DM n^{o}7

PREMIER EXERCICE

Il s'agit d'un résultat classique

Cryptographie

Le but de se problème est l'étude du principe de criptage RSA, qui permet de communiquer de façon sure des données. Ce résultat est à connaitre

Dans tout le problème φ désignera l'indicatrice d'Euler.

1. CHIFFREMENT DU MESSAGE

   On étudie le cryptage d'un message par un expéditeur. Soient p et q des nombres premiers distincts et n leur produit : $n = pq$. On appelle n *module de chiffrement*

   (a) Donner sans démonstration, en fonction de p et q, la valeur de $\varphi(n)$.

   (b) Soit e un entier premier avec $\varphi(n)$. On appelle e *exposant de chiffrement.* Montrer qu'il existe un entier naturel d tel que $ed \equiv 1\,[\varphi(n)]$

   Le couple (n, e) est appelé clef publique (elle peut être transmise à l'expéditeur), le couple (n, d) est appelé clef privée, elle reste connue du seul destinataire du message.

   Dans la suite on considère un entier M (représentant le message) strictement inférieur à n. On note C l'élément de $\{0, 1, \ldots, n-1\}$ congru à M^e modulo n. Cet entier représente le message codé qui est transmis.

2. DÉCHIFFREMENT DU MESSAGE

   On se propose de montrer que C^d est congru à M *modulo* n, ce qui permet au destinataire de trouver M, grâce à sa clef (n, d).

   (a) Montrer que M^{ed} est congru à M *modulo* p. On distinguera les deux cas M premier avec p et M non premiers avec p.

   (b) En déduire que $C^d \equiv M[n]$.

   Remarque : pour trouver d à partir de e et n il faut savoir inverser e dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$ ce qui nécessite de connaitre $\varphi(n)$ et donc le couple (p, q). La décomposition de n en facteurs premiers peut être très difficile si les nombres premiers p et q ont été choisis très grands.

SECOND EXERCICE

(Pour tous : 1.,2.,3.,4. et 5. le reste est facultatif.)

Entiers de Gauss

Soient $\mathbf{Z}[i]$ l'ensemble des nombres complexes de la forme $u + iv$, avec $(u, v) \in \mathbf{Z}^2$ et l'application. φ ; $\mathbf{Z}[i] \to \mathbf{N}$; $a \mapsto \bar{a}a$.

1. Montrer que $\mathbf{Z}[i]$ est un sous-anneau du corps $\mathbf{C}$.
2. Déterminer $\mathbf{Z}[i]^*$, ensemble des éléments inversibles de $\mathbf{Z}[i]$.
3. Montrer que pour tout élément a de $\mathbf{Z}[i]$ et tout élément b de $\mathbf{Z}[i]^*$, il existe un couple (q, r) d'éléments de $\mathbf{Z}[i]$ tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$. On dit que l'anneau $\mathbf{Z}[i]$ est euclidien pour φ.
4. Montrer que tout idéal de $\mathbf{Z}[i]$ est de la forme $a\mathbf{Z}[i]$, on dit que $\mathbf{Z}[i]$ est principal.
5. Soit a un élément de $\mathbf{Z}[i]$. Montrer que si $\varphi(a)$ est premier, alors a est un élément irréductible de $\mathbf{Z}[i]$. Rappelons qu'un élément a d'un anneau intègre est dit irréductible si par définition il n'est pas inversible et si il admet la décomposition $a = bc$, alors a ou b est inversible.
6. Soit p un nombre premier impair et y un élément de $(\mathbf{Z}/p\mathbf{Z})^*$, on dit que y est un carré s'il existe un élément z de $(\mathbf{Z}/p\mathbf{Z})^*$ tel que $z^2 = y$.

(a) Montrer que $\prod_{x\in(\mathbf{Z}/p\mathbf{Z})^*} x = \begin{cases} -y^{\frac{p-1}{2}}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}}, & \text{sinon .}\end{cases}$

Indication : on pourra regrouper deux à deux dans le produit les termes x et yx^{-1}.

(b) En déduire

$$\begin{cases} y^{\frac{p-1}{2}} = \bar{1}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}} = -\bar{1}, & \text{sinon .}\end{cases}$$

7. Soit p un nombre premier, impaire OU NON. Montrer l'équivalence entre les propriétés suivantes :
   i. p est irréductible dans $\mathbf{Z}[i]$;
   ii. $p \equiv 3$ [4] ;
   iii. Il n'existe pas d'élément a de $\mathbf{Z}[i]$ tel que $p = \phi(a)$.
8. En déduire les irréductibles de $\mathbf{Z}[i]$.

PROBLÈME

Première partie : Un exemple d'extension du corps $\mathbf{Q}$

1. Soit P le polynôme $X^3 - X - 1$.
   Montrer que P n'a pas de racines rationnelles. En déduire que P est irréductible dans $\mathbf{Q}[X]$.
   Montrer que P a une racine réelle que l'on notera ω.
2. Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par $\left(\omega^i\right)_{i\in\mathbf{N}}$.
   Montrer que $\mathbf{K}$ est de dimension finie, et donner une base simple de K.
3. Montrer que $\mathbf{K}$ est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$, muni de sa structure naturelle de $\mathbf{Q}$-algèbre.
4. Montrer que $\mathbf{K}$ est un sous-corps de $\mathbf{R}$.

Deuxième partie : Cas général d'extension de $\mathbf{Q}$

Soit a un réel.

1. Montrer que tout sous-corps de $\mathbf{R}$ contient $\mathbf{Q}$.
2. Montrer que l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a admet un plus petit élément pour l'inclusion. On le notera dans la suite $\mathbf{Q}(a)$.
3. Montrer que $\phi\ :\ \mathbf{Q}[X] \to \mathbf{R}\,;\ P \mapsto P(a)$ est un morphisme de la $\mathbf{Q}$-algèbres $\mathbf{Q}[X]$ dans la $\mathbf{Q}$ algèbre $\mathbf{R}$. On note $\mathbf{Q}[a]$ son image.
4. Soit $I := \{P \in \mathbf{Q}[X], P(a) = 0\}$. Montrer que I est un idéal de $\mathbf{Q}[X]$.
5. Le réel a est dit algébrique (sur $\mathbf{Q}$), si, par définition, a est racine d'un polynôme non nul à coefficients entiers.
   Montrer que a est algèbrique si et seulement si I est non réduit à $\{0\}$.
   Dans cette partie on suppose dans la suite que que a est algèbrique, sauf à la dernière question.
6. Montrer qu'il existe un et un seul élément de $\mathbf{Q}[X]$ unitaire, μ_a, tel que $I = \mu_a\mathbf{Q}[X]$.
   Montrer que μ_a est irréductible dans $\mathbf{Q}[X]$. Montrer que si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2. Déterminer μ_a pour $a = \sqrt{2}$ et pour $a = \sqrt{\frac{1+\sqrt{5}}{2}}$.
7. Montrer que $\mathbf{Q}[a]$ est un corps. Montrer que $\mathbf{Q}(a) = \mathbf{Q}[a]$.
   Montrer que $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension n, où n est le degré de μ_a, dont on donnera une base simple.
8. Si a est non algébrique, montrer qu'alors $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie[1].

Troisième partie : Corps finis
Facultatif.

Soit $(\mathbf{F}, +, \times)$ un corps. On note $1_\mathbf{F}$ l'unité de $\mathbf{F}$ et pour tout entier k et tout élément a de $\mathbf{F}$, $k \cdot a$, désigne l'élément $\underbrace{a + a + \cdots + a}_{k \text{ termes}}$ pour $k \geq 1$, l'élément $\underbrace{(-a) + (-a) + \cdots + (-a)}_{-k \text{ termes}}$ pour $k \leq -1$ et enfin $1_\mathbf{F}$ pour $k = 0$

On admet le résultat élémentaire suivant :
L'application

$$\varphi\ :\ \mathbf{Z} \to \mathbf{F}\,;\ k \mapsto k \cdot 1_\mathbf{F}$$

1. On pourrait montrer que $\mathbf{Q}(a)$ est isomorphe en tant que corps au corps $\mathbf{Q}(X)$.

est un morphisme d'anneaux.

Son noyau est donc un sous groupe de $(\mathbf{Z}, +)$, donc de la forme pZ, où p désigne un élément de $\mathbf{N}$. L'entier naturel p s'appelle caractéristique de $\mathbf{F}$.

1. Montrer que si p est nul alors $\mathbf{F}$ est infini.

   Dans toute la suite on supposera que F est fini, donc que p est non nul.

2. Montrer qu'il existe une et une seule application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ tel que $\varphi = \tilde{\varphi} \circ \pi_p$, où π_p désigne la surjection (dite canonique) de $\mathbf{Z}$ sur $Z/p\mathbf{Z}$, qui à un entier x associe sa classe modulo p.
3. Montrer que $\tilde{\varphi}$ est un morphisme d'anneaux injectif.
4. On note $\mathbf{k} = \tilde{\varphi}\left(\mathbf{Z}/p\mathbf{Z}\right)$. Montrer que $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ isomorphe à $\mathbf{Z}/p\mathbf{Z}$. En déduire que p est un nombre premier.
5. Montrer que $\mathbf{k}$ est le plus petit sous-corps de $\mathbf{F}$.

   Le sous-corps $\mathbf{k}$ est appelé sous corps premier de $\mathbf{F}$, on vient de voir qu'il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$

6. En munissant $\mathbf{F}$ d'une structure d'espace vectoriel sur $\mathbf{k}$, montrer que le cardinal de $\mathbf{F}$ est une puissance de p.

L'étude de la réciproque est traitée dans un DM bis.

PREMIER EXERCICE

1. Chiffrement du message

   (a)
   $$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

   (b) Le lemme de Bezout assure l'existence d'entiers u et v tels que :
   $$(u + k\varphi(n))e + (v - ke)\varphi(n) = 1$$
   On choisi k, pour queb : $u + k\varphi(n)$ soit strictement positif...

2. déchiffrement du message

   (a)
   - Premier cas : *M premier avec p.*
     Donc p ne divise pas M.D'après 2.(b), il existe un entiet h tel que $ed = 1 + h(p-1)$. Donc $M^{ed} = M \times (M^{(p-1)})^h$ donc $M^{ed} \equiv M\ [p]$ (Fermat).
   - Second cas : *M non premier avec p.*
     Comme p est premier, il divise M et donc M^{ed}...
     Dans tous les cas $\boxed{M^{ed} \equiv M\ [p]}$

   (b) De la précédente question et comme p et q sont premiers entre eux, $pq|M^{ed} - M$ Soit $M^{ed} \equiv M\ [n]$. Mais $C \equiv M^e\ [n]$. Donc $C^d \equiv M^{ed}[n]$ et finalement $\boxed{C^d \equiv M[n]}$.

Entiers de Gauss

1. Sans problème.
2. Si Z est inversible dans $\mathbf{Z}[i]$, alors φ est inversible dans l'anneau $\mathbf{Z}$ donc vaut 1. On trouve sans mal les élément de $\mathbf{Z}[i]$ de module 1 et l'on montre instantanément qu'ils sont inversibles...
3. Le complexe $\frac{a}{b}$ est élément d'un carré de côté 1 dont les sommets sont des entier de Gauss, prendre pour q le ou l'un des sommets plus proche de $\frac{b}{a}$...
4. cf. sous-groupes de $\mathbf{Z}$ ou idéaux de $\mathbf{K}[X]$.
5. Résulte directement de $\varphi(bc) = \varphi(b)\varphi(c)$ ...
6. Regrouper deux à deux dans le produit les termes x et yx^{-1}, l'application de $\mathbf{Z}/p\mathbf{Z})^*$ qui à x associe yx^{-1} est une involution si y est le carré de z alors deux et seulement deux élément z et $-z$ sont leur propre image sinon aucun !
7. Facile
8. Soit p un nombre premier, impaire OU NON. Montrer l'équivalence entre les propriétés suivantes :

   Par la question précédente $(\bar{1})$ n'est pas un carré si et seulement si $p \equiv 3\ [4]$.

   i.$\Longrightarrow$ii.

   On raisonne par l'absurde si ii. est faux, -1 sécrit $a^2 + kp$ et donc p divide dans $\mathbf{Z}[i]$ $(a+i)(a-i)$, absurde !

   ii.$\Longrightarrow$iii.

   Par l'absurde, si $p = \alpha^2 + \beta^2$ on a pas ii. en regardant la congruence modulo 4 d'un carré.

   iii.$\Longrightarrow$i. On suppose iii. et p de la forme $p = ab$ on a $p^2 = \phi(a)\phi(b)$, si ni $\varphi(a) = 1$ ni $\varphi(b) = 1$ alors $\varphi(a) = \varphi(b) = p$.....
9. On a montrer que les les entier premier congrus à 3 modulo 4 et les entier de Gauss a tels que $\phi(a)$ soit premier sont irreductibles.

   Montrer que ce sont les seuls, à un inversible près... On prendra un irreductible a et on raisonnera sur les diviseurs premier p de $\phi(a)$.

   On a que a divise $\phi(a)$, donc a divise un facteur premier p de $\phi(a)$ $p = ab$. Puis $p^2 = \phi(a)\phi(b)$

   Deux cas b inversible ou non .

Extensions de corps

Première partie

1. Donc on déduit (cf. exercice du cours) que les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1$, $P(-1) = -1$. Donc P n'admet pas de racines rationnelles.

   Le polynôme P est de degré *impair* à coefficients *réels*, il admet donc une racine réelle ω.

2. Soit c un élément de $\mathbf{K}$. Par définition de $\mathbf{K}$, il existe un entier naturel n et des rationnels $a_0, a_1, \ldots, a_n$ tels que : $c = \sum_{i=0}^{n} a_i \omega^i$. Soit l'élément de $\mathbf{Q}[X]$, $C = \sum_{i=0}^{n} a_i X^i$. Par division euclidienne de C par P dans $\mathbf{Q}[X]$ on obtient que $\mathbf{K}$ est le Q-espace vectoriel engendré par la sous famille de $(\omega^i)_{i\in\mathbf{N}}$, $(\omega^0, \omega^1, \omega^2)$.

   La famille $(\omega^0, \omega^1, \omega^2)$ est libre. Soit λ, μ et ν des rationnels tels que : $\lambda\omega^2 + \mu\omega + \nu = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda X^2 + \mu X + \nu$. Supposons C non nul. Alors par division euclidienne : $P = \tilde{Q}C + uX + v$ avec $\tilde{Q} \in \mathbf{Q}[X]$, u et v des rationnels. En substituant dans cette égalité ω à l'indéterminée, il vient $0 = u\omega + v$. Comme ω est irrationnel $u = 0$ et donc $v = 0$, et donc C divise P, irréductible,...

   Finalement $(\omega^0, \omega^1, \omega^2)$ est une base de K.

3.
   - K est *stable par combinaison linéaire.*
   - *K est stable par produit.*
   - Enfin $1 = \omega^0 \in K$.

   De ces trois points on déduit : K est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$.

4. D'après (c), K est un sous-anneau de $\mathbf{R}$, il est donc *commutatif* et *non trivial.*

   Soit, par ailleurs, x un élément non nul de K. Il existe, d'après (b), des rationnels a, b et c non tous nuls, tels que $x = a\omega^2 + b\omega + c$. Soit $D = aX^2 + bX + C$. P et D sont, dans $Q[X]$, premiers entre eux, par Bezout x est inversible... Conclusion : K est un sous-corps de $\mathbf{R}$.

Deuxième partie Cas général :

Soit a un réel.

1. Soit K_0 un sous-corps de $\mathbf{R}$. Il contient 1, est stable par somme et différence et par passage à l'inverse et multiplication il contient donc $\mathbf{Q}$.

2. Soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a. considérer

$$\mathbf{Q}(a) = \bigcap_{K\in\mathcal{K}} K.$$

3. Facile !D'après la question précédente, ϕ induit notamment un morphisme de l'anneau $\mathbf{Q}[X]$ sur l'anneau $\mathbf{R}$. I en est le *noyau*, c'est donc un idéal de $\mathbf{Q}[X]$.

4.
   - Hypothèse : I non réduit à 0.
     Il existe donc un polynôme P élément de $\mathbf{Q}[X]$, non nul tel que $P(a) = 0$. Multiplier P par le produit des dénominateurs de ses coefficients...
   - Hypothèse : a est algébrique.
     Presque immédiatement : I est non réduit à $\{0\}$.

5. I est un idéal de $\mathbf{Q}[X]$, donc, d'après le programme, il existe P élément de $\mathbf{Q}[X]$ (appelé générateur de I), tel que $I = P\mathbf{Q}[X]$, I étant non nul, $P \neq 0$. Soit $\tilde{P}$ un générateur de I. $\tilde{P} \in I$ donc $P|\tilde{P}$. par symétrie des rôles $\tilde{P}|P$ donc $\tilde{P}$ et P sont associés. Les générateurs de I sont associés, il en existe donc un et un seul unitaire, μ_a, qui est défini par $\mu_a = a^{-1}P$, avec a le coefficient dominant de P.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. $A(a)B(a) = \mu_a(a) = 0$ Montre que l'un des polynômes A ou B est inversible car sinon I contiendrait un polynôme de degré strictement plus petit que celui de μ_a Donc μ_a est irréductible.

   Le degré de μ_a est supérieur ou égal à 2 , sinon il serait égal à 1 et a serait rationnel.

$$\mu_{\sqrt{2}} = X^2 - 2.$$

   Maintenant $a = \sqrt{\frac{1+\sqrt{5}}{2}}$. L'élément de $\mathbf{Q}[X]$, $X^4 - X^2 - 1$ admet a comme racine. Donc $\mu_a | X^4 - X^2 - 1$. On peut montrer que $X^4 - X^2 - 1$ est irréductible dans $\mathbf{Q}[X]$ (regarder ses racines). Donc

$$\mu_a = X^4 - X^2 - 1.$$

6. $\mathbf{Q}[a]$ est l'image par le morphisme d'anneaux ϕ de l'anneau $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-anneau* de $\mathbf{R}$. Comme $\mathbf{R}$ est un corps, l'anneau $\mathbf{Q}[a]$ est *commutatif et non trivial.* Soit x un élément non nul de $\mathbf{Q}[a]$. Il existe $P \in \mathbf{Q}[X]$ tel que $x = P(a)$. La division euclidienne de P par μ_a conduit à l'existence de Q et R éléments de $\mathbf{Q}[X]$ tels que : $P = Q\mu_a + R$ et $\mathrm{d}^{\mathrm{o}}R < \mathrm{d}^{\mathrm{o}}\mu_a$. D'où $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$. x étant non nul, R est non nul, Donc μ_a ne saurait divisé R, polynôme dont le degré est inférieur au sien. Or μ_a est irréductible dans $\mathbf{Q}[X]$ (cf. 6.), donc R et μ_a sont premiers entres eux dans $\mathbf{Q}[X]$. Le lemme de Bezout permet de montrer l'inversibilité de x.

   CONCLUSION : $\underline{\mathbf{Q}[a] \text{ est un corps.}}$

   $\mathbf{Q}[a]$ est un corps qui contient a. Donc $\mathbf{Q}(a) \subset \mathbf{Q}[a]$
   Soit Soit x un élément de $\mathbf{Q}[a]$. Il sécrit
   $$x = \sum_{i=0}^{n} c_i a^i,$$
   avec n un naturel et $c_0, c_1, \ldots, c_n$ des rationnels. le corps $\mathbf{Q}(a)$ contenant 1 et a et étant stable par multiplication, il contient a^i, pour $i = 0, 1 \ldots, n$. Par ailleurs $c_i \in \mathbf{Q}(a)$ (cf. 1.). Donc le corps $\mathbf{Q}(a)$ étant stable par multiplication est addition, il contient $\sum_{i=0}^{n} c_i a^i = x$. Donc $\mathbf{Q}[a] \subset \mathbf{Q}(a)$.

   CONCLUSION : $\underline{\mathbf{Q}(a) = \mathbf{Q}[a]}$. $\mathbf{Q}[a]$ est l'image par ϕ, morphisme de $\mathbf{Q}$-espaces vectoriels, de l'espace vectoriel $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-espace vectoriel* du Q-espace vectoriel $\mathbf{R}$. En raisonnant comme dans le début de la question on montre que
   $$Q[a] = \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1}).$$
   la famille *la famille* $(a^0, a^1, \ldots, a^{n-1})$ *engendre donc* $\mathbf{Q}[a]$.

   On montre que la famille $(a^0, a^1, \ldots, a^{n-1})$ est libre. Soient $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ des rationnels tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{n-1}a^{n-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{n-1}X^{n-1}$.

   Supposons C non nul. Alors par division euclidienne : $\mu_a = \tilde{Q}C + R$ avec $\tilde{Q} \in \mathbf{Q}[X]$, $R \in \mathbf{Q}[X]$ et $\mathrm{d}^{\mathrm{o}}R \leq n-1$. Reste à montrer la nulité de R...

   Finalement $\underline{(a^0, a^1, \ldots, a^{n-1}) \text{ est une base de } \mathbf{Q}[a], \text{ qui est donc de dimension } n.}$
7. facile !
8. Si a est non algébrique, $(a^n)_{n\in\mathbf{N}^*}$ est libre...

Troisième partie : CORPS FINIS

1. Montrer que si p est nul alors φ est infini...
2. Montrer qu'il existe une et une seule application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ tel que $\varphi = \tilde{\varphi} \circ \pi_p$, où π_p désigne la surjection (dite canonique) de $\mathbf{Z}$ sur $Z/p\mathbf{Z}$, qui à un entier x associe sa classe modulo p. Il faut poser $\tilde{\varphi}(\bar{x}) = \varphi(x)$ en ayant soin de montrer que cette quantitée ne dépend pas du représentant x de $\bar{x}$; cf. structure des groupes cycliques
3. Pas bien dur...
4. On note $\mathbf{k} = \tilde{\varphi}\,(\mathbf{Z}/p\mathbf{Z})$. $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ isomorphe à $\mathbf{Z}/p\mathbf{Z}$, par injectivité de $\tilde{\varphi}$. Reste à remarquer que $\mathbf{k}$ est intègre.
5. Tout sous-corps de $\mathbf{F}$ contient 1, donc $\mathbf{k}$ est le plus petit sous-corps de $\mathbf{F}$.

   Le sous-corps $\mathbf{k}$ est appelé sous corps premier de $\mathbf{F}$, on vient de voir qu'il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$
6. Facile !

Correction du DM n°7

PREMIER EXERCICE

1. Chiffrement du message

(a) On a que p est premier donc un entier k n'est pas premier avec p si et seulement si p divise k, donc $\varphi(p) = p-1$ ($1, 2, \dots, p-1$ sont premiers avec p). De même $\varphi(q) = q-1$. Or p et q, nombres premiers distincts sont premiers entre eux, donc d'après 1. (a),

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

(b) Le lemme de Bezout assure l'existence d'entiers u et v tels que : $ue + v\varphi(n) = 1$. Plus généralement pour tout entier k,

$$(u + k\varphi(n))e + (v - ke)\varphi(n) = 1$$

En prenant pour $k > |u|$, $u + k\varphi(n)$ est strictement positif, en notant d ce nombre,

$$\boxed{ed \equiv 1\,[\varphi(n)]}$$

2. Déchiffrement du message

(a)
- Premier cas : *M premier avec p.*
  Donc p ne divise pas M. Le petit théorème de Fermat donne alors : $M^{p-1} \equiv 1\,[p]$. Par ailleurs,d'après 2.(b), il existe un entiet h tel que $ed = 1 + h(p-1)$. Donc $M^{ed} = M \times (M^{(p-1)})^h$ et $(M^{(p-1)})^h \equiv 1^h \equiv 1\,[p]$, donc $M^{ed} \equiv M\,[p]$
- Second cas : *M non premier avec p.*
  Comme p est premier, il divise M, donc M et M^{ed} sont tous deux congrus à 0 modulo p.
  Dans tous les cas $\boxed{M^{ed} \equiv M\,[p]}$

(b) De la précédente question, il vient : $p|M^{ed} - M$ et de même $q|M^{ed} - M$. Comme p et q sont premiers entre eux, $pq|M^{ed} - M$ Soit $M^{ed} \equiv M\,[n]$. Mais $C \equiv M^e\,[n]$. Donc $C^d \equiv M^{ed}[n]$ et finalement $\boxed{C^d \equiv M[n]}$.

PROBLÈME

Première partie

1. Soit P le polynôme $X^3 - X - 1$.
Supposons que P ait une racinne rationnelle r. Elle s'écrit : $r = \dfrac{p}{q}$ avec $p \in \mathbf{Z}$, $q \in \mathbf{N}$ et p et q premiers entre eux. On a donc : $r^3 - r - 1 = 0$, Soit

$$p^3 - pq^2 - q^3 = 0. \tag{1}$$

On déduit de cette égalité que p divise q^3. Or p et q sont premiers entre eux donc le théorème de Gauß dit que p divise q^2. Une nouvelle application du thèorème de gauß donne que p divise q, enfin une dernière application de ce théorème donne que p divise 1. Donc :

$$p = 1. \tag{2}$$

On déduit aussi de (1) que q divise p^3. Un raisonnement analogue au précédent donne $q|1$. Donc

$$q = \pm 1. \tag{3}$$

Donc on déduit de (2–3), que les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1$, $P(-1) = -1$. Donc P <u>n'admet pas de racines rationnelles</u>.

Montrons que P est irréductible dans $\mathbf{Q}[X]$. En premier lieu P n'est pas inversible. Ensuite, supposons que P s'écrive $P = AB$, avec A et B éléments de $\mathbf{Q}[X]$. Alors $\mathrm{d}^\circ A + \mathrm{d}^\circ B = \mathrm{d}^\circ P$. Or ni A ni B ne sont de degré 1, car un élément de $\mathbf{Q}[X]$ de degré 1 admet une racine rationnelle et P n'en admet pas. Donc $\mathrm{d}^\circ A = 0$ et $\mathrm{d}^\circ B = 3$ où $\mathrm{d}^\circ B = 0$ et $\mathrm{D}^\circ A = 3$.
En conclusion <u>P est irréductible dans $\mathbf{Q}[X]$</u>.

Le polynôme P est de degré *impair* à coefficients *réels*, il admet donc une racine réelle ω.

2. Soit c un élément de $\mathbf{K}$. Par définition de $\mathbf{K}$, il existe un entier naturel n et des rationnels $a_0, a_1, \dots, a_n$ tels que : $c = \sum_{i=0}^{n} a_i \omega^i$. Soit l'élément de $\mathbf{Q}[X]$, $C = \sum_{i=0}^{n} a_i X^i$. Par division euclidienne de C par P dans $\mathbf{Q}[X]$ on obtient :

$$C = QP + rX^2 + sX + t, \tag{4}$$

avec $Q \in \mathbf{Q}[X]$, r, s et t des rationnels. En substituant ω à l'indéterminée dans (4), il vient : $c = C(\omega) = Q(\omega)P(\omega) + r\omega^2 + s\omega + t = r\omega^2 + s\omega + t$. Donc c étant quelconque, on a : $\mathbf{K}$ est le Q-espace vectoriel engendré par la sous famille de $(\omega^i)_{i\in\mathbf{N}}$, $(\omega^0, \omega^1, \omega^2)$.

Montrons que la famille $(\omega^0, \omega^1, \omega^2)$ est libre. Soit λ, μ et ν des rationnels tels que : $\lambda\omega^2 + \mu\omega + \nu = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda X^2 + \mu X + \nu$. Supposons C non nul. Alors par division euclidienne : $P = \tilde{Q}C + uX + v$ avec $\tilde{Q} \in \mathbf{Q}[X]$, u et v des rationnels. En substituant dans cette égalité ω à l'indéterminée, il vient $0 = u\omega + v$. Comme ω est irrationnel $u = 0$ et donc $v = 0$, et donc C divise P. Mais P étant irréductible C est constant non nul, ce qui contredit $C(\omega) = 0$. Donc C est nul, c'est-à-dire : $\lambda = \mu = \nu = 0$. D'où la liberté de $(\omega^0, \omega^1, \omega^2)$.

Finalement $\underline{(\omega^0, \omega^1, \omega^2) \text{ est une base de } K}$.

3.
   - K sous-espace vectoriel sur Q de $\mathbf{R}$ est *stable par combinaison linéaire*.
   - soient x et x' des éléments de K. Il existe des rationnels a, b, c, a', b', c' tels que $x = a\omega^2 + b\omega + c$, $x' = a'\omega^2 + b'\omega + c'$. Alors

   $$xx' = aa'\omega^4 + (ab' + a'b)\omega^3 + (ac' + a'c + bb')\omega^2 + (bc' + c'b)\omega + cc'.$$

   Donc $xx' \in \underset{\mathbf{Q}}{\operatorname{vect}}(\omega^i)_{i\in\mathbf{N}} = K$. Donc *$K$ est stable par produit.*
   - Enfin $1 = \omega^0 \in K$.

   De ces trois points on déduit : $\underline{K \text{ est une } \mathbf{Q}\text{-sous-algèbre de } \mathbf{R}}$.

4. D'après (c), K est un sous-anneau de $\mathbf{R}$, il est donc *commutatif* et *non trivial.*

   Soit, par ailleurs, x un élément non nul de K. Il existe, d'après (b), des rationnels a, b et c non tous nuls, tels que $x = a\omega^2 + b\omega + c$. Soit $D = aX^2 + bX + C$. P et D sont, dans $Q[X]$, premiers entre eux, en effet P est irréductible (cf. 1.) et ne divise pas D, puisque $\mathrm{d}^\circ P > \mathrm{d}^\circ D > -\infty$. Le lemme de Bezout assure donc l'existence de U et V éléments de $\mathbf{Q}[X]$ tels que : $UD + VP = 1$. En substituant ω à l'indéterminée X dans cette égalité, il vient :

   $$U(\omega)D(\omega) + V(\omega)P(\omega) = xD(\omega) = 1.$$

   Donc $D(\omega)$ est l'inverse de x. *L'inverse de x est donc élément de K.*

   Conclusion : $\underline{K \text{ est un sous-corps de } \mathbf{R}.}$

Deuxième partie CAS GÉNÉRAL :

Soit a un réel.

1. Soit K_0 un sous-corps de $\mathbf{R}$. Il contient 1, donc, étant stable par somme et différence il contient $\mathbf{Z}$. K_0 étant stable par passage à l'inverse et multiplication il contient $\mathbf{Q}$.
2. Soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a. Soit $\mathbf{Q}(a)$, l'intersection de tous les éléments de $\mathcal{K}$:

   $$\mathbf{Q}(a) = \bigcap_{K\in\mathcal{K}} K.$$

   - $\mathbf{Q}(a)$ est un sous-corps de $\mathbf{R}$ comme intersection non vide ($\mathbf{R} \in \mathcal{K}$) de sous-corps.
   - Pour tout élément K de $\mathcal{K}$, $a \in K$, donc $a \in \mathbf{Q}(a)$.
   - Soit K_0 un sous-corps de $\mathbf{R}$ qui contient a, par définition de $\mathcal{K}$, $K_0 \in \mathcal{K}$ donc

   $$\mathbf{Q}(a) = \bigcap_{K\in\mathcal{K}} K \subset K_0.$$

   Donc l'ensemble $\mathcal{K}$ des sous-corps de $\mathbf{R}$ qui contiennent a,
   admet $\underline{\mathbf{Q}(a) \text{ comme plus petit élément pour l'inclusion}}$.
3. Soient P et Q des éléments de $\mathbf{Q}[X]$, λ et μ des rationnels.
   - $\phi(\lambda P + \mu Q) = (\lambda P + \mu Q)(a) = \lambda P(a) + \mu Q(a) = \lambda\phi(P) + \mu\phi(Q)$.
   - $\phi(P \times Q) = (P \times Q)(a) = P(a) \times Q(a) = \phi(P) + \phi(Q)$.
   - $\phi(1) = 1$.

   Donc ϕ est $\underline{\text{un morphisme de la } \mathbf{Q}\text{-algèbre } \mathbf{Q}[X] \text{ dans la } \mathbf{Q}\text{-algèbre } \mathbf{R}}$.
4. D'après la question précédente, ϕ induit notamment un morphisme de l'anneau $\mathbf{Q}[X]$ sur l'anneau $\mathbf{R}$. I en est le *noyau*, c'est donc $\underline{\text{un idéal de } \mathbf{Q}[X]}$.

5. • Hypothèse : I non réduit à 0.
   Il existe donc un polynôme P élément de $\mathbf{Q}[X]$, non nul tel que $P(a) = 0$. Notons d le degré de P et pour $i = 0, 1, \dots, d$, a_i sont coefficient de degré i. Pour tout $i \in \{0, 1, \dots, n\}$, a_i s'écrit $\frac{p_i}{q_i}$, avec $p_i \in \mathbf{Z}$ et $q_i \in \mathbf{N}^*$. Posons $\delta = q_0 \times q_1 \times \cdots \times q_d$. δP est un polynôme non nul à coefficients entiers et $(\delta P)(a) = 0$. Donc a *est algébrique.*
   • Hypothèse : a est algébrique.
   Donc a est racine d'un polynôme P non nul à coefficients entiers. Donc I admet P comme élément et I *est non réduit à* 0.

   Donc a est algèbrique si et seulement si I est non réduit à $\{0\}$.

6. I est un idéal de $\mathbf{Q}[X]$, donc, d'après le programme, il existe P élément de $\mathbf{Q}[X]$ (appelé générateur de I), tel que $I = P\mathbf{Q}[X]$, I étant non nul, $P \neq 0$. Soit $\tilde{P}$ un générateur de I. $\tilde{P} \in I$ donc $P|\tilde{P}$. par symétrie des rôles $\tilde{P}|P$ donc $\tilde{P}$ et P sont associés. Les générateurs de I sont associés, il en existe donc un et un seul unitaire, μ_a, qui est défini par $\mu_a = a^{-1}P$, avec a le coefficient dominant de P.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. $A(a)B(a) = \mu_a(a) = 0$. L'intégrité de $\mathbf{Q}$ assure donc que $A(a)$ ou $B(a)$ est nul. Prenons par exemple $A(a)$ nul. Alors $A \in I$ donc $\mu_a|A$, or $A|\mu_a$ donc A et μ_a sont associés et donc B est de degré 0. Donc μ_a est irréductible.

   Supposons que $\mathrm{d}^\circ\mu_a \leq 1$. $\mathrm{d}^\circ\mu_a \neq -\infty$ (I non nul) et $\mathrm{d}^\circ\mu_a \neq 0$ car $\mu_a(a) = 0$, donc $\mathrm{d}^\circ\mu_a = 1$. Il existe donc s et t rationels tels que $s \neq 0$ et $\mu_a = sX + t$. De $\mu_a(a) = 0$ on déduit $a = -\frac{t}{s}$, et donc $a \in \mathbf{Q}$. Par contaposition :
   si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2.

   L'élément de $\mathbf{Q}[X]$, $X^2 - 2$ admet $\sqrt{2}$ comme racine. Donc $X^2 - 2|\mu_{\sqrt{2}}$. Or $\sqrt{2}$ est notoirement irrationnel donc, comme on vient de le voir, $\mathrm{d}^\circ\mu_{\sqrt{2}} \geq 2$. Donc $X^2 - 2$ qui est unitaire est égal à $\mu_{\sqrt{2}}$.

$$\mu_{\sqrt{2}} = X^2 - 2.$$

   Maintenant $a = \sqrt{\frac{1+\sqrt{5}}{2}}$. L'élément de $\mathbf{Q}[X]$, $X^4 - X^2 - 1$ admet a comme racine. Donc $\mu_a|X^4 - X^2 - 1$. Montrons que $X^4 - X^2 - 1$ est irréductible dans $\mathbf{Q}[X]$. Supposons qu'il existe A et B éléments de $\mathbf{Q}[X]$ tels que :

$$X^4 - X^2 - 1 = AB.$$

   En notant $a' = \sqrt{\frac{-1+\sqrt{5}}{2}}$. $X^4 - X^2 - 1$ admet quatre racines complexes, $a, -a, ia', -ia'$. $\sqrt{5}$ étant irrationnel, on montre qu'aucune de ses racines n'est rationnelle, donc ni A ni B n'est de degré 1. Supposons que $\mathrm{d}^\circ A = 2$ et donc $\mathrm{d}^\circ B = 2$. L'un des deux polynômes A et B, disons pour fixer les idées A, admet ia' comme racine, étant à coefficients rationnels donc réels, il admet aussi comme racine $\overline{ia'} = -ia'$. Donc il existe $c \in \mathbf{R}^*$, tel que $A = c(X^2 - \frac{1-\sqrt{5}}{2})$. A étant à coefficients rationnels, c est rationnel, mais alors $c\frac{1-\sqrt{5}}{2}$ est rationnel ce qui conduit à la rationnalité de $\sqrt{5}$, ce qui est faux. Donc finalement un des polynômes A et B est de degré 0, et donc $X^4 - X^2 - 1$ est *irréductible*.
   Donc μ_a, diviseur de $X^4 - X^2 - 1$ est associé à $X^4 - X^2 - 1$. Ces deux polynômes étant unitaires ils sont égaux :

$$\mu_a = X^4 - X^2 - 1.$$

7. $\mathbf{Q}[a]$ est l'image par le morphisme d'anneaux ϕ de l'anneau $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-anneau* de $\mathbf{R}$. Comme $\mathbf{R}$ est un corps, l'anneau $\mathbf{Q}[a]$ est *commutatif et non trivial*. Soit x un élément non nul de $\mathbf{Q}[a]$. Il existe $P \in \mathbf{Q}[X]$ tel que $x = P(a)$. La division euclidienne de P par μ_a conduit à l'existence de Q et R éléments de $\mathbf{Q}[X]$ tels que : $P = Q\mu_a + R$ et $\mathrm{d}^\circ R < \mathrm{d}^\circ\mu_a$. D'où $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$. x étant non nul, R est non nul, Donc μ_a ne saurait divisé R, polynôme dont le degré est inférieur au sien. Or μ_a est irréductible dans $\mathbf{Q}[X]$ (cf. 6.), donc R et μ_a sont premiers entres eux dans $\mathbf{Q}[X]$. Le lemme de Bezout affirme donc l'existence de deux éléments U et V de $\mathbf{Q}[X]$ tels que $UR + V\mu_a = 1$. En substituant a à l'indéterminé X, on obtient :

$$1 = U(a)R(a) + V(a)\mu_a(a) = U(a)x.$$

   Donc $U(a) = x^{-1}$ et donc $x^{-1} \in \mathbf{Q}[a]$. Autrement dit $\mathbf{Q}[a]$ est *stable par passage à l'inverse.*

   Conclusion : $\mathbf{Q}[a]$ est un corps.

$\mathbf{Q}[a]$ est un corps qui contient a. Donc $\mathbf{Q}(a) \subset \mathbf{Q}[a]$
Soit Soit x un élément de $\mathbf{Q}[a]$. Il sécrit

$$x = \sum_{i=0}^{n} c_i a^i,$$

avec n un naturel et $c_0, c_1, \dots, c_n$ des rationnels. le corps $\mathbf{Q}(a)$ contenant 1 et a et étant stable par multiplication, il contient a^i, pour $i = 0, 1 \dots, n$. Par ailleurs $c_i \in \mathbf{Q}(a)$ (cf. 1.). Donc le corps $\mathbf{Q}(a)$ étant stable par multiplication est addition, il contient $\sum_{i=0}^{n} c_i a^i = x$. Donc $\mathbf{Q}[a] \subset \mathbf{Q}(a)$.

CONCLUSION : $\mathbf{Q}(a) = \mathbf{Q}[a]$. $\mathbf{Q}[a]$ est l'image par ϕ, morphisme de $\mathbf{Q}$-espaces vectoriels, de l'espace vectoriel $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-espace vectoriel* du Q-espace vectoriel $\mathbf{R}$. En raisonnant comme dans le début de la question on montre que tout élément x de $\mathbf{Q}[a]$ est de la forme $x = R(a)$ où R est un élément de $\mathbf{Q}[X]$, de degré inférieur strictement à n, degré de μ_a. En notant c_i le coefficient d'ordre i de R, pour $i = 0, 1, 2 \dots, n-1$, x s'écrit :

$$x = \sum_{i=0}^{n-1} c_i a^i.$$

Donc $\mathbf{Q}[a] \subset \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \dots, a^{n-1})$. L'inclusion inverse étant évidente,

$$Q[a] = \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \dots, a^{n-1}).$$

la famille *la famille $(a^0, a^1, \dots, a^{n-1})$ engendre donc* $\mathbf{Q}[a]$.

Montrons que la famille $(a^0, a^1, \dots, a^{n-1})$ est libre. Soient $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ des rationnels tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \dots + \lambda_{n-1} a^{n-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda_0 X^0 + \lambda_1 X^1 + \dots + \lambda_{n-1} X^{n-1}$. Supposons C non nul. Alors par division euclidienne : $\mu_a = \tilde{Q}C + R$ avec $\tilde{Q} \in \mathbf{Q}[X]$, $R \in \mathbf{Q}[X]$ et $\mathrm{d}^{\circ} R \leq n-1$. En substituant dans cette égalité a à l'indéterminée, il vient $0 = R(a)$. Donc $R(a)$ est élément de I, il est donc divisible par μ_a, mais son degré étant inférieur strictement à celui de μ_a, c'est qu'il est nul. Donc C divise μ_a. Mais μ_a étant irréductible C est constant non nul, ce qui contredit $C(a) = 0$. Donc C est nul, c'est-à-dire : $\lambda_0 = \lambda_0 = \dots = \lambda_{n-1} = 0$. D'où la liberté de $(a^0, a^1, \dots, a^{n-1})$.

Finalement $(a^0, a^1, \dots, a^{n-1})$ est une base de $\mathbf{Q}[a]$, qui est donc de dimension n.

8. Supposons que la famille $(a_i)_{i \in \mathbf{N}}$ soit liée. Montrons qu'alors a est algèbrique. Par hypothèse il existe $m \in \mathbf{N}$, $\lambda_0, \lambda_1, \dots, \lambda_{m-1}$ des rationnels non tous nuls, tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \dots + \lambda_{m-1} a^{m-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$,

$$D = \lambda_0 X^0 + \lambda_1 X^1 + \dots + \lambda_{m-1} X^{m-1}.$$

D est non nul et $D \in I$, donc d'après 5., a est algébrique. Par contraposée, si a est non algébrique, alors la famille d'éléments de $\mathbf{Q}(a)$, $(a_i)_{i \in \mathbf{N}}$ est libre et donc $\mathbf{Q}(a)$ est de dimension infinie.

Quatrième partie : Corps finis

1. Supposons p nul, alors φ est injectif et réalise donc une bijection de $\mathbf{Z}$ sur $\varphi(\mathbf{Z})$, ensemble qui est donc infini. Donc *a fortiori* F est infini.

   Dans toute la suite on supposera que F est fini, donc que p est non nul.

2. • Analyse. Supposons qu'une application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ satisfasse $\varphi = \tilde{\varphi} \circ \pi_p$.
   Alors nécéssairement pour $k = 0, 1, ..., p-1$ on a $\tilde{\varphi}(\bar{k}) = \varphi(k)$.
   • Synthèse. Soit $\tilde{\varphi} \;:\; \mathbf{Z}/p\mathbf{Z} \to \mathbf{F}$ qui est définie par
   $$\forall k \in [\![0, p-1]\!]\,; \tilde{\varphi}(\bar{k}) = \varphi(k).$$
   Soit alors un entier x. Notons k le représentant de $\bar{x}$ élément de $[\![0, p-1]\!]$. Alors
   $$k - x \in p\mathbf{Z} = \ker(\varphi).$$
   Donc
   $$\tilde{\varphi}(\pi_p(x)) = \tilde{\varphi}(\bar{k}) = \varphi(k) = \varphi(x + (k-x) = \varphi(x) + \varphi(k-x) = \varphi(x) + O_{\mathbf{F}} = \varphi(x).$$
   Donc on a bien $\varphi = \tilde{\varphi} \circ \pi_p$.
   Finalement il existe une et une seule application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ satisfaisant $\varphi = \tilde{\varphi} \circ \pi_p$.

3. Montrer que $\tilde{\varphi}$ est un morphisme d'anneaux injectif. (facile)

4. Comme $\tilde{\varphi}$ est un morphisme d'anneau $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ et comme $\tilde{\varphi}$ est injectif il induit un isomorphisme d'anneaux de $\mathbf{Z}/p\mathbf{Z}$ sur $\tilde{\varphi}\,(\mathbf{Z}/p\mathbf{Z})$, autrement dit :

   $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ isomorphe à $\mathbf{Z}/p\mathbf{Z}$.
   L'intégrité du corp $\mathbf{F}$ assure celle de l'anneau $\mathbf{k}$, donc par isomorphisme celle de l'anneau $\mathbf{Z}/p\mathbf{Z}$. Donc p est un nombre premier.

5. Comme p est premier, voilà que $\mathbf{Z}/p\mathbf{Z}$ est un corps et donc $\mathbf{k}$ qui lui est isomorphe itou.
   Mais tout sous-corps de $\mathbf{F}$ contient $1_{\mathbf{F}}$ et, par stabilité par addition et passage à l'opposé, $\varphi(Z)$. Or
   $$\mathbf{k} = \tilde{\varphi}\,(\mathbf{Z}/p\mathbf{Z}) = \varphi(\pi_p(\mathbf{Z})) = \varphi(\mathbf{Z}).$$
   Donc le sous-corps $\mathbf{k}$ est le plus petit sous corps de $\mathbf{F}$.

6. On muni $\mathbf{F}$ de sa structure naturelle de $\mathbf{k}$-espace vectoriel (l'oppération de $\mathbf{k}$ sur $\mathbf{F}$ est t simplement la retsriction à $\mathbf{k} \times \mathbf{F}$ de la multiplication du corps $\mathbf{F}$).
   Comme $\mathbf{F}$ est fini et non réduit à $\{0_{\mathbf{F}}\}$, l'espace vectoriel $\mathbf{F}$ sur $\mathbf{k}$ est de dimension n non nulle finie. Donc $\mathbf{F}$ est isomorphe $\mathbf{k}^n$, un isomorphisme pouvant être l'application coordonnée dans une base.
   Donc $\boxed{|\mathbf{F}| = |\mathbf{k}|^n = p^n}$.