Feuille d'exercices 3

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

Corps finis

1. Généralités

Exercice 1.1. — *Soit K un corps fini de cardinal q.*

1. *Montrer que tout élément de K est la somme de deux carrés dans K.*
2. *Soit G le groupe des matrices de taille (n, n) inversibles à coefficients dans K. Quel est l'ordre de G ?*
3. *Démontrer que l'on a*
$$\sum_{x \in K^*} x = 0 \quad si \quad q > 2 \quad et \quad \prod_{x \in K^*} x = -1.$$
4. *Donner une condition nécessaire et suffisante pour que tout élément de K^*, autre que 1, soit un générateur de K^*.*

Exercice 1.2. — *Soit p un nombre premier.*

1. *Montrer que l'on a $(p-1)! \equiv -1 \mod p$ (théorème de Wilson).*
2. *Si p est impair, en déduire la congruence*
$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p.$$
En particulier, si l'on a $p = 4m + 1$ où $m \in \mathbb{Z}$, alors -1 est un carré dans $\mathbb{F}_p$ et $(2m)!$ est une racine carrée de -1 modulo p.

2. Premiers exemples

Exercice 2.3. — *Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :*
(i) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/(X^2 + X + 1)$;
(ii) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/(X^3 + X + 1)$;
(iii) $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(X^4 + X + 1)$; *donner dans cet isomorphisme l'image de* $\mathbf{F}_4 \subset \mathbf{F}_{16}$ *et en déduire* $\mathbf{F}_{16} \simeq \mathbf{F}_2[X, Y]/(Y^2 + Y + 1, X^2 + X + Y)$.
(iv) $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2 + X - 1)$.

Exercice 2.4. — *On dira d'une extension de corps $k \subset \bar{k}$ qu'elle est une clôture algébrique si :*
(a) tout élément $x \in \bar{k}$ est algébrique sur k, i.e. il existe une polynôme $P \in k[X]$ tel que $P(x) = 0$;
(b) tout polynôme $P \in \bar{k}[X]$ est totalement décomposé dans $\bar{k}$.
Pour tout n divisant n' on fixe une injection $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{n'}}$. Montrez alors que $\bar{\mathbb{F}}_p := \bigcup_{n>1} \mathbb{F}_{p^{n!}}$ est une cloture algébrique de $\mathbf{F}_p$.

Exercice 2.5. — *1. Donner tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbb{F}_2$.*
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 $\mathbb{F}_4$.
4. Expliciter les polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

Exercice 2.6. — *1. Le nombre 2 est-il un carré dans $\mathbb{F}_5$? Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_5$.*

2. *Soit $P(X) \in \mathbb{F}_5[X]$ un polynôme unitaire irréductible de degré deux. Montrer que le quotient*
$$\frac{\mathbb{F}_5[X]}{(P(X))}$$
est isomorphe au corps $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.
3. *On note α une racine de X^2+X+1 dans $\mathbb{F}_{25}$. Montrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire $a\alpha+b$ avec a et b dans $\mathbb{F}_5$.*
4. *Soit $P = X^5 - X + 1$. Montrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $P(\beta) \neq 0$. En déduire que P est irréductible sur $\mathbb{F}_5$. P est-il irréductible sur $\mathbb{Q}$?*

Exercice 2.7. — *On considère le polynôme $Q(X) = X^9 - X + 1$ sur $\mathbb{F}_3$.*
(a) Montrer que le polynôme Q n'a pas de racines dans $\mathbb{F}_3, \mathbb{F}_9$.
(b) Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3-X-1)}$.
(c) Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ du polynôme $X^3 - X - 1$ est une racine du polynôme Q.
(d) Déterminer toutes le racines de Q dans $\mathbb{F}_{27}$.
(e) Factoriser le polynôme Q sur le corps $\mathbb{F}_3$.

Exercice 2.8. — *A quelle condition un polynôme P à coefficients dans $\mathbb{F}_p$ de degré n est-il irréductible sur $\mathbb{F}_{p^m}$? Dans le cas où P est irréductible sur $\mathbb{F}_p$, on donnera des précisions sur les degrés des facteurs irréductibles de P sur $\mathbb{F}_{p^m}$. En particulier pour $n = 5$, donner m minimal tel que tout polynôme de degré 5 à coefficients dans $\mathbb{F}_p$ soit totalement décomposé (resp. possède une racine) sur $\mathbb{F}_{p^m}$.*

3. Théorie de Galois

Exercice 3.9. — ***(Automorphisme de Frobenius)*** *Soit K un corps fini de cardinal q et de caractéristique p. Posons $q = p^n$ et notons G le groupe des automorphismes de K. Soit $\sigma : K \to K$ l'application définie pour tout $x \in K$ par $\sigma(x) = x^p$.*

1. *Montrer que σ appartient à G. On l'appelle l'automorphisme de Frobenius de K.*
2. *Montrer σ est un élément d'ordre n dans G.*
3. *Montrer que G est cyclique d'ordre n engendré par σ.*

Exercice 3.10. — *On se propose de prouver l'énoncé suivant : **Théorème** Soient p un nombre premier et F un polynôme de $\mathbb{F}_p[X]$ de degré $n \geq 1$ tel que $F(0) \neq 0$. Il existe un entier non nul $m < p^n$ tel que F divise $X^m - 1$.*

1. *En utilisant le théorème de division euclidienne, montrer qu'il existe un entier k tel que F divise $X^k - 1$ avec $1 \leq k \leq p^n$.*
2. *Montrer que l'on peut choisir $k < p^n$.*
3. *Trouver l'entier non nul $m < 8$ tel que $X^3 + X + 1$ divise $X^m - 1$ dans $\mathbb{F}_2[X]$.*

4. Polynômes

Exercice 4.11. — ***(Polynômes cyclotomiques)*** *: Soient ℓ et p deux nombres premiers distincts. On note*
$$\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{F}_\ell[X],$$
le p-ième polynôme cyclotomique à coefficients dans $\mathbb{F}_\ell$.

1. *Soit F un facteur irréductible de Φ_p dans $\mathbb{F}_\ell[X]$. Montrer que le degré de F est l'ordre de la classe de ℓ modulo p.*
2. *En déduire que Φ_p est irréductible sur $\mathbb{F}_\ell$ si et seulement si la classe de ℓ modulo p est un générateur de $\mathbb{F}_p^*$.*
3. *Quels sont les nombres premiers ℓ pour lesquels Φ_5 soit irréductible sur $\mathbb{F}_\ell$?*

Exercice 4.12. — *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 que Φ_n est réductible modulo tout nombre premier.

Exercice 4.13. — ***(Critère d'irréductibilité sur $\mathbb{F}_p$)*** *: Soient p un nombre premier et $F \in \mathbb{F}_p[X]$ un polynôme de degré $n \geq 1$.*

1. Montrer que les deux conditions suivantes sont équivalentes :

(a) F est irréductible sur $\mathbb{F}_p$.

(b) F divise $X^{p^n}-X$ et l'on a $F \wedge \left(X^{p^{\frac{n}{q}}}-X\right)=1$ pour tout diviseur premier q de n.

2. En déduire que le polynôme $X^7+X+1 \in \mathbb{F}_2[X]$ est irréductible sur $\mathbb{F}_2$.

Exercice 4.14. — *Soit $P(X)=X^4-10X^3+21X^2-10X+11$*
(a) Décomposer P en facteurs irréductibles modulo 2,3,5.
(b) Montrer que P est irréductible sur $\mathbb{Q}$.

Exercice 4.15. — *Soient p et l deux nombres premiers impairs. On suppose que p engendre $(\mathbb{Z}/l\mathbb{Z})^*$ et que $l \equiv 2 \mod 3$. On note $P(X)=X^{l+1}-X+p$. On veut montrer que P est irréductible sur $\mathbb{Z}$.*

1. Montrer que P n'a pas de racine rationnelle.

2. On raisonne par l'absurde et on suppose $P=QR$ avec $Q,R \in \mathbb{Z}[X]$ unitaire et de degré au moins 2. Montrer que $\bar{P}=X(X-1)\bar{\Phi}_l$ est la décomposition en polynômes irréductibles de $\bar{P}$ sur $\mathbf{F}_p$; en déduire alors que $\bar{Q}=\bar{\Phi}_l$ et $\bar{R}=X(X-1)$.

3. En passant modulo 2, en déduire une contradiction. Comme exemple on propose le polynôme $X^{72}-X+47$.

Exercice 4.16. — *Soient ℓ et p deux nombres premiers. Quel est le nombre de polynômes unitaires irréductibles de degré ℓ dans $\mathbb{F}_p[X]$?*

5. Applications

Exercice 5.17. — *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 5.18. — ***(Sommes de puissances)*** *: soient K un corps fini de cardinal q et n un entier naturel. On pose*

$$S_n=\sum_{x\in K^*} x^n.$$

Montrer que l'on a $S_n=-1$ si $q-1$ divise n et que $S_n=0$ sinon.

Exercice 5.19. — ***(Théorème de Wolstenholme)*** *Soit p un nombre premier ≥ 5. On pose*

$$S=1+\frac{1}{2}+\cdots+\frac{1}{p-1}.$$

Posons $S = \frac{N}{D}$ où N et D sont deux entiers premiers entre eux. L'objectif de cet exercice est de démontrer le résultat suivant établit par Wolstenholme en 1862 : ***Théorème*** *L'entier N est divisible par p^2.*

Remarquons que si l'on écrit S sous la forme $\frac{u}{(p-1)!}$, cet énoncé est équivalent au fait que p^2 divise u, car p ne divise pas $(p-1)!$.

1. *En regroupant les termes de S convenablement deux à deux, montrer que p divise N.*
2. *Montrer que $\frac{N}{p}$ modulo p est égal, à un facteur près, à la somme des carrés de $\mathbb{F}_p^*$.*
3. *En déduire le résultat.*

Exercice 5.20. — ***(Les coefficients binomiaux C_{2p-1}^{p-1})*** *On démontre ici le résultat suivant :* ***Théorème*** *Pour tout nombre premier $p \geq 5$, on a la congruence*

$$C_{2p-1}^{p-1} \equiv 1 \mod p^3.$$

Dans cet énoncé C_{2p-1}^{p-1} désigne le coefficient binomial usuel i.e. le nombre de parties à $p-1$ éléments dans un ensemble de cardinal $2p-1$. Posons

$$F = \prod_{i=1}^{p-1}(X-i) \in \mathbb{Z}[X],$$

et pour tout i tel que $1 \leq i \leq p-1$, notons $A_i \in \mathbb{Z}$ la i-ème fonction symétrique élémentaire des racines de F.

1. *Démontrer l'égalité*
$$p^{p-2} - A_1 p^{p-3} + A_2 p^{p-4} + \cdots - A_{p-2} = 0.$$
2. *En déduire que l'on a*
$$\prod_{i=1}^{p-1}(p+i) = 2\big(p^{p-1} + A_2 p^{p-3} + \cdots + A_{p-3}p^2\big) + A_{p-1}.$$
3. *En déduire le théorème. Signalons que l'on ne connaît pas d'entiers n non premiers vérifiant la congruence $C_{2n-1}^{n-1} \equiv 1 \mod n^3$. On conjecture en fait qu'il n'y en a pas. Si tel était le cas, pour tout $n \geq 5$, on aurait l'équivalence*
$$C_{2n-1}^{n-1} \equiv 1 \mod n^3 \iff n \text{ est premier ?}$$
4. *Retrouver le théorème de Wolstenholme en utilisant directement l'égalité démontrée dans la première question.*

Exercice 5.21. — ***(Algorithme de Berlekamp)*** *Soient K un corps fini de cardinal q et $P \in K[X]$ un polynôme unitaire de degré $n \geq 1$ tel que $P \wedge P' = 1$ i.e. P n'est pas divisible par le carré d'un polynôme irréductible. Soit*

$$P = P_1 \cdots P_r \quad (r \geq 1)$$

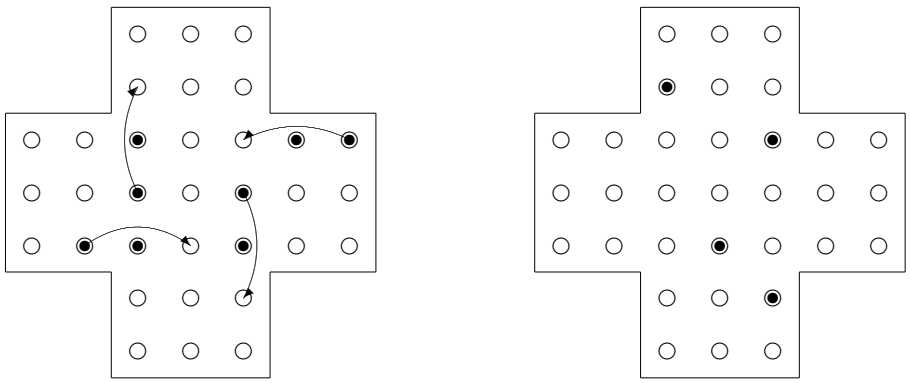
la décomposition de P en produit de polynômes irréductibles unitaires $P_i \in K[X]$ (deux à deux distincts). On décrit ici l'algorithme de Berlekamp qui permet, si q n'est pas trop grand, de déterminer les P_i. On considère pour cela la K-algèbre

$$A = K[X]/(P).$$

1. *Montrer que l'application $f : A \to A$ définie pour tout $x \in A$ par $f(x) = x^q$ est un endomorphisme du K-espace vectoriel A.*
2. *Montrer que r est la dimension du sous-espace vectoriel $\mathrm{Ker}(f - \mathrm{Id})$ (où Id désigne l'identité de A). En particulier, si cette dimension vaut 1, alors P est irréductible. Supposons désormais $r \geq 2$. On détermine dans ce qui suit un procédé pour trouver un diviseur non trivial de P. Il suffit ensuite d'itérer ce procédé pour obtenir la décomposition cherchée.*
3. *Soit B une base de $\mathrm{Ker}(f - \mathrm{Id})$. Montrer qu'il existe $Q \in K[X]$ dont la classe appartienne à B tel que $1 \leq \deg(Q) < n$.*
4. *Montrer qu'il existe $\alpha \in K$ tel que $P \wedge \big(Q - \alpha\big)$ soit un diviseur non trivial de P.*

5. *On prend $K = \mathbb{F}_2$ et $P = X^5+X^4+1$. Déterminer la décomposition de P en produit de polynômes irréductibles de $\mathbb{F}_2[X]$.*

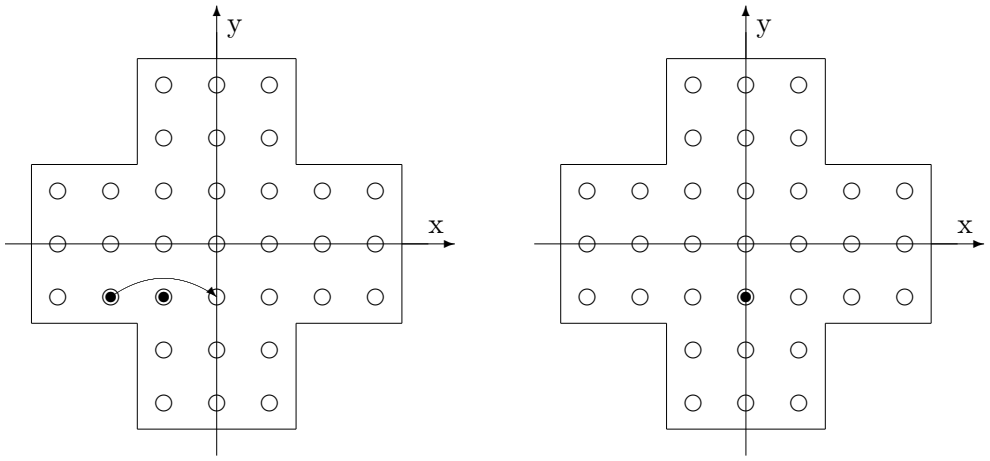
Exercice 5.22. — *Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. A chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure suivante*



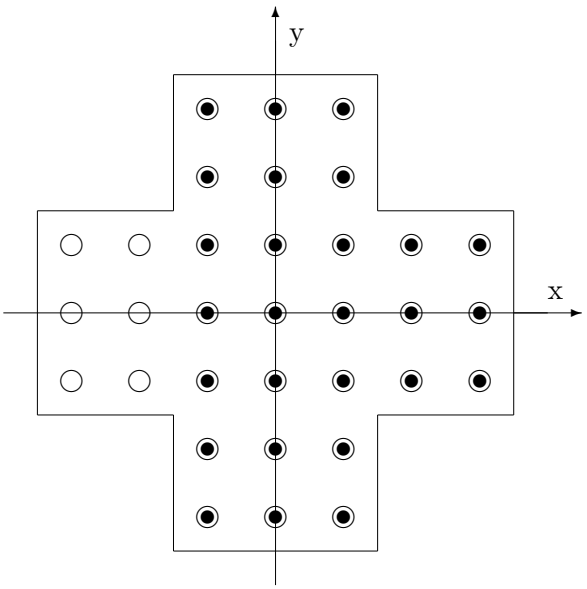
Soit alors O placé au centre du plateau et un repère (O, x, y) comme dans la figure suivante et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit

$$\alpha_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x+y} \in \mathbb{F}_4 \quad \beta_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x-y} \in \mathbb{F}_4$$

où j est un générateur de $\mathbb{F}_4^\times$.



(1) Montrer que (α, β) est un invariant du jeu.
(2) Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul disons (x_0, y_0) et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).
(3) Partant de la configuration suivante, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.



5.1. Codes correcteurs. —

Exercice 5.23. — ***Codes linéaires cycliques*** *Un code linéaire cyclique est un sous-espace vectoriel $C \subset \mathbb{F}_q^n$ stable par l'automorphisme de décalage cyclique $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ défini par*

$$T(a_1, \cdots, a_n) = (a_n, a_1, \cdots, a_{n-1})$$

.

1. *Considérons l'isomorphisme naturel d'espace vectoriel $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/Q(X)$ où $Q(X) = X^n - 1$ défini par*

$$\psi(x_1, \cdots, x_n) = x_1 X^{n-1} + \cdots + x_{n-1} X + x_n.$$

Montrer que le sous-espace $C \subset \mathbb{F}_q^n$ est cyclique si et seulement si son image par ψ est un idéal ; en déduire que les codes cycliques de longueur n sont en bijection avec les polynômes unitaires divisant $X^n - 1$.

Remarque : le diviseur unitaire g de $X^n - 1$ associé au code linéaire cyclique C s'appelle le polynôme générateur de C ; la dimension de C est $k = n - \deg g$. Le procédé de codage systématique est donné par la division euclidienne par g : le vecteur $(x_1, \cdots, x_k) \in \mathbb{F}_q^k$ est codé par le polynôme $c = c_I - c_R$ où $C_i = c_1 X^{n-1} + \cdots + x_k X^{n-k}$ et c_R de degré $< n - k$ est le reste de la division euclidienne de c_I par g, i.e. c_I porte l'information et c_R la redondance.

2. *On suppose $n \wedge p = 1$; montrer que les codes linéaires cycliques de longueur n sur $\mathbb{F}_q$ sont en bijection avec les parties $I \subset \mathbb{Z}/n\mathbb{Z}$ stables par la multiplication par q.*

3. *La distance de C est par définition le nombre minimal de composantes non nuls d'un élément de C écrit dans la base canonique. Soit C un code linéaire cyclique de longueur n sur $\mathbb{F}_q$ associé à $I \subset \mathbb{Z}/n\mathbb{Z}$ et supposons qu'il existe i et s tels que $\{i+1, i+2, \cdots, i+s\} \subset I$. Montrer alors que La distance minimale d de C est $\geq s + 1$.*

Exercice 5.24. — ***Code du minitel***

(a) Montrez que le polynôme $P(X) = X^7 + X^3 + 1$ est irréductible sur $\mathbb{F}_2$ et en déduire que $\mathbb{F}_{128} \simeq \mathbb{F}_2[X]/(X^7 + X^3 + 1)$ et montrez que X est un générateur du groupe multiplicatif.

(b) Pour envoyer un message de 15 octets (soit 120 bits) de la forme $M = a_0 a_1 \cdots a_{119}$ où les a_i sont des éléments de $\mathbb{F}_2$ (des bits), on considère l'élément suivant de $\mathbb{F}_{128}$

$$\beta = a_0 \alpha^{126} + \cdots + a_{119} \alpha^7 = a_{120} \alpha^6 + \cdots + a_{125} \alpha + a_{126}$$

On envoie alors le message $a_0 a_1 \cdots a_{126} a_{127}$ où a_{127} est un bit de parité, soit 16 octets. Le message reçu est $a'_0 \cdots a'_{127}$ où certains a'_i sont distincts de a_i à cause d'une erreur de transmission. On suppose toutefois que les erreurs de transmission sont suffisamment rares pour qu'au plus une erreur se soit produite, par exemple

au bit k, i.e. $a_i = a'_i$ pour $i \neq k$ et $a'_k = a_k + 1$. Expliquez comment décoder le message et commentez le choix de 128.

Exercice 5.25. — ***Les disques compacts***

(a) Montrez que $P(X) = X^8 + X^7 + X^6 + X^5 + X^4 + X^2 + 1$ est irréductible sur $\mathbb{F}_2$ et en déduire que $\mathbb{F}_{256} \simeq \mathbb{F}_2[X]/(P(X))$. Montrez que α, l'image de X, est un générateur du groupe multiplicatif.

(b) On représente un octet par un élément de $\mathbb{F}_{256}$. Considérons un mot $M = a_0 \cdots a_{250}$ constitué de 251 octets, i.e. $a_i \in \mathbb{F}_{256}$. On considère

$$(\sum_{i=0}^{250} a_i X^i)(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4) = \sum_{i=0}^{254} b_i X^i$$

et on transmet le message $M = b_0 \cdots b_{255} b_{256}$ où b_{256} est un bit de parité.

(i) Supposons que deux erreurs au plus se produisent dans la lecture de M. Comment savoir s'il y a eu zéro, une ou deux erreurs et expliquez comment les corriger.

(ii) On suppose désormais que quatre octets quelconques de M sont illisibles. Expliquez comment retrouver les bonnes valeurs.

(iii) Dans un CD, on code les informations musicales par paquets de 24 octets auxquels on adjoint 4 octets comme précédemment afin de pouvoir corriger deux erreurs ou 4 effacements. On obtient ainsi des mots de 28 octets, dont le $i$ème mot est noté M_i de k-ème octet est $M_i(k)$. Les mots sont alors entrelacés comme suit : chaque sillon est constitué de 28 octets, le i-ème sillon contient alors les octets suivants

$$M_i(1)\ M_{i-4}(2)\ M_{i-8}(3) \cdots M_{i-108}(28)$$

ou de manière équivalente M_i est constitué de $S_i(1)S_{i+4}(2)\cdots S_{i+108}(28)$. Chaque sillon de 28 octets est complété de 4 octets comme précédemment. Expliquez comment nos lecteurs de CD se jouent des rayures (de 2mm de large).

6. Solutions

1.1 1) Soit $f : K^* \to K^*$ l'application définie pour tout $x \in K$ par $f(x) = x^2$. C'est un morphisme de groupes. Soit p la caractéristique de K. Si $p = 2$, tout élément de K est un carré dans K, car dans ce cas f est injectif, donc est surjectif car K est fini. Supposons p impair. Le noyau de f est alors $\{\pm 1\}$. Si q est le cardinal de K, le sous-groupe des carrés non nuls de K est donc d'ordre $\frac{q-1}{2}$, et l'ensemble K^2 des carrés de K est de cardinal $(q+1)/2$. Considérons un élément $a \in K$. L'ensemble $S = \{a - x^2 \mid x \in K\}$ est aussi de cardinal $(q+1)/2$. On en déduit que $S \cap K^2$ n'est pas vide. Il existe ainsi deux éléments x et y de K tels que l'on ait $a - x^2 = y^2$, d'où le résultat.

2) L'ordre de G est le nombre de bases du K-espace vectoriel K^n. Il s'agit donc de dénombrer l'ensemble de ces bases. On remarque pour cela qu'un n-uplet $(u_1, \cdots, u_n)$ d'éléments de K^n est une base de K^n si et seulement si la condition suivante est satisfaite : u_1 n'est pas nul et pour tout $i \geq 2$, u_i n'appartient pas au sous-espace vectoriel engendré par $u_1, \cdots, u_{i-1}$. Il y a $q^n - 1$ choix possibles pour u_1. Pour tout $i \geq 2$, il y a $q^n - q^{i-1}$ choix possibles pour u_i, à savoir tous les vecteurs de K^n qui ne sont pas dans le sous-espace engendré par les $i-1$ premiers vecteurs déjà choisis. On en déduit que l'ordre de G est

$$\prod_{i=0}^{n-1} (q^n - q^i).$$

3) Donnons deux démonstrations de la première égalité. On peut remarquer que les éléments de K sont exactement les racines du polynôme $X^q - X$. La somme de ses racines, qui est l'opposé du coefficient de X^{q-1}, est donc nulle si $q > 2$. On peut aussi utiliser le fait que K^* est cyclique. Soit α l'un de ses générateurs. Puisque $q > 2$, on a $\alpha \neq 1$. On a ainsi les égalités

$$\sum_{x \in K^*} x = \sum_{i=0}^{q-2} \alpha^i = \frac{\alpha^{q-1} - 1}{\alpha - 1} = 0.$$

En ce qui concerne la deuxième égalité, on peut utiliser l'égalité dans $K[X]$

$$X^{q-1} - 1 = \prod_{a \in K^*} (X - a).$$

En substituant l'indéterminée X par 0, on obtient l'égalité annoncée.

4) Posons $q = p^n$ où p est premier. Vérifions que tout élément de K^*, autre que 1, est un générateur de K^* si et seulement si on est dans l'un des deux cas suivants :

(i) on a $n = 1$ et $p \in \{2, 3\}$.

(ii) On a $p = 2$ et $2^n - 1$ est un nombre premier (auquel cas n est aussi premier).

Tout d'abord si (i) ou (ii) est réalisée, la condition de l'énoncé est satisfaite car K^* est trivial (si $K = \mathbb{F}_2$) ou bien est un groupe d'ordre premier. Inversement, supposons que tout élément de K^*, autre que 1, soit un générateur de K^* et que K ne soit pas $\mathbb{F}_2$. Dans ce cas, on a $q \geq 3$ et $q - 1$ est premier. En effet, si $q - 1$ a un diviseur r distinct de 1 et $q - 1$, il existe dans K^* un élément d'ordre r car K^* est cyclique, et un tel élément n'est donc pas générateur. Par ailleurs, $q - 1 = p^n - 1$ est divisible par $p - 1$. On a ainsi $q - 1 = p - 1$ ou bien $p - 1 = 1$. Si $p - 1 = 1$, on a $p = 2$ et la condition (ii) est satisfaite. Supposons $p - 1 = q - 1$. Dans ce cas, on a $n = 1$, et les entiers p et $p - 1$ étant des nombres premiers, on a donc $p = 3$, d'où le résultat.

1.2 1) C'est une conséquence directe de la deuxième égalité de la question 4 de l'exercice 1.

2) On a l'égalité

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

La congruence $(p-1)! \equiv -1 \mod p$ entraîne alors l'assertion.

2.3 (i) On vérifie rapidement que $X^2 + X + 1$ n'a pas de racines dans $\mathbb{F}_2$, étant de degré 2 il y est alors irréductible de sorte que $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps, une extension de degré 2 de $\mathbb{F}_2$ et donc isomorphe à $\mathbb{F}_4$ qui par convention est **le** corps de cardinal 4 contenu dans une clôture algébrique $\bar{\mathbb{F}}_2$ de $\mathbb{F}_2$ fixée une fois pour toute. Comme $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, tout élément autre que $0, 1$ est un générateur de $\mathbb{F}_4^\times$, soit X et $X + 1$.

(ii) De même, on vérifie que X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps de cardinal 8 et donc isomorphe à $\mathbb{F}_8$. Comme $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ tout élément autre que $0,1$ est un générateur du groupe des inversibles, par exemple X.

(iii) Encore une fois X^4+X+1 n'a pas de racines sur $\mathbb{F}_2$ mais cela ne suffit pas pour conclure à son irréductibilité ; il nous faut montrer que X^4+X+1 n'a pas de racines dans $\mathbb{F}_4$. Soit donc $x \in \mathbb{F}_4$ n'appartenant pas à $\mathbb{F}_2$; on a alors $x^3=1$ de sorte que $x^4+x+1 = x+x+1 = 1 \neq 0$. Ainsi X^4+X+1 n'a pas de racines dans les extensions de degré $\leq 4/2$ de $\mathbb{F}_2$ et est donc irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^4+X+1)$ est un corps de cardinal 16 qui est donc isomorphe à $\mathbb{F}_{16}$.

Pour savoir si X est un générateur du groupe multiplicatif, il suffit de vérifier qu'il n'est pas d'ordre 3 ou 5. Or dans la base $1, X, X^2, X^3$, $X^3-1 \neq 0$ et $X^5-1 = X^2+X+1 \neq 0$.

On cherche les éléments de $\mathbb{F}_4$ autres que $0,1$, i.e. des éléments d'ordre 3. Un candidat naturel est $X^5 = X^2+X =: \chi$, on a alors $\chi^2 = X^4+X^2$ et $\chi^2+\chi+1=0$ et $\chi^3=1$ de sorte que le sous ensemble $\{0,\chi,\chi^2,\chi^3\}$ de $\mathbb{F}_{16}$ correspond au sous-corps $\mathbb{F}_4$. En outre $X^2+\chi X+1$ n'a pas de racines dans $\mathbb{F}_2[\chi]$ et il y est donc irréductible de sorte que $\mathbb{F}_{16} \simeq \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+YX+1)$.

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

2.4 Evidemment $\bigcup_{n=1}^N \mathbb{F}_{p^{n!}} = \mathbb{F}_{p^{N!}}$ de sorte que $k = \bigcup_{n=1}^\infty \mathbb{F}_{p^{n!}}$ est une réunion croissante de corps et est donc un corps ; en effet pour $x,y \in k$, il existe n tels que $x,y \in \mathbb{F}_{p^{n!}}$ et $x+y, xy$ sont définis dans $\mathbb{F}_{p^{n!}}$. Il est en outre immédiat que k est algébrique sur $\mathbb{F}_p$ car tout $x \in k$ est un élément d'un $\mathbb{F}_{p^{n!}}$ pour n assez grand. Il reste alors à voir que k est algébriquement clos ; soit donc $P(X) \in k(X)$ irréductible et soit $\mathbb{F}_{p^m}$ une extension contenant les coefficients de P et soit L un corps de rupture de P dans $\bar{\mathbb{F}}_p$ sur $\mathbb{F}_{p^m}$; L est alors une extension finie de $\mathbb{F}_{p^m}$ et est donc égale à un certain $\mathbb{F}_{p^r}$ et donc inclus dans $\mathbb{F}_{p^{r!}} \subset k$. Ainsi tout polynôme irréductible sur k est de degré 1 soit k algébriquement clos.

Remarque : En général il est pratique de fixer une clôture algébrique $\bar{\mathbb{F}}_p$ et de noter pour tout n, $\mathbb{F}_{p^n}$ **le** corps de décomposition dans $\bar{\mathbb{F}}_p$ du polynôme $X^{p^n}-X$.

2.5 (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 $X^4+X^3+X^2+X+1 = (X^2+jX+1)(X^2+j^2X+1)$.

2.6 (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 $P(x) := X^2 + X + 1$, $P(0)$, $P(+1)$ et $P(+2)$ 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.

(3) 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.

2.7 (a) 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 s[illegible]ue a^9 [illegible]nc Q n'a pas de racine dans $\mathbb{F}_9$.

(b) Afin de c[illegible] da[illegible]par le décrire concrètement : on vérifie aisément que $X^3 - X - 1$ n'a pas de racin[illegible]et est donc irr[illegible]e sur $\mathbb{F}_3$ et $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(X^3 - X - 1)$.

(c) Soit alors [illegible]tel que $\alpha^3 = \alpha + 1$[illegible] alors $\alpha^9 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$ et donc finalement α est une racine de Q dan[illegible]e sorte que Q possè[illegible]acteur irréductible de degré 3 sur $\mathbb{F}_3$, à savoir $X^3 - X - 1$, soit $X^9 - X + 1 = ($[illegible]$ - 1)(X^6 + X^4 + X$[illegible]$ - X - 1)$.

(d) Cherchon[illegible]anière générale tout[illegible]racines dans $\mathbb{F}_{27}$; un élément quelconque s'écrit sous la forme $x = a\alpha^2 + b\alpha +$[illegible] $a, b, c \in \mathbb{F}_3$. On a al[illegible]$= a\alpha^{18} + b\alpha^9 + c$ avec $\alpha^9 = \alpha - 1$ et donc $\alpha^{18} = \alpha^2 + \alpha + 1$ de sorte que $x^9 - x$[illegible]$a\alpha + a - b + 1$ ce qu[illegible]se $a = 0$ et $b = 1$ soit $x = \alpha, \alpha + 1, \alpha - 1$.

(e) On en dé[illegible]rs que $X^6 + X^4 + X$[illegible]$^2 - X - 1$ n'a pas de racines dans $\mathbb{F}_{27}$ comme il n'en avait pas non plus dans $\mathbb{F}$[illegible]nc irréductible.

2.8 Si P est réd[illegible]sur $\mathbb{F}_p$, il l'est sur to[illegible]ension $\mathbb{F}_{p^m}$. Supposons donc P irréductible sur $\mathbb{F}_p$ de sorte que toutes les racine[illegible]ues dans $\bar{\mathbb{F}}_p$, sont d[illegible], et aucune n'appartient à un sous-corps strict. On regarde alors P comme un po[illegible]dans $\mathbb{F}_{p^m}[X]$ dont o[illegible]mande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines [illegible]pour $r \leq n/2$ et [illegible]$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{mr}}$, soit n divise mr qui est possible si et seulement si n et m ne so[illegible]premiers entre eux. [illegible]re 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. $10 + 5.2$).

3.9 1) Puisque K est de caractéristique p, on a l'égalité $(x+y)^p = x^p + y^p$ pour tous x et y dans K, donc σ est un morphisme de groupes. Par ailleurs, on a $(xy)^p = x^p y^p$ (K est commutatif) et $\sigma(1) = 1$. Ainsi σ est un morphisme de corps, donc est injectif. Le fait que K soit fini entraîne que σ est une surjection de K sur K.

2) Soit x un élément de K. Le corps K étant de cardinal q, on a $x^q = x$. Ainsi, on a

$$\sigma^n(x) = x^{p^n} = x^q = x,$$

donc

et $f(\alpha)$ est donc une racine de P dans K. Puisque α est un générateur de K^*, le morphisme d'anneaux $\psi : \mathbb{F}_p[X] \to K$ défini par $\psi(F) = F(\alpha)$, est surjectif. Le noyau de ψ est l'idéal (P), par suite les corps K et $\mathbb{F}_p[X]/(P)$ sont isomorphes. Le cardinal de K étant p^n, il en résulte que le degré de P est n. On en déduit l'égalité

$$P = \prod_{i=0}^{n-1} \big(X - \alpha^{p^i}\big).$$

En effet, pour tout $i = 0, \cdots, n-1$, on a $P\big(\alpha^{p^i}\big) = 0$ et $p^n - 1$ étant l'ordre de α dans K^*, on a $\alpha^{p^i} \neq \alpha^{p^j}$ pour tous i et j tels que $0 \leq i < j \leq n-1$ (si $\alpha^{p^i} = \alpha^{p^j}$, on obtient $\alpha^{p^j - p^i} = 1$ et l'on a $1 \leq p^j - p^i < p^n - 1$). Il existe donc un entier i compris entre 0 et $n-1$ tel que l'on ait $f(\alpha) = \alpha^{p^i}$. Le fait que α soit un générateur de K^* entraîne alors que $f = \sigma^i$, d'où le résultat.

3.10 1) Pour tout entier k compris entre 1 et p^n, il existe des polynômes Q_k et R_k de $\mathbb{F}_p[X]$ tels que l'on ait

$$X^k - 1 = FQ_k + R_k \quad \text{avec} \quad \deg R_k < n.$$

Supposons que F ne divise pas $X^k - 1$ pour tout $k = 1, \cdots, p^n$. Dans ce cas, on a $R_k \neq 0$ pour tout $k = 1, \cdots, p^n$. L'ensemble des polynômes de $\mathbb{F}_p[X]$ de degré $< n$ étant de cardinal p^n, il existe donc deux entiers distincts k et k' tels que l'on ait $1 \leq k' < k \leq p^n$ et $R_k = R_{k'}$. On a l'égalité

$$X^{k'}\big(X^{k-k'} - 1\big) = F(Q_k - Q_{k'}).$$

Puisque $F(0) \neq 0$, cela entraîne que F divise $X^{k-k'} - 1$. On obtient ainsi une contradiction car on a $1 \leq k - k' \leq p^n$.

2) Posons $q = p^n$. Supposons que F divise $X^q - 1$. Il s'agit de prouver qu'il existe un entier j tel que $1 \leq j < q$ et que F divise $X^j - 1$. On a $X^q - 1 = (X-1)^q$. Le polynôme F étant de degré n, on en déduit que $F = (X-1)^n$. Considérons alors l'entier $a \geq 0$ tel que l'on ait

$$p^{a-1} < n \leq p^a.$$

Vérifions que l'entier $j = p^a$ convient. On a $(X-1)^{p^a} = X^{p^a} - 1$. L'inégalité $n \leq p^a$ entraîne que F divise $X^{p^a} - 1$. Tout revient à montrer l'inégalité

$$p^a < q. \tag{1}$$

On remarque pour cela que l'on a $n \leq p^{n-1}$ (on vérifie cette inégalité par récurrence sur n : elle est vraie si $n = 1$; soit $n \geq 2$ un entier tel que $n - 1 \leq p^{n-2}$. On a alors $n \leq 2(n-1) \leq p(n-1) \leq pp^{n-2} = p^{n-1}$). L'entier p^a étant la plus petite puissance de p supérieure ou égale à n, on a donc $a \leq n - 1$, d'où l'inégalité (1).

3) Posons $F = X^3 + X + 1 \in \mathbb{F}_2[X]$. On vérifie dans $\mathbb{F}_2[X]$ les égalités

$$X^4 - 1 = XF + X^2 + X + 1, \quad X^5 - 1 = (X^2+1)F + X^2 + X, \quad X^6 - 1 = F^2 + X^2,$$
$$X^7 - 1 = (X^4 + X^2 + X + 1)F.$$

C'est donc $m = 7$.

4.11 1) Notons n le degré de F. On considère l'anneau quotient

$$K = \mathbb{F}_\ell[X]/(F).$$

Puisque F est irréductible sur $\mathbb{F}_\ell$, l'anneau K est un corps fini de cardinal ℓ^n. Identifions $\mathbb{F}_\ell$ à un sous-corps de K. Soient α la classe de X modulo F et d l'ordre de la classe de ℓ modulo p. On a $F(\alpha) = 0$, et l'égalité $X^p - 1 = (X-1)\Phi_p$ entraîne $\alpha^p = 1$. Puisque ℓ et p sont distincts, on a $\alpha \neq 1$ et α est donc d'ordre p dans K^* (F divisant Φ_p, on a $\Phi_p(\alpha) = 0$, de sorte que si $\alpha = 1$, p est nul modulo ℓ, d'où $\ell = p$). Le groupe K^* étant d'ordre $\ell^n - 1$, on a $\alpha^{\ell^n - 1} = 1$, d'où $\ell^n \equiv 1 \mod p$ et d divise n. Par ailleurs, la congruence $\ell^d \equiv 1 \mod p$ et l'égalité $\alpha^p = 1$ entraînent $\alpha^{\ell^d} = \alpha$. Si σ est l'automorphisme de Frobenius de K, on a ainsi

$$\sigma^d(\alpha) = \alpha.$$

Le système $\big(1, \alpha, \cdots, \alpha^{n-1}\big)$ étant une base de K sur $\mathbb{F}_\ell$, on en déduit que σ^d est l'identité de K. Puisque σ est un automorphisme de K d'ordre n, il en résulte que n divise d. Par suite, on a $n = d$ et le résultat.

2) Supposons que Φ_p soit irréductible sur $\mathbb{F}_\ell$. La question 1 entraîne que la classe de ℓ est d'ordre $p-1$ dans $\mathbb{F}_p^*$. Inversement, supposons que la classe de ℓ soit un générateur de $\mathbb{F}_p^*$. Soit $F \in \mathbb{F}_\ell[X]$ un facteur irréductible de Φ_p. D'après la question 1, son degré est $p-1$, d'où $F = \Phi_p$ et Φ_p est irréductible sur $\mathbb{F}_\ell$.

3) On déduit de ce qui précède que Φ_5 est irréductible sur $\mathbb{F}_\ell$ si et seulement si on a $\ell \equiv 2, 3 \mod 5$. Notons que dans $\mathbb{F}_5[X]$, on a l'égalité $\Phi_5 = (X-1)^4$ et Φ_5 est donc réductible sur $\mathbb{F}_5$.

4.12 (i) 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.

(ii) 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.

4.13 Rappelons que pour tout entier $m \geq 1$, l'ensemble des diviseurs irréductibles du polynôme $X^{p^m} - X \in \mathbb{F}_p[X]$ est formé des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré divisant m. 1) Supposons F irréductible sur $\mathbb{F}_p$. Puisque le degré de F est n, F divise donc $X^{p^n} - X$. Soit q un diviseur premier de n. Si F et $X^{p^{\frac{n}{q}}} - X$ ne sont pas premiers entre eux, F étant irréductible, c'est un alors diviseur de $X^{p^{\frac{n}{q}}} - X$. Cela conduit à une contradiction vu que n ne divise pas $\frac{n}{q}$. Inversement, supposons la condition b réalisée. Supposons F réductible sur $\mathbb{F}_p$. Soit G un facteur irréductible de F de degré $k < n$. D'après l'hypothèse faite, G divise $X^{p^n} - X$, par suite k divise n. Posons $n = kd$ où $d \in \mathbb{Z}$. On a $d \geq 2$. Soit q un facteur premier de d. L'entier k divise $\frac{n}{q}$, donc G divise $X^{p^{\frac{n}{q}}} - X$, ce qui contredit le fait que $F \wedge X^{p^{\frac{n}{q}}} - X = 1$, d'où l'assertion. 2) Posons $F = X^7 + X + 1 \in \mathbb{F}_2[X]$. Vérifions que l'on a la congruence

$$X^{128} \equiv X \mod F. \tag{1}$$

On a $X^7 \equiv X+1 \mod F$, d'où il résulte que

$$X^{126} \equiv (X+1)^{18} \equiv (X^2+1)^8(X^2+1) = (X^{16}+1)(X^2+1) \mod F.$$

On a $X^{14} \equiv X^2+1 \mod F$, d'où $X^{16} \equiv X^4 + X^2 \mod F$. On en déduit que l'on a

$$X^{128} \equiv (X^4+X^2+1)(X^4+X^2) = X^8 + X^2 \equiv X \mod F,$$

d'où la congruence (1). Par ailleurs, F est premier avec $X^2 - X$. D'après la question 1, F est donc irréductible sur $\mathbb{F}_2$.

4.14 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 $\bar{P} = (X^2+X+1)(X^2+4X+1)$.

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 $\mathbb{Z}$.

4.15 (1) Si $x = a/b \in \mathbb{Q}$ avec $(a,b) = 1$, est une racine de P alors comme P est unitaire on a b divise 1 et donc $x \in \mathbb{Z}$. En outre modulo 2, $x^{l+1} - x + 1 \equiv 1 \mod 2$ de sorte que P n'a pas de racine modulo 2 et donc n'a pas de racine dans $\mathbb{Z}$.

(2) Modulo p, on a $\bar{P} = X(X-1)\bar{\Phi}_l$; il suffit donc de prouver que $\bar{\Phi}_l$ est irréductible ce qui découle d'un exercice précédent car p engendre $(\mathbb{Z}/l\mathbb{Z})^\times$. On peut en donner une preuve directe en considérant pour $1 \leq n < (l+1)/2$, $x \in \mathbb{F}_{p^n}$ une racine de $\bar{\Phi}_l$. On a $x \neq 1$ car $\bar{\Phi}_l(1) = \bar{l} \neq 0$ et $x^{l+1} = x$ avec l premier implique que l est l'ordre de

x dans $\mathbb{F}_{p^n}^\times$ et donc l divise p^n-1 soit $p^n \equiv 1 \mod l$. Or comme p engendre $(\mathbb{Z}/l\mathbb{Z})^\times$, on en déduit que n est un multiple de $l-1$ ce qui contredit le fait que $n < (l+1)/2$.

(3) Modulo 2, $\bar{P}$ admet donc un diviseur de degré 2 qui est donc irréductible car $\bar{P}$ n'a pas de racine. Or sur $\mathbb{F}_2$, il y a un unique polynôme irréductible de degré 2, à savoir X^2+X+1. Ainsi sur $\mathbb{F}_4$, on doit avoir $P(j)=0$ où j est un générateur de $\mathbb{F}_4^\times$, soit $j^{l+1} = j+1 = j^2$ et donc $l+1 \equiv 2 \mod 3$ ce qui n'est pas.

4.16 Soit N le nombre cherché. On a l'égalité

$$X^{p^\ell} - X = \prod f,$$

où f parcourt l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré divisant ℓ. Il y a p polynôme unitaires de degré 1. Puisque ℓ est premier, on a donc l'égalité $p^\ell = p + N\ell$, d'où

$$N = \frac{p^\ell - p}{\ell}.$$

5.17 (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 $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

5.18 Pour tout $x \in K^*$, on a $x^{q-1} = 1$. Si $q-1$ divise n, on a donc $S_n = q-1$ i.e. $S_n = (q-1)1_K$. Puisque q est une puissance de la caractéristique de K, on a $q1_K = 0$, d'où $S_n = -1$. Supposons que $q-1$ ne divise pas n. Il existe alors $y \in K^*$ tel que $y^n \neq 1$. En effet, K^* est cyclique et il suffit de prendre pour y un élément d'ordre $q-1$ (car si $y^n = 1$, alors $q-1$ divise n). Par ailleurs, l'application $K^* \to K^*$ qui à x associe xy est une bijection. On a donc

$$S_n = \sum_{x \in K^*} x^n = \sum_{x \in K^*} (xy)^n,$$

d'où l'égalité $(1-y^n)S_n = 0$, puis $S_n = 0$.

On peut aussi utiliser l'argument suivant. Supposons que $q-1$ ne divise pas n. Soit ω un générateur de K^*. On a

$$S_n = \sum_{j=0}^{q-2} (\omega^j)^n = \sum_{j=0}^{q-2} (\omega^n)^j.$$

On a $\omega^n \neq 1$, d'où

$$S_n = \frac{1-(\omega^n)^{q-1}}{1-\omega^n} = 0.$$

5.19 1) On regroupe deux à deux les termes de la forme $\frac{1}{k} + \frac{1}{p-k}$ pour $k = 1, \cdots, \frac{p-1}{2}$. On obtient

$$\frac{N}{D} = \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} + \frac{1}{p-k} \right) = p \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)}. \tag{1}$$

Il existe deux entiers a et b premiers entre eux, avec b non divisible par p, tels que l'on ait

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)} = \frac{a}{b}.$$

Il en résulte l'égalité $Nb = paD$, donc p divise N. 2) Posons $M = \frac{N}{p} \in \mathbb{Z}$. On déduit de (1) que l'on a dans $\mathbb{F}_p^*$ l'égalité

$$\overline{M} = -\overline{D} \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{\overline{k}^2}.$$

Par ailleurs, on a

$$2 \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{\overline{k}^2} = \sum_{x \in \mathbb{F}_p^*} x^2,$$

d'où le résultat. 3) On a $p \geq 5$. D'après l'exercice 11, la somme des carrés de $\mathbb{F}_p^*$ est nulle. Par suite, on a $\overline{M} = 0$, autrement dit, p divise M i.e. p^2 divise N.

5.20 1) On a l'égalité

$$F = X^{p-1} - A_1 X^{p-2} + A_2 X^{p-3} + \cdots - A_{p-2} X + A_{p-1}. \tag{1}$$

En substituant X par p dans (1), on obtient

$$(p-1)! = p^{p-1} - A_1 p^{p-2} + A_2 p^{p-3} + \cdots - A_{p-2} p + A_{p-1}.$$

Le fait que l'on ait $(p-1)! = A_{p-1}$ entraîne alors le résultat. 2) En substituant X par $-p$ dans (1), on obtient

$$\prod_{i=1}^{p-1} (p+i) = p^{p-1} + A_1 p^{p-2} + \cdots + A_{p-2} p + A_{p-1}.$$

D'après la première question, on a l'égalité

$$p^{p-1} + A_2 p^{p-3} + \cdots + A_{p-3} p^2 = A_1 p^{p-2} + A_3 p^{p-4} + \cdots + A_{p-2} p,$$

d'où l'égalité annoncée. 3) On a

$$(p-1)!\, C_{2p-1}^{p-1} = \prod_{i=1}^{p-1} (p+i). \tag{2}$$

Par ailleurs, d'après le petit théorème de Fermat, en posant $\overline{A_i} = A_i + p\mathbb{Z}$, on a dans $\mathbb{F}_p[X]$ l'égalité

$$X^{p-1} - 1 = X^{p-1} - \overline{A_1} X^{p-2} + \overline{A_2} X^{p-3} + \cdots - \overline{A_{p-2}} X + \overline{A_{p-1}}. \tag{3}$$

En particulier, on a $A_{p-3} \equiv 0 \mod p$. Il résulte alors de la question 2 et de l'égalité (2) que l'on a la congruence

$$(p-1)!\, C_{2p-1}^{p-1} \equiv A_{p-1} \mod p^3,$$

d'où le théorème vu que $A_{p-1} = (p-1)!$. 4) Compte tenu de l'égalité (3), on a

$$A_i \equiv 0 \mod p \quad \text{pour tout } i \text{ tel que } 1 \leq i \leq p-2.$$

Par suite, d'après première question, on a

$$A_{p-2} \equiv 0 \mod p^2.$$

L'égalité

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{A_{p-2}}{(p-1)!},$$

implique alors le théorème de Wolstenholme.

5.21 1) Soit p la caractéristique de K. L'entier q est donc une puissance de p. L'anneau A est aussi de caractéristique p (le noyau du morphisme d'anneaux $\mathbb{Z} \to A$ qui à n associe $n1_A = n1_K + (P)$, est l'idéal $p\mathbb{Z}$). Rappelons que la structure de K-espace vectoriel sur A est donnée par la formule

$$\lambda.\big(F + (P)\big) = \lambda F + (P) \quad \text{pour tout } \lambda \in K \text{ et } F \in K[X].$$

Pour tout $j = 1, \cdots, p-1$, le coefficient binomial C_p^j étant divisible par p, on a pour tous $x, y \in A$ l'égalité $(x+y)^p = x^p + y^p$. On en déduit par récurrence que l'on a

$$(x+y)^{p^m} = x^{p^m} + y^{p^m} \quad \text{pour tout } m \geq 0.$$

En particulier, on a $(x+y)^q = x^q + y^q$ i.e. $f(x+y) = f(x) + f(y)$. Par ailleurs, pour tout $\lambda \in K$ et tout $x \in A$, on a $f(\lambda x) = (\lambda x)^q = \lambda^q x^q = \lambda x^q = \lambda f(x)$ car λ appartient à K, d'où l'assertion. 2) Pour $i = 1, \cdots, r$, posons $L_i = K[X]/(P_i)$. D'après le théorème chinois, l'application

$$\theta : A \to L_1 \times L_2 \times \cdots \times L_r,$$

définie pour tout $F + (P) \in A$ par l'égalité

$$\theta\big(F + (P)\big) = \big(F + (P_1), \cdots, F + (P_r)\big),$$

est un isomorphisme de K-algèbres. Posons $N = \mathrm{Ker}(f - \mathrm{Id})$ et pour tout $i = 1, \cdots, r$,

$$N_i = \Big\{ y \in L_i \mid y^q = y \Big\}.$$

Le morphisme θ induit un isomorphisme de N sur $N_1 \times \cdots \times N_r$. Par ailleurs, l'application $K \to L_i$ qui à $\lambda \in K$ associe $\lambda + (P_i)$ est un morphisme injectif de K-algèbres. Soit B_i son image. Vérifions que $B_i = N_i$. Pour tout $x \in K$, on a $x^q = x$, donc B_i est contenu dans N_i. Le polynôme P_i étant irréductible, L_i est un corps, donc $X^q - X \in L_i[X]$ a au plus q racines dans L_i i.e. on a $|N_i| \leq q$. Puisque B_i, qui est isomorphe à K, est de cardinal q, cela entraîne l'égalité annoncée. Les K-algèbres N_i sont donc isomorphes à K, et sont ainsi de dimension 1 sur K. Par suite, le produit des N_i est un K-espace vectoriel de dimension r et il en est de même de N. 3) Posons $B = \big(F_1 + (P), \cdots, F_r + (P)\big)$ où les F_i sont des polynômes de $K[X]$ tels que $0 \leq \deg(F_i) < n$. Puisque l'on a $r \geq 2$, l'un des F_i n'est pas dans K. En effet, deux éléments $\lambda + (P)$ et $\mu + (P)$ où $\lambda, \mu \in K$ sont dépendants sur K. Il existe donc un polynôme F_i de degré au moins 1. 4) Soit $Q \in K[X]$ comme dans la question 3. Puisque $\theta\big(Q + (P)\big)$ appartient au produit des N_i, pour tout $i = 1, \cdots, r$, il existe $\alpha_i \in K$ tel que l'on ait

$$\theta\big(Q + (P)\big) = \big(\alpha_1 + (P_1), \cdots, \alpha_r + (P_r)\big).$$

(On utilise ici le fait que la flèche $K \to N_i$ qui à $\lambda \in K$ associe $\lambda + (P_i)$ est un isomorphisme.) Les α_i ne sont pas tous égaux. En effet, dans le cas contraire, il existerait $a \in K$ tel que $Q \equiv a \mod P_i$ pour tout i, et P étant le produit des P_i, P diviserait $Q - a$, ce qui conduit à une contradiction car on a $1 \leq \deg(Q) < n$. Posons

$$\alpha = \alpha_1.$$

Pour tout $i = 1, \cdots, r$, on a l'équivalence

$$P_i \text{ divise } Q - \alpha \Longleftrightarrow \alpha_i = \alpha.$$

Par suite, le pgcd D de P et $Q - \alpha$ est le produit des P_i où i parcourt les indices entre 1 et r tels que $\alpha_i = \alpha$. Puisque 1 est l'un de ces indices, P_1 divise D et par ailleurs, on a $P \neq D$ car il existe i tel que $\alpha \neq \alpha_i$. Ainsi D est un diviseur non trivial de P, d'où le résultat. 5) On vérifie que l'on a

$$P + (X+1)P' = 1,$$

donc P et P' sont premiers entre eux. Soit $\alpha \in A$ la classe de X modulo P. On a

$$\alpha^5 + \alpha^4 + 1 = 0.$$

On détermine la matrice M de $f : A \to A$ qui à x associe x^2 dans la base $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ de A sur K. On vérifie que l'on a

$$f(1) = 1, \quad f(\alpha) = \alpha^2, \quad f(\alpha^2) = \alpha^4, \quad f(\alpha^3) = 1 + \alpha + \alpha^4, \quad f(\alpha^4) = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4.$$

On a donc

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \text{ et} M - \mathrm{Id} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

On vérifie que le rang de $M - \mathrm{Id}$ est 3. Ainsi, la dimension de $\mathrm{Ker}(f - \mathrm{Id})$ vaut 2, d'où $r = 2$ i.e. P est le produit de deux polynômes irréductibles de $\mathbb{F}_2[X]$. Par ailleurs, on constate que le système $(1, \alpha^2 + \alpha^3 + \alpha^4)$ est une base de $\mathrm{Ker}(f - \mathrm{Id})$. Par suite, on peut prendre pour Q le polynôme

$$Q = X^2 + X^3 + X^4 \in \mathbb{F}_2[X].$$

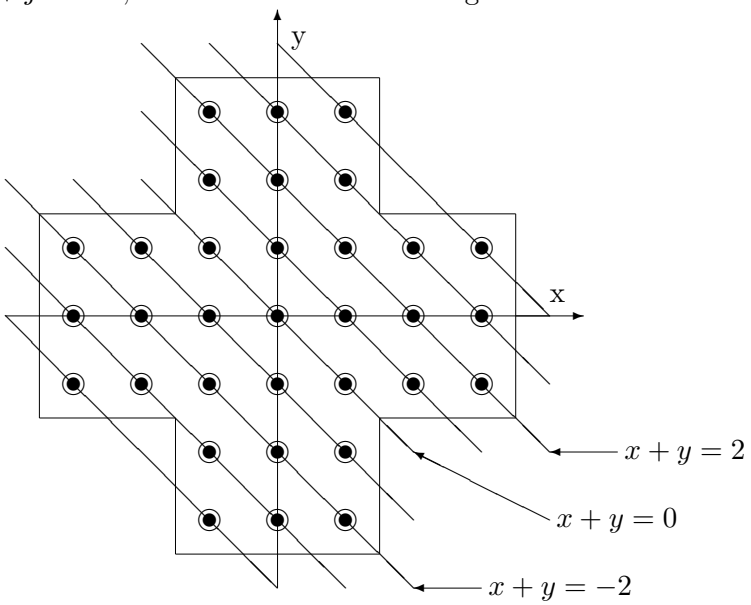
Conformément à l'algorithme de Berlekamp, $P \wedge Q$ ou $P \wedge (Q - 1)$ est un diviseur non trivial de P. On vérifie que $P \wedge (Q - 1) = 1$ et que $P \wedge Q = 1 + X + X^2$. Il en résulte que

$$P = (1 + X + X^2)(1 + X + X^3)$$

est la décomposition cherchée, car $1 + X + X^3$ n'ayant pas de racines dans $\mathbb{F}_2$ et étant de degré 3, il est irréductible dans $\mathbb{F}_2[X]$.

5.22 (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 $\mathbb{F}_4$ (on rappelle que dans $\mathbb{F}_4$, 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 $(j^{x_0+y_0}, j^{x_0-y_0})$.

5.23 1) L'automorphisme T de $\mathbb{F}_q^n$ dans l'identification donnée par ψ, correspond à la multiplication par X de sorte que C est cyclique si et seulement si $\psi(C)$ est un sous-espace vectoriel de $\mathbb{F}_q[X]$ stable par la multiplication par X et donc par tout élément de $\mathbb{F}_q[X]$; c'est donc un idéal de $\mathbb{F}_q[X]/(Q(X))$. La fin de la proposition découle du fait que les idéaux du quotient $\mathbb{F}_q[X]/(X^n - 1)$ sont en bijection avec les diviseurs de $X^n - 1$.

2) D'après la proposition **??**, les racines d'un polynôme irréductible P sur $\mathbb{F}_q$ sont de la forme $\{\alpha, \alpha^q, \cdots, \alpha^{q^{r-1}}\}$ avec $\alpha^{q^r} = \alpha$ est une racine de P. Dans le cas où P est un facteur irréductible de $X^n - 1$ ces racines sont des racines n-ème de l'unité lesquelles, une fois choisie une racine primitive, peuvent être vues comme des éléments de $\mathbb{Z}/n\mathbb{Z}$ de sorte que si α s'envoie sur k, α^q s'envoie sur qk, ce qui donne le résultat en considérant tous les facteurs irréductibles du polynôme générateur.

3) Soient donc $0 \leq l_1 < \cdots < l_s < n$ et $\lambda_1, \cdots, \lambda_s \in \mathbb{F}_q$ tels que, avec $R(X) = \sum_{i=1}^{s} \lambda_i X^{l_i}$, on ait $R(\alpha^k) = 0$ pour tout $i + 1 \leq k \leq i + s$. Ces équations s'écrivent matriciellement en faisant intervenir une matrice de Vandermonde qui est inversible de sorte que les λ_i sont tous nuls ce qui prouve le résultat.

5.24 (a) Le polynôme $P(X)$ n'a pas de racines dans $\mathbb{F}_2$, ni dans $\mathbb{F}_4$ car $P(j) = j$ et $P(j^2) = j^2$. Par ailleurs un élément α non nul de $\mathbb{F}_8$ vérifie $\alpha^7 = 1$ et donc $P(\alpha) = \alpha^3 + 1$ qui est non nul car dans $\bar{\mathbb{F}}_2$ seuls $j, j^2 \in \mathbb{F}_4$ vérifient $X^3 + 1 = 0$. Ainsi $\mathbb{F}_{2^7} \simeq \mathbb{F}_2[X]/(X^7 + X^3 + 1)$ et l'ordre de la classe α de X est un diviseur de 127 qui est premier de sorte que α est un générateur du groupe multiplicatif.

(b) Il s'agit d'un code de Hamming ; si $\sum_{i=0}^{126} a'_i \alpha^i = 0$ alors le mot reçu appartient au code et s'il y a au plus une erreur, il s'agit du mot initial. Sinon k est l'unique entier entre 0 et 126 tel que $\alpha^k = \sum_{i=0}^{126} a'_i \alpha^i$.
Remarque : on se sert du bit de parité pour tester s'il y a deux erreurs auquel cas on demande à renvoyer le message. Au final on peut corriger une erreur et détecter s'il y a deux erreurs.

5.25 (a) On écrit $P(X) = \frac{X^9+1}{X+1} + X(X^2 + 1)$; celui-ci n'a pas de racines dans $\mathbb{F}_2$ ni dans $\mathbb{F}_4$ puisque $j^9 + 1 = 0$ et $j^3 + j = 1 \neq 0$. Dans $\mathbb{F}_8$, on a $X^9 = X^2$ et donc $P(X) = X + 1 + X^3 + X = X^3 + 1$ qui n'a pas de racines dans $\mathbb{F}_8$. Si $\alpha \in \mathbb{F}_{16} - \mathbb{F}_4$, est tel que $P(\alpha) = 0$ alors $\alpha^9 + 1 = \alpha(\alpha + 1)^3$ et donc en prenant la puissance cinquième et en utilisant $(\alpha + 1)^{15} = 1$ car $\alpha \neq 1$, on obtient

$$(\alpha^9 + 1)^5 = \alpha^{45} + \alpha^{36} + \alpha^9 + 1 = \alpha^5$$

ce qui donne $\alpha^9 + \alpha^6 + \alpha^5 = 0$ soit $\alpha^4 + \alpha + 1 = 0$. Ainsi en réinjectant l'égalité $\alpha + 1 = \alpha^4$ on obtient $\alpha^9 + 1 = \alpha^13$ ce qui après multiplication par α^3 donne $\alpha^{12} = \alpha^3 + \alpha$ avec

$$\alpha^{12} = (\alpha^4)^3 = (\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha + 1$$

et donc $\alpha = \alpha^{12} + \alpha^3 = \alpha^2 + \alpha + 1$ ce qui donne $\alpha^2 = 1$ et comme 2 ne divise pas 15, on obtient α d'ordre $1 = 2 \wedge 15$ soit $\alpha = 1$ qui ne convient pas.

(b-i) Il s'agit d'un code de Reed-Solomon qui est donc 2-correcteur. Si on suppose qu'il y a au plus deux erreurs, on teste si $\alpha, \alpha^2, \alpha^3$ et α^4 sont racines du polynôme $\sum_{i=0}^{254} b_i X^i$: si oui alors il n'y a pas eu d'erreurs sinon le bit de parité permet de savoir s'il y a eu 1 ou 2 erreurs et on calcule les α^k puis les $\alpha^i + \alpha^j$ pour savoir quels bits corriger.

(b-ii) Notons i_1, i_2, i_3, i_4 les indices des bits en question ; il s'agit alors de trouver quelle somme $\sum_{k=1}^{4} \epsilon_k X^{i_k} = 0$ avec $\epsilon_i = 0, 1$ prend en α^j pour $j = 1, 2, 3, 4$, la valeur $\sum_{i=0}^{254} b_i X^i$ où pour $k = 1, \cdots, 4$ on a posé $b_{i_k} = 0$. Si on avait 2 quadruplets de ϵ_k distincts, alors par soustraction, on aurait un polynôme formé d'au plus 4 monômes ayant α^j pour $j = 1, \cdots, 4$ comme racines et donc multiple de $(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4) = X^4 + \beta_1 X^3 + \beta_2 X^2 + \beta_3 X + \beta_4$ avec $\beta_j \neq 0$ pour tout $j = 1, \cdots, 4$ de sorte que le polynôme a forcément 5 termes non nuls, d'où la contradiction.

(b-iii) Si moins de 16 sillons sont illisibles, d'après (ii) on peut alors reconstituer le mot qui rappelons le est constitué de lettres de 8 bits...