mathbb{N}^* | \ell \text{ divise } n\} \cup \{p\ell | \ell \in \mathbb{N}^* \text{ et } \ell \text{ divise } n\}.$$

Soient $A = \{\ell \in \mathbb{N}^* | \ell \text{ divise } n\}$ et $A' = A \setminus \{n\}$. Alors,

$$\begin{aligned}\Phi_{pn}(X) &= \frac{X^{pn}-1}{\prod_{\ell\in A}\Phi_\ell(X)\prod_{\ell'\in A'}\Phi_{p\ell'}(X)} = \frac{((X^p)^n-1)}{\prod_{\ell\in A}\Phi_\ell(X)\prod_{\ell'\in A'}\Phi_{p\ell'}(X)}\\ &= \frac{((X^p)^n-1)}{(X^n-1)\prod_{\ell'\in A'}\Phi_{p\ell'}(X)} = \frac{((X^p)^n-1)\prod_{\ell'\in A'}\Phi_{\ell'}(X)}{(X^n-1)\prod_{\ell'\in A'}\Phi_{\ell'}(X^p)}\\ &= \frac{\frac{((X^p)^n-1)}{\prod_{\ell'\in A'}\Phi_{\ell'}(X^p)}}{\frac{(X^n-1)}{\prod_{\ell'\in A'}\Phi_{\ell'}(X)}} = \frac{\Phi_n(X^p)}{\Phi_n(X)},\end{aligned}$$

où l'on a utilisé dans la troisième égalité que $X^n - 1 = \prod_{\ell\in A}\Phi_d(X)$, par définition des polynômes cyclotomiques, la récurrence dans la quatrième égalité et la définition des polynômes cyclotomiques dans la dernière égalité.

Cela implique que $\Phi_{14}(X) = \Phi_7(-X) = \sum_{\ell=0}^{6}(-X)^\ell$ et

$$\Phi_{15}(X) = \Phi_5(X^3)/\Phi_5(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

(*b*) On rappelle que les polynômes cyclotomiques sont définis à partir de

$$\Phi_n(X) = \frac{X^n-1}{\prod\limits_{\substack{d|n\\ d<n}}\Phi_d(X)},$$

pour tout $n \in \mathbb{N}^*$ tel que $n > 1$, et $\Phi_1(X) = X - 1$. C'est clair alors que $\Phi_p(X) = (X^p - 1)/(X - 1) = \sum_{\ell=0}^{p-1} X^\ell$.

On va maintenant montrer que $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$ pour tout $\alpha \in \mathbb{N}^*$. Si $\alpha = 1$, il n'y a rien à démontrer. Si $\alpha \in \mathbb{N}^*$,

$$\begin{aligned}\Phi_{p^{\alpha+1}}(X) &= \frac{X^{p^{\alpha+1}}-1}{\prod_{\ell=0}^{\alpha}\Phi_{p^\ell}(X)} = \frac{\left((X^{p^\alpha})^p - 1^p\right)}{\prod_{\ell=0}^{\alpha}\Phi_{p^\ell}(X)} = \frac{(X^{p^\alpha}-1)(\sum_{\ell=0}^{p-1}(X^{p^\alpha})^\ell)}{\prod_{\ell=0}^{\alpha}\Phi_{p^\ell}(X)}\\ &= \sum_{\ell=0}^{p-1}(X^{p^\alpha})^\ell = \Phi_p(X^{p^\alpha}).\end{aligned} \tag{7}$$

On laisse à la lectrice/au lecteur la preuve (aussi par récurrence) de l'identité (plus générale) $\Phi_{pn}(X) = \Phi_n(X^p)$, pour tout p premier positif et tout $n > 1$ divisible par p.

⋆ **13.** Soit K une extension finie de $\mathbb{Q}$. Montrer qu'il n'y a qu'un nombre fini de racines de l'unité dans K.

Solution. Si ζ_n est une racine primitive de l'unité d'ordre n, $\Phi_n = \mathsf{Irr}(\zeta_n, \mathbb{Q})$. On sait que $\deg \Phi_n = \varphi(n)$, où φ est la fonction d'Euler. Si K contient un nombre infini de racines de l'unité, alors pour tout $n \in \mathbb{N}^*$ il existe $N \in \mathbb{N}^*$ tel que une racine primitive de l'unité ζ_N d'ordre N appartient à K. En particulier, $[K : \mathbb{Q}] \in \mathbb{N}^*$ est divisible par $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N)$. Comme $\varphi(N)$ tend vers $+\infty$ quand $N \to +\infty$, on trouve un absurde.

⋆ **14.** Soit p la caractéristique du corps fini $\mathbb{F}_q$.

(*a*) Soit $n \in \mathbb{N}^*$ tel que $\mathsf{PGCD}(q, n) = 1$. Montrer que le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ si et seulement si q est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(*b*) Pour les entiers $n \in \{3, 4, 5, 6, 7, 8, 12\}$, discuter selon les valeurs de q de l'irréductibilité sur $\mathbb{F}_q$ de la réduction modulo p du polynôme cyclotomique Φ_n.

(*c*) Factoriser Φ_{14} sur $\mathbb{F}_2$.

Solution.

(*a*) On sait que les racines de $\Phi_n \in \mathbb{Q}[X]$ sont les $\varphi(n)$ racines primitives de l'unité d'ordre n, où φ est la fonction d'Euler. Soit $\alpha \in \bar{\mathbb{F}}_q$ une racine primitive de l'unité d'ordre n (*i.e.* une racine de $\bar{\Phi}_n \in \mathbb{F}_q[X]$). Alors, $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^m}$, avec $m \in \mathbb{N}$. En particulier, $\mathbb{F}_q(\alpha)^*$ est un groupe cyclique (fini) et $n | q^m - 1$, vu que $X^n - 1$ divise $X^{q^m} - 1$ (puisque $\alpha^n - 1 = 0$). En outre, on sait que le polynôme minimal de α sur $\mathbb{F}_q$ est précisément

$$P = \prod_{\ell=0}^{m-1} (X - \alpha^{q^\ell}).$$

C'est clair que $P | \bar{\Phi}_n$, puisque $\bar{\Phi}_n(\alpha) = 0$. Alors, $\bar{\Phi}_n$ est irréductible si et seulement si $\bar{\Phi}_n = P$. Cela équivaut à dire que l'ensemble $\{\alpha^{q^\ell} : \ell \in \{0, \dots, m-1\}\}$ coïncide avec l'ensemble de racines de $\bar{\Phi}_n$. Comme les racines de $\bar{\Phi}_n$ sont donnés par $\{\alpha^a : a \in \{1, \dots, n-1\}$ et $\mathsf{PGCD}(a, n) = 1\}$, on voit que cette condition équivaut à $\{q^\ell : \ell \in \{0, \dots, m-1\}\} = (\mathbb{Z}/n\mathbb{Z})^\times$.

(*b*) Il s'agit d'une application directe de l'item précédent.

(*c*) C'est facile à vérifier que $\Phi_{14}(X) = \Phi_7(-X) = \Phi_7(X) = (X^3 + X^2 + 1)(X^3 + X + 1)$. En plus, comme les polynômes $X^3 + X^2 + 1, X^3 + X + 1 \in \mathbb{F}_2$ n'ont pas de racines dans $\mathbb{F}_2$, ils sont irréductibles.

⋆ **15.** Soient p un nombre premier et $n \in \mathbb{N}^*$ tel que $n = p^\alpha m$ avec $\alpha \in \mathbb{N}^*$ et $p \nmid m$. Soit Φ_n le n-ème polynôme cyclotomique.

(*a*) Montrer que dans $\mathbb{F}_p[X]$, on a $\Phi_n = (\Phi_m)^{p^{\alpha}-1}$.

(*b*) Montrer que Φ_n est réductible sur $\mathbb{F}_p$ sauf éventuellement si $(p, \alpha) = (2, 1)$.

Solution.

(a) On remarque que, si p est un nombre premier positif, $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ si n n'est pas divisible par p, et $\Phi_{pn}(X) = \Phi_n(X^p)$ si $p|n$. La preuve de ces propriétés suit facilement de la définition. Cela implique que, si $n = p^\alpha m$ avec $\alpha \in \mathbb{N}^*$ et $p \nmid m$,

$$\Phi_n(X) = \frac{\Phi_m(X^{p^\alpha})}{\Phi_m(X)} = \frac{\Phi_m(X)^{p^\alpha}}{\Phi_m(X)} = \Phi_m(X)^{p^\alpha - 1}.$$

(b) C'est clair que $p^\alpha - 1 > 1$ si $(p, \alpha) \neq (2, 1)$. Cela implique que Φ_n est réductible sur $\mathbb{F}_p$ dans ce cas.