TD3 : Ensembles algébriques, topologie de Zariski, anneaux noethériens et modules

Diego Izquierdo

Les exercices 0, 1, 4, 6 ont été traités pendant la séance de TD. Les exercices 8 (sans la question 3) et 10 seront traités ultérieurement.

Exercice 0 (à préparer) : Retour au TD2

1. Combien l'anneau $\mathbb{R}[X]/(X^5(X^4-1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?
2. Montrer que, dans $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, l'idéal (3) n'est pas premier, mais il est contenu dans exactement deux idéaux premiers, qui sont maximaux.

Exercice 1 (à préparer) : Topologie de Zariski

Pour chaque idéal I de $\mathbb{C}[X_1, ..., X_n]$, on note :

$$V(I) = \{(z_1, ..., z_n) \in \mathbb{C}^n | \forall f \in I, f(z_1, ..., z_n) = 0\}.$$

Les $V(I)$ sont appelés sous-ensembles algébriques de $\mathbb{C}^n$.

1. Montrer que les sous-ensembles algébriques de $\mathbb{C}^n$ sont les fermés d'une topologie sur $\mathbb{C}^n$.

On appelle cette topologie la **topologie de Zariski** de $\mathbb{C}^n$. Si V est un sous-ensemble algébrique de $\mathbb{C}^n$, la topologie de Zariski de V est par définition celle induite par la topologie de Zariski sur $\mathbb{C}^n$.

2. Comparer la topologie de Zariski sur $\mathbb{C}^n$ à la topologie usuelle.
3. Pour $f \in \mathbb{C}[X_1, ..., X_n]$, on note $D(f)$ l'ensemble des $(x_1, ..., x_n) \in \mathbb{C}^n$ tels que $f(x_1, ..., x_n) \neq 0$. Montrer que les $D(f)$ forment une base de voisinages ouverts de $\mathbb{C}^n$ (muni de la topologie de Zariski).
4. Décrire explicitement la topologie de Zariski sur $\mathbb{C}$.

Exercice 2 : Produit et topologie de Zariski

1. Montrer que la topologie de Zariski sur $\mathbb{C}^2$ ne coïncide pas la topologie produit sur $\mathbb{C} \times \mathbb{C}$ où $\mathbb{C}$ est muni de la topologie de Zariski.

Indications : Soit $\Delta = \{(x,x)|x \in \mathbb{C}\}$. Comme :

$$\Delta = \{(x,y) \in \mathbb{C}^2 | x - y = 0\},$$

l'ensemble Δ est fermé dans $\mathbb{C}^2$ muni de la topologie de Zariski. Cependant, comme les ouverts non vides de $\mathbb{C}$ (muni de la topologie de Zariski) sont les parties cofinies de $\mathbb{C}$, l'ensemble $\mathbb{C}^2 \setminus \Delta$ ne contient aucun sous-ensemble de la forme $U \times V$ avec U et V ouverts non vides de $\mathbb{C}$ (muni de la topologie de Zariski). On en déduit que Δ n'est pas fermé dans $\mathbb{C} \times \mathbb{C}$ muni de la topologie produit.

2. Soit $n \geq 1$ un entier. Montrer que la projection $p : \mathbb{C}^{n-1} \times \{0\} \to \mathbb{C}^{n-1}$ est un homéomorphisme entre $\mathbb{C}^{n-1} \times \{0\}$ muni de la topologie induite par la topologie de Zariski sur $\mathbb{C}^n$ et $\mathbb{C}^{n-1}$ muni de la topologie de Zariski.

Indications : Soit I un idéal de $\mathbb{C}[X_1, ..., X_n]$. Soit J l'image de I par la projection $\mathbb{C}[X_1, ..., X_n] \to \mathbb{C}[X_1, ..., X_{n-1}]$. Alors :

$$p(V(I) \cap (\mathbb{C}^{n-1} \times \{0\})) = V(J).$$

Donc l'image d'un fermé par p est un fermé.

Réciproquement, soit J un idéal de $\mathbb{C}[X_1, ..., X_{n-1}]$. Soit I l'idéal engendré par J dans $\mathbb{C}[X_1, ..., X_n]$. Alors :

$$p^{-1}(V(J)) = V(I) \cap (\mathbb{C}^{n-1} \times \{0\}).$$

Donc l'image réciproque d'un fermé par p est un fermé.

On en déduit que p est un homémorphisme.

Exercice 3 : Séparation

Soit $n \geq 1$ un entier. Montrer que la topologie de Zariski sur $\mathbb{C}^n$ n'est pas séparée.

Indications : A l'aide la question 2 de l'exercice 2, il suffit de remarquer que la topologie de Zariski de $\mathbb{C}$ n'est pas séparée. Cela découle immédiatement du fait que la topologie de Zariski sur $\mathbb{C}$ est la topologie cofinie.

Exercice 4 (à préparer) : Adhérence

On munit toujours $\mathbb{C}^n$ de la topologie de Zariski.

1. Quelle est l'adhérence de $\Gamma_1 = \mathbb{Z}$ dans $\mathbb{C}$?

2. Quelle est l'adhérence de $\Gamma_2 = \{(t, t^2, t^3) | t \in \mathbb{C}\}$ dans $\mathbb{C}^3$?

3. Quelle est l'adhérence de $\Gamma_3 = \{(n, 2^n, 3^n) | n \in \mathbb{N}\}$ dans $\mathbb{C}^3$?

Exercice 5 : Questions diverses sur l'irréductibilité et la connexité

On rappelle qu'un espace topologique non vide est irréductible s'il n'est pas réunion de deux fermés stricts.

1. Montrer que tout sous-espace de $\mathbb{C}^n$ connexe pour la topologie stan-

dard est aussi connexe pour la topologie de Zariski.

> **Indications :** Cela découle du fait que la topologie standard est plus fine que la topologie de Zariski !

2. Exhiber un contre-exemple à la réciproque.

> **Indications :** Prenons $n = 1$ et $X = \mathbb{Z}$. Bien sûr, X n'est pas connexe pour la topologie standard. Par contre, comme les fermés de $\mathbb{C}$ pour la topologie de Zariski sont $\mathbb{C}$ et les parties finies de $\mathbb{C}$, on ne peut pas écrire $X = F_1 \cup F_2$ avec F_1 et F_2 fermés stricts de X disjoints. Donc X est connexe pour la topologie de Zariski.

3. Exhiber l'exemple d'un espace Zariski connexe mais non irréductible.

> **Indications :** Prendre la courbe d'équation $xy = 0$ dans $\mathbb{C}^2$.

4. Montrer qu'un espace irréductible est connexe.

> **Indications :** Soit X irréductible. Soient F_1 et F_2 des fermés disjoints tels que $X = F_1 \cup F_2$. Comme X est irréductible, cela impose que $F_1 = X$ ou $F_2 = X$. Donc X est connexe.

5. Montrer que l'image d'un espace irréductible par une application continue est irréductible.

> **Indications :** Soit $f : X \to Y$ une fonction continue entre espace topologiques, et supposons X irréductible. Soient F_1 et F_2 des fermés de $f(X)$ tels que $f(X) = F_1 \cup F_2$. Alors $X = f^{-1}(F_1) \cup f^{-1}(F_2)$ et les espaces $f^{-1}(F_1)$ et $f^{-1}(F_2)$ sont fermés dans X. Donc $f^{-1}(F_1) = X$ ou $f^{-1}(F_2) = X$. D'où $F_1 = f(X)$ ou $F_2 = f(X)$. Cela signifie que $f(X)$ est irréductible.

6. Soit V un espace topologique. Soit W une partie dense de V. Montrer que V est irréductible si, et seulement si, W l'est.

> **Indications :** Supposons V irréductible. Soient F_1 et F_2 des fermés de W tels que $W = F_1 \cup F_2$. Alors, en prenant l'adhérence dans V, on obtient $V = \overline{F_1} \cup \overline{F_2}$. Comme V est irréductible, $\overline{F_1} = V$ ou $\overline{F_2} = V$. Supposons par exemple que $\overline{F_1} = V$. Dans ce cas, $W = \overline{F_1} \cap W = F_1$. Donc W est irréductible.
>
> Réciproquement, supposons W irréductible. Soient F_1 et F_2 des fermés de V tels que $V = F_1 \cup F_2$. Alors, on obtient $W = (F_1 \cap W) \cup (F_2 \cap W)$. Comme W est irréductible, $F_1 \cap W = W$ ou $F_2 \cap W = W$. Supposons par exemple que $F_1 \cap W = W$. Dans ce cas, $F_1 = W$ car W est dense dans V. Donc V est irréductible.

Exercice 6 : Connexité et topologie de Zariski

Soit V un sous-ensemble algébrique de $\mathbb{C}^n$ muni de la topologie de Zariski. On admet la conséquence suivante du Nullstellensatz : si I est un idéal propre de $\mathcal{O}(V)$, alors $V(I) \neq \emptyset$.

1. Soit e un idempotent primitif de $\mathcal{O}(V)$. Montrer que

$$V_e = \{(z_1, ..., z_n) \in V | e(z_1, ..., z_n) = 1\}$$

est une composante connexe de V.

2. On admet que V possède un nombre fini de composantes connexes. Soit W une composante connexe de V. Montrer qu'il existe un unique idempotent primitif e de $\mathcal{O}(V)$ tel que $W = V_e$.

3. On considère la courbe C d'équation

$$xy(xy-1)=0$$

dans $\mathbb{C}^2$. Vérifier que $\mathcal{O}(C)=\mathbb{C}[X,Y]/(XY(XY-1))$. Quelles sont les composantes connexes de C ? Sont-elles irréductibles ? Quels sont les idempotents primitifs de $\mathcal{O}(C)$ correspondants ?

Exercice 7 (culturel) : Espace tangent

Soit $A=\mathbb{C}[X_1,...,X_n]$.

1. Soit $x=(x_1,...,x_n)\in\mathbb{C}^n$. Montrer que $\mathfrak{m}_x=\{f\in A | f(x_1,...,x_n)=0\}$ est un idéal maximal de A.

2. On note $\overline{X_1},...,\overline{X_n}$ les images de $X_1,...,X_n$ dans $A/\mathfrak{m}_x^2$. Vérifier que $\mathfrak{m}_x/\mathfrak{m}_x^2$ est un $\mathbb{C}$-espace vectoriel de base $\overline{X_1}-x_1,...,\overline{X_n}-x_n$.

3. Montrer que :

$$\begin{aligned}\phi :& A/\mathfrak{m}_x^2 \to A/\mathfrak{m}_x \oplus \mathfrak{m}_x/\mathfrak{m}_x^2\\ & f\mapsto \left(f(x),\sum_{i=1}^n \frac{\partial f}{\partial X_i}(x)(\overline{X_i}-x_i)\right)\end{aligned}$$

est un isomorphisme de $\mathbb{C}$-espaces vectoriels. En géométrie algébrique, l'**espace cotangent** à $\mathbb{C}^n$ en x est par définition le $\mathbb{C}$-espace vectoriel $\mathfrak{m}_x/\mathfrak{m}_x^2$ et l'**espace tangent** est $\mathrm{Hom}_{\mathbb{C}}(\mathfrak{m}_x/\mathfrak{m}_x^2,\mathbb{C})$.

4. Plus généralement, soit V un sous-ensemble algébrique de $\mathbb{C}^n$. Soit $x=(x_1,...,x_n)\in V$. Montrer que $\mathfrak{m}_{V,x}=\{f\in\mathcal{O}(V) | f(x_1,...,x_n)=0\}$ est un idéal maximal de $\mathcal{O}(V)$.

5. L'**espace cotangent** à V en x est par définition le $\mathbb{C}$-espace vectoriel $T^*_{V,x}=\mathfrak{m}_{V,x}/\mathfrak{m}^2_{V,x}$ et l'**espace tangent** est $T_{V,x}=\mathrm{Hom}_{\mathbb{C}}(\mathfrak{m}_{V,x}/\mathfrak{m}^2_{V,x},\mathbb{C})$. Soit $I(V)$ l'idéal noyau de la surjection $\psi : A\to\mathcal{O}(V)$. Montrer que ψ induit une application linéaire surjective $\psi^* : T^*_{\mathbb{C}^n,x}\to T^*_{V,x}$ de noyau l'image de :

$$\begin{aligned}d_x :& I(V)\to T^*_{\mathbb{C}^n,x}\\ & f\mapsto \frac{\partial f}{\partial X_i}(x)(\overline{X_i}-x_i).\end{aligned}$$

6. Soit $d_xX_1^*,...,d_xX_n^*$ la base de $T_{\mathbb{C}^n,x}$ qui est la base duale de $\overline{X_1}-x_1,...,\overline{X_n}-x_n$. Déduire de la question précédente que $T_{V,x}$ s'identifie au sous-espace de $T_{\mathbb{C}^n,x}$ constitué des éléments $\sum_{i=1}^n\lambda_i d_xX_i^*$ tels que $\sum_{i=1}^n\lambda_i\frac{\partial f}{\partial X_i}(x)=0$.

7. Calculer les espaces tangents en $(0,0)$ des courbes d'équations :

$$x^7 + xy = y^7 + y \quad \text{et} \quad x^2 = y^3$$

dans $\mathbb{C}^2$.

8. Soit V un sous-ensemble algébrique de $\mathbb{C}^n$. On note ϵ la classe de X dans $\mathbb{C}[X]/(X^2)$, de sorte que $\mathbb{C}[X]/(X^2) = \mathbb{C}[\epsilon]$. Soit θ la projection naturelle $\mathbb{C}[\epsilon] \to \mathbb{C}$. Elle induit une fonction :

$$\theta^* : \mathrm{Hom}_{\mathbb{C}-\text{algèbres}}(\mathcal{O}(V), \mathbb{C}[\epsilon]) \to \mathrm{Hom}_{\mathbb{C}-\text{algèbres}}(\mathcal{O}(V), \mathbb{C}).$$

Soit $x \in V$. Soit $\mathrm{ev}_x : \mathcal{O}(V) \to \mathbb{C}$ l'évaluation en x. On a $\mathrm{ev}_x \in \mathrm{Hom}_{\mathbb{C}-\text{algèbres}}(\mathcal{O}(V), \mathbb{C})$. Montrer que $(\theta^*)^{-1}(\{\mathrm{ev}_x\})$ s'identifie à l'espace tangent de V en x.

Remarque : Le Nullstellensatz que vous verrez plus tard dans le cours montre que tout morphisme dans $\mathrm{Hom}_{\mathbb{C}-\text{algèbres}}(\mathcal{O}(V), \mathbb{C})$ est de la forme ev_x pour un certain $x \in V$.

Exercice 8 : Un exemple d'anneau non noethérien

Soit $A = \{P \in \mathbb{Q}[X] \mid P(0) \in \mathbb{Z}\}$.

1. Montrer que A n'est pas factoriel.

2. Montrer que A n'est pas noethérien.

3. Montrer que A est de Bézout, c'est-à-dire que tout idéal de type fini de A est principal.

Indications : Par récurrence, on est ramené à prouver que tout idéal de A engendré par deux éléments $a + XP$ et $b + XQ$ avec $a, b \in \mathbb{Z}$ et $P, Q \in \mathbb{Q}[X]$ est principal.
Supposons dans un premier temps $a \neq 0$ et $b \neq 0$. Soit alors $R \in \mathbb{Q}[X]$ l'unique polynôme vérifiant $(a + XP, b + XQ) = (1 + XR)$ dans $\mathbb{Q}[X]$. Aussi, soit c le pgcd de a et b dans $\mathbb{Z}$. Montrons que $(a + XP, b + XQ) = (c + cXR)$ dans A. L'inclusion $\subseteq$ est directe par définition de c et de R. Réciproquement, il existe $u + XU$ et $v + XV \in \mathbb{Q}[X]$ vérifiant

$$(a + XP)(u + XU) + (b + XQ)(v + XV) = c(1 + XR). \tag{1}$$

En particulier, on remarque $au + bv = c$ (mais non nécessairement à coefficients dans $\mathbb{Z}$). Prenons $\alpha, \beta \in \mathbb{Z}$ avec $a\alpha + b\beta = c$; on a alors $a(\alpha - u) + b(\beta - v) = 0$. On écrit alors

$$(a+XP)(u+XU+\frac{\alpha-u}{b}(b+XQ))+(b+XQ)(v+XV+\frac{\beta-v}{a}(a+XP)) = c+cXR.$$

Cela prouve l'inclusion $\supseteq$ dans le cas $ab \neq 0$.

Maintenant, si on a $a \neq 0$ et $b = 0$ (l'autre cas étant symétrique), on procède comme précédemment jusqu'à obtenir (1). Là, on remarque $au = c = \pm a$ (puisque $b = 0$) et donc $u \in \mathbb{Z}$. Reste à écrire

$$vXQ = (a + XP)(\frac{v}{a}XQ) + (XQ)(-\frac{v}{a}XP)$$

pour voir que l'on a

$$c(1 + XR) = (a + XP)(u + XU + \frac{v}{a}XQ) + (XQ)(XV - \frac{v}{a}XP).$$

Enfin, si on a $a = 0$ et $b = 0$, il existe $n, m \in \mathbb{N}^*$ tels que l'on puisse écrire

$$XP = \frac{1}{n}X^m(a' + XP'), \quad XQ = \frac{1}{n}X^m(b' + XQ'),$$

avec $a', b' \in \mathbb{Z}$, l'un des deux au moins étant non nul. Cela nous ramène aux cas précédents et termine la preuve.

Exercice 9 : Un autre exemple d'anneau non noethérien

On rappelle qu'un nombre complexe x est un *entier algébrique* s'il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire tel que l'on ait $P(x) = 0$. On note $\overline{\mathbb{Z}}$ l'anneau des entiers algébriques.

1. Rappeler pourquoi $\overline{\mathbb{Z}}$ est un anneau.

   Indications : Corollaire 3.4 du polycopié d'Algèbre 1.

2. Montrer que $\overline{\mathbb{Z}}$ n'est pas factoriel.

   Indications : Pour chaque entier $n \geq 1$, on a $2 = (\sqrt[n]{2})^n$. Il suffit donc de montrer que $x_n = \sqrt[n]{2}$ n'est pas inversible dans $\overline{\mathbb{Z}}$. Comme $x_n^{-n} = \frac{1}{2}$, il suffit de montrer que $\frac{1}{2} \notin \overline{\mathbb{Z}}$. Cela découle immédiatement de la remarque suivante : le coefficient dominant d'un polynôme à coefficients dans $\mathbb{Z}$ annulant $\frac{1}{2}$ est pair.

3. Montrer que $\overline{\mathbb{Z}}$ n'est pas noethérien.

   Indications : Pour chaque entier $n \geq 1$, on note $I_n = (\sqrt[n!]{2})$. On a alors $I_n \subseteq I_{n+1}$ pour tout n. Supposons qu'il existe $n \geq 1$ tel que $I_n = I_{n+1}$. Cela impose que $x_0 = 2^{\frac{1}{(n+1)!} - \frac{1}{n!}} \in \overline{\mathbb{Z}}$. On en déduit que $2^{n-1}x_0^{(n+1)!} = \frac{1}{2} \in \overline{\mathbb{Z}}$: absurde (voir question 2) ! Donc $\overline{\mathbb{Z}}$ n'est pas noethérien.

4. Comme dans l'exercice 3, on peut montrer que $\overline{\mathbb{Z}}$ est un anneau de Bézout, mais la preuve dépasse largement le cadre de ce cours.

Exercice 10 : Et encore un exemple d'anneau non noethérien

Soit k un corps. Montrer que la sous-k-algèbre de $k[X, Y]$ engendrée par les X^nY pour $n > 0$ n'est pas noethérienne.

Exercice 11 : Anneau des fonctions continues

Soit X un espace topologique métrisable. À quelle condition sur X l'anneau des fonctions continues de X dans $\mathbb{R}$ est-il noethérien ?

Indications : Notons $C(X)$ l'anneau des fonctions continues de X dans $\mathbb{R}$. Si X est fini, on a $C(X) \cong \mathbb{R}^X$, qui est bien noethérien. Réciproquement, supposons que $C(X)$ est noethérien. Soit $x_0 \in X$. Supposons que $\{x_0\}$ n'est pas ouvert. Pour chaque $n \geq 1$, on note $f_n : X \to \mathbb{R}, x \mapsto d(x, x_0)^{1/n!}$ et $I_n = (f_n)$. La suite (I_n) est une suite croissante d'idéaux qui ne stationne pas : absurde ! Donc $\{x_0\}$ est ouvert et X est muni de la topologie discrète. On en déduit que $C(X) \cong \mathbb{R}^X$. Comme $C(X)$ est noethérien, X est fini.

Exercice 12 : Modules de type fini

Soient A un anneau, M un A-module de type fini et $n \in \mathbb{N}$. Considérons un morphisme surjectif de A-modules $u : M \to A^n$. Montrer que $\mathrm{Ker}(u)$ est un A-module de type fini.

Indications : Soit $(e_1, ..., e_n)$ la base canonique de A^n. Pour chaque i, soit $x_i \in M$ tel que $u(x_i) = e_i$. Soit $f : A^n \to M, e_i \mapsto x_i$. On remarque alors que $A^n \oplus \mathrm{Ker}(u) \to A, (x, y) \mapsto f(x) + y$ est un isomorphisme. Par conséquent, $\mathrm{Ker}(u)$ est un quotient de M, qui est de type fini. Cela achève la preuve.

Exercice 13 : Théorème de Cayley-Hamilton

Soit R un anneau.

1. Soit M un R-module de type fini. Soient $m_1, ..., m_n$ des générateurs de M. Soit f un endomorphisme de M, et considérons une matrice $A = (a_{ij}) \in \mathcal{M}_n(R)$ telle que $f(m_i) = \sum_{j=1}^n a_{ij} m_j$ pour $1 \leq i \leq n$. On note $P(X) = \det(XI_n - A)$. Montrer que $P(f) = 0$.

Indications : Voir le théorème 3.2 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

2. Soit M un R-module de type fini.

(a) Soit I un idéal de R tel que $IM = M$. Montrer qu'il existe $a \in I$ tel que $(1 - a)M = 0$.

Indications : Voir le corollaire 3.5 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

(b) Déduire qu'un endomorphisme surjectif de M est un isomorphisme. Comparer ce résultat à la question 1. de l'exercice précédent.

Indications : Voir le corollaire 3.3 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

3. Montrer que, si m et n sont deux entiers naturels et $g : R^m \to R^n$ est un morphisme injectif de R-modules, alors $m \leq n$.

Indications : Supposons $m > n$. Soit $\tilde{g} : R^m \to R^m = R^n \times R^{m-n}, x \mapsto (g(x), 0)$. On note $(e_1, ..., e_n)$ la base canonique de R^n. D'après la question 1., il existe un polynôme unitaire P à coefficients dans R tel que $P(\tilde{g}) = 0$. Soit P_0 un tel polynôme de degré minimal. On remarque que $0 = P_0(e_n) = P_0(0)e_n$. Par conséquent, $P_0(0) = 0$ et il existe $Q \in R[X]$ unitaire tel que $P_0 = XQ$ et $\deg Q = \deg P_0 - 1$. On a alors $\tilde{g} \circ Q(\tilde{g}) = 0$. Mais par hypothèse, le morphisme $\tilde{g}$ est injectif, et donc $Q(\tilde{g}) = 0$: absurde !

Exercice 14 : Modules projectifs et injectifs

Soit A un anneau.

1. Soient M, N et P trois A-modules. Si l'on a une suite exacte $0 \to M \to N \to P \to 0$, peut-on en déduire que $N \cong M \oplus P$?

> **Indications :** Non : Prendre la suite exacte de $\mathbb{Z}$-modules naturelle :
>
> $$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

2. Soient M, N et P trois A-modules. Montrer que les trois conditions suivantes sont équivalentes :

- il existe un isomorphisme $N \cong M \oplus P$.
- il existe une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ et un morphisme de A-modules $s : P \to N$ tel que $g \circ s = \mathrm{Id}_P$.
- il existe une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ et un morphisme de A-modules $t : N \to M$ tel que $t \circ f = \mathrm{Id}_M$.

> **Indications :** La première propriété implique les deux autres de manière évidente. Si la deuxième propriété est vérifiée, on remarque que $M \oplus P \to N, (m,p) \mapsto f(m) + s(p)$ est un isomorphisme, d'où la première propriété. Si la troisième propriété est vérifiée, on remarque que $N \to M \oplus P, n \mapsto (t(n), g(n))$ est un isomorphisme, d'où la première propriété.

3. On dit qu'un A-module P est *projectif* si la propriété suivante est vérifiée : si M et N sont des A-modules tels qu'il existe une suite exacte $0 \to M \to N \to P \to 0$, alors il existe un isomorphisme $N \cong M \oplus P$.

(a) Montrer qu'un A-module est projectif si, et seulement si, il est un facteur direct d'un A-module libre.

> **Indications :** Soit P un A-module projectif. Soit R le A-module libre de base $(e_p)_{p \in P}$. Le morphisme $f : R \to P, e_p \mapsto p$ est surjectif. On en déduit que $R \cong \mathrm{Ker}(f) \oplus P$, ce qui montre que P est un facteur direct d'un A-module libre. Réciproquement, soit P un A-module facteur direct d'un A-module libre R. On écrit $R = P \oplus T$. Considérons une suite exacte $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. On a alors une suite exacte :
>
> $$0 \to M \oplus T \to N \oplus T \to R \to 0.$$
>
> Soit (e_i) une base de R. Pour chaque i, soit $x_i \in N \oplus T$ tel que l'image de x_i dans R est e_i. Soit $u : R \to N \oplus T, e_i \mapsto x_i$. Ce morphisme induit naturellement un morphisme $s : P \to N$ vérifiant $g \circ s = Id$. La question 2 permet alors de conclure que $N \cong M \oplus P$, ce qui achève la preuve.

(b) Montrer que si A est un corps, alors tout A-module est projectif.

> **Indications :** Dans ce cas, tout A-module est libre, donc projectif.

(c) Montrer que si $A = \mathbb{Z}$, un A-module de type fini est projectif si, et seulement si, il est libre. En utilisant la classification des modules de type fini sur un anneau principal que vous verrez en cours plus tard, on peut montrer que ce résultat subsiste si A est principal.

Indications : Si M est un groupe abélien de type fini projectif, alors il est facteur direct d'un groupe abélien libre : il n'a donc pas de torsion et est lui-même libre d'après la classification des groupes abéliens de type fini.

(d) Supposons que $A = B \times C$ où B et C sont des anneaux non nuls. Montrer que B est un A-module projectif non libre.

Indications : Comme B est un facteur direct de A, il est projectif. Par contre, il n'est pas libre puisqu'il est annulé par $\{0\} \times C$.

On se place dans le cas où A est l'anneau des fonctions continues 2π-périodiques de $\mathbb{R}$ dans $\mathbb{R}$.

(e) Soit P le A-module formé des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ telles que $f(x + 2\pi) = -f(x)$ pour tout $x \in \mathbb{R}$. En construisant un isomorphisme de A-modules $P \oplus P \cong A \oplus A$, montrer que P est projectif. Est-il libre ?

Indications : Les morphismes de A-modules suivants son bien définis et sont inverses l'un de l'autre :

$$\begin{array}{ccc} A \oplus A & \xrightarrow{\sim} & P \oplus P \\ (f, g) & \mapsto & \left(f\cos\left(\frac{x}{2}\right) + g\sin\left(\frac{x}{2}\right), f\sin\left(\frac{x}{2}\right) - g\cos\left(\frac{x}{2}\right)\right) \end{array} ;$$

$$\begin{array}{ccc} P \oplus P & \xrightarrow{\sim} & A \oplus A \\ (f, g) & \mapsto & \left(f\cos\left(\frac{x}{2}\right) + g\sin\left(\frac{x}{2}\right), f\sin\left(\frac{x}{2}\right) - g\cos\left(\frac{x}{2}\right)\right) \end{array} .$$

On a donc un isomorphisme $P \oplus P \cong A \oplus A$ qui montre que P est projectif comme A-module.
Supposons P libre. D'après l'isomorphisme précédent, il serait de rang 1, engendré par un certain $p \in P$. Parce que p vérifie $p(2\pi) = -p(0)$, p s'annule en un point $x \in [0, 2\pi[$: il s'ensuit que tout élément de P s'annule en ce même point x, ce qui est absurde (on peut translater le graphe de p horizontalement).

(f) Soit N le A-module constitué des fonctions continues f de $\mathbb{R}$ dans $\mathbb{R}$ à décroissance rapide (c'est-à-dire telles que, pour tout $n \geq 0$, on a $\lim\limits_{x\to+\infty} x^n f(x) = \lim\limits_{x\to-\infty} x^n f(x) = 0$). Montrer qu'il existe un facteur direct du A-module N isomorphe à P.

Indications : Soit $f \in N$. On note $F(f) : \mathbb{R} \to \mathbb{R}, x \mapsto \sum_{k\in\mathbb{Z}}(-1)^k f(x + 2k\pi)$. On remarque que F définit un morphisme de A-modules $N \to P$. Soit $\lambda : \mathbb{R} \to \mathbb{R}$ qui est affine sur chaque intervalle $[2k\pi, 2(k + 1)\pi]$ pour $k \in \mathbb{Z}$ et telle que $\lambda(2k\pi) = \frac{1}{3\cdot 2^{|k|}}$. On vérifie que λ est continue à décroissance rapide et que $\sum_{k\in\mathbb{Z}} \lambda(x + 2k\pi) = 1$ pour tout $x \in \mathbb{R}$. On en déduit que, si $g \in P$, alors $F(\lambda g) = g$. Le morphisme $F : N \to P$ est donc surjectif. Comme P est projectif, il existe un facteur direct du A-module N isomorphe à P.

4. On dit qu'un A-module M est *injectif* si la propriété suivante est vérifiée : si N et P sont des A-modules tels qu'il existe une suite exacte $0 \to M \to N \to P \to 0$, alors il existe un isomorphisme $N \cong M \oplus P$.

(a) Montrer qu'un A-module M est injectif si, et seulement si, pour tout idéal I de A, tout morphisme de A-modules $I \to M$ s'étend en un morphisme de A-modules $A \to M$.

Indications : Supposons M injectif. Soient I un idéal de A et $f : I \to M$ un morphisme de A-modules. On note $i : I \to A$ l'injection canonique. Soit $N = (M \oplus A)/\{(f(x), i(x)) | x \in I\}$. On considère les deux morphismes $g : A \to N, a \mapsto (0, a)$ et $h : M \to N, m \mapsto (-m, 0)$. On remarque que h est injective et que le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{g} & N \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle h} \\ I & \xrightarrow{f} & M. \end{array}$$

Comme h est injective et M est un module injectif, il existe un morphisme de A-modules $t : N \to M$ tel que $t \circ h = \mathrm{Id}_M$. On remarque alors que, pour $x \in I$, on a $t(g(i(x))) = t(h(f(x))) = f(x)$. Donc $t \circ g : A \to M$ prolonge f.

Réciproquement, supposons que pour tout idéal I de A, tout morphisme de A-modules $I \to M$ s'étend en un morphisme de A-modules $A \to M$. Considérons une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. Soit $\mathcal{E}$ la famille des couples (N', t') où N' est un sous-module de N contenant M et t' est un morphisme $N' \to M$ vérifiant $t \circ f = Id$. On munit $\mathcal{E}$ de l'ordre suivant : $(N', t') \prec (N'', t'')$ si $N' \subseteq N''$ et $t''|_{N'} = t'$. La famille $\mathcal{E}$ est non vide, et l'ordre $\prec$ est inductif. Donc, d'après le lemme de Zorn, $\mathcal{E}$ possède un élément maximal (N_0, t_0). Supposons que $N_0 \neq N$. Soit $n \in N \setminus N_0$. Soit $N_1 = N_0 + An$. Soient $u : A \to N_1, a \mapsto an$ et $v : N_1 \to N_1/N_0$ la projection canonique. Soient $I = \mathrm{Ker}(v \circ u)$ et $w : I \to M, x \mapsto t_0(u(x))$. Par hypothèse, w s'étend en un morphisme $z : A \to M$. On vérifie alors que $t_1 : N_1 = N_0 + An \to M, n_0 + an \mapsto t_0(n_0) + z(a)$ (pour $n_0 \in N_0$ et $a \in A$) est un morphisme de A-modules bien défini tel que $t_1 \circ f = Id$: absurde par maximalité de (N_0, t_0) ! Donc $N_0 = N$, et la question 2. permet de conclure.

(b) Montrer que si A est un corps, alors tout A-module est injectif.

Indications : Dans ce cas, les idéaux de A sont (0) et A, et donc l'énoncé est évident.

(c) Est-ce que $\mathbb{Z}$ est un $\mathbb{Z}$-module injectif ? Pour $n > 0$, est-ce que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif ?

Indications : Le groupe abélien $\mathbb{Z}$ n'est pas injectif, puisque l'on a une suite exacte :

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

mais $\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
Montrons que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif. Soient I un idéal de $\mathbb{Z}/n\mathbb{Z}$ et $f : I \to \mathbb{Z}/n\mathbb{Z}$ un morphisme de $\mathbb{Z}/n\mathbb{Z}$-modules. Il existe $m|n$ et $k \in \mathbb{Z}$ tels que $I = m\mathbb{Z}/n\mathbb{Z}$ et $f(\overline{m}) = k\overline{m}$. Soit $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme qui envoie $\overline{1}$ sur $\overline{k}$. On remarque alors que $\tilde{f}|_I = f$. Cela montre que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif.

On se place maintenant dans le cas $A = \mathbb{Z}$.

(d) Montrer qu'un groupe abélien M est injectif si, et seulement si, il est divisible, c'est-à-dire que pour tout $m \in M$ et tout $n \in \mathbb{N}^*$, il existe $m' \in M$ tel que $m = nm'$.

Indications : Soit M un groupe abélien divisible. Soient I un idéal de $\mathbb{Z}$ et $f : I \to M$ un morphisme. Il existe $n \in \mathbb{N}$ et $m \in M$ tels que $I = (n)$ et $f(n) = m$. Comme M est divisible, il existe $m' \in M$ tel que $nm' = m$. Si l'on définit le morphisme $\tilde{f} : \mathbb{Z} \to M, 1 \mapsto m'$, on remarque que $\tilde{f}|_I = f$. Par conséquent M est injectif.
Réciproquement, soit M un groupe abélien injectif. Soient $n \in \mathbb{N}^*$ et $m \in M$. On définit $f : n\mathbb{Z} \to M, n \mapsto m$. Comme M est injectif, il existe $\tilde{f} : \mathbb{Z} \to M$ tel que $\tilde{f}|_{n\mathbb{Z}} = f$. On remarque que $nf(1) = m$, et donc M est divisible.

(e) Quels sont les groupes abéliens de type fini injectifs ?

Indications : D'après la question précédente et le théorème de classification des groupes abéliens de type fini, le seul groupe abélien de type fini injectif est la groupe trivial.

(f) Montrer que le groupe abélien $\mathbb{R}/\mathbb{Z}$ possède un facteur direct isomorphe à $\mathbb{R}/\mathbb{Q}$.

Indications : On a une suite exacte :

$$0 \to \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Q} \to 0.$$

Le groupe abélien $\mathbb{Q}/\mathbb{Z}$ est divisible, donc injectif. Par conséquent :

$$\mathbb{R}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Q}.$$