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*).

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.

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

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

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.

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 $k(x^2) = k(x)$.

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

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

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.

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.

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.

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

4 Perfection

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

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

Exercice 15.
a) Soit K un corps et $P \in K[X]$ un polynôme irréductible. Montrer que $P' = 0$ ou $\mathrm{pgcd}(P, P') = 1$.
b) Soit K un corps parfait et $P \in K[X]$. Montrer que si P est irréductible, alors $\mathrm{pgcd}(P, P') = 1$.
c) Soit K un corps qui n'est pas parfait. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ irréductible tel que $P' = 0$.
d) En déduire qu'un corps est parfait si et seulement si toutes ses extensions finies sont séparables.

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.

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 $K^{\mathrm{pf}} = \{x \in K' : \exists n \in \mathbb{N}, x^{p^n} \in K\}$. 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 $K^{\mathrm{pf}} \to L$.

Exercice 18. Algorithme de Berlekamp
a) Soit A une $\mathbb{F}_p$-algèbre. Montrer que $\mathrm{Fr}_p : A \to A$ définie par $f(x) = x^p$ est $\mathbb{F}_p$-linéaire.
b) Montrer que si A est un corps, alors $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension 1.
c) Montrer que si $A = K_1 \times \cdots \times K_n$ est un produit de n corps, alors $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension n.
d) Soit $P \in \mathbb{F}_p[X]$ tel que $\mathrm{pgcd}(P, P') = 1$. On pose $A = \mathbb{F}_p[X]/(P)$. Montrer que $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-espace vectoriel de A de dimension le nombre de facteurs irréductibles de 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 $\mathbb{Q}[X]$.