DM Bis n° 12

Pour les $\frac{5}{2}$ candidats aux ENS et à l'X, éventuellement pour quelques 3/2

Les deux premières parties sont consacrées à l'étude d'extensions du corps $\mathbf{Q}$, c'est-à-dire de sur-corps de $\mathbf{Q}$. La troisième partie définit de façon abstraite la construction d'extentions d'un corps quelconque. La quatième partie étudie les corps finis en utilisant notamment les résultats de la partie précédente, enfin le devoir s'achève par le dénombrement de polynômes iréductibles sur $\mathbf{Z}/p\mathbf{Z}$, permettant de prouver un résultat admis dans la quatrième.

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 : Extension de corps

$\mathbf{K}$ désigne un corps et P_0 un élément de $\mathbf{K}[X]$ *irréductible*. On rappelle qu'un élément P de $\mathbf{K}[X]$ est irréductible si :

— il est non inversible ;

— pour tout couple (A, B) d'éléments de $\mathbf{K}[X]$, tel que $P = AB$, A ou B est inversible.

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

Enfin $\mathfrak{I}$ désignera l'idéal engendré par P_0,

$$\mathfrak{I} = P_0\mathbf{K}[X]$$

On définit sur $\mathbf{K}[X]$ la relation $\mathcal{R}$ définie par : pour tout P et tout Q éléments de $\mathbf{K}[X]$, $P\mathcal{R}Q$ si $P-Q \in \mathfrak{I}$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
   On notera $\bar{P}$ la classe d'équivalence d'un élément P de $\mathbf{K}[X]$ et $\mathbf{K}[X]/\mathfrak{I}$ l'ensemble des classes d'équivalences.
2. Montrer que l'on peut définir deux lois internes $+$ et $\times$ sur $\mathbf{K}[X]/\mathfrak{I}$ telles que pour tout couple (P,Q) d'éléments de $\mathbf{K}[X]$
   $$\bar{P}+\bar{Q} = \overline{P+Q} \text{ et } \bar{P}\times\bar{Q} = \overline{P\times Q}$$
3. Montrer sommairement que $(\mathbf{K}[X]/\mathfrak{I}, +, \times)$ est un anneau commutatif et que l'application
   $$\pi : \mathbf{K}[X] \to \mathbf{K}[X]/\mathfrak{I}\,;\ P \mapsto \bar{P}$$
   est un morphisme d'anneaux
4. Montrer que $\mathbf{K}[X]/\mathfrak{I}$ peut être muni d'une structure de $\mathbf{K}$-algèbre qui fasse de π un morphisme d'algèbres.
5. Déterminer la dimension de la $\mathbf{K}$-algèbre $\mathbf{K}[X]/\mathfrak{I}$ en fonction du degré de P_0 et en donner une base.
6. *Exemple* — Dans cette question on prend pour $\mathbf{K}$ le corps des réels et pour P_0 le polynôme X^2+1. A quel corps est isomorphe $\mathbf{R}[X]/\mathfrak{I}$

Quatrième partie : Corps finis

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 et au programme de MP suivant :
L'application

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

est un morphisme d'anneaux.

Son noyau est donc un sous groupe de $(\mathbf{Z},+)$, donc de la forme 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 $\mathbf{k} = \tilde{\varphi}(\mathbf{Z}/p\mathbf{Z})$. 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.

   On se propose d'étudier la réciproque. On admettra le théorème suivant :
   Théorème : *Tout corps $\mathbf{K}$ admet un sur-corps $\bar{\mathbf{K}}$ tel que l'on ait :*
   — *$\bar{\mathbf{K}}$ est algébriquement clos ;*
   — *Tout élément de $\bar{\mathbf{K}}$ est racine d'un polynôme à coefficients dans $\mathbf{K}$ on dit est algébrique sur $\mathbf{K}$.*
   Un tel sur-corps $\bar{\mathbf{K}}$ est appelé cloture algébrique de $\mathbf{K}$.
   On a l'unicité de la cloture algébrique, en ce sens que deux clotures algébriques de $\mathbf{K}$ sont des corps isomorphes par un isomorphisme induisant sur $\mathbf{K}$ l'identité. On parle donc de LA *cloture algébrique d'un corps.*
   Par exemple $\mathbf{C}$ est la cloture algébrique de $\mathbf{R}$.

   Dans la suite p désigne un nombre premier, $\mathbf{F}_p$ désignera le corps $\mathbf{Z}/p\mathbf{Z}$ et n un entier naturel non nul. On pose $q = p^n$ et l'on va étudier l'existence d'un corps à q éléments.
7. On suppose provisoirement qu'il existe un élément de $\mathbf{F}_p[X]$ irréductile de degré n.

(a) Montrer en utilisant la partie précédente qu'il existe un corps à q élément $\mathbf{F}_q$ qui soit une $\mathbf{F}_p$ algèbre. Quelle est la caractéristique de $\mathbf{F}_q$. Dans la suite on identifira un élément a de $\mathbf{F}_p$ et l'élément $a \cdot 1_{\mathbf{F}_q}$, (1_{F_q} est l'unité de $\mathbf{F}_q$). En particulier on identifira $1_{\mathbf{F}_q}$ et l'élément de $\bar{1}$ de $\mathbf{F}_p$ et le sous-corps $\mathbf{F}_p \cdot 1_{\mathbf{F}_q}$ et $\mathbf{F}_p$.

(b) Montrer que $f \,:\, \mathbf{F}_q \to \mathbf{F}_q\,;\; x \mapsto x^p$ est morphisme de corps, on l'appelle morphisme de Frobenius.

(c) Montrer que tout élément x de $\mathbf{F}_q$ vérifie $x^q = x$.

(d) Montrer que $\mathbf{F}_q$ est l'ensemble des racines du polynôme $X^q - X$ qui est un élément de $\mathbf{F}_q[X]$ à coefficients dans $\mathbf{F}_p$.

On ne suppose plus l'existence d'un élément de $\mathbf{F}_p[X]$ irréductile de degré n.

8. Montrer que $\bar{\mathbf{F}}_p$ admet un et un seul sous-corps à q éléments, on le notera $\mathbf{F}_q$. On étudira le polynôme $X^q - X$.
9. Donner la structure du groupe aditif de $\mathbf{F}_4$ et du groupe multiplicatif $(F_4^*, \times)$

Cinquième partie : Polynômes irréductibles de $\mathbf{F}_p[X]$

1. Montrer que pour tout entier naturel $m \geq 1$, $\mathbf{F}_{p^m}$ est un sous-corps de $\mathbf{F}_{p^n}$ si et seulement si m divise n.
2. *Formule d'inversion de Moebius* —
Pour tout élément n de $\mathbf{N}^*$, $\mathcal{D}_n$ désigne l'ensemble des diviseurs positifs de n. On munit $\mathcal{F}(\mathbf{N}^*, \mathbf{Z})$, ensemble des applications de $\mathbf{N}^*$ dans $\mathbf{Z}$, de la loi de composition interne $\star$ définie par,

$$f \star g \;:\; \mathbf{N}^* \to \mathbf{Z}\,;\; n \mapsto \sum_{d \in \mathcal{D}_n} f(d) g\left(\frac{n}{d}\right),$$

pour tout couple (f, g) d'éléments de $\mathcal{F}(\mathbf{N}^*, \mathbf{Z})$.

(a) Montrer que la loi $\star$ est commutative, associative et admet pour élément neutre l'application

$$e \;:\; \mathbf{N}^* \to \mathbf{Z}\,;\; n \mapsto \begin{cases} 1, & \text{pour } n = 1, \\ 0, & \text{sinon.} \end{cases}$$

(b) Soit l'application μ de $\mathbf{N}^*$ dans $\mathbf{Z}$ définie ainsi :
— $\mu(1) = 1$,
— pour tout entier $n \geq 2$ de décomposition en facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, où les $\alpha_i,\ i = 1 \ldots k$ sont non nuls $\mu(n)$ vaut zéro si l'un des α_i est supérieure ou égal à 2 et $\mu_n = (-1)^k$ si tous les α_i sont égaux à 1.
Montrer que

$$\sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 & \text{pour } n = 1, \\ 0 & \text{sinon.} \end{cases}$$

(c) Soient f et g des applications de $\mathbf{N}^*$ dans $\mathbf{Z}$ telles que pour tout entier $n \geq 1$,

$$g(n) = \sum_{d \in \mathcal{D}_n} f(d).$$

Déduire des questions précédentes que pour tout $n \in \mathbf{N}^*$,

$$f(n) = \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) g(d).$$

Remarque : Cette formule donne pour tout entier $n \geq 1$, d'exprimer $\varphi(n)$, (φ désigne de l'indicatrice d'Euler) :

$$\varphi(n) = \sum_{d \in \mathcal{D}_n} d\mu\left(\frac{n}{d}\right).$$

Pour tout entier $m \geq 1$, I_m désigne le nombre de polynômes, de $\mathbf{F}_p[X]$ irréductibles, unitaires, de degré m.

3. Par n on désigne toujours un entier naturel non nul. Soit Q un facteur irréductible de $X^{p^n} - X$ de degré d et α une racine de Q dans $\bar{\mathbf{F}}_p$. Montrer que le $\mathbf{F}_p$-espace vectoriel engendré par $(\alpha,^0, \alpha^1 \ldots, \alpha^{d-1})$ est un sous-corps de $\mathbf{F}_{p^n}$ et un espace vectoriel de dimension d. En déduire que $d|n$ et $\alpha \in \mathbf{F}_{p^n}$.

4. Soit Q' un polynôme irréductible de $\mathbf{F}_p$ dont le degré d divise n. Montrer que Q' divise $X^{p^n} - X$.
5. Prouver que :
$$p^n = \sum_{d \in \mathcal{D}_n} dI_d.$$
En déduire que :
$$I_n = \frac{1}{n} \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) p^d.$$
6. En déduire qu'il existe au moins un polynôme irréductible de $\mathbf{F}_p$ de degré n.