# TD5 : Modules sur un anneau principal ; Discriminant

Diego Izquierdo

***Attention : Cette semaine il y aura aussi un TD le jeudi 12 mars à 17h30. Il y aura une autre feuille de TD pour cette séance-là. N'oubliez pas de la prendre aussi !***

*Les exercices 1, 2 et 3 sont des exercices de révision du cours d'Algèbre 1. Ils ne seront pas traités pendant la séance, mais si vous ne vous sentez pas à l'aise avec les calculs de base, il est conseillé de les faire chez soi. Les exercices 5, 8 et 12 sont à préparer avant le TD. Pendant la séance de TD, les exercices seront traités dans l'ordre suivant : 5, 8, 12, 16, 20. Si le temps le permet, nous traiterons aussi l'exercice 22.*

**Exercice 1 (révision) : Facteurs invariants**
Trouver les facteurs invariants du $\mathbb{Z}$-module :

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}.$$

**Exercice 2 (révision) : Examen 2012**

1. Soient $n \geq 1$ un entier et $u_1$, ..., $u_n$ des éléments de $\mathbb{Z}^n$ linéairement indépendants dans l'espace vectoriel $\mathbb{Q}^n$. Soit $M$ le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Montrer que l'indice de $M$ dans $\mathbb{Z}^n$ est égal à la valeur absolue du déterminant des vecteurs $u_1, ..., u_n$ dans la base canonique.
2. Soit $M$ sous-groupe de $\mathbb{Z}^3$ engendré par $u_1 = (2, 1, 1)$, $u_2 = (1, 2, 1)$ et $u_3 = (1, 1, 2)$. Calculer $\mathbb{Z}^3/M$.
3. Plus généralement, soit $(u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ la matrice telle que $u_{i,j} = 2$ si $i = j$ et $u_{i,j} = 1$ sinon, et notons $u_1$, ..., $u_n$ les vecteurs colonne de cette matrice. Soit $M$ le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Calculer $\mathbb{Z}^n/M$.

**Exercice 3 (révision) : Bases adaptées**

1. Donner une base adaptée pour le sous-$\mathbb{Z}$-module $M$ de $\mathbb{Z}^4$ engendré par $(2, -1, 0, 0)$, $(-1, 2, -1, -1)$, $(0, -1, 2, 0)$ et $(0, -1, 0, 2)$. Calculer le quotient $\mathbb{Z}^4/M$.
2. Même question pour le sous-$\mathbb{Z}$-module $M$ de $\mathbb{Z}^3$ engendré par $(4, 8, 16)$, $(1, 5, 10)$, $(6, 2, 4)$ et $(5, 8, 6)$.
3. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $5x+7y+35z = 0$.
4. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $x + 2y + 3z \equiv 0 \mod 4$.

**5.** Même question pour le sous-$\mathbb{C}[[X]]$-module de $\mathbb{C}[[X]]^2$ engendré par $((1-X)^{-1}, (1-X^2)^{-1})$ et $((1+X)^{-1}, (1+X^2)^{-1})$.

**6.** Exhiber deux sous-$\mathbb{Z}$-modules $M$ et $N$ de $\mathbb{Z}^2$ de rang 2 tels qu'il n'existe pas une base $(e_1, e_2)$ de $\mathbb{Z}^2$ pour laquelle on peut trouver des entiers $a, b, c, d$ tels que $(ae_1, be_2)$ est une base de $M$ et $(ce_1, de_2)$ est une base de $N$.

**Exercice 4 : $\mathbb{Z}[i]$-modules finis**

**1.** Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal 3 à isomorphisme près ? de cardinal 5 ? de cardinal 9 ?

**2.** *(plus difficile)* Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal $5^3 \cdot 6^4$ à isomorphisme près ?

**Exercice 5 (à préparer) : Retour sur le théorème des deux carrés**

Soit $p$ un nombre premier congru à 1 modulo 4. Montrer qu'il est possible de munir $\mathbb{Z}/p\mathbb{Z}$ d'une structure de $\mathbb{Z}[i]$-module. En déduire qu'il deux entiers $a$ et $b$ tels que $p = a^2 + b^2$.

**Exercice 6 : Une caractérisation des anneaux principaux**

Soit $A$ un anneau commutatif unitaire intègre et noethérien. Montrer que $A$ est principal si, et seulement si, tout module de type fini sans torsion sur $A$ est libre.

**Exercice 7 : Matrices à coefficients dans des anneaux euclidiens**

Soit $A$ un anneau euclidien. Soit $M \in \mathcal{M}_{m,n}(A)$.

**1.** Montrer qu'il existe $P \in \mathcal{M}_m(A)$ et $Q \in \mathcal{M}_n(A)$ produits de matrices élémentaires telles que $PMQ$ est de la forme :

$$\begin{pmatrix} d_1 & 0 & 0 & ... & 0 & ... & 0 \\ 0 & d_2 & 0 & ... & 0 & ... & 0 \\ 0 & 0 & d_3 & ... & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & ... & \vdots \\ 0 & 0 & 0 & ... & d_r & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & ... & \vdots \\ 0 & 0 & 0 & ... & 0 & ... & 0 \end{pmatrix}$$

où $d_1, ..., d_r$ sont des éléments de $A$ tels que $d_1|d_2|d_3|...|d_r$.

**2.** Montrer que, si $M \in GL_n(A)$, alors il existe $P \in \mathcal{M}_n(A)$ produit de

matrices élémentaires telle que :

$$PM = \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & \det(M) \end{pmatrix}.$$

En déduire que le sous-groupe de $GL_n(A)$ engendré par les matrices élémentaires est $SL_n(A)$.

**Exercice 8 (à préparer) : Partiel 2014**

Soit $A$ un groupe abélien. Pour $n \in \mathbb{N}^*$, on note $S(A,n)$ l'ensemble des sous-groupes de $A$ d'indice $n$.

1. Soit $X \in S(A,n)$. Montrer que $nA \subseteq X$.
2. Montrer qu'il existe une bijection entre $S(A,n)$ et $S(A/nA,n)$.
3. Soient $m \in \mathbb{N}^*$ et $N \in \mathbb{N}^*$. Montrer que, si $m \wedge n = 1$, alors il existe une bijection entre $S((\mathbb{Z}/mn\mathbb{Z})^N, mn)$ et $S((\mathbb{Z}/m\mathbb{Z})^N, m) \times S((\mathbb{Z}/n\mathbb{Z})^N, n)$.
4. Montrer que $S(\mathbb{Z}^2, 2)$ possède 3 éléments, que l'on explicitera.
5. Faire la liste des éléments de $S(\mathbb{Z}^2, n)$. Pour ce faire, on pourra faire la liste des $X \in S(\mathbb{Z}^2, n)$ tels que $X \cap (\mathbb{Z} \oplus 0) = a\mathbb{Z} \oplus 0 \subseteq \mathbb{Z}^2$ pour chaque diviseur positif $a$ de $n$. En déduire que $|S(\mathbb{Z}^2, n)| = \sum_{a|n} a$, puis expliciter les séries génératrices $\sum_{r \geq 0} |S(\mathbb{Z}^2, p^r)| T^r$ et $\sum_{n \geq 1} |S(\mathbb{Z}^2, n)| n^{-s}$.
6. Faire la liste des éléments de $S(\mathbb{Z}^3, n)$. En déduire que $|S(\mathbb{Z}^3, n)| = \sum_{ab|n} a^2 b$, puis expliciter les séries génératrices $\sum_{r \geq 0} |S(\mathbb{Z}^3, p^r)| T^r$ et $\sum_{n \geq 1} |S(\mathbb{Z}^3, n)| n^{-s}$.

**Exercice 9 : Arbre de Bruhat-Tits**

Soit $p$ un nombre premier. On note $V_0$ le $\mathbb{Z}$-module $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$. Soit $\mathcal{V}_1$ l'ensemble des sous-$\mathbb{Z}$-modules d'indice $p$ dans $V_0$.

1. Montrer que $\mathcal{V}_1$ a exactement $p+1$ éléments.

Soient $V_1$ un élément de $\mathcal{V}_1$ et $\mathcal{V}_2$ l'ensemble de ses sous-modules d'indice $p$.

2. Montrer que $\mathcal{V}_2$ a exactement $p+1$ éléments et qu'il contient un unique sous-module homothétique à $V_0$.

On munit l'ensemble (de sommets)

$$\mathcal{T}_p = \{\text{sous-}\mathbb{Z}\text{-modules de } \mathbb{Z}^2 \text{ d'indice une puissance de } p\}/(\text{homothétie})$$

de la structure de graphe suivante : une arête relie $v$ à $v'$ s'il existe des représentants $V$ et $V'$ de $v$ et $v'$ respectivement tels que $V$ est un sous-module d'indice $p$ de $V'$.

**3.** Montrer que l'on a une arête $v \to v'$ si et seulement si il existe une arête $v' \to v$.

Les questions suivantes établissent alors que la structure de graphe conférée à $\mathcal{T}_p$ est en fait un arbre non orienté. Soient $v$ et $v'$ deux sommets de $\mathcal{T}_p$.

**4.** Montrer qu'il existe des représentants $V_{(0)}$ et $V_{(n)}$ de $v$ et $v'$ respectivement ainsi que des $V_{(i)}$ pour $1 \leq i \leq n-1$ vérifiant $V_{(0)} \supseteq V_{(1)} \supseteq \cdots \supseteq V_{(n)}$ et tels que $V_{(i+1)}$ est d'indice $p$ dans $V_{(i)}$ pour tout $i$.

Soient $v_0, v_1, \ldots, v_{n-1}, v_n = v_0$ des sommets où chaque $v_i$ est relié à $v_{i+1}$ par une arête.

**5.** Montrer que l'on a $n = 0$ ou bien ($n \geq 2$ et il existe $1 \leq i \leq n-1$ avec $v_{i+1} = v_{i-1}$).

**Exercice 10 : Polynôme caractéristique et similitude**

Soient $K$ un corps, $n \geq 1$ un entier et $P \in K[X]$ un polynôme unitaire de degré $n$. On note $p$ la fonction partition, qui à un entier $i \geq 1$ associe le nombre de façons distinctes de représenter $i$ comme somme d'entiers.

**1.** Exprimer, en fonction de la décomposition en facteurs irréductibles de $P$, le nombre de classes de similitude de matrices de $\mathcal{M}_n(K)$ ayant $P$ pour polynôme caractéristique.

**2.** Expliciter le résultat pour $P = X^2(X-1)^3(X+1)$.

**3.** Combien y a-t'il de classes de similitude dans $\mathcal{M}_3(\mathbb{Z}/2\mathbb{Z})$ ?

**Exercice 11 : Endomorphismes de polynôme minimal donné**

Soient $K$ un corps et $P \in K[X]$ un polynôme non constant. Soit $\Sigma$ l'ensemble des entiers naturels $n$ tels qu'il existe un $K$-espace vectoriel $V$ de dimension $n$ muni d'un endomorphisme linéaire $u$ de polynôme minimal égal à $P$. Montrer qu'il existe $N \in \mathbb{N}$ et $d \in \mathbb{N}^*$ tels que $\Sigma \cap [N, +\infty[ = d\mathbb{N} \cap [N, +\infty[$. Que vaut $d$ ?

**Exercice 12 (à préparer) : Examen 2011**

Soit $K$ un corps. Pour chaque polynôme unitaire $P \in K[X]$, on note $C(P)$ la matrice compagnon associée. Si $P$ et $Q$ sont deux polynômes unitaires, déterminer les invariants de similitude de la matrice :

$$\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}.$$

**Exercice 13 : Commutant**

Soient $K$ un corps infini et $V$ un $K$-espace vectoriel non nul de dimension finie. Pour $u$ un endomorphisme de $V$, on note $\mathcal{C}(u) = \{v \in \mathrm{End}_K(V) \mid uv = vu\}$ et $\mathcal{P}(u) = \{P(u) \mid P \in K[X]\}$.

1. Soit $u \in \mathrm{End}_K(V)$. Montrer que $\mathcal{P}(u) = \bigcap_{v \in \mathcal{C}(u)} \mathcal{C}(v)$.
2. Soit $u \in \mathrm{End}_K(V)$. Montrer que les propriétés suivantes sont équivalentes :
   (i) $u$ est cyclique ;
   (ii) le polynôme minimal de $u$ est égal (au signe près) au polynôme caractéristique ;
   (iii) $\mathcal{C}(u) = \mathcal{P}(u)$ ;
   (iv) $V$ n'a qu'un nombre fini de sous-espace stables par $u$.

Pour les deux exercices qui suivent, on rappelle que les racines du polynôme $x^3 + px + q = 0$ sont les :

$$\zeta \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

pour $\zeta$ parcourant les racines cubiques de l'unité.

**Exercice 14 : Résolution d'équations**

1. Exhiber une solution réelle de l'équation $x^3 - 3x^2 - 6x - 4 = 0$.
2. Même question pour $x^6 + 3x^5 - 3x^4 + 2x^3 - 3x^2 + 3x + 1 = 0$.

**Exercice 15 : Calculs de nombres algébriques**

1. Calculer les parties réelle et imaginaire d'une racine cubique de :

$$z = 3\sqrt{3} + i\sqrt{5}.$$

2. Soit $j$ une racine cubique primitive de l'unité. Montrer qu'il existe des rationnels $a, x, y$, que l'on déterminera, tels que :

$$\cos\left(\frac{2\pi}{7}\right) = a + \sqrt[3]{x + yj} + \sqrt[3]{x + yj^2}.$$

**Exercice 16 : Calcul de discriminant - Examen 2014**

Soient $a$ et $b$ deux éléments de $\mathbb{C}$. Soit $n \geq 2$. Calculer le discriminant du polynôme $X^n + aX + b$.

**Exercice 17 : Discriminant d'un polynôme cyclotomique**

Soient $p$ un nombre premier et $n$ un entier naturel non nul. Calculer le discriminant de $\phi_{p^n} = \sum_{k=0}^{p-1} X^{kp^{n-1}}$ au signe près.

**Exercice 18 : Résultant et discriminant**

Soit $A$ un anneau commutatif. Pour $n \in \mathbb{N}$, on note $A_n[X]$ le $A$-module des polynômes de degré strictement plus petit que $n$. On appellera base canonique de $A_n[X]$ la base $(X^{n-1}, X^{n-2}, ..., 1)$. Pour $(P, Q) \in A[X] \times A[X]$ avec $\deg P = n$ et $\deg Q = m$, on note $\mathrm{Res}(P, Q)$ le déterminant dans les bases canoniques de l'application $A$-linéaire $A_m[X] \times A_n[X] \to A_{m+n}[X]$ qui envoie $(U, V)$ sur $PU + QV$.

**1.** Écrire $\mathrm{Res}(P, Q)$ comme déterminant d'une matrice.

**2.** Comparer $\mathrm{Res}(P, Q)$ et $\mathrm{Res}(Q, P)$.

**3.** On suppose que $P$ est un polynôme unitaire.

(a) Montrer que $\mathrm{Res}(P, Q)$ est égal au déterminant de la multiplication par $Q$ sur l'anneau $A[X]/(P)$ dans la base $(X^{n-1}, X^{n-2}, ..., 1)$.

(b) Considérons $Q_1 \in A[X]$ et $Q_2 \in A[X]$ de degrés respectifs $m_1$ et $m_2$. Calculer $\mathrm{Res}(P, Q_1Q_2)$ en fonction de $\mathrm{Res}(P, Q_1)$ et $\mathrm{Res}(P, Q_2)$.

(c) Exprimer $\mathrm{Res}(P, (X-\lambda_1)...(X-\lambda_m))$ en fonction de $P(\lambda_1)...P(\lambda_m)$.

(d) En déduire une formule explicite pour $\Delta^2 = \prod_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, ..., X_n]$ en fonction des polynômes symétriques élémentaires.

**Exercice 19 : Fractions rationnelles fixées par le groupe alterné**

Soit $K$ un corps de caractéristique différente de 2. Montrer que, pour $n \geq 2$, le sous-corps de $K(x_1, ..., x_n)$ fixé par $\mathcal{A}_n$ est : $K(x_1, ..., x_n)^{\mathcal{A}_n} = \{f + g\Delta | f, g \in K(x_1, ..., x_n)^{\mathcal{S}_n}\}$, où $\Delta = \prod_{i<j}(x_i - x_j)$.

**Exercice 20 : Fractions rationnelles fixées par un groupe cyclique**

**1.** Soit $n > 0$ un entier. Soit $G$ un sous-groupe cyclique de $GL_n(\mathbb{C})$. On fait agir naturellement $G$ sur $\mathbb{C}(x_1, ..., x_n)$. Montrer que le corps $\mathbb{C}(x_1, ..., x_n)^G$ est isomorphe à $\mathbb{C}(y_1, ..., y_n)$.

**2.** Exhiber un isomorphisme explicite entre les corps $\{F \in \mathbb{C}(x_1, ..., x_n) \mid F(x_1, x_2, ..., x_n) = F(x_2, x_3, ..., x_n, x_1)\}$ et $\mathbb{C}(y_1, ..., y_n)$.

**Exercice 21 : Formules de Newton**

Soit $K$ un corps. Soient $\sigma_1, ..., \sigma_n$ les polynômes symétriques élémentaires de $K[X_1, ..., X_n]$. Pour $k > n$, on pose $\sigma_k = 0$. On note $S_i = X_1^i + ... + X_n^i$ pour $i > 0$. Montrer que, pour $k > 1$, on a $S_k = (-1)^{k+1}k\sigma_k + \sum_{i=1}^{k-1}(-1)^{k+1-i}\sigma_{k-i}S_i$.

**Exercice 22 : Quelques calculs explicites**

**1.** Déterminer le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.

**2.** Déterminer le polynôme minimal de $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$ sur $\mathbb{Q}$.

**3.** Calculer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ où $\alpha = 10^{1/5} + 7^{1/3}$.

*Je ne suis pas sûr d'avoir été clair dans la correction de la question 7 de l'exercice 1 du TD4. Voici donc un corrigé.*

**Exercice 1 (à préparer) : Vrai ou faux ?**
Soit $A$ un anneau. Il existe un $\mathbb{Z}$-module qui n'a pas de famille génératrice minimale.

**Indications :** VRAI : Le groupe abélien $\mathbb{Q}$ n'a pas de famille génératrice minimale. En effet, soit $(x_i)_{i\in I}$ une famille génératrice. On vérifie immédiatement que $I$ est infini. On peut donc trouver $i_0 \in I$ tel que $1 \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. Montrons que $(x_i)_{i\in I\setminus\{i_0\}}$ est une famille génératrice. Il suffit de voir que $x_{i_0} \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. On écrit, pour $i \in I$, $x_i = p_i/q_i$ avec $p_i, q_i \in \mathbb{Z}$ tels que $p_i \wedge q_i = 1$. On peut écrire $1/q_{i_0}^2 = \sum_{i\in I\setminus\{i_0\}} a_i x_i + a_{i_0} x_{i_0}$ pour une famille presque nulle d'entiers $(a_i)_{i\in I}$. Donc $1/q_{i_0}^2 - a_{i_0}x_{i_0} \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. Donc $1/q_{i_0} - a_{i_0}p_{i_0} \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. Mais $1 \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. Donc $1/q_{i_0} \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$ et $x_{i_0} \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$.

*Remarque 1 :* En TD, j'affirmais que je pouvais choisir $i_0$ quelconque, sans supposer forcément $1 \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$. Cela est vrai mais il faut travailler plus que ce que je prétendais en TD. En fait, on note $d$ le pgcd de $(p_i)_{i\in I\setminus\{i_0\}}$ et on suppose $d \neq 1$. Soit $p$ un nombre premier divisant $d$. On remarque que $p$ ne divise pas $q_i$ pour $i \neq i_0$. Donc, si $n = v_p(q_{i_0})$, le dénominateur d'un élément de $(x_i)_{i\in I}$ ne peut pas être multiple de $p^{n+1}$ : absurde car $(x_i)_{i\in I_0}$ est génératrice ! Donc $d = 1$. On en déduit que forcément $1 \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$.

*Remarque 2 :* En TD, j'affirmais que la famille $(x_i)_{i\in I}$ était génératrice si, et seulement si, $\sup_i v_p(q_i) = +\infty$ pour chaque premier $p$. L'implication directe est évidente. Pour la réciproque, supposons que $\sup_i v_p(q_i) = +\infty$ pour chaque premier $p$. Comme dans la remarque 1, on montre que le pgcd de $(p_i)_{i\in I}$ est forcément 1, ce qui montre que $1 \in \langle (x_i)_{i\in I}\rangle$. Par conséquent, pour chaque premier $p$ et entier naturel $n$, on a $1/p^n \in \langle (x_i)_{i\in I}\rangle$. Or la famille de $1/p^n$ pour $p$ premier et $n$ entier naturel est génératrice. Donc $(x_i)_{i\in I}$ est génératrice.
Cette équivalence montre aussi que, si $(x_i)_{i\in I}$ est génératrice, toute sous-famille obtenue en enlevant un élément est génératrice.

*Remarque 3 :* On aurait aussi pu prendre $\mathbb{Q}/\mathbb{Z}$ au lieu de $\mathbb{Q}$, ce qui nous aurait permis d'éviter de devoir prendre $i_0$ tel que $1 \in \langle (x_i)_{i\in I\setminus\{i_0\}}\rangle$ ou de passer par les difficultés des deux remarques précédentes.