

Chapitre 1

Généralités

Tous les anneaux sont supposés commutatifs, unitaires et non triviaux.

Compléments au cours de L3 sur les anneaux de fractions

Soient A un anneau commutatif non trivial et S une partie multiplicative de A , c'est-à-dire contenant 1 et stable pour la multiplication. Dans le cours de L3, l'anneau de fractions $S^{-1}A$ a été défini dans le cas où A est intègre, comme sous-anneau du corps des fractions de A . Cependant, en adaptant la construction du corps des fractions, il est possible de définir des anneaux de fractions en toute généralité. Nous le ferons en laissant les démonstrations en exercice ; voir là-dessus les ouvrages cités en bibliographie de ce chapitre.

Sur l'ensemble produit $A \times S$, on définit une relation \sim et deux lois de composition interne $+$ et \cdot comme suit :

$$\begin{aligned}(a, s) \sim (a', s') &\iff \exists t \in S : t(as' - a's) = 0, \\ (a, s) + (b, t) &:= (at + bs, st), \\ (a, s) \cdot (b, t) &:= (ab, st).\end{aligned}$$

La relation \sim est alors une relation d'équivalence compatible avec les lois $+$ et \cdot et les lois induites sur l'ensemble quotient $(A \times S) / \sim$ font de ce dernier un anneau commutatif. On note $S^{-1}A$ cet anneau et a/s la classe de $(a, s) \in A \times S$ dans $S^{-1}A$. L'application $\phi : a \mapsto a/1$ de A dans $S^{-1}A$ est un morphisme d'anneaux.

Remarque 1.0.2 Si l'on avait simplement défini $(a, s) \sim (a', s')$ par $a's = as'$, on ne pourrait pas prouver la transitivité pour un anneau A arbitraire (non supposé intègre) ?

Exercice 1.0.3 À quelle condition l'anneau $S^{-1}A$ est-il trivial ? Quel est le noyau du morphisme ϕ ? En déduire une condition pour que ϕ soit injectif.

Le morphisme ϕ possède la *propriété universelle* suivante : pour tout anneau commutatif B et tout morphisme d'anneaux $f : A \rightarrow B$ tel que $f(S) \subset B^*$, il existe un unique morphisme d'anneaux $g : S^{-1}A \rightarrow B$ tel que $f = g \circ \phi$.

Soient maintenant S_1, S_2 deux parties multiplicatives de A telles que $S_1 \subset S_2$ et soient $\phi_i : A \rightarrow S_i^{-1}A$ ($i = 1, 2$) les morphismes associés. Il découle de la propriété universelle ci-dessus qu'il existe un unique morphisme d'anneaux $\psi : S_1^{-1}A \rightarrow S_2^{-1}A$ tel que $\phi_2 = \psi \circ \phi_1$. (Lorsque A est intègre et $S_2 = A \setminus \{0\}$, on reconnaît la réalisation de $S_1^{-1}A$ comme sous-anneau du corps des fractions, voir le cours de L3).

Exercice 1.0.4 On note \bar{S} (*saturé* de S) l'ensemble des diviseurs des éléments de S . Montrer que c'est une partie multiplicative contenant S et que le morphisme $S^{-1}A \rightarrow \bar{S}^{-1}A$ déduit de la propriété ci-dessus est un isomorphisme.

Soit I un idéal de A . On vérifie que $S^{-1}I$ s'identifie naturellement à un idéal de $S^{-1}A$, et que ce dernier est engendré par $\phi(I)$. Soit J un idéal de $S^{-1}A$ et soit $I := \phi^{-1}(J)$ (qui est donc un idéal de A). Alors $J = S^{-1}I$. En particulier, si A est un anneau "noetherien" (*i.e.* tel que tout idéal est de type fini), resp. principal, $S^{-1}A$ l'est également.

Exercice 1.0.5 Montrer que les applications $\mathfrak{P} \mapsto S^{-1}\mathfrak{P}$ et $\mathfrak{Q} \mapsto \phi^{-1}(\mathfrak{Q})$ sont des bijections réciproques l'une de l'autre entre l'ensemble des idéaux premiers de A ne rencontrant pas S et l'ensemble des idéaux premiers de $S^{-1}A$.

1.1 Modules, sous-modules

Définition 1.1.1 Soit A un anneau. Un *module (à gauche) sur A* , ou *A -module (à gauche)* est un groupe abélien $(M, +)$ muni en outre d'une loi de composition externe $A \times M \rightarrow M$, $(a, x) \mapsto ax$, telle que, quels que soient $a, b \in A$ et $x, y \in M$:

$$\begin{aligned}(a+b)x &= ax + bx, \\ a(x+y) &= ax + ay, \\ 1x &= x, \\ a(bx) &= (ab)x.\end{aligned}$$

Remarque 1.1.2 En développant $(1+1)(x+y)$ de deux façons, on voit que $x+y = y+x$; autrement dit, la commutativité du groupe $(M, +)$ est conséquence des autres axiomes.

Exercice 1.1.3 Vérifier que les quatre axiomes ci-dessus équivalent à la condition suivante : l'application $a \mapsto (x \mapsto ax)$ est un morphisme d'anneaux de A dans l'anneau des endomorphismes du groupe $(M, +)$.

On déduit très facilement des propriétés similaires à celles des espaces vectoriels. Cependant, l'une de ces propriétés est ici en défaut :

$$ax = 0_M \not\iff (a = 0_A \text{ ou } x = 0_M).$$

Cherchez parmi les exemples ci-dessous lesquels ne la vérifient pas.

Exemples 1.1.4 1. Lorsque A est un corps, les A -modules sont les A -espaces vectoriels.

2. Tout groupe abélien est un \mathbf{Z} -module d'une unique manière : si $m \in \mathbf{N}$, on pose $mx := x + \dots + x$ (somme de m termes), si $m \in -\mathbf{N}$, on pose $mx := -|m|x$.

3. Tout idéal de A est de façon naturelle un A -module.
4. Pour tout ensemble I , les groupes A^I (ensemble des familles d'éléments de A indexées par I) et $A^{(I)}$ (sous-ensemble de A^I formé des familles à support fini, *i.e.* des $(a_i)_{i \in I} \in A^I$ tels que presque tous les a_i sont nuls) sont des A -modules avec la définition évidente de la loi externe : $a(a_i)_{i \in I} := (aa_i)_{i \in I}$.
5. De manière générale, si l'on a une famille de A -modules M_i , le groupe produit $\prod M_i$ est un A -module avec la définition évidente de la loi externe : $a(x_i)_{i \in I} := (ax_i)_{i \in I}$. Il en est de même du sous-groupe somme-directe $\bigoplus M_i$ de $\prod M_i$ (formé des $(x_i)_{i \in I} \in \prod M_i$ tels que presque tous les x_i sont nuls).
6. Soit M un A -module et soit $f : A' \rightarrow A$ un morphisme d'anneaux. En posant $a'x := f(a')x$, on fait de M un A' -module. En particulier, si A' est un sous-anneau de A , la restriction à $A' \times M$ de la loi externe $A \times M \rightarrow M$ fait de M un A' -module (*restriction des scalaires*).

Un exemple particulièrement important. Cet exemple constitue (avec l'exemple ci-dessus des \mathbf{Z} -modules) une application essentielle de ce chapitre. Pour bien le comprendre, il est souhaitable de réviser le cours d'algèbre linéaire de L2 sur la réduction des endomorphismes, en particulier tout ce qui concerne les polynômes d'endomorphismes. Soient K un corps commutatif arbitraire et $A := K[X]$.

- Soit M un A -module. Par restriction des scalaires $K \subset A$, on en fait un K -espace vectoriel que nous noterons V (pour bien clarifier ce qui va suivre). L'application $\phi : x \mapsto Xx$ de V dans lui-même est un endomorphisme du K -espace vectoriel V .
- Réciproquement, soient V un espace vectoriel sur K et ϕ un endomorphisme de V . On définit une loi externe $A \times V \rightarrow V$ en posant $Px := (P(\phi))(x)$. On obtient ainsi un A -module que nous noterons M (pour le distinguer de l'espace vectoriel V). Le moins trivial à vérifier des quatre axiomes est le dernier ; il découle de la règle bien connue $(P(\phi)) \circ (Q(\phi)) = PQ(\phi)$.

Remarque 1.1.5 En un certain sens, un \mathbf{Z} -module “est la même chose” qu'un groupe abélien et un $K[X]$ -module “est la même chose” qu'un K -espace vectoriel muni d'un endomorphisme. On peut donc prévoir que la théorie des modules sur les anneaux principaux (ici \mathbf{Z} et $K[X]$) aura des applications à l'étude des groupes abéliens et des endomorphismes.

Définition 1.1.6 Un *sous-module* d'un A -module M est un sous-groupe M' de $(M, +)$ qui est de plus stable pour la loi externe : $\forall a \in A, \forall x \in M', ax \in M'$.

La loi externe de M induit donc une loi externe sur M' qui en fait un A -module. Noter qu'il suffit de vérifier que M' est non vide et stable pour l'addition et pour la loi externe. Noter aussi qu'un sous-module M' est *stable par combinaisons linéaires*, autrement dit, pour toute famille $(x_i)_{i \in I}$ d'éléments de M' , toutes les *combinaisons linéaires* $\sum_{i \in I} a_i x_i$ sont des éléments de M' ; comme toujours en algèbre, on suppose que presque tous les coefficients a_i (*i.e.* tous sauf un nombre fini) sont nuls : $(a_i)_{i \in I} \in A^{(I)}$.

- Exemples 1.1.7**
1. Si A est un corps, un sous-module est un sous-espace vectoriel (et réciproquement).
 2. Si $A = \mathbf{Z}$, un sous-module est un sous-groupe (et réciproquement).
 3. Les sous-modules du A -module A sont ses idéaux.

4. Si $x \in M$, le sous-ensemble $Ax := \{ax \mid a \in A\}$ est un sous-module de M . Plus généralement, si $(x_i)_{i \in I}$ est une famille d'éléments de M , l'ensemble des combinaisons linéaires $\sum_{i \in I} a_i x_i$ forme un sous-module de M , noté $\sum_{i \in I} Ax_i$.
5. $A^{(I)}$ est un sous-module de A^I .
6. $\bigoplus M_i$ est un sous-module de $\prod M_i$.
7. Si le $K[X]$ -module M correspond au couple (V, ϕ) par la correspondance décrite plus haut, les sous-modules de M correspondent aux couples (V', ϕ') , où V' est un sous-espace vectoriel de V stable par ϕ et où $\phi' = \phi|_{V'}$.

Soient M un A -module et $x \in M$. On pose :

$$\text{Ann}_A(x) := \{a \in A \mid ax = 0\}.$$

C'est un idéal de A , appelé *annulateur* de x . On définit de même, pour tout sous-ensemble E de M :

$$\text{Ann}_A(E) := \{a \in A \mid \forall x \in E, ax = 0\} = \bigcap_{x \in E} \text{Ann}_A(x).$$

C'est encore un idéal de A , appelé *annulateur* de E .

Un élément $x \in M$ est dit *de torsion* si l'idéal $\text{Ann}_A(x)$ n'est pas trivial, *i.e.* s'il existe $a \neq 0$ tel que $ax = 0$. L'ensemble des éléments de torsion de M est noté $\text{Tor}_A(M)$. Il est évidemment stable pour la loi externe, et il contient 0 ; mais il n'est pas nécessairement stable pour l'addition. Par exemple, lorsque $M = A$, les éléments de torsion sont les diviseurs de 0, et ils ne forment pas nécessairement un idéal.

Exemple 1.1.8 On prend $A = M = \mathbf{Z}/6\mathbf{Z}$. Alors $\bar{2}$ et $\bar{3}$ sont des diviseurs de 0 et des éléments de torsion, mais pas leur somme.

Proposition 1.1.9 Si A est intègre, $\text{Tor}_A(M)$ est un sous-module de M , appelé sous-module de torsion de M .

Preuve. - Si $ax = 0$ et $by = 0$ avec $a, b \neq 0$, on a $(ab)(x + y) = 0$ avec $ab \neq 0$. \square

Dans le cas d'un espace vectoriel, le module de torsion est évidemment trivial.

Module quotient. Pour tout sous-module M' du A -module M , la relation de congruence modulo M' est une relation d'équivalence compatible avec l'addition, ce qui permet de munir l'ensemble quotient d'une loi de composition interne telle que l'addition des classes vérifie :

$$\forall x, y \in M, \bar{x} + \bar{y} = \overline{x + y}.$$

On obtient ainsi un groupe, appelé groupe quotient et noté M/M' . En fait, des implications :

$$\forall a \in A, \forall x, y \in M, x \equiv y \pmod{M'} \iff x - y \in M' \implies ax - ay = a(x - y) \in M' \iff ax \equiv ay \pmod{M'},$$

on déduit que la relation de congruence modulo M' est une relation d'équivalence compatible avec la loi externe, ce qui permet de munir le groupe quotient M/M' d'une loi de composition interne telle que :

$$\forall a \in A, \forall x \in M, a\bar{x} = \overline{ax}.$$

On vérifie immédiatement que l'on obtient ainsi un module, encore noté M/M' et appelé *module quotient de M par M'* . Dans le cas où A est un corps, resp. où $A = \mathbf{Z}$, on retrouve la notion d'espace vectoriel quotient, resp. de groupe quotient. Dans le cas où $M = A$ et où M' est un idéal I de A , on obtient une structure de A -module sur A/I (et non sa structure d'anneau quotient). Dans le cas où $A = K[X]$ et où M, M' correspondent respectivement à (V, ϕ) et à (V', ϕ') , on obtient le $K[X]$ -module correspondant à (V'', ϕ'') , où $V'' = V/V'$ (espace vectoriel quotient) et où ϕ'' est induit par ϕ par passage au quotient.

1.2 Morphismes

Définition 1.2.1 Soient M et N deux A -modules. On dit qu'un morphisme de groupes $f : M \rightarrow N$ est *A -linéaire*, ou que c'est un *morphisme de A -modules* si :

$$\forall a \in A, \forall x \in M, f(ax) = af(x).$$

On dit que f est un *isomorphisme* s'il est bijectif, que c'est un *endomorphisme* si $M = N$ et que c'est un *automorphisme* si c'est un endomorphisme bijectif. De même, f est un *monomorphisme*, resp. un *épimorphisme* s'il est injectif, resp. surjectif.

Le composé de deux morphismes est un morphisme et Id_M est un endomorphisme de M , ce qui justifie¹ la terminologie "morphisme". De même, l'application réciproque d'un morphisme bijectif est elle-même un morphisme, ce qui justifie la terminologie "isomorphisme".

- Exemples 1.2.2**
1. Si A est un corps, les morphismes sont les applications linéaires au sens des espaces vectoriels.
 2. Si $A = \mathbf{Z}$, tous les morphismes de groupes sont des \mathbf{Z} -linéaires, donc des morphismes de modules.
 3. L'inclusion canonique d'un sous-module $M' \rightarrow M$ est un morphisme, ainsi que la projection canonique $M \rightarrow M/M'$.
 4. Les projections canoniques $\prod M_i \rightarrow M_{i_0}$ et les injections canoniques $M_{i_0} \rightarrow \bigoplus M_i$ sont des morphismes. (Ce sont des cas particuliers de l'exemple précédent : le vérifier !)

Exercice 1.2.3 Si les $K[X]$ -modules M et N correspondent respectivement aux couples (V, ϕ) et (W, ψ) , alors les morphismes de modules $f : M \rightarrow N$ sont les applications K -linéaires $f : V \rightarrow W$ telles que $f \circ \phi = \psi \circ f$. (Indication : cette dernière égalité signifie exactement que $f(Xx) = Xf(x)$.)

1. Dans la présentation "catégorique" d'une théorie mathématique, il y a des objets et des morphismes et ces derniers doivent satisfaire des propriétés formelles analogues à celles que nous énonçons ; dans ce cadre, un isomorphisme se définit comme un morphisme $f : M \rightarrow N$ inversible, i.e. tel qu'il existe $g : N \rightarrow M$ tel que $g \circ f = \text{Id}_M$ et $f \circ g = \text{Id}_N$.

Proposition 1.2.4 Soit $f : M \rightarrow N$ un morphisme de A -modules.

(i) Pour tout sous-module $M' \subset M$, l'image $f(M')$ est un sous-module de N . En particulier, $\text{Im} f$ est un sous-module de N .

(ii) Pour tout sous-module $N' \subset N$, l'image réciproque $f^{-1}(N')$ est un sous-module de M . En particulier, $\text{Ker} f$ est un sous-module de M .

Preuve. - C'est exactement la même que dans le cas des espaces vectoriels. \square

Théorème 1.2.5 (Premier théorème d'isomorphisme) Soit $f : M \rightarrow N$ un morphisme de A -modules. L'application induite $\bar{f} : M/\text{Ker} f \rightarrow \text{Im} f$ est un isomorphisme.

Preuve. - Rappelons simplement la construction de \bar{f} . Si $x, y \in M$ ont même classe dans $M/\text{Ker} f$, alors $x - y \in \text{Ker} f \Rightarrow f(x) = f(y)$. Ainsi, $f(x)$ ne dépend que de $\bar{x} := x \pmod{\text{Ker} f} \in M/\text{Ker} f$, et l'on peut poser :

$$\bar{f}(\bar{x}) := f(x).$$

Pour le reste, la preuve est exactement la même que dans le cas des espaces vectoriels. \square

Exemple 1.2.6 (Modules monogènes) On dit que le module M est *monogène* s'il existe $x \in M$ tel que $M = Ax$. Dans ce cas, l'application $a \mapsto ax$ est un épimorphisme de A sur M de noyau $\text{Ann}_A(x)$, et donc $A/\text{Ann}_A(x) \simeq M$.

Réciproquement, tout module A/I est monogène engendré par $\bar{1}_A$. Les modules monogènes sont donc, à isomorphisme près, les modules A/I .

Théorème 1.2.7 (Deuxième théorème d'isomorphisme) Soient $M'' \subset M'$ des sous-modules du A -module M . Alors M'/M'' est un sous-module de M/M'' et le quotient est canoniquement isomorphe à M'/M'' .

Preuve. - C'est la même que dans le cas des espaces vectoriels : l'application $x \pmod{M''} \mapsto x \pmod{M'}$ de M/M'' dans M/M' est bien définie, elle est linéaire surjective et son noyau est M'/M'' ; on peut donc appliquer le premier théorème d'isomorphisme. \square

Remarque 1.2.8 Il est facile de vérifier que tous les sous-modules de M/M'' s'obtiennent de cette manière, et que l'on a donc une bijection $M' \mapsto M'/M''$ de l'ensemble des sous-modules de M qui contiennent M'' sur l'ensemble des sous-modules de M/M'' .

Exercice 1.2.9 Décrire tous les sous-modules d'un module monogène.

Avant de formuler le troisième théorème d'isomorphisme, quelques constructions élémentaires. Il est clair que l'intersection $\bigcap M_i$ d'une famille de sous-modules $M_i \subset M$ est un sous-module de M . Par exemple l'intersection de tous les sous-modules de M contenant un sous-ensemble arbitraire $E \subset M$ est le plus petit sous-module contenant E , on dit que c'est le *sous-module engendré par E* .

Prenons $E := M_1 \cup M_2$, où M_1 et M_2 sont des sous-modules de M . Tout sous-module contenant E contient également toutes les sommes $x_1 + x_2$, $x_1 \in M_1$, $x_2 \in M_2$. Mais l'ensemble de ces sommes est un sous-module de M (prouvez-le !). On note donc :

$$M_1 + M_2 := \{x_1 + x_2 \mid x_1 \in M_1, x_2 \in M_2\}.$$

C'est le sous-module engendré par $M_1 \cup M_2$ et on l'appelle *somme de M_1 et M_2* .

Exercice 1.2.10 Décrire de manière analogue le sous-module $\sum M_i$ engendré par la réunion $\cup M_i$ d'une famille de sous-modules de M .

Théorème 1.2.11 (Troisième théorème d'isomorphisme) Soient M_1 et M_2 des sous-modules de M . On a un isomorphisme naturel de $M_1/(M_1 \cap M_2)$ sur $(M_1 + M_2)/M_2$.

Preuve. - Comme dans le cas des espaces vectoriels, on vérifie que le morphisme composé $M_1 \rightarrow M_1 + M_2 \rightarrow (M_1 + M_2)/M_2$ est surjectif et a pour noyau $M_1 \cap M_2$, ce qui permet d'appliquer le premier théorème d'isomorphisme. \square

1.3 Familles

Pour toute famille $(x_i)_{i \in I}$ d'éléments de M , l'intersection de tous les sous-modules de M qui contiennent tous les x_i est un sous-module de M : c'est le plus petit-sous-module de M contenant tous les x_i , on dit qu'il est *engendré par les x_i* . Concrètement c'est le sous-module $\sum_{i \in I} Ax_i$ de toutes les combinaisons linéaires des x_i . De manière équivalente, c'est l'image du morphisme :

$$\begin{cases} (a_i)_{i \in I} \mapsto \sum_{i \in I} a_i x_i, \\ A^{(I)} \rightarrow M. \end{cases}$$

Définition 1.3.1 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *famille génératrice* (ou encore que les x_i *engendrent* M) si $M = \sum_{i \in I} Ax_i$, autrement dit, si le morphisme ci-dessus est surjectif.

Les *relations* entre les x_i sont les familles de coefficients $(a_i)_{i \in I} \in A^{(I)}$ telles que $\sum_{i \in I} a_i x_i = 0$, autrement dit, les éléments du noyau du morphisme ci-dessus.

Définition 1.3.2 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *famille libre* (ou encore que les x_i sont *linéairement indépendants*) si toute relation entre les x_i est triviale :

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

autrement dit, si le morphisme ci-dessus est injectif.

Définition 1.3.3 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *base* si elle est libre et génératrice :

$$\forall x \in M, \exists ! (a_i)_{i \in I} \in A^{(I)} : x = \sum_{i \in I} a_i x_i,$$

autrement dit, si le morphisme ci-dessus est bijectif.

Si $\mathcal{B} := (x_i)_{i \in I}$ est une base de M et si $x \in M$ s'écrit $x = \sum_{i \in I} a_i x_i$, on dira que les a_i sont les *coordonnées* de x dans la base \mathcal{B} .

Exercice 1.3.4 Montrer que les bases du A -module A sont les familles à un élément (x) telles que $x \in A^*$.

Naturellement, dans le cas où A est un corps, le vocabulaire ci-dessus est cohérent avec le vocabulaire usuel des espaces vectoriels. Cependant, il faut prendre garde que, lorsque A n'est pas un corps, de nombreuses propriétés usuelles tombent en défaut². Voici les principales "anomalies".

1. Un A -module n'admet pas nécessairement une base. Soit par exemple I un idéal de A qui n'est égal ni à $\{0\}$ ni à A (par hypothèse il en existe puisque A n'est pas un corps). Alors deux éléments quelconques de I sont liés, il n'y a donc pas de famille libre ayant strictement plus d'un élément, de sorte que I ne peut être un A -module libre que si c'est un idéal principal ; et même cela ne suffit pas si A n'est pas intègre (vérifiez-le). D'autre part, tout élément de A/I est de torsion, il n'y a donc aucune famille libre non vide dans A/I , donc aucune base.
2. Si le module M admet une base, un sous-module de M n'admet pas nécessairement une base : voir l'exemple ci-dessus.
3. Une famille libre maximale n'est pas nécessairement une base. Par exemple, dans le \mathbf{Z} -module \mathbf{Z} , la famille à un élément (2) est libre maximale, mais ce n'est pas une base ; et elle n'est strictement contenue dans aucune famille libre.
4. Une famille génératrice minimale n'est pas nécessairement une base. Par exemple, dans le \mathbf{Z} -module \mathbf{Z} , la famille à deux éléments $(2, 3)$ est génératrice, mais ce n'est pas une base ; et elle ne contient strictement aucune famille génératrice.

Définition 1.3.5 On dit qu'un module est *libre* s'il admet une base.

Il existe une théorie générale des modules libres, mais, comme pour les espaces vectoriels, on s'intéressera surtout (en algèbre) au cas des modules admettant une base finie.

Calcul matriciel avec les familles

On ne manipulera ici que des familles finies (bien que le cas général puisse être traité de façon semblable) et on les écrira systématiquement sous forme de suites finies $\mathcal{X} := (x_1, \dots, x_n) \in M^n$, $\mathcal{Y} := (y_1, \dots, y_p) \in M^p$, etc.

Soit $x := a_1 x_1 + \dots + a_n x_n$ une combinaison linéaire des x_i . Notant $C := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in A^n$ le vecteur

colonne des coefficients a_i , on adoptera l'écriture matricielle :

$$x = \mathcal{X}C.$$

². Cependant certaines d'entre elles seront rétablies dans le cas d'un anneau A principal : cela vaudra donc la peine de revenir ici après lecture complète de ce chapitre.

Noter qu'elle comporte un certain abus, puisque, en calcul matriciel usuel, on devrait avoir $\mathcal{X}C = x_1a_1 + \dots + x_na_n$, ce qui n'a pas de sens (scalaires à droite des "vecteurs"). Il est possible de justifier cet abus mais on se contentera d'observer que les calculs qui en résultent sont cohérents.

Supposons que les y_j soient tous combinaisons linéaires des x_i :

$$y_j = \sum_{i=1}^n a_{i,j}x_i, \quad j = 1, \dots, p.$$

Alors on a une écriture matricielle :

$$\mathcal{Y} = \mathcal{X}P, \quad \text{où } P := \begin{pmatrix} a_{1,1} & \dots & a_{1,p} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,p} \end{pmatrix} \in \text{Mat}_{n,p}(A).$$

Soit maintenant $\mathcal{Z} := (z_1, \dots, z_q) \in M^q$ une famille d'éléments qui sont combinaisons linéaires des y_j :

$$z_k = \sum_{j=1}^p b_{j,k}y_j, \quad k = 1, \dots, q.$$

On a donc $\mathcal{Z} = \mathcal{Y}Q$, où $Q \in \text{Mat}_{p,q}(A)$ a pour coefficients les $b_{j,k}$. L'associativité du produit matriciel permet de prévoir les égalités :

$$\mathcal{Z} = \mathcal{Y}Q = (\mathcal{X}P)Q = \mathcal{X}(PQ) = \mathcal{X}R, \quad \text{où } R := PQ \in \text{Mat}_{n,q}(A).$$

Et l'on vérifie en effet sans peine les relations $z_k = \sum_{i=1}^n c_{i,k}y_j$, $k = 1, \dots, q$, les coefficients $c_{i,k}$ de R étant donnés par la formule habituelle $c_{i,k} := \sum_{j=1}^p a_{i,j}b_{j,k}$, $i = 1, \dots, n$, $k = 1, \dots, q$.

Exercice 1.3.6 Expliquer et prouver les relations :

$$\mathcal{X}(P + P') = \mathcal{X}P + \mathcal{X}P', \quad (\mathcal{X} + \mathcal{X}')P = \mathcal{X}P + \mathcal{X}'P, \quad \mathcal{X}I_n = \mathcal{X}, \quad \mathcal{X}P = \mathcal{Y} \Leftrightarrow \mathcal{X} = \mathcal{Y}P^{-1}.$$

On traduit simplement les notions de familles libres et génératrices dans ce langage :

- La famille \mathcal{X} est libre si, chaque fois que l'on a $\mathcal{X}P = 0$ (famille triviale), on peut en déduire $P = 0$ (matrice nulle). Plus généralement, si $\mathcal{X}P = \mathcal{X}P'$, alors $P = P'$.
- La famille \mathcal{X} est génératrice si toute famille \mathcal{Y} peut s'écrire $\mathcal{Y} = \mathcal{X}P$ (la matrice P ayant le bon format).

À titre d'exemple (parmi beaucoup : inventez-en !) d'utilisation de ce formalisme, voici un résultat important.

Théorème 1.3.7 Si M admet une base de n éléments $\mathcal{X} := (x_1, \dots, x_n)$, alors toutes les bases de M ont n éléments.

Preuve. - Soit $\mathcal{Y} = (y_1, \dots, y_p)$ une autre base de M . Puisque ces deux familles sont génératrices, on peut écrire $\mathcal{Y} = \mathcal{X}P$ et $\mathcal{X} = \mathcal{Y}Q$ pour certaines matrices P, Q . On en déduit $\mathcal{X} = \mathcal{X}(PQ)$ et $\mathcal{Y} = \mathcal{Y}(QP)$. Mais puisque $\mathcal{X} = \mathcal{X}I_n$ et $\mathcal{Y} = \mathcal{Y}I_p$ et que ces familles sont libres, on en tire $PQ = I_n$ et $QP = I_p$. On applique alors le lemme ci-dessous. \square

Lemme 1.3.8 Soit A un anneau non trivial et soient $P \in \text{Mat}_{n,p}(A)$ et $Q \in \text{Mat}_{p,n}(A)$ telles que $PQ = I_n$, $QP = I_p$. Alors $n = p$.

Preuve. - On choisit un idéal maximal quelconque \mathfrak{M} de A (théorème de Krull) et l'on note $K := A/\mathfrak{M}$ l'anneau quotient, qui est un corps (le "corps résiduel"). En réduisant modulo \mathfrak{M} les relations précédentes, on obtient des égalités entre matrices à coefficients dans K :

$$\overline{P}\overline{Q} = I_n \text{ et } \overline{Q}\overline{P} = I_p;$$

mais l'algèbre linéaire usuelle (sur un corps) nous dit alors que $n = p$. \square

Remarque 1.3.9 La démonstration ci-dessus ne prouve pas qu'il n'existe pas de base infinie. Ce point est laissé au lecteur courageux.

Définition 1.3.10 Un module admettant une base de n éléments est dit *libre de rang n* . Son *rang* (qui est bien défini d'après le théorème précédent) est n .

Corollaire 1.3.11 Soit M un module libre de rang n et soit X une base de M . Alors l'application $P \mapsto XP$ est une bijection du groupe $GL_n(A)$ des matrices inversibles à coefficients dans A sur l'ensemble des bases de M .

\square

Rappelons que les éléments de $GL_n(A)$ sont les matrices $P \in \text{Mat}_n(A)$ telles que $\det P \in A^*$. En effet :

- Si $PQ = I_n$, alors $(\det P)(\det Q) = 1$, d'où $\det P \in A^*$.
- Si $\det P \in A^*$, notant \tilde{A} la transposée de la matrice des cofacteurs de A , on a, d'après les formules de Cramer, $A\tilde{A} = \tilde{A}A = (\det A)I_n$ et $(\det A)^{-1}\tilde{A}$ est inverse de A .

Exercice 1.3.12 Soient M un A -module libre de rang n et X une base de M . Donner une condition sur $P \in \text{Mat}_{n,p}(A)$ pour que la famille XP soit libre, resp. génératrice, resp. une base.

Écriture matricielle des morphismes. Soient $\mathcal{B} := (e_1, \dots, e_n)$ une base du module M (qui est donc libre de rang n) et $\mathcal{C} := (f_1, \dots, f_p)$ une base du module N (qui est donc libre de rang p). On en déduit des isomorphismes $A^n \rightarrow M$ et $A^p \rightarrow N$, respectivement définis (dans l'écriture classique en vecteurs colonnes) par $X \mapsto \mathcal{B}X$ et $\mathcal{Y} \mapsto C\mathcal{Y}$. Si $x = \mathcal{B}X \in M$, resp. $y = C\mathcal{Y} \in N$, les composantes (x_1, \dots, x_n) de X , resp. les composantes (y_1, \dots, y_p) de \mathcal{Y} , sont les coordonnées de x dans la base \mathcal{B} , resp. les coordonnées de y dans la base \mathcal{C} .

Soit $f : M \rightarrow N$ un morphisme. Il existe une unique matrice $P \in \text{Mat}_{p,n}(A)$ telle que $f(\mathcal{B}) = CP$. c'est la matrice de l'application linéaire f relative aux bases \mathcal{B} et \mathcal{C} . On a :

$$f(x) = y \iff f(\mathcal{B}X) = C\mathcal{Y} \iff f(\mathcal{B})X = C\mathcal{Y} \iff CPX = C\mathcal{Y} \iff Y = PX.$$

La matrice $P = (a_{j,i})_{\substack{1 \leq j \leq p \\ 1 \leq i \leq n}}$ relie donc les coordonnées de x et de $y = f(x)$ par les formules :

$$y_j = \sum_{i=1}^n a_{j,i}x_i, \quad j = 1, \dots, p.$$

Exercice 1.3.13 À quelle condition sur P le morphisme f est-il injectif, resp. surjectif, resp. bijectif ?

1.4 Changement de base

On a vu que si $f : A \rightarrow B$ est un morphisme d'anneaux, on peut canoniquement associer à tout B -module un A -module (*restriction des scalaires*). Il existe de même un processus d'*extension des scalaires* qui permet d'associer à tout A -module un B -module. Nous l'étudierons seulement dans deux cas particuliers importants. Mais d'abord, un peu de métaphysique.

Fonctorialité de la restriction des scalaires. Nous nous contenterons de l'illustrer sur le cas le plus simple, celui de la restriction à un sous-anneau. Soit donc A' un sous-anneau de A . On introduit une catégorie \mathcal{C} , dont les *objets* sont les A -modules et telle que, pour deux tels objets M et N , on se donne un ensemble $\text{Mor}_{\mathcal{C}}(M, N)$ de *morphismes* (dans notre cas, les applications A -linéaires). De plus, pour tout objet M il y a un morphisme particulier $\text{Id}_M \in \text{Mor}_{\mathcal{C}}(M, M)$; et pour trois objets M, N, P , il y a une application de composition :

$$\text{Mor}_{\mathcal{C}}(M, N) \times \text{Mor}_{\mathcal{C}}(N, P) \rightarrow \text{Mor}_{\mathcal{C}}(M, P), (f, g) \mapsto g \circ f.$$

Les axiomes qui font de cette structure une catégorie sont (en un sens évident mais inhabituel, que le lecteur précisera) l'associativité de la composition et la neutralité des Id_M .

Par restriction de scalaires, on associe à chaque objet M de \mathcal{C} un objet $F(M)$ de la catégorie \mathcal{C}' des A' -modules. Mais également, on associe à chaque morphisme $f \in \text{Mor}_{\mathcal{C}}(M, N)$ un morphisme $f' \in \text{Mor}_{\mathcal{C}'}(F(M), F(N))$, qui (dans ce cas) n'est autre que f lui-même : en effet, la A -linéarité implique trivialement la A' -linéarité. On dit alors que $F : \mathcal{C} \rightsquigarrow \mathcal{C}'$ est un *foncteur* parce qu'il vérifie les propriétés suivantes (immédiates à vérifier) : $F(\text{Id}_M) = \text{Id}_{F(M)}$ et $F(g \circ f) = F(g) \circ F(f)$.

Exercice 1.4.1 Dédurre de manière purement formelle des propriétés de ce foncteur que si $M \simeq N$ (isomorphisme de A -modules) alors $F(M) \simeq F(N)$ (isomorphisme de A' -modules).

Extension des scalaires de A à A/I . Soient A un anneau commutatif, I un idéal de A et $A' := A/I$. Pour tout A -module M , l'ensemble des combinaisons linéaires $\sum i_k x_k$ où les $i_k \in I$ et les $x_k \in M$ est un sous-module de M que nous noterons IM . Pour tout morphisme $f \in \text{Mor}_{\mathcal{C}}(M, N)$, on a clairement $f(IM) \subset IN$, d'où, par passage au quotient, un morphisme de A' -modules $f' : M/IM \rightarrow N/IN$. On définit ainsi un foncteur de la catégorie \mathcal{C} des A -modules dans la catégorie \mathcal{C}' des A' -modules.

Exemple 1.4.2 On peut utiliser un tel foncteur pour montrer à nouveau, mais sans calcul, que le rang d'un module libre est bien défini. Supposons que M soit isomorphe à A^n et à A^p , donc que $A^n \simeq A^p$ (isomorphisme de A -modules). Pour tout idéal maximal \mathfrak{M} de A , notant $K := A/\mathfrak{M}$ son corps résiduel, on en déduit que $K^n \simeq K^p$ (isomorphisme de K -modules, c'est-à-dire de K -espaces vectoriels). L'algèbre linéaire usuelle nous dit alors que $n = p$.

Extension des scalaires de A à $S^{-1}A$. Soit S une partie multiplicative de l'anneau non trivial A . On peut définir, pour tout A -module M , un *module de fractions* $M' := S^{-1}M$ sur l'anneau de fractions $A' := S^{-1}A$. Pour cela, on munit l'ensemble $M \times S$ d'une relation d'équivalence \sim , d'une loi de composition interne $+$ et d'une loi de composition externe \cdot par $A \times S$ avec des formules en

tous points similaires à celles utilisées dans la définition de $S^{-1}A$:

$$\begin{aligned}(m, s) \sim (m', s') &\iff \exists t \in S : t(s'm - sm') = 0, \\ (m, s) + (n, t) &:= (tm + sn, st), \\ (a, s).(m, t) &:= (am, st).\end{aligned}$$

(Bien entendu, $a \in A, s, s', t \in S$ et $m, m', n \in M$.) On prouve encore la compatibilité des relations et lois de composition concernées, et l'on en déduit par passage au quotient un $S^{-1}A$ -module $S^{-1}M$. On note m/s ou $s^{-1}m$ la classe de (m, s) .

Exercice 1.4.3 Vérifier que si M est de type fini, $S^{-1}M$ l'est également.

Pour tout sous-module N de M , le A' -module $N' := S^{-1}N$ s'identifie canoniquement à un sous-module de $M' := S^{-1}M$. Réciproquement, tous les sous-modules de M' s'obtiennent ainsi : si N' est un tel sous-module, $N := \{m \in M \mid m/1 \in N'\}$ est un sous-module de M et $N' = S^{-1}N$.

Exercice 1.4.4 Démontrer que, si M est noetherien (*i.e.* si tous ses sous-modules sont de type fini), $S^{-1}M$ l'est également.

Soit $f : M \rightarrow N$ un morphisme de A -modules. L'application $(m, s) \mapsto (f(m), s)$ de $M \times S$ dans $N \times S$ passe au quotient et induit un morphisme de $S^{-1}A$ -modules $\bar{f} : S^{-1}M \rightarrow S^{-1}N$ tel que $m/s \mapsto f(m)/s$. On vérifie immédiatement que $\overline{\text{Id}_M} = \text{Id}_{S^{-1}M}$ et que $\overline{g \circ f} = \bar{g} \circ \bar{f}$, autrement dit, on a défini un foncteur $M \rightsquigarrow S^{-1}M$ de la catégorie des A -modules dans celle des $S^{-1}A$ -modules.

Soit maintenant $g : N \rightarrow P$ un autre morphisme de A -modules. Il est clair d'après ce qui précède que, si $\text{Im} f \subset \text{Ker} g$, *i.e.* si $g \circ f = 0$ (morphisme trivial), alors $\bar{g} \circ \bar{f} = 0$ donc $\text{Im} \bar{f} \subset \text{Ker} \bar{g}$.

Exercice 1.4.5 Montrer que si $\text{Im} f = \text{Ker} g$ alors $\text{Im} \bar{f} = \text{Ker} \bar{g}$. (On dit que le foncteur est *exact*, voir le chapitre suivant.) En déduire que si f est injectif, resp. surjectif, \bar{f} l'est également.

1.5 Exercices sur le chapitre 1

Exercice 1.5.1 1) Soit \mathfrak{P} un idéal premier de l'anneau commutatif A . Montrer que $S := A \setminus \mathfrak{P}$ est une partie multiplicative de A et que $S^{-1}A$ a un unique idéal maximal. L'anneau local $A_{\mathfrak{P}} := S^{-1}A$ est appelé *localisé de A en \mathfrak{P}* .

2) Soit x un élément non nilpotent de A . Montrer qu'il existe un idéal premier \mathfrak{P} de A tel que $x \notin \mathfrak{P}$. (Si $S := \{x^n \mid n \in \mathbf{N}\}$, l'anneau $S^{-1}A$ n'est pas trivial.) En déduire que l'ensemble des éléments nilpotents de A est égal à l'intersection des idéaux premiers de A (*radical de A*).

Exercice 1.5.2 (i) Soit I un idéal de l'anneau A . Décrire tous les sous-modules M' du module $M := A/I$ et les quotients M/M' correspondants.

(ii) Soit \mathfrak{M} un idéal maximal de l'anneau A . Montrer que le module $M := A/\mathfrak{M}$ est *simple*, autrement dit, il est non trivial et ses seuls sous-modules sont $\{0\}$ et lui-même. Réciproque ?

Exercice 1.5.3 1) Soient A un anneau intègre, K son corps des fractions et M le module quotient K/A . Décrire le sous-module $\text{Tor}_A(M)$, les idéaux $\text{Ann}_A(x)$ pour $x \in M$ et l'idéal $\text{Ann}_A(M)$.

2) Mêmes questions pour $M := A/I$ où A est quelconque et I un idéal de A .

Exercice 1.5.4 1) Soient M' un sous-module du A -module M et $p : M \rightarrow M/M'$ l'épimorphisme canonique. Soient $N_1 \subset N_2$ deux sous-modules de M tels que $N_1 \cap M' = N_2 \cap M'$ et $p(N_1) = p(N_2)$. Démontrer que $N_1 = N_2$.

2) On prend pour A un corps K , puis $M := K^2$, $M' := K \times \{0\}$ et $N_\lambda := \{(x, y) \in K^2 \mid y = \lambda x\}$. Montrer que, pour tout $\lambda \neq 0$, on a $N_\lambda \cap M' = \{(0, 0)\}$ et $p(N_\lambda) = M/M'$. So what ? (Miles)

Exercice 1.5.5 1) Soit M un A -module. On appelle *longueur de M* et l'on note $\ell(M)$ la borne supérieure des entiers n tels qu'il existe une suite strictement croissante $M_0 \subset \dots \subset M_n$ de sous-modules. Donc $\ell(M) \in \mathbf{N} \cup \{+\infty\}$. Quels sont les modules de longueur 0, de longueur 1 ? Que vaut la longueur dans le cas où A est un corps ?

2) Que dire d'une suite strictement croissante $M_0 \subset \dots \subset M_n$ lorsque $n = \ell(A)$?

3) Soit M' un sous-module de M . Démontrer l'égalité $\ell(M) = \ell(M') + \ell(M/M')$ (avec les règles usuelles sur $+\infty$ et l'addition). (Pour l'une des deux majorations, utiliser l'exercice précédent.)

4) Démontrer que, s'il existe une suite strictement croissante maximale $M_0 \subset \dots \subset M_n$, alors $n = \ell(A)$. On définira le terme "maximale".

Exercice 1.5.6 Soit $f : M \rightarrow N$ un morphisme surjectif de modules et soit $g : N \rightarrow P$ une application de N dans un module P . Montrer que, si $g \circ f$ est linéaire, alors g est linéaire.

Exercice 1.5.7 Soient $X := (x_1, \dots, x_n) \in M^n$ et $P \in M_n(A)$. Notons $\mathcal{Y} := (y_1, \dots, y_n) := XP$. Montrer que les sous-modules $M' := XA^n$ et $M'' := \mathcal{Y}A^n$ respectivement engendrés par X et \mathcal{Y} vérifient :

$$(\det P)M' \subset M'' \subset M'.$$

(Utiliser les formules de Cramer sous forme matricielle.)

Exercice 1.5.8 Déduire de l'exercice 1.5.7 le théorème de Cayley-Hamilton.

Exercice 1.5.9 1) Soit A un anneau n'ayant qu'un idéal maximal \mathfrak{M} (donc un anneau *local*). Démontrer que $A^* = A \setminus \mathfrak{M}$.

2) Soit M un module "de type fini", c'est-à-dire engendré par un nombre fini d'éléments. On suppose que $\mathfrak{M}M = \{0\}$. Démontrer que $M = \{0\}$. (Utiliser l'exercice 1.5.7.)

3) Soit M un module de type fini et soit N un sous-module tel que $M = \mathfrak{M}M + N$. Démontrer que $M = N$ ("Lemme de Nakayama").

Exercice 1.5.10 Soit A un anneau intègre local d'idéal maximal \mathfrak{M} . Soient $K := S^{-1}A$, où $S := A \setminus \{0\}$, son corps des fractions et $k := A/\mathfrak{M}$ son *corps résiduel*. Soient enfin M un A -module de type fini, $V := S^{-1}M$, resp. $W := M/\mathfrak{M}M$ les espaces vectoriels sur K et k déduits par extension des scalaires. À l'aide du lemme de Nakayama, démontrer que $\dim_K(V) \leq \dim_k(W)$.

Exercice 1.5.11 (i) On suppose que $M = M_1 \oplus M_2$, c'est-à-dire que $M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$. Montrer que l'application $(x_1, x_2) \mapsto x_1 + x_2$ est un isomorphisme de $M_1 \times M_2$ sur M .

(ii) Définir des endomorphismes p, q de M tels que $p^2 = p$, $q^2 = q$, $pq = qp = 0$, $p + q = \text{Id}_M$, $\text{Im} p = M_1$ et $\text{Im} q = M_2$.

(iii) Soient p un endomorphisme idempotent de M et $q := \text{Id}_M - p$. Montrer que $q^2 = q$, $pq = qp = 0$, $\text{Im} p = \text{Ker} q$ et $\text{Im} q = \text{Ker} p$. Notant M_1 et M_2 ces derniers, montrer que $M = M_1 \oplus M_2$.

Exercice 1.5.12 1) Soient I un idéal de A et M un A -module. On note IM le sous-module de M engendré par les xm , $x \in I$, $m \in M$. Montrer comment faire de M/IM un (A/I) -module \overline{M} de manière naturelle.

2) À tout morphisme $f : M \rightarrow N$, associer de manière naturelle un morphisme $\overline{f} : \overline{M} \rightarrow \overline{N}$ et vérifier que $\overline{\text{Id}_M} = \text{Id}_{\overline{M}}$ (quel que soit M) et que $\overline{g \circ f} = \overline{g} \circ \overline{f}$ (quels que soient f et g composables). On parle alors du *foncteur* $M \rightsquigarrow \overline{M}$.

3) En déduire que, si M et N sont isomorphes, alors \overline{M} et \overline{N} le sont, puis une nouvelle preuve de l'unicité du rang d'un module libre.

4) Montrer que, si f est surjectif, \overline{f} l'est aussi. Donner un contre-exemple à la propriété analogue pour l'injectivité.

Exercice 1.5.13 1) Munir l'ensemble $\text{Hom}_A(M, N)$ des morphismes de M dans N d'une structure de A -module puis faire de $N \rightsquigarrow \text{Hom}_A(M, N)$ un foncteur (en supposant M fixé).

2) Montrer que ce foncteur transforme les surjections en surjections et donner un contre-exemple à la propriété analogue pour l'injectivité.

3) reprendre ces questions pour le foncteur $M \rightsquigarrow \text{Hom}_A(M, N)$ (où N est fixé).

Exercice 1.5.14 (i) À l'aide des injections canoniques $f_{i_0} : M_{i_0} \rightarrow \bigoplus M_i$, déterminer un isomorphisme :

$$\text{Hom}_A\left(\bigoplus M_i, N\right) \rightarrow \prod \text{Hom}_A(M_i, N).$$

(ii) À l'aide des surjections canoniques $g_{i_0} : \prod N_i \rightarrow N_{i_0}$, déterminer un isomorphisme :

$$\text{Hom}_A\left(M, \prod N_i\right) \rightarrow \prod \text{Hom}_A(M, N_i).$$

(iii) Formuler les propriétés universelles correspondantes.

Exercice 1.5.15 Soient A un anneau intègre et $S := A \setminus \{0\}$. Soient M un A -module et $L := M/\text{Tor}_A(M)$. Montrer que L est sans torsion, que $S^{-1}\text{Tor}_A(M) = \{0\}$ et que $S^{-1}M \rightarrow S^{-1}L$ (morphisme déduit de $M \rightarrow L$) est un isomorphisme.