GÉNÉRALITÉS SUR LES ANNEAUX ET LES MODULES

JEAN-MARC COUVEIGNES

RÉSUMÉ. On rappelle quelques définitions et résultats élémentaires concernant les anneaux et les modules.

TABLE DES MATIÈRES

1. CONSÉQUENCES DE L'AXIOME DU CHOIX

L'axiome du choix affirme que pour tout ensemble E il existe une application

$$f : \mathcal{P}(E) \smallsetminus \{\varnothing\} \to E$$

telle que pour toute partie non-vide X de E l'on ait

$$f(X) \in X.$$

Une autre formulation affirme que pour toute famille d'ensembles $(E_i)_{i\in I}$ tous non-vides il existe une famille $(x_i)_{i\in I}$ telle que $x_i \in E_i$ pour tout $i \in I$.

Une conséquence fréquemment utilisée de l'axiome du choix est le lemme de Zorn.

Une **chaîne** d'un ensemble ordonné $(E, \leqslant)$ est un sous-ensemble C de E qui est totalement ordonné.

Si F est un sous-ensemble d'un ensemble ordonné $(E, \leqslant)$, on appelle **majorant** de F un élément M de E tel que $M \geqslant x$ pour tout $x \in F$.

On appelle élément **maximal** de E un élément M de E tel que pour tout $x \in E$

$$x \geqslant M \implies x = M.$$

Théorème 1 (Lemme de Zorn)**.** *Soit $(E, \leqslant)$ un ensemble ordonné dont toute chaîne C admet un majorant. Alors $(E, \leqslant)$ a un élément maximal.*

On trouve une démonstration [6] sur la page de Paul Rozière.

Une conséquence fameuse en algèbre est le théorème de la base incomplète.

Date: 8 septembre 2018.

Théorème 2 (Théorème de la base incomplète)**.** *Soit K un corps et E un espace vectoriel sur K. Soit L une partie libre de E. Soit G une partie génératrice de E. Si $L \subset G$ alors il existe une base B de E telle que $L \subset B \subset G$.*

Soit $\mathcal{L}$ l'ensemble des parties libres de E contenant L et contenues dans G. L'ensemble $\mathcal{L}$ est ordonné par la relation d'inclusion. Soit C une chaîne dans $\mathcal{L}$. Si C est vide, elle est majorée par L. On suppose que C est non-vide. L'union U des éléments de C est un sous-ensemble de E qui contient L et est contenu dans G. C'est une partie libre de E. Soit en effet X un sous-ensemble fini de U. Pour tout $x \in X$ il existe un L_x dans C tel que $x \in L_x$. Comme C est totalement ordonné et X fini, l'union des L_x est égale à l'un d'eux, disons L_o pour un o dans X. Donc $X \subset L_o$ est libre. Comme tout sous-ensemble fini de U est libre, U est libre. Donc U est dans $\mathcal{L}$ et majore tous les éléments de C. Les hypothèse du lemme de Zorn sont satisfaites. Il existe donc un élément maximal B dans $\mathcal{L}$. Il est clair que B est une base de E contenue dans G. □

La preuve du théorème suivant utilise le lemme de Zorn et l'arithmétique des nombres cardinaux. Gabriel Nagy a rédigé un résumé [5] de cette arithmétique.

Théorème 3. *Soit K un corps et E un K-espace vetoriel. Soient A et B deux bases de E. Elles ont le même cardinal. Autrement dit, il existe une bijection entre A et B.*

Si A ou B est finie c'est un résultat élémentaire. On suppose donc que A et B sont infinies. Tout élément a de A s'écrit comme combinaison linéaire d'un sous-ensemble fini de B. Soit $S(a)$ l'ensemble des vecteurs de B qui apparaissent avec un coefficient non-nul quand on exprime a dans la base B. On définit ainsi une application $S : A \to \mathrm{Finies}(B)$ de A dans l'ensemble des parties finies de B. Bien que S ne soit pas injective, le nombre d'antécédents d'une partie finie $P \subset B$ par S est au plus égal au cardinal de P, qui est fini. Donc $|A| \leqslant \aleph_0 \times |\mathrm{Finies}(B)|$. Mais $|\mathrm{Finies}(B)| = |B|$ car B est infini. Donc $|A| \leqslant \aleph_0 \times |B| \leqslant |B| \times |B|$ car B est infini. Mais $|B| \times |B| = |B|$ car $|B|$ est infini. Donc $|A| \leqslant |B|$. On montre de même que $|B| \leqslant |A|$. Le théorème de Cantor-Bernstein permet de conclure. □

2. Anneaux commutatifs

Un **anneau** est un triplet $(A, +, .)$ tel que

(1) $(A, +)$ est un groupe abélien. On note 0_A l'élément neutre de A et $-a$ l'opposé de $a \in A$.

(2) La loi de composition $. : A \times A \to A$ est associative et possède un élément neutre noté 1_A.

(3) Pour tout a, b, c dans A on a $a.(b + c) = a.b + a.c$ et $(b + c).a = b.a + c.a$.

Un **morphisme d'anneaux** est une applications $f : A \to B$ telle que $f(1_A) = 1_B$ et pour $a, b \in A$ on ait $f(a + b) = f(a) + f(b)$ et $f(a.b) = f(a).f(b)$.

Cela implique $f(0_A) = 0_B$ et $f(-a) = -f(a)$.

Un **idéal à gauche** de A est un sous-groupe additif $I \subset A$ stable par multiplication à gauche : pour tout $a \in A$ et $x \in I$ on a $a.x \in I$.

Un anneau est dit commutatif si sa multiplication est commutative. Dans ce cas, tout idéal à gauche $I \subset A$ est un idéal à droite et le groupe quotient $(A/I, +)$ hérite d'une structure d'anneau.

Les vingt premières pages du livre [4] de Matsumura exposent les rudiments de la théorie des anneaux commutatifs. On peut consulter aussi le chapitre 2 du livre [2] de Lang.

Dans le reste de cette section on suppose que A est un anneau commutatif.

Un anneau commutatif A est dit **intègre** si $1_A \neq 0_A$ et si le produit de deux éléments non-nuls de A est non-nul.

Un anneau intègre A est dit **principal** si tout idéal de A est principal. L'anneau $\mathbf{Q}[x, y]$ n'est pas principal.

Un idéal I d'un anneau commutatif A est dit **premier** si et seulement si $I \neq A$ et si, pour tous $a, b \in A$,

$$ab \in I \implies a \in I \text{ ou } b \in I.$$

Donc I est premier si et seulement si le quotient A/I est intègre.

On dit que $a \in A$ est **premier** si $a \neq 0$ et l'idéal aA est premier. En particulier a n'est pas une unité.

On note que (0) est un idéal premier si A est intègre bien que 0 ne soit pas premier.

Un idéal I d'un anneau commutatif A est dit **maximal** s'il est maximal pour l'inclusion parmi les idéaux stricts de A. Un idéal I est maximal si et seulement si A/I est un corps. Tout anneau commutatif A admet un idéal maximal. En effet, l'ensemble des idéaux stricts de A satisfait les hypothèses du lemme de Zorn.

Si $I, J \subset A$ sont deux idéaux d'un anneau commutatif, on note $I + J$ l'idéal engendré par $I \cup J$ et IJ l'idéal engendré par les produits xy avec $x \in I$ et $y \in J$. On dit que I et J sont premiers entre eux si $I + J = A$.

En général $IJ \subset I \cap J$ et on a l'égalité si $I + J = A$. Dans ce cas, on vérifie que A/IJ est isomorphe à $A/I \times A/J$.

Soit A un anneau intègre. On dit que $a \in A$ est **irréductible** si $a \neq 0$, a n'est pas une unité, et $a = bc$ implique que b ou c est une unité. Un élément premier est irréductible. Deux éléments irréductibles p et q sont dits **associés** s'il existe une unité u telle que $q = up$. On définit ainsi une relation d'équivalence sur l'ensemble des éléments irréductibles.

Un anneau intègre est dit **factoriel** si tout élément non nul admet une unique décomposition en produit d'irréductibles (à une unité près). Dans un tel anneau, tout élément irréductible est premier. Et toute paire d'éléments non nuls de A admet un plus grand commun diviseur (pgcd) et un plus petit multiple (ppcm). Ils sont définis à une unité près.

Théorème 4. *Un anneau principal (donc intègre donc commutatif) est factoriel.*

Une preuve se trouve dans le chapitre 2 du cours [3] de Qing Liu. □

Théorème 5. *Si A est un anneau factoriel alors $A[x]$ est factoriel.*

Une preuve se trouve dans le chapitre 2 du cours [3] de Qing Liu. □

Si a et b sont deux éléments non-nuls d'un anneau A principal, alors le pgcd de a et b est le générateur de l'idéal $aA + bA$. De même, le ppcm de a et b est le générateur de l'idéal $aA \cap bA$.

Un anneau intègre A est dit **euclidien** s'il existe une application $v : A \setminus \{0_A\} \to \mathbf{N}$ telle que

(1) Si $a, b \in A$ et $b \neq 0_A$ il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0_A$ ou $v(r) < v(b)$.

(2) Si $a, b \in A \setminus \{0_A\}$ alors $v(ab) \geqslant v(a)$.

Exemples : l'anneau $\mathbf{Z}$ des entiers, l'anneau $K[x]$ des polynômes à une indeterminée et à coefficients dans un corps K.

Tout anneau euclidien est principal et donc factoriel.

3. MODULES

Soit A un anneau (unitaire mais pas nécessairement commutatif).

Un A-module (à gauche) est un triplet $(M, +, .)$ tel que $(M, +)$ soit un groupe abélien et la loi de composition externe $. : A \times M \to M$ vérifie pour tous $a, b \in A$ et $x, y \in M$

(1) $a.(x + y) = a.x + a.y$,

(2) $(a + b).x = a.x + b.x$,

(3) $(ab).x = a.(b.x)$,

(4) $1_A.x = x$.

On en déduit que $0_A.x = 0_M$ et $(-a).x = -(a.x)$.

Un morphisme de A-modules (appelé aussi **application linéaire**) est une application $f : A \to B$ entre deux modules telle que pour tous $a \in A$ et $x, y \in M$

(1) $f(x + y) = f(x) + f(y)$,

(2) $f(a.x) = a.f(x)$,

La composée de deux applications linéaires est une application linéaire. Une application linéaire inversible est appelée isomorphisme de A-modules. Son inverse est une application linéaire.

Si A est un corps, un A-module n'est autre qu'un A-espace vectoriel. Et un morphisme de A-modules n'est autre qu'un morphisme de A-espaces vectoriels.

Pour tout entier positif n le produit cartésien A^n muni de la multiplication

$$a.(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

est un A-module.

L'ensemble des applications linéaires entre deux A-modules M et N est noté $\mathrm{Hom}_A(M, N)$. C'est un groupe abélien. Si A est commutatif alors $\mathrm{Hom}_A(M, N)$ est un A-module. Dans ce cas, le A-module $\mathrm{Hom}_A(M, A)$ est appelé **dual** de M. Ses éléments sont appelés des **formes linéaires** sur M.

On note $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$. On le munit des lois + et $\circ$. C'est alors un anneau.

Exercice 1 : Soit A un anneau. Montrer que A est un A-module. Quel est l'anneau $\mathrm{Hom}_A(A, A)$?

Un $\mathbf{Z}$-module n'est autre qu'un groupe commutatif. Les morphismes de $\mathbf{Z}$-modules sont les morphismes de groupes commutatifs.

Soit M un A-module. Pour tout $a \in A$ la multiplication par a définit un endomorphisme du groupe additif M

$$\varphi(a) : \qquad M \longrightarrow M$$

$$x \longmapsto a.x$$

donc $\varphi(a) \in \mathrm{End}_{\mathbf{Z}}(M)$ et l'application

$$\varphi : \qquad A \longrightarrow \mathrm{End}_{\mathbf{Z}}(M)$$

$$a \longmapsto \varphi(a)$$

est un morphisme d'anneaux.

Inversement, la donnée d'un tel morphisme d'anneaux définit une structure de A-module sur M. Si $f : B \to A$ est un morphisme d'anneaux alors la composée $\psi = \varphi \circ f$ définit donc une structure de B-module sur M. Un scalaire $b \in B$ agit sur M par $b.x \overset{\text{def}}{=} f(b).x$.

Exercice 2 :

1. Soit $A = (\mathbf{Z}, +, \times)$ l'anneau des entiers muni des ses lois ordinaires. Soit $M = (\mathbf{Z}/3\mathbf{Z}, +)$ le groupe à trois éléments. Donnez l'ensemble des structures de A-module sur M.

On cherche des morphismes d'anneaux de $\mathbf{Z}$ dans $\mathrm{End}_{\mathbf{Z}}(\mathbf{Z}/3\mathbf{Z}, +) = (\mathbf{Z}/3\mathbf{Z}, +, \times)$. Un tel morphisme envoie 1 sur 1. Donc il existe un unique tel morphisme défini par $\varphi(a) = a \bmod 3$. On trouve la structure naturelle de $\mathbf{Z}$-module.

2. Même question pour $A = (\mathbf{Z}/2\mathbf{Z}, +, \times)$ et $B = (\mathbf{Z}, +)$.

Ici $\mathrm{End}_{\mathbf{Z}}(\mathbf{Z}) = \mathbf{Z}$. S'il existe un morphisme d'anneau φ de $(\mathbf{Z}/2\mathbf{Z}, +, \times)$ dans $\mathbf{Z}$ il envoie $1 \bmod 2$ sur 1 et donc $2 = 2\varphi(1 \bmod 2) = \varphi(2 \bmod 2) = \varphi(0 \bmod 2) = 0$. Contradiction. Il n'y a pas de structure de $(\mathbf{Z}/2\mathbf{Z})$-module sur $\mathbf{Z}$.

Exercice 3 :

1. Soient $A = (\mathbf{Z}, +, \times)$ et $(M, +)$ un groupe commutatif. Donnez l'ensemble des structures de A-module sur M.

Soit φ un morphisme de $\mathbf{Z}$ dans M. Il envoie 1 sur l'identité dans $\mathrm{End}_{\mathbf{Z}}(M)$ car c'est l'élément unité de cet anneau. Donc $\varphi(n) = n\mathrm{Id}$. On trouve la structure naturelle de $\mathbf{Z}$-module.

2. Même question pour $A = (\mathbf{Z}/U\mathbf{Z}, +, \times)$ et $M = (\mathbf{Z}/V\mathbf{Z}, +)$ où U et V sont deux entiers $\geqslant 2$.

L'anneau $(\mathrm{End}_{\mathbf{Z}}(\mathbf{Z}/V\mathbf{Z}), +, \circ)$ est $((\mathbf{Z}/V\mathbf{Z}), +, \times)$. On cherche un morphisme d'anneaux φ de $\mathbf{Z}/U\mathbf{Z}$ dans $\mathbf{Z}/V\mathbf{Z}$. Comme $\varphi(1 \bmod U) = 1 \bmod V$ on a

$$U \bmod V = U\varphi(1 \bmod U) = \varphi(0 \bmod U) = 0$$

donc V divise U.

Donc si V ne divise pas U il n'y pas de structure d'anneau. Et si V divise U il y a une unique structure donnée par $(a \bmod U).(x \bmod V) = ax \bmod V$.

Exercice 4 : Soit $i \in \mathbf{C}$ la racine carrée de -1 de partie imaginaire positive. Soit $A = (\mathbf{Z}[i], +, \times)$ l'anneau des entiers de Gauss.

1. Soit $M = (\mathbf{Z}, +)$. Déterminer l'ensemble des structures de A-module sur M.

On cherche un morphisme d'anneaux φ de $\mathbf{Z}[i]$ dans $\mathbf{Z}$. L'image $\varphi(i)$ de i par φ est un entier naturel qui vérifie $\varphi(i)^2 + 1 = \varphi(i^2 + 1) = \varphi(0) = 0$. On sait qu'un tel entier naturel n'existe pas. Il n'y a pas de structure d'anneau.

2. Soit $M = (\mathbf{Z}/5\mathbf{Z}, +)$. Déterminer l'ensemble des structures de A-module sur M.

On cherche un morphisme d'anneaux φ de $\mathbf{Z}[i]$ dans $\mathbf{Z}/5\mathbf{Z}$. L'image $\varphi(i)$ de i par φ vérifie $\varphi(i)^2 + 1 = \varphi(i^2 + 1) = \varphi(0) = 0$. Cette équation a deux solutions dans $\mathbf{Z}/5\mathbf{Z}$. On peut avoir $\varphi(i) = 2 \bmod 5$ ou $\varphi(i) = 3 \bmod 5$.
La première structure de $\mathbf{Z}[i]$-module est donnée par $(a+bi).(x \bmod 5) = (a+2b)x \bmod 5$ et la deuxième structure de $\mathbf{Z}[i]$-module est donnée par $(a + bi).(x \bmod 5) = (a + 3b)x \bmod 5$.

3. Soit $M = (\mathbf{Z}/3\mathbf{Z}, +)$. Déterminer l'ensemble des structures de A-module sur M.

Exercice 5 : Soit $P(x)$ un polynôme unitaire à coefficients entiers et de degré $\geqslant 1$. Soit U un entier $\geqslant 2$. Soit $A = (\mathbf{Z}[x]/P(x), +, \times)$ et $M = (\mathbf{Z}/U\mathbf{Z}, +)$.
Déterminer l'ensemble des structures de A-module sur M.

On cherche un morphisme d'anneaux φ de $\mathbf{Z}[x]/P(x)$ dans $\mathbf{Z}/U\mathbf{Z}$.
L'image $a = \varphi(x \bmod P(x))$ de $x \bmod P(x)$ par φ vérifie

$$P(a) = P(\varphi(x \bmod P(x))) = \varphi(P(x \bmod P(x))) = \varphi(P(x) \bmod P(x)) = \varphi(0) = 0 \bmod U.$$

Pour toute racine a de $P(x)$ dans $\mathbf{Z}/U\mathbf{Z}$ on a une structure d'anneau définie par $(Q(x) \bmod P(x)).(x \bmod U) = Q(a).x \bmod U$.

Si $(M_i)_{i\in I}$ est une famille de A-modules on note $\prod_{i\in I} M_i$ le **produit** des M_i. Il hérite d'une structure de A-module. La **somme directe** $\oplus_{i\in I} M_i$ est le sous-module de $\prod_{i\in I} M_i$ formé des $(x_i)_{i\in I}$ de support fini. Si tous les M_i sont égaux à un module M on notera plutôt M^I pour le produit et $M^{(I)}$ pour la somme directe.

4. Sous-modules

Un sous-module d'un A-module M est un sous-ensemble N non-vide de M qui soit stable par addition et multiplication scalaire. C'est en particulier un sous-groupe de $(M, +)$. C'est même un A-module, et l'inclusion $N \subset M$ est linéaire.

Soit $f : M \to N$ une application linéaire entre deux A-modules. L'image par f d'un sous-module de M est un sous-module de N. L'image inverse par f d'un sous-module de N est un sous-module de M.

Une intersection de sous-modules est un sous-module. Si $S \subset M$ est un sous-ensemble d'un module M, l'intersection de tous les sous-modules de M contenant S est un sous-module de M

appelé **module engendré** par S. C'est l'ensemble des combinaisons linéaires d'éléments de S. Si M est engendré par S on dit que S est une partie **génératrice** de M.

Si $(M_i)_{i\in I}$ est une famille de sous-modules de M, on appelle **somme** des M_i et on note $\sum_{i\in I} M_i$ le sous-module engendré par l'union des M_i.

On dit qu'un (sous)-module est de **type fini** s'il est engendré par un ensemble fini. Un module est dit **nœthérien** si tous ses sous-modules sont de type fini. Un anneau A est dit nœthérien s'il est nœthérien comme A-module.

Si $(M_i)_{i\in I}$ est une famille de sous-modules d'un module M il existe une application A-linéaire naturelle de sommation $\oplus_{i\in I} M_i \to M$. Cette application est bijective si et seulement si tout élément x de M s'écrit de façon unique comme somme finie d'éléments $x_i \in M_i$. On identifiera alors M et la somme directe $\oplus_{i\in I} M_i$.

Si $N \subset M$ est un sous-module, on appelle **supplémentaire** de N un sous-module P de M tel que $M = N \oplus P$.

Théorème 6. *Un sous-module N de M admet un supplémentaire si et seulement s'il existe une application linéaire $p : M \to M$ telle que $p \circ p = p$ et $\mathrm{Im}(p) = N$. Dans ce cas, le noyau de p est un supplémentaire de N.*

Si N admet un supplémentaire Q alors $M = N \oplus Q$. On note $p : M \to M$ l'application qui envoie $m \in M$ sur n où $m = n + q$ avec $n \in N$ et $q \in Q$ est l'unique décomposition de m comme somme d'un élément de N et d'un élément de Q. On vérifie que p est une application linéaire, que le noyau de p est Q, que l'image de p est N, et que la restriction de p à N est l'identité. On en déduit que $p \circ p = p$.

Réciproquement, s'il existe une application $p : M \to M$ telle que $p \circ p = p$ et $\mathrm{Im}(p) = N$ alors posons $Q = \mathrm{Ker}(p)$.

Tout élément m de M s'écrit $m = (m - p(m)) + p(m)$ avec $p(m) \in N$ et $m - p(m) \in Q$ car $p(m - p(m)) = p(m) - p(p(m)) = 0$.

Si $m \in N \cap Q$ alors $m = p(r)$ pour un r dans M et $p(m) = 0 = p(p(r)) = p(r) = m$.

Donc $M = N \oplus Q$. □

On dit qu'une famille $(x_i)_{i\in I}$ d'éléments de M est **libre** si toute combinaison linéaire des x_i est triviale :

$$\forall (a_i)_{i\in I} \in A^{(I)}, \sum_i a_i x_i = 0 \implies \forall i \in I, a_i = 0.$$

Une famille $(x_i)_{i\in I}$ libre et génératrice est appelée **base** du module. Si M admet une base $(x_i)_{i\in I}$ on dit qu'il est **libre**. On a alors

$$M = \oplus_{i\in I} A x_i.$$

Pour tout ensemble I le module $A^{(I)}$ est libre. En effet, posant $e_i = (\delta_{i,j} 1_A)_{j\in I}$ on vérifie que $(e_i)_{i\in I}$ est une base de $A^{(I)}$. On l'appelle la **base canonique**.

Théorème 7. *Soit A un anneau commutatif et r un entier positif. Soit M un A-module et b_1, b_2, …, b_r des éléments de M. On suppose que $(b_1, \ldots, b_r)$ est une base de M. Pour tout i tel que $1 \leqslant i \leqslant r$ on définit une forme linéaire $\varphi_i : M \to A$ par*

$$\varphi_i\Big(\sum_{1\leqslant j\leqslant r} a_j.b_j\Big) = a_i.$$

Les $(\varphi_i)_{1\leqslant i\leqslant r}$ forment une base de $\hat{M}$. On les appelle les formes coordonnées associées à la base $(b_i)_{1\leqslant i\leqslant r}$.

On note d'abord que les φ_i sont bien définies car tout vecteur de M s'écrit de façon unique comme combinaison des éléments de la base $(b_1,\dots,b_r)$.

Soient $(u_i)_{1\leqslant i\leqslant r}$ des éléments de A. Si la forme $\psi = \sum_{1\leqslant i\leqslant r} u_i\varphi_i$ est nulle alors $\psi(b_j) = u_j = 0$ pour tout j. Donc les formes linéaires $(\varphi_i)_{1\leqslant i\leqslant r}$ sont linéairement indépendantes.

Soit $\psi \in \mathrm{Hom}_A(M,A)$ une forme linéaire. On vérifie que $\psi = \sum_{1\leqslant i\leqslant r} \psi(b_i)\varphi_i$. Donc les formes linéaires $(\varphi_i)_{1\leqslant i\leqslant r}$ engendrent $\hat{M}$. □

Théorème 8. *Soit A un anneau. Soit M un A-module libre et $(x_i)_{i\in I}$ une base de M. Soit N un A-module et $(y_i)_{i\in I}$ des éléments de N. Il existe une unique application linéaire de M dans N qui envoie x_i sur y_i pour tout i.*

Soit $f : M \to N$ l'application qui à $\sum_{i\in I} a_i x_i$ associe $\sum_{i\in I} a_i y_i$. Cette application est bien définie, linéaire, et elle envoie x_i sur y_i. L'unicité de f est évidente. □

Théorème 9. *Soit A un anneau commutatif. Toutes les bases d'un A-module libre ont le même cardinal.*

Il suffit de montrer que si les modules $A^{(X)}$ et $A^{(Y)}$ sont isomorphes alors $|X| = |Y|$. Soit I un idéal maximal de A. L'anneau quotient $K = A/I$ est un corps. S'il existe un isomorphisme de A-modules $f : A^{(X)} \to A^{(Y)}$ alors l'application f envoie le sous-module $I^{(X)}$ dans $I^{(Y)}$. Elle induit donc un morphisme de groupes additifs F entre les groupes quotients

$$F : K^{(X)} \to K^{(Y)}$$

qui est un isomorphisme de K-espaces vectoriels. Le théorème 3 permet de conclure. □

Le cardinal commun à toutes les bases d'un module libre sur un anneau commutatif est appelé **rang** de ce module.

Exercice 6 : Montrez que le $\mathbf{Z}$-module $(\mathbf{Q}/\mathbf{Z},+)$ n'est pas de type fini.

Exercice 7 : Montrez que $S = \{2,3\}$ est un système de générateurs minimal au sens de l'inclusion pour le $\mathbf{Z}$-module $\mathbf{Z}$. Est-ce une base ?

Exercice 8 : Soit Q le sous-ensemble de $\mathbf{Q}^*$ formé de tous les carrés.

1. Montrez que Q est un sous-groupe du groupe abélien $(\mathbf{Q}^*,\times)$.

2. Montrez que le groupe quotient $M = \mathbf{Q}^*/Q$ est un espace vectoriel sur le corps à deux éléments $\mathbf{F}_2$.

3. Donnez une base de M.

Si $N \subset M$ est un sous-module, le groupe additif quotient M/N est muni d'une unique structure de A-module qui rend l'application quotient $\pi : M \to M/N$ linéaire. Le A-module M/N est appelé **module quotient** de M par N.

Théorème 10. *Pour toute application linéaire $f : M \to P$ qui s'annule sur N il existe une unique application linéaire $\tilde{f} : M/N \to P$ telle que $f = \tilde{f} \circ \pi$.*

Si $m+N$ est une classe dans M/N on pose $\tilde{f}(m+N) = f(m)$. L'application $\tilde{f}$ est bien définie car f s'annule sur N. Elle est linéaire car f est linéaire. On a $f = \tilde{f} \circ \pi$ par définition. L'unicité résulte de la surjectivité de π. □

Cette propriété caractérise le module quotient M/N. Une conséquence évidente du théorème ci-dessus :

Théorème 11. *Soit $f : M \to N$ une application linéaire entre deux A-modules. Alors les A-modules $\mathrm{Im}(f)$ et $M/\mathrm{Ker}(f)$ sont isomorphes.*

Soit $F : M \to \mathrm{Im}(f)$ l'application définie par $F(m) = f(m)$ pour tout m dans M. Comme F s'annule sur $\mathrm{Ker}(f) = \mathrm{Ker}(F)$ le théorème précédent donne une application linéaire $\tilde{F} : M/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ telle que $\tilde{F}(m + \mathrm{Ker}(f)) = f(m)$. Il est immédiat que F est injective et surjective. □

Soit M un A-module et $(x_i)_{i\in I}$ une famille d'éléments de M. Soit $(e_i)_{i\in I}$ la base canonique de $A^{(I)}$. On a $e_i = (\delta_{i,j}1_A)_{j\in I}$. Il existe une unique application linéaire $f : A^{(I)} \to M$ telle que $f(e_i) = x_i$. On a $f((a_i)_{i\in I}) = \sum_{i\in I} a_i x_i$. Le noyau de f est appelé **module des relations** entre les x_i. Si la famille $(x_i)_{i\in I}$ est génératrice alors f est surjective et M est isomorphe au quotient de $A^{(I)}$ par le module des relations.

Exercice 9 : Montrer que tout A-module est quotient d'un module libre.

Soit M un A-module. Soit $(g_i)_{i\in I}$ une partie génératrice. Soit $f : A^{(I)} \to M$ l'application linéaire qui envoie $(a_i)_{1\le i\le I}$ sur $\sum_{1\le i\le I} a_i g_i$. L'image de f est M. Donc M est isomorphe au quotient de $A^{(I)}$ par $\mathrm{Ker}(f)$.

Exercice 10 : Soit $A = \mathbf{Z}$ et $M = \mathbf{Z}^2$. Soit N le sous-module de M engendré par $(3, 2)$.

1. Donnez un supplémentaire de N.

Le sous-module P de M engendré par $(1, 1)$ est un supplémentaire de N.
D'abord $(1, 0) = (3, 2) - 2.(1, 1)$ et $(0, 1) = 3.(1, 1) - (3, 2)$. Donc $N + P = M$.
Un élément de l'intersection de N et P s'écrit $x.(3, 2) = y.(1, 1)$. On en déduit que $3x - y = 0$ et $2x - y = 0$. Donc $x = y = 0$ et l'intersection $N \cap P$ est nulle.

2. Décrivez tous les supplémentaires de N.

Si R est un supplémentaire de N dans M alors $M = N \oplus R$. Donc R est isomorphe à M/N. Donc tous les supplémentaires sont isomorphes entre eux. Donc R est isomorphe à P. Donc c'est

un module libre de rang 1. Soit (a,b) un générateur de R. Comme $M = R + N$ il existe quatre scalaires x, y, z, t tels que $x.(a,b) + y.(3,2) = (1,0)$ et $z.(a,b) + t.(3,2) = (0,1)$. Autrement dit

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \times \begin{pmatrix} a & b \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Donc le déterminant de la matrice $\begin{pmatrix} a & b \\ 3 & 2 \end{pmatrix}$ est une unité de $\mathbf{Z}$. Donc $2a - 3b = \pm 1$.

Donc tout supplémentaire de N est de la forme $\mathbf{Z}.(a,b)$ avec a et b des entiers tels que

$$2a - 3b = \pm 1.$$

La réciproque se prouve comme à la première question.

3. Donnez un sous-module de M qui n'admet pas de supplémentaire.

Soit $N = 2M$ le sous-module formé des vecteurs lignes à coefficients pairs. Si N a un supplémentaire P alors $P \subset M$ est isomorphe à M/N donc à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$. En particulier $2P$ est le module nul. Mais tout m dans M tel que $2.m = 0$ est nul. Donc $P = \{0\}$. Mais $\{0\}$ n'est pas un supplémentaire de N. Donc il n'y a pas de supplémentaire.

Exercice 11 : Soit $f : M \to N$ une application linéaire surjective entre deux A-modules. Montrer que si N est libre il existe une application linéaire $s : N \to M$ telle que $f \circ s = \mathrm{Id}_N$.

Exercice 12 : Soit X un ensemble infini et A un anneau. Montrer que l'anneau A^X n'est pas nœthérien.

Théorème 12. *Soit A un anneau et M un A-module. Alors M est nœthérien si et seulement si toute suite croissante de sous-modules de M est stationnaire.*

Supposons que M est nœthérien et soient $(N_k)_{k\in\mathbf{N}}$ des sous-modules de M qui forment une suite croissante pour l'inclusion

$$N_0 \subset N_1 \subset N_2 \subset \dots.$$

On note U l'union des N_k. C'est un sous-module de M.

En effet si u et v sont dans U alors il existe deux entiers a et b tels que $u \in N_a$ et $v \in N_b$. Supposons par exemple que $a \geqslant b$. Alors u et v sont tous les deux dans le sous-module N_a. Donc toutes leurs combinaisons linéaires $\lambda.u + \mu.v$ sont dans N_a donc dans U.

Le sous-module U est de type fini car M est nœthérien. Soit donc $(g_1, \dots, g_m)$ une famille génératrice de U. Il existe des entiers $k_1, \dots, k_m$ tels que $g_i \in N_{k_i}$ pour $1 \leqslant i \leqslant m$. Soit ℓ le plus grand des k_i. On vérifie que les g_i sont tous dans N_ℓ. Donc U est inclus dans N_ℓ et donc $N_k = U$ pour tout $k \geqslant \ell$. La suite stationne à partir de ℓ.

Supposons maintenant que toute suite croissante de sous-modules de M est stationnaire et montrons que M est nœthérien. Soit N un sous-module de M. Si N est nul il est de type fini. Si N n'est pas nul on pose $N_0 = \{0\}$ et on choisit un élément n_1 dans $N - N_0$. Si N est engendré

par n_1 il est de type fini. Sinon appelons N_1 le module engendré par n_1 et choisissons un élément n_2 dans $N - N_1$. Si N est engendré par $\{n_1, n_2\}$ il est de type fini. Sinon appelons N_2 le module engendré par (n_1, n_2) et choisissons un élément n_3 dans $N - N_2$.

Si N n'est pas de type fini on construit ainsi une suite infinie de sous-modules strictement croissante. Contradiction. □

Théorème 13. *Si M est un A-module et $N \subset M$ un sous-module, alors M est nœthérien si et seulement si N et M/N le sont.*

Supposons que M est nœthérien. Tout sous-module de N est un sous-module de M. Il est donc de type fini. Donc N est nœthérien. Soit maintenant P un sous-module de M/N et appellons Q l'image réciproque de P par l'application quotient $M \to M/N$. C'est un sous-module de M. Il est de type fini car M est nœthérien. Soit $(g_1, \dots, g_n)$ une famille génératrice de Q. Les classes $G_i = g_i + N$ forment une famille génératrice de P. Donc P est nœthérien.

Supposons maintenant que N et M/N sont nœthériens et montrons que M est nœthérien.

Soit P un sous-module de M.

Soit Q l'image de P dans M/N. C'est un sous-module de M/N. Il est de type fini car M/N est nœthérien. Soit $(G_1, \dots, G_n)$ une famille génératrice de Q. Les G_i sont des classes modulo N. Pour tout i entre 1 et n on choisit un g_i dans G_i.

Soit $R = P \cap N$ l'intersection de P et N. C'est un sous-module de N. C'est un module de type fini car N est nœthérien. Soit $(h_1, \dots, h_m)$ une famille génératrice de R. L'ensemble des g_i et des h_j est une famille génératrice de P.

En effet, si $x \in P$, la classe $x + N$ est une combinaison des G_i

$$x + N = \sum_{1 \leqslant i \leqslant n} a_i G_i,$$

donc la différence $y = x - \sum_{1 \leqslant i \leqslant n} a_i g_i$ est dans N. On peut donc écrire

$$y = \sum_{1 \leqslant j \leqslant m} b_j h_j.$$

On a donc

$$x = \sum_{1 \leqslant i \leqslant n} a_i g_i + \sum_{1 \leqslant j \leqslant m} b_j h_j.$$

Le sous-module P est donc de type fini. Ainsi M est nœthérien. □

Théorème 14. *Si un anneau A est nœthérien (comme A-module) alors tout A-module de type fini est nœthérien.*

L'application répétée du théorème 13 montre que A^n est un module nœthérien pour tout $n \geqslant 0$. Un module de type fini est quotient d'un module libre de type fini, il est donc nœthérien. □

Le théorème suivant est dû à Hilbert.

Théorème 15. *Si A est un anneau nœthérien, l'anneau des polynômes $A[X]$ est nœthérien.*

Soit I un idéal de $A[X]$. C'est un $A[X]$-module. C'est aussi un A-module. Pour tout $n \geqslant 0$ on note $I_n \subset A$ l'ensemble des scalaires a tels qu'il existe un polynôme $P(X)$ dans I de la forme

$$aX^n + \sum_{0 \leqslant i < n} c_i X^i$$

avec $c_i \in A$. On vérifie que I_n est un idéal de A. C'est l'ensemble des coefficients de X^n dans les polynômes de I qui sont de degré $\leqslant n$. Les $(I_n)_{n\geqslant 0}$ forment une suite croissante d'idéaux de A. Comme A est nœthérien, il existe un entier p tel que $I_n = I_p$ pour $n \geqslant p$. Pour tout entier $n \leqslant p$ on choisit un système de générateurs $a_{n,1}, a_{n,2}, \ldots, a_{n,s_n}$ du A-module I_n. Il existe des polynômes $P_{n,1}(X), P_{n,2}(X), \ldots, P_{n,s_n}(X)$ dans I de degré $\leqslant n$ tels que le coefficient de X^n dans $P_{n,k}(X)$ est $a_{n,k}$. On montre que la famille $\mathcal{P}$ constituée de tous les $P_{n,k}(X)$ pour $0 \leqslant n \leqslant p$ et $1 \leqslant k \leqslant s_n$ engendre l'idéal I.

Supposons le contaire.

Soit $J \subset A[X]$ l'idéal engendré par les $P_{n,k}(X)$ pour $0 \leqslant n \leqslant p$ et $1 \leqslant k \leqslant s_n$.

Soit $Q(X)$ un polynôme de degré minimum dans le complémentaire $I \smallsetminus J$ de J dans I. Soit d le degré de $Q(X)$. Soit b le coefficient directeur de $Q(X)$. Donc $b \in I_d$.

Si $d \geqslant p$ alors $I_d = I_p$ et il existe des scalaires $u_1, \ldots, u_{s_p}$ tels que

$$b = u_1 a_{p,1} + u_2 a_{p,2} + \cdots + u_{s_p} a_{p,s_p}.$$

Le polynôme

$$R = Q - u_1 X^{d-p} P_{p,1} - u_2 X^{d-p} P_{p,2} - \cdots - u_{s_p} X^{d-p} P_{p,s_p}$$

est de degré $< d$. Il est dans I car I est un idéal de $A[X]$. Il n'est pas dans J sinon

$$Q = R + u_1 X^{d-p} P_{p,1} + u_2 X^{d-p} P_{p,2} + \cdots + u_{s_p} X^{d-p} P_{p,s_p}$$

y serait aussi. On a donc trouvé un polynôme dans $I \smallsetminus J$ de degré $< d$. Contradiction.

Si $d < p$ alors il existe des scalaires $u_1, \ldots, u_{s_d}$ tels que

$$b = u_1 a_{d,1} + u_2 a_{d,2} + \cdots + u_{s_d} a_{d,s_d}.$$

Le polynôme

$$R = Q - u_1 P_{d,1} - u_2 P_{d,2} - \cdots - u_{s_d} P_{d,s_d}$$

est de degré $< d$. Il est dans I car I est un idéal de $A[X]$. Il n'est pas dans J sinon

$$Q = R + u_1 P_{d,1} + u_2 P_{d,2} + \cdots + u_{s_p} P_{p,s_p}$$

y serait aussi. On a donc trouvé un polynôme dans $I \smallsetminus J$ de degré $< d$. Contradiction. □

Si x est un élément d'un A-module M on note $\mathrm{Ann}(x)$ et on appelle **annulateur** de x l'ensemble des $a \in A$ tels que $a.x = 0_M$. C'est un idéal (à gauche) de A.

Si S est un sous-ensemble de M on note $\mathrm{Ann}(S)$ et on appelle **annulateur** de S l'intersection des $\mathrm{Ann}(x)$ pour $x \in S$.

On note M_{tors} et on appelle **sous-ensemble de torsion** de M l'ensemble des $x \in M$ tels que $\mathrm{Ann}(x) \neq \{0\}$. Si A est commutatif et intègre, le sous-ensemble de torsion de M est un sous-module.

Soit $a \in A$ un scalaire et M un A-module. La multiplication par a est une application linéaire de M dans M. Son image est notée aM. Le quotient M/aM est annulé par a.

Exercice 13 : Soit A un anneau et M et N deux A-modules. Montrer que $a(M \oplus N) = aM \oplus aN$.

Exercice 14 : Soit A un anneau principal. Soit M un A-module. Soit p un élément irréductible de A.

1. Montrer que M/pM est un espace vectoriel sur le corps $K = A/p$.

2. Montrer que si $M = M_1 \oplus M_2$ alors M/pM est isomorphe à $(M_1/pM_1) \oplus (M_2/pM_2)$.

3. On note $M(p)$ l'ensemble des éléments de M qui sont annulés par p. Donc

$$M(p) = \{x \in M \mid p.x = 0\}.$$

Montrer que $M(p)$ est un sous-module de M.

4. Montrer que $M(p)$ est un espace vectoriel sur le corps $K = M/p$.

5. Montrer que si $M = M_1 \oplus M_2$ alors $M(p)$ est isomorphe à $M_1(p) \oplus M_2(p)$.

6. On suppose que $A = \mathbf{Z}$ et $p = 3$ et $M = (\mathbf{Z}/45\mathbf{Z}) \times (\mathbf{Z}/270\mathbf{Z})$. Calculer la dimension de $M(p)$ et M/pM.

7. On suppose que $A = \mathbf{Z}$ et $p = 3$ et $M = \mathbf{Q}/\mathbf{Z}$. Calculer la dimension de $M(p)$ et M/pM.

Exercice 15 : Soit A un anneau principal.

Soient a et b deux scalaires non-nuls. On pose $M = A/bA$.

1. Montrer que si a et b sont premiers entre eux l'application $[a] : x \mapsto a.x$ est une bijection de M.

Il existe deux scalaires λ et μ dans A tels que $\lambda a + \mu b = 1$. Soit $m = x + bA$ dans M. On vérifie que $\lambda am = m$. Donc $[a]$ est une bijection d'application réciproque $[\lambda]$.

2. Montrer que si a divise b l'image de $[a]$ est isomorphe à A/cA avec $b = ac$ et $c \in A$. Et le noyau de $[a]$ est isomorphe à A/aA.

On définit une application linéaire $f : A \to aA$ entre les deux A-modules A et aA par $f(x) = a.x$. L'image de cA par f est acA. Il existe donc une application $F : A/cA \to aA/acA$ telle que $F(x + cA) = ax + acA$. On vérifie que cette application est bijective. Or aA/acA est l'image de $[a]$ dans A/acA. Donc l'image de $[a]$ est isomorphe à A/cA.

Un élément $x + bA$ de A/bA est dans le noyau de a si et seulement si $b = ac$ divise ax. C'est le cas si et seulement si c divise x car a est non-nul. Donc le noyau de $[a]$ est cA/bA. On montre que l'application linéaire $G : A/aA \to cA/acA$ définie par $G(x + aA) = cx + acA$ est bijective. Donc le noyau de $[a]$ est isomorphe à A/aA.

3. Montrer qu'en général le noyau $A(a)$ de $[a]$ est isomorphe à $A/\mathrm{pgcd}(a, b)A$ et son image est isomorphe à A/cA avec $c = b/\mathrm{pgcd}(a, b)$.

On pose $d = \mathrm{pgcd}(a, b)$. On écrit $b = dc$ et $a = de$ avec e premier à b. Donc $[a] = [d] \circ [e] = [e] \circ [d]$. Comme $[e]$ est bijective, le noyau de $[a]$ est le noyau de $[d]$ et l'image de $[a]$ est l'image de $[d]$.

RÉFÉRENCES

[1] Olivier Brinon. *Cours de Master 1 : modules, espaces quadratiques*. Université de Bordeaux, 2017. https://www.math.u-bordeaux.fr/~obrinon/enseignement/modules/modules.pdf.

[2] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[3] Qing Liu. *Cours de Licence 3 : structure algébrique 2*. Université de Bordeaux, 2017. https://www.math.u-bordeaux.fr/~qliu/Enseignement/poly-2017.pdf.

[4] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[5] Gabriel Nagy. *Cardinal arithmetic*. Kansas State University. https://www.math.ksu.edu/~nagy/real-an/ap-b-card.pdf.

[6] Paul Rozière. *Démonstration du Lemme de Zorn*. Université Paris 7, 2016. https://www.irif.fr/~roziere/thEnsL/zorn.pdf.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, BORDEAUX INP, INRIA, CNRS, UMR 5251, F-33400 TALENCE, FRANCE.

E-mail address: Jean-Marc.Couveignes@u-bordeaux.fr