TD n°6.

1 Modules sur un anneau principal

Exercice 1. Soit A un anneau principal. Soit M un A-module. Soit K le corps de fractions de A. On munit $\mathrm{Hom}_A(M, K/A)$ de la structure de A-module définie par $(af + bg)(x) = af(x) + bg(x)$. On note $M_K = S^{-1}A$ où $S = A - \{0\}$ (c'est un K-esapce vectoriel). Soit $j : M \to M_K$ l'application définie par $j(m) = m/1$.

a) Soit N un sous-module de M et $f : N \to K/A$ un application A-linéaire. On veut prolonger f en une application linéaire $M \to K/A$ (et donc montrer que K/A est un A-module injectif).
   i) Soit E l'ensemble des couples (N', ϕ) où N' est un sous-module de M contenant N et $\phi : N' \to K/A$ est une application linéaire telle que $\phi_{|N} = f$. On muni E de la relation d'ordre $(N_1, \phi_1) \leq (N_2, \phi_2)$ ssi $N_1 \subset N_2$ et $\phi_{2,|N_1} = \phi_1$. Montrer que E admet un élément maximal (N_0, ϕ_0).
   ii) Soit $x \in M$ et $N_1 = N_0 + (x)$. On note $I = \{a \in A, ax \in N_0\}$. Soient b un générateur de I. Montrer qu'il existe un morphisme A-linéaire $\psi : A \to K/A$ tel que $\psi(b) = \phi_0(bx)$.
   iii) Montrer qu'il existe un unique morphisme $\phi_1 : N_1 \to K/A$ tel que $\phi_1(n + ax) = \phi_0(n) + \psi(a)$ pour tout $(n, a) \in N_0 \times A$.
   iv) En déduire que $N_0 = M$ et conclure.

b) On note $T(M) := \{x \in M : \exists a \in A - \{0\}, ax = 0\}$. Montrer que $\mathrm{Ker}(j) = T(M)$. On dit que M est sans torsion si $T(M) = 0$ et que M est de torsion si $T(M) = M$. Montrer que $M/T(M)$ est sans torsion.

c) On suppsose que M est de torsion. Si p est un élément irréductible de A, on note $M(p) := \{x \in M : \exists n \in \mathbb{N}, p^n x = 0$. Montrer que si $\mathfrak{P}$ est un système de représentants d'irréductibles de A, $M = \bigoplus_{p \in \mathfrak{P}} M(p)$.

d) Soit p un élément irréductible. On suppose $M(p) = M$ et M de type fini.
   i) Montrer qu'il existe $k \in \mathbb{N}$ tel que $\mathrm{Ann}(M) = (p^k)$ et qu'il existe $x \in M$ tel que $\mathrm{Ann}(x) = (p^k)$.
   ii) Montrer qu'il existe $f \in \mathrm{Hom}(M, K/A)$ tel que $f(x)$ soit la classe de $1/p^k$.
   iii) Montrer que $M = (x) \oplus \mathrm{Ker}(f)$.
   iv) En déduire qu'il existe $k_0 = k \geq k_1 \geq \cdots \geq k_n$ et un isomorphisme $M \simeq \bigoplus_{i=0}^{n} A/(p^{k_i})$.

e) i) On suppose que M est de type fini et que M est sans torsion. On identifie M à un sous-A-module de M_K. Soit $x \neq 0 \in M_K$ et $M_1 = M \cap Kx$. Montrer que M_1 est un sous-A-module de M isomorphe à A (on pourra montrer que tout sous-A-module de type fini de K est monogène) et que M/M_1 est sans torsion.
   ii) Montrer qu'il existe une suite de sous-module de M : $0 = M_0 \subset M_1 \subset \cdots \subset M_{k-1} \subset M_k = M$ tel que $M_i/M_{i-1} \simeq A$.
   iii) Soit $x \in M$ dont l'image engendre M_k/M_{k-1}. Montrer que $M = M_{k-1} \oplus (x)$. En déduire que M est un A-module libre.

f) On suppose seulement que M est de type fini. Montrer qu'il existe $n \in \mathbb{N}$ et $d_1 | \cdots | d_k \neq 0$ dans A tel que $M \simeq A^n \oplus \bigoplus_{i=1}^{k} A/(d_i)$

Exercice 2. Soit k un corps, V un k-espace vectoriel de dimension fini et $f \in \mathrm{Hom}_k(V, V)$ un endomorphisme k-linéaire de V.

a) Montrer que $P \cdot v = P(f)(v)$ pour $(P, v) \in k[X] \times V$ définit une structure de $k[X]$-module sur V.

b) Montrer que V est un $k[X]$-module de type fini et de torsion. Déduire de l'exercice 1 un isomorphisme $V \simeq \bigoplus_{p \in \mathfrak{P}} \bigoplus_{i=0}^{n_p} k[X]/p^{k_{p,i}}$ de $k[X]$-modules, où $\mathfrak{P}$ est un ensemble fini d'éléments irréductibles de $k[X]$.

c) On suppose k algébriquement clos. Montrer qu'il existe une k-base B de V tel que la matrice de f dans la base B soit une matrice de Jordan.

2 Entiers algébriques

Exercice 3. Montrer que dans $\mathbb{Z}[\sqrt{-5}]$, 3, 7, $2+\sqrt{-5}$, $4+\sqrt{-5}$ sont irréductibles.
Montrer que la décomposition de 21 en facteurs irréductibles dans $\mathbb{Z}[\sqrt{-5}]$ n'est pas unique ($\mathbb{Z}[\sqrt{-5}]$ n'est pas *factoriel*).

Solution. Les équations $a^2+5b^2)=3$ et $a^2+5b^2=7$ n'ont pas de solutions, donc il n'y a pas d'élément de $\mathbb{Z}[\sqrt{-5}]$ de norme 3 ou 7. En particulier, si z est de norme 9, 21 ou 49, un diviseur propre non inversible de z devrait être de norme 3 ou 7 : z est donc irréductible. Ici $N(3)=N(2+\sqrt{-5})=9$, $N(7)=49$ et $N(4+\sqrt{-5})=21$.
On a $21=3\cdot 7=(4+\sqrt{-5})\cdot(4-\sqrt{-5})$ et l'on obtient deux décompositions en facteurs irréductibles.

Exercice 4. Montrer que, si z est un élément irréductible de $\mathbb{Z}[i]$, alors $N(z)$ est un nombre premier ou le carré d'un nombre premier.

Solution. Comme z est irréductible, $barz$ aussi (l'irréductibilité est invariante par automorphisme d'anneau, en particulier par conjugaison complexe). On a $z\bar{z}=N(z)$ et z et $\bar{z}$ sont irréductibles. Par unicité de la décomposition en facteur irréductibles, la décomposition en facteur premiers de $N(z)$ contient au plus deux éléments. Si elle n'en contient qu'un, alors $N(z)$ est premier. Si elle en contient deux, $N(z)=pq$, et p et q doivent être associés à z et $\bar{z}$. Comme $p^2=N(z)=N(\bar{z})=q^2$, on obtient $p=q$ et $N(z)=p^2$ comme voulu.

Exercice 5. Donner un polynôme unitaire de $\mathbb{Z}[X]$ annulant $\sqrt{2}+\sqrt{3}$.

Solution. On pose $x=\sqrt{2}+\sqrt{3}$. On a alors

$$x^2=5+2\sqrt{6}$$

$$(x^2-5)^2=24$$

Le polynôme $(X^2-5)^2-24$ convient donc.

On peut aussi appliquer l'algorithme donné dans la preuve du théorème disant que la somme de deux entiers algébriques est encore un entier algébrique, ce qui nous donne que $x=\sqrt{2}+\sqrt{3}$ vérifient

$$M\begin{pmatrix}1\\ \sqrt{2}\\ \sqrt{3}\\ \sqrt{6}\end{pmatrix}=x\begin{pmatrix}1\\ \sqrt{2}\\ \sqrt{3}\\ \sqrt{6}\end{pmatrix}$$

où

$$M=\begin{pmatrix}0&2&3&0\\ 1&0&0&3\\ 1&0&0&2\\ 0&1&1&0\end{pmatrix}.$$

En particulier le polynôme caractéristique de M convient.

Exercice 6. Parmi les nombres algébriques suivants, lesquels sont entiers ?

a) $\beta=\frac{\sqrt{11}+\sqrt{13}}{2}$,

b) $\gamma=\frac{\sqrt{5}+\sqrt{13}}{2}$,

c) $\delta=\frac{i+\sqrt{11}+\sqrt{13}}{2}$,

d) $\frac{1+\sqrt[4]{17}}{2}$.

Solution. a) On vérifie comme dans l'exercice précédent que si α était entier $\alpha'=\frac{1-\sqrt[4]{17}}{2}$ le serait aussi. Or $\alpha\alpha'=\frac{1-\sqrt{17}}{4}$, qui n'est pas entier d'après l'exercice précédent, donc α n'est pas entier.

b) On a $\beta^2=6+\frac{\sqrt{143}}{2}$, qui n'est pas entier d'après l'exercice précédent donc, β n'est pas entier.

c) $\gamma=\frac{\sqrt{5}+1}{2}+\frac{-1+\sqrt{13}}{2}$ est entier comme somme de deux entiers.

d) Si δ était entier, $\delta\bar{\delta}=\frac{25+2\sqrt{143}}{4}$ le serait aussi, or ce n'est pas le cas d'après l'exercice précédent.

3 Extensions finies de corps

Exercice 7. Montrer que pour tout corps K, il existe une infinité de polynômes unitaires irréductibles. En déduire que tout corps algébriquement clos est infini.

Solution. Si $P_1, \cdots P_n$ est une famille finie d'élément irréductible unitaire, alors $P_1 \cdots P_n + 1$ n'est divisible par aucun des P_i et n'est pas inversible : il existe donc un élément irréductible unitaire divisant $P_1 \cdots P_n + 1$ et donc distinct de tous les P_i.
Si K est algébriquement clos, les polynômes irréductibles unitaires sont les $X - a$ pour $a \in K$, et leur ensemble a donc le même cardinal que celui de K. Donc K est infini.

Exercice 8. Une extension finie de corps K/k est dite monogène s'il existe $x \in K$ tel que $K = k(x)$.

a) Montrer que toute extension de degré premier est monogène.

b) Soient K/k une extension et P un polynôme irréductible sur k. Montrer que si le degré de P est premier au degré de K/k, alors P est irréductible sur K.

c) Soient k un corps et x un élément algébrique sur k de degré impair. Montrer que $k(x^2) = k(x)$.

Solution. a) Soit $x \in K - k$. On a $k \subset k(x) \subset K$ donc $[k(x) : k] | [K : k] = p$. Comme $k(x) \neq k$, $[k(x) : k] \neq 1$, donc $[k(x) : k] = p$ donc $k(x) = K$.

b) Soit R un facteur irréductible de P dans $K[X]$. Soit $L = K[X]/R$ le corps de rupture de R et notons x la classe de X. Alors $R(x) = 0$ donc $P(x) = 0$. Comme P est irréductible sur k, $k(x)$ est le corps de rupture de x sur k, donc $degP = [k(x) : k] | [L : k] = [L : K][K : k]$. Comme $degP$ et $[K : k]$ sont premier entre eux, on obtient $degP | [L : K] = degR$ ce qui n'est possible que si R est associé à P.

c) On a $[k(x) : k(x^2)] \leq 2$ car x est racine de $X^2 - x^2 \in k(x^2)[X]$. Or $[k(x) : k(x^2)] | [k(x) : k]$ qui est impair donc $[k(x) : k(x^2)] \neq 2$. D'où l'égalité voulue.

Exercice 9. Déterminer le degré des extensions suivantes de $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}), \qquad \mathbb{Q}(i, \sqrt[4]{2}), \qquad \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}), \qquad \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \qquad \mathbb{Q}(i, \sqrt{2 + \sqrt{2}}).$$

Solution. On a $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ car $\sqrt{2}$ est racine de $X^2 - 2$ qui est irréductible (sinon on aurait $\sqrt{2} \in \mathbb{Q}$). Remarquons que $\sqrt{18} = 3\sqrt{2}$ est dans $\mathbb{Q}(\sqrt{2})$. Comme $\sqrt{-7})$ est racine de $X^2 + 7$, on a $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Or, comme $\sqrt{-7} \notin \mathbb{R}$ et $[\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, on a donc $\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) \neq \mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}(\sqrt{2})] = 2$ et $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}] = 4$ par multiplicativité.
On a $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(i, \sqrt[4]{2})$.
On a $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ comme précédemment.
On a $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] \leq 2$ car $\sqrt[4]{2}$ est racine de $X^2 - \sqrt{2}$. Si $\sqrt[4]{2} \in \mathbb{Q}(\sqrt{2})$, on aurait $(a + b\sqrt{2})^2 = \sqrt{2}$ avec $a, b \in \mathbb{Q}$, on obtient, en décomposant dans la base $1, \sqrt{2}$, $a^2 + 2b^2 = 0$ et $2ab = 1$, on obtient $a^4 = -1/2$ dans $\mathbb{Q}$ ce qui n'est pas possible. Donc $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$.
De même $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$, car i est solution de $X^2 - 1$. Comme $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ mais $i \notin \mathbb{R}$, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$.
Par multiplicativité, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.

Le polynome $X^3 - 2$ est irréductible sur $\mathbb{Q}$ car sinon il aurait un facteur de degré 1, et donc aurait une racine dans $\mathbb{Q}$ ce qui n'est pas le cas. Donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. De même $X^2 - 3$ est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Q}(\sqrt[3]{2})$ d'après exo 9.b. Donc $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, et donc le degré cherché est 6 par multiplicativité

On a $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. L'important est de savoir si $2+\sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Or $N(2+\sqrt{2}) = 2$, qui n'est pas un carré dans $\mathbb{Q}$, donc $2 + \sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2 + \sqrt{2}}) : \mathbb{Q}(\sqrt{2})] = 2$, et $[\mathbb{Q}(\sqrt{2 + \sqrt{2}}) : \mathbb{Q}] = 4$ par multiplicativité.

On a $\mathbb{Q}(\sqrt{2 + \sqrt{2}}) \subset \mathbb{R}$ et $i \notin \mathbb{R}$, donc comme précédemment $[\mathbb{Q}(i, \sqrt{2 + \sqrt{2}}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2 + \sqrt{2}}) : \mathbb{Q}] = 8$.

Exercice 10. Soit K une extension de k de degré 2.

a) On suppose que la caractéristique de k est différente de 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

b) On suppose que k est de caractéristique 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$ ou à $KkX]/(X^2 - X - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

Solution. Soit $x \in K \backslash k$. La famille $1, x$ est libre sur k donc $x^2 = bx + c$. En caractéristique différente de 2, on obtient $(x + b/2)^2 = c + b^2/4$. En posant $a = c + b^2/4$ et en envoyant X sur $x + b/2$, on obtient un morphisme $k[X]/(X^2 - a) \to K$, qui est un isomorphisme car $1, x + b/2$ forment une base de K sur k. Si $b \in k$ est un carré dans $k[X]/(X^2 - a)$, alors $b = (c + d\sqrt{a})^2$, et donc $2cd = 0$ et $b = c^2 + ad^2$. Donc soit b soit b/a est un carré dans k. Or si b est un carré $k[X]/(X^2 - a)$ n'est pas un corps. Donc $k[X]/(X^2 - a)$ et $k[X]/(X^2 - b)$ sont isomorphes si et seulement si b/a est un carré.
Notons y une racine de a dans K. Si σ est un automorphisme de K fixant k. On a $\sigma(y)^2 = \sigma(y^2) = \sigma(a) = a$ donc $\sigma(y)$ est y ou $-y$. Comme y engendre K, on obtient au plus deux automorphismes possibles. On vérifie facilement que $\sigma(e + fy) = e - fy$ définit bien un automorphisme

Exercice 11. On dit qu'un nombre algébrique x est constructible à la règle et au compas si il existe une tour d'extensions de corps

$$k_0 = \mathbb{Q} \subset k_1 \subset \cdots \subset k_n$$

avec $[k_{i+1} : k_i] = 2$ et $x \in k_n$.

a) Montrer que $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

b) Montrer que $\cos(\frac{\pi}{9})$ n'est pas constructible à la règle et au compas.

Solution. Supposons qu'il existe $k_1, \ldots, k_n$ comme dans l'énoncé avec $\sqrt[3]{2} \in k_n$. Alors $[k_n : \mathbb{Q}] = 2^n$ et $[\sqrt[3]{2} : \mathbb{Q}]$ divise 2^n donc doit être une puissance de 2. Or on a déjà dans l'exercice 11 que $[\sqrt[3]{2} : \mathbb{Q}] = 3$, donc $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.
On a $(e^{it}+e^{-it})^3 = e^{3it}+e^{-3it}+3(e^{it}+e^{-it})$. Donc $2\cos(\frac{\pi}{9})$ est racine de $P = X^3-3X-2cos(\pi/3) = X^3-3X-1$. On vérifie que $\mathbb{Q}$ est irréductible sur $\mathbb{Q}$ en vérifiant qu'il n'a pas de racine : une telle racine a serait un entier algébrique, donc un entier. Donc $1 = a^3 - 3a$ est divisible par a ce qui montre que $a = 1$ ou -1. On vérifie que 1 et -1 ne sont pas solutions.
Donc $[\mathbb{Q}(cos(\frac{\pi}{9})) : \mathbb{Q}]$ est divisible par 3, ce qui prouve la non constructibilité de $\cos(\frac{\pi}{9})$

Exercice 12. Soit L/K une extension de corps de degré 3 et soient $\alpha, \beta \in L$ tels que $L = K[\alpha] = K[\beta]$. Montrer qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ tel que $\beta = g \cdot \alpha = \frac{a\alpha+b}{c\alpha+d}$. Discuter l'unicité de g.

Solution. $E = \text{vect}(1, \alpha)$ est un sous-K-espace vectoriel de L dimension 2. L'application f de L dans L définie par $f : (x) = x\beta$ est K-linéaire (même L-linéaire en fait) et bijective. Donc $f(E)$ est un sous-K-espace vectoriel de dimension 2. Comme $\dim E + \dim f(E) > \dim_K L$, on en déduit qu'il existe $x \neq 0 \in E \cap f(E)$. D'où $a, b, c, d\mathbb{K}$ non tous nuls tels que $\beta(c\alpha + d) = a\alpha + b$ (mais a priori la matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est seulement dans $M_2(K)$).
En intervertissant le rôle de α et β dans l'autre sens, on obtient $g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ telle que $\alpha = (a'\beta+b')/(c'\beta+d')$.
On a donc $g'g \cdot \alpha = g \cdot \beta\alpha$, c'est-à-dire $(c''\alpha^2 + d''\alpha) = (a''\alpha + b'')$ et donc $g'g = a''\text{Id}$, avec $a'' \neq 0$, donc $g \in GL_2(K)$.
Supposons par l'absurde que $f(E) = E$. Alors $1 \in E$ et donc par récurrence $\beta^n \in E$, et donc $K[\beta] \subset E$ contrairement à l'hypothèse. Donc $E \cap f(E)$ est de dimension 1 sur K, ce qui montre l'unicité de a, b, c, d à multiplication par un scalaire commun près.

Exercice 13. Montrer que tout automorphisme de corps de $\mathbb{R}$ est l'identité (on pourra montrer qu'un tel automorphisme est nécessairement croissant).

Solution. Un tel automorphisme s conserve la propriété d'être un carré, donc la propriété d'être positif. Donc si $a \leq b$, $s(b) - s(a) = s(b - a) \leq 0$, donc s est croissant. De plus s est l'identité sur $\mathbb{Q}$ comme tout morphisme de corps. Soit $x \in \mathbb{R}$. Soit (a_n) (resp. (b_n)) une suite de rationnels tendants vers x par valeurs inférieures (par valeurs supérieurs). Alors, comme s est croissante, $a_n = s(a_n) \leq s(x) \leq s(b_n) = b_n$. En prenant la limite quand n tend vers l'infini, on obtient $s(x) = x$.

4 Perfection

Un corps est dit parfait si $Car(k) = 0$ ou si $p := Car(k) > 0$ et $\text{Fr}_p : K \to K$ est surjectif ($\text{Fr}_p(x) = x^p$).

Exercice 14. Montrer que $K = \mathbb{F}_p(X)$ n'est pas un corps parfait.

Solution. Comme $A = \mathbb{F}_p[X]$ est factoriel (même principal),$K = \text{Frac}(A)$ et X est irréductible, le polynôme $T^p - X$ est irréductible dans $K[T]$, donc n'a pas de racine. Donc X n'est pas dans l'image du frobenius.

Exercice 15. Soit K un corps parfait et $P \in K[X]$. Montrer que si P est irréductible, alors $\text{pgcd}(P, P') = 1$. Soit K un corps qui n'est pas parfait. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ irréductible tel que $P' = 0$.

Solution. Si $P' \neq 0$, alors $\deg \text{pgcd}(P, P') \leq \deg P' < \deg P$, et $\text{pgcd}(P, P')|P$, donc si P est irréductible $\text{pgcd}(P, P') = 1$. Il suffit donc de montrer que $P' \neq 0$ (ce qui est évident si $p := carK = 0$, on suppose dorénavant $p \neq 0$). Supposons $P' = 0$ et écrivons $P = \sum_k a_k X^k$. Alors $P' = \sum_k k a_k X^{k-1} = 0$ donc $a_k = 0$ si k n'est pas divisible par p. Donc $P = \sum_j a_{pj} X^{pj}$. Comme K est supposé parfait, il existe b_j tel que $b_j^p = a_p j$. Alors $P = \sum_j (b_j X^j)^p = (\sum_j b_j X^j)^p$, ce qui contredit l'irréductibilité de P.

Exercice 16. Soit K un corps parfait de caractéristique $p > 0$ et K' une extension finie de K.

a) Soient $(x_i)_i$ une base du K-espace vectoriel K' et $f : K' \to K'$ l'unique application K-linéaire telle que $f(x_i) = x_i^p$ pour tout i. Montrer que f est injective.

b) En déduire que K' est parfait.

c) on ne suppose plus K'/K finie, mais seulement algébrique. Montrer que K' est parfait.

Solution. a) Soit $y = \sum_i a_i x_i \in \ker f$ avec $a_i \in K$. Comme K est parfait, soit $b_i \in K$ tel que $b_i^p = a_i$. Alors $0 = f(y) = (\sum_i b_i x_i)^p$, donc comme (x_i) est une famille libre, pour tout i, $b_i = 0$, donc $a_i = 0$, donc $y = 0$.

b) Soit $y \in K'$. Comme K' est de dimension finie sur K, l'injectvité de f implique sa surjectivité. Il existe donc $z = \sum_i a_i x_i$ avec $a_i \in K$ tel que $f(z) = y$. Comme K est parfait, il existe $b_i \in K$ tel que $b_i^p = a_i$. On a alors $y = (\sum_i b_i x_i)^p$, ce qui prouve que K' est parfait.

c) Soit $y \in K'$. Alors $K(y)$ est une extension finie de K, donc $K(y)$ est parfait d'après 2. Il existe donc $z \in K(y) \subset K'$ tel que $z^p = y$, ce qui montre que K' est parfait.

Exercice 17. Soit K un corps de caractéristique $p > 0$.

a) Montrer qu'il existe une extension K' de K tel que K soit un corps parfait (on pourra prendre pour K' une clôture algébrique de K) .

b) On note $K^{\text{pf}} = \{x \in K' : \exists n \in \mathbb{N}, x^{p^n} \in K\}$. Montrer que K^{pf} est un sous-corps parfait de K' contenant K.

c) Montrer que K^{pf} vérifie la propriété universelle suivante : pour toute extension L de K telle que L soit un corps parfait, il existe un unique morphisme de K-algèbres $K^{\text{pf}} \to L$.

Solution. a) Soit K' une clôture algébrique de K. Soit $x \in K'$. Comme K' est algébriquement clos, le polynôme $X^p - x$ admet une racine, et donc x est dans l'image du frobenius. Donc K' est parfait.

b) Si $x, y \in K^{\text{pf}}$, il existe n, m tels que $x^{p^n}, y^{p^m} \in K$. On peut supposer $n = m$ quitte à les remplacer par le maximum des deux. Alors $(x-y)^{p^n} = x^{p^n} - y^{p^n} \in K$ et si $y \neq 0$, $(x/y)^{p^n} = x^{p^n}/y^{p^n} \in K$, donc K^{pf} est un sous-corps de K'. De plus si $x \in K$, $x^{p^0} = x \in K$ donc K^{pf} contient K.
Enfin, si $x \in K^{\text{pf}}$, soit n tel que $x^{p^n} \in K$. Comme K' est parfait il existe $y \in K'$ tel que $y^p = x$. Alors $y^{p^{n+1}} = x^{p^n} \in K$ donc $y \in K^{\text{pf}}$, ce qui montre que K^{pf} est parfait.

c) Soit L comme dans l'énoncé. Soit $x \in K^{\text{pf}}$. Il existe n tel que $x^{p^n} \in K \subset L$. Comme L est parfait le polynôme $X^{p^n} - x^{p^n}$ admet une racine y, unique par injectivité du frobenius.
Soit f un morphisme de K-algèbres $K^{\text{pf}} \to L$. Alors $f(x)^{p^n} = f(x^{p^n}) = y^{p^n}$, donc par injectivité du frobenius, $f(x) = y$, ce qui montre l'unicité de f.
Réciproquement, posons $f(x) = y$ (ceci ne dépend pas du choix de n). Si $x_1, x_2 \in K^{\text{pf}}$, il existe n tels que $x_1^{p^n}, x_2^{p^n} \in K$. Alors $(f(x_1) + f(x_2))^{p^n} = f(x_1)^{p^n} + f(x^2)^{p^n} = x_1^{p^n} + x_2^{p^n} = (x_1 + x_2)^{p^n} = f(x_1 + x_2)^{p^n}$, et donc par injectivité du frobenius f est additive. La multiplicativité de f se prouve de la même façon.

Exercice 18. Algorithme de Berlekamp

a) Soit A une $\mathbb{F}_p$-algèbre. Montrer que $\text{Fr}_p : A \to A$ définie par $f(x) = x^p$ est $\mathbb{F}_p$-linéaire.

b) Montrer que si A est un corps, alors $E := \ker(\text{Fr}_p - \text{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension 1.

c) Montrer que si $A = K_1 \times \cdots K_n$ est un produit de n corps, alors $E := \ker(\text{Fr}_p - \text{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension n.

d) Soit $P \in \mathbb{F}_p[X]$ tel que $\text{pgcd}(P, P') = 1$. On pose $A = \mathbb{F}_p[X]/(P)$. Montrer que $E := \ker(\text{Fr}_p - \text{Id}_A)$ est un sous-espace vectoriel de A de dimension le nombre de facteurs irréductibles de P.

Solution. a) Si $a, b \in \mathbb{F}_p$, alors $\mathrm{Fr}_p(ax+by) = \sum_{k=0}^{p} \binom{p}{k} a^k x^k b^{p-k} y^{p-k} = a^p x^p + b^p y^p$ car les coefficients binomiaux pour $k \neq 0, p$ sont divisibles par p. Or $a^p = a$ et $b^p = b$ d'après le petit théorème de Fermat, donc Fr_p est bien $\mathbb{F}_p$ linéaire.

b) E est l'ensemble des racines de $X^p - X$. Comme A est un corps, il y a au plus p telles racines. Les éléments de $\mathbb{F}_p \subset A$ sont de telles racines, et donc $E = \mathbb{F}_p$ est bien un $\mathbb{F}_p$-espace vectoriel de dimension 1.

c) $(x_1, \cdots, x_n) \in E$ si et seulement si $x_i^p = x_i$ pour tout i, si et seulement si $x_i \in \mathbb{F}_p$ d'après la question précédente. Donc $E = \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ est de dimension n.

d) Comme $\mathrm{pgcd}(P, P') = 1$, les facteurs irréductibles de P apparaissent avec multiplicité 1 dans la factorisation de P. Donc $P = Q_1 \cdots Q_n$ où les Q_i sont tous distincts. Le théorème des restes chinois affirme que $A = \prod_i \mathbb{F}_p[X]/Q_i$ et $K_i = \mathbb{F}_p[X]/Q_i$ est un corps puisque Q_i est irréductible. La question précédente nous dit donc que E est de dimension n sur $\mathbb{F}_p$.

Exercice 19. Soit p un nombre premier et $a \in \mathbb{F}_p$. Soit $P = X^p - X - a \in \mathbb{F}_p[X]$.

a) Si $a = 0$, donner la décomposition en facteur irréductible de P. On suppose dorénavant $a \neq 0$.

b) Montrer que $P(X+1) = P(X)$.

c) Soit Q un facteur irréductible de P. Montrer que $Q(X+1)$ est aussi un facteur irréductible de P.

d) Montrer que $Q(X+1) = Q(X)$ (on pourra considérer une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des facteurs irréductibles de P).

e) Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leq p-1$ et $R(X+1) = R(X)$, alors R est un polynôme constant.

f) En déduire que P est irréductible.

g) Soit $b \in \mathbb{Z}$ premier à p. Montrer que $X^p - X - b$ est un polynôme irréductible de $\mathbb{Q}[X]$.

Solution. a) Si $x \in \mathbb{F}_p$, $P(x) = 0$ donc $\prod_{x \in \mathbb{F}_p}(X - x)$ divise P, et comme les deux polynômes sont de même degré et de même coefficient dominant, ils sont égaux.

b) $P(X+1) = (X+1)^p - (X+1) - a = X^p + 1 - X - 1 - a = X^p - X - a$.

c) L'application $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$ qui à R associe $R(X+1)$ est un isomorphisme d'anneaux, donc préserve l'irréductibilité et la relation de divisibilité. Donc $Q(X+1)$ est irréductible et $Q(X+1)$ divise $P(X+1) = P$, comme voulu.

d) On considère l'action $k.Q \mapsto Q(X+k)$. Le stabilisateur de Q est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, c'est donc soit $\mathbb{Z}/p\mathbb{Z}$ (auquel cas $Q(X+1) = Q$ comme voulu), soit $\{0\}$. Si le stabilisateur est $\{0\}$, alors l'orbite de Q est de cardinal p. Or comme P est de degré p, s'il a au moins p facteurs irréductibles, ils doivent être de degré 1, et donc P devrait avoir une racine. Or si $x \in \mathbb{F}_p$, $P(x) = -a \neq 0$. Contradiction.

e) Soit z une racine de R dans une extensions K de $\mathbb{F}_p$. Alors $(z+a)_{a \in \mathbb{F}_p}$ est une famille de p racines distinctes de R, ce qui contredit $\deg R < p-1$.

f) Si Q est un facteur irréductible de P, alors $Q(X+1) = Q(X)$ d'après d), donc $\deg Q \geq p$ d'après e, ce qui prouve que P est irréductible.

g) Si $P = X^p - X - b$ était réductible, son image $\bar{P}$ dans $\mathbb{F}_p[X]$ par réduction modulo p serait aussi réductible puisque P est unitaire, ce qui est en contradiction avec f). Donc P est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$