



## DM n°7

## PREMIER EXERCICE

*Il s'agit d'un résultat classique à connaître*

## Cryptographie

*Le but de ce problème est l'étude du principe de cryptage RSA, qui permet de communiquer de façon sûre des données. Ce résultat est à connaître*

## 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*

- Donner sans démonstration, en fonction de  $p$  et  $q$ , la valeur de  $\varphi(n)$ .
- Soit  $e$  un entier premier avec  $\varphi(n)$ . On appelle  $e$  *exposant de chiffrement*. Montrer qu'il existe un entier naturel  $d$  tel que  $ed \equiv 1 \pmod{\varphi(n)}$

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  $\{0, 1, \dots, n-1\}$  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*  $(n, d)$ .

- Montrer que  $M^{ed}$  est congru à  $M$  modulo  $p$ . On distinguera les deux cas  $M$  premier avec  $p$  et  $M$  non premiers avec  $p$ .
- En déduire que  $C^d \equiv M \pmod{n}$ .

**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 connaître  $\varphi(n)$  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 (3/2 : 1., 2., 3., 4. et 5. ; 5/2 : tout )

## 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.  $\varphi : \mathbf{Z}[i] \rightarrow \mathbf{N}$ ;  $a \mapsto \bar{a}a$ .

- Montrer que  $\mathbf{Z}[i]$  est un sous-anneau du corps  $\mathbf{C}$ .
- Déterminer  $\mathbf{Z}[i]^*$ , ensemble des éléments inversibles de  $\mathbf{Z}[i]$ .
- 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  $\varphi$ .
- Montrer que tout idéal de  $\mathbf{Z}[i]$  est de la forme  $a\mathbf{Z}[i]$ , on dit que  $\mathbf{Z}[i]$  est principal.
- 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.
- 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  $z^2 = y$ .

- 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.  $p \equiv 3 \pmod{4}$  ;
  - 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 $\mathbf{Q}$ (3/2)

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  $\omega$ .
2. Soit  $\mathbf{K}$  le  $\mathbf{Q}$ -espace vectoriel engendré par  $(\omega^i)_{i \in \mathbf{N}}$ .  
Montrer que  $\mathbf{K}$  est de dimension finie, et donner une base simple de  $\mathbf{K}$ .
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 $\mathbf{Q}$ (5/2)

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  $\phi : \mathbf{Q}[X] \rightarrow \mathbf{R}; P \mapsto P(a)$  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 algébrique si et seulement si  $I$  est non réduit à  $\{0\}$ .  
**Dans cette partie on suppose dans la suite que  $a$  est algébrique, sauf à la dernière question.**
6. Montrer qu'il existe un et un seul élément de  $\mathbf{Q}[X]$  unitaire,  $\mu_a$ , tel que  $I = \mu_a \mathbf{Q}[X]$ .  
Montrer que  $\mu_a$  est irréductible dans  $\mathbf{Q}[X]$ . Montrer que si  $a$  est irrationnel, alors le degré de  $\mu_a$  est supérieur ou égal à 2. Déterminer  $\mu_a$  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  $\mu_a$ , 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<sup>1</sup>.

### Troisième partie : CORPS FINIS (5/2) (3/2)

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

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

est un morphisme d'anneaux.

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

---

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

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

**Dans toute la suite on supposera que  $\mathbf{F}$  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  $\pi_p$  désigne la surjection (dite canonique) de  $\mathbf{Z}$  sur  $\mathbf{Z}/p\mathbf{Z}$ , qui à un entier  $x$  associe sa classe modulo  $p$ .
3. Montrer que  $\tilde{\varphi}$  est un morphisme d'anneaux injectif.
4. On note  $\mathbf{k} = \tilde{\varphi}(\mathbf{Z}/p\mathbf{Z})$ . 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 le DM 1-ter.

## 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 que  $u + k\varphi(n)$  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 entier  $h$  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  $M^{ed} \equiv M [p]$ .Dans tous les cas  $M^{ed} \equiv M [p]$ (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  $C^d \equiv M [n]$ .

## Entiers de Gauss

1. Sans problème.
2. Si  $Z$  est inversible dans  $\mathbf{Z}[i]$ , alors  $\varphi$  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 entiers 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 éléments  $z$  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.  $\implies$  ii.  
On raisonne par l'absurde si ii. est faux,  $-1$  s'écrit  $a^2 + kp$  et donc  $p$  divise dans  $\mathbf{Z}[i]$   $(a+i)(a-i)$ , absurde!  
ii.  $\implies$  iii.  
Par l'absurde, si  $p = \alpha^2 + \beta^2$  on a pas ii. en regardant la congruence modulo 4 d'un carré.  
iii.  $\implies$  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 montré que les entiers premiers congrus à 3 modulo 4 et les entiers de Gauss  $a$  tels que  $\phi(a)$  soit premier sont irréductibles.  
Montrer que ce sont les seuls, à un inversible près... On prendra un irréductible  $a$  et on raisonnera sur les diviseurs premiers  $p$  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  $\omega$ .

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 que  $\mathbf{K}$  est le  $\mathbf{Q}$ -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  $\lambda, \mu$  et  $\nu$  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  $\omega$  à l'indéterminée, il vient  $0 = u\omega + v$ . Comme  $\omega$  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  $\mathbf{Q}[X]$ , 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,  $\phi$  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,  $\mu_a$ , qui est défini par  $\mu_a = a^{-1}P$ , avec  $a$  le coefficient dominant de  $P$ .

$\mu_a(a) = 0$ , donc  $\mu_a$  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  $\mu_a$  Donc  $\mu_a$  est irréductible.

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

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

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

$$\underline{\mu_a = X^4 - X^2 - 1.}$$

6.  $\mathbf{Q}[a]$  est l'image par le morphisme d'anneaux  $\phi$  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  $\mu_a$  conduit à l'existence de  $Q$  et  $R$  éléments de  $\mathbf{Q}[X]$  tels que :  $P = Q\mu_a + R$  et  $\deg R < \deg \mu_a$ . D'où  $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$ .  $x$  étant non nul,  $R$  est non nul, Donc  $\mu_a$  ne saurait diviser  $R$ , polynôme dont le degré est inférieur au sien. Or  $\mu_a$  est irréductible dans  $\mathbf{Q}[X]$  (cf. 6.), donc  $R$  et  $\mu_a$  sont premiers entres eux dans  $\mathbf{Q}[X]$ . Le lemme de Bezout permet de montrer l'inversibilité de  $x$ .

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  $x$  un élément de  $\mathbf{Q}[a]$ . Il s'écrit

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

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 et 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  $\phi$ , morphisme de  $\mathbf{Q}$ -espaces vectoriels, de l'espace vectoriel  $\mathbf{Q}[X]$  (cf. 3.), c'est donc un *sous-espace vectoriel* du  $\mathbf{Q}$ -espace vectoriel  $\mathbf{R}$ . En raisonnant comme dans le début de la question on montre que

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

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

On montre 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  $\deg R \leq n-1$ . Reste à montrer la nullité de  $R$ ...

Finalement  $(a^0, a^1, \dots, a^{n-1})$  est une base de  $\mathbf{Q}[a]$ , 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 (5/2) (3/2)

1. Montrer que si  $p$  est nul alors  $\varphi$  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  $\pi_p$  désigne la surjection (dite canonique) de  $\mathbf{Z}$  sur  $\mathbf{Z}/p\mathbf{Z}$ , 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 quantité 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!