Algèbre année 2, semestre 2 : anneaux, modules

David Renard
Centre de Mathématiques Laurent Schwartz
Ecole Polytechnique

email : david.renard@polytechnique.edu

Page web du cours : http ://www.cmls.polytechnique.fr/perso/renard/USTC2.html

17 février 2022

Table des matières

Avertissement et remerciements. Ce texte emprunte de larges passages au cours d'Olivier Debarre « Algèbre 2 » à l'Ecole Normale Supérieure de Paris, ainsi que des éléments d'un cours de Master 1, « Groupes, anneaux, modules et représentations », que j'enseigne à l'Ecole Polytechnique. J'ai adapté ce matériel aux objectifs de ce cours en ajoutant des exemples et des exercices d'application immédiate.

Je le remercie Oliver Debarre d'avoir mis ses fichiers Tex à disposition, ce qui a permis une compilation rapide de ces notes de cours.

Chapitre I

Arithmétique des anneaux

I.1 Quelques définitions générales

I.1.1 Anneaux, morphismes d'anneaux, sous-anneaux, idéaux, éléments inversibles

La structure d'anneau est centrale en mathématiques, le lecteur connait déjà sans doute des dizaines d'exemples d'anneaux.

Définition I.1.1 (Anneau)**.** Un anneau est un ensemble A muni de deux opérations, appelées addition et multiplication et notée respectivement $(a, b) \mapsto a + b$ et $(a, b) \mapsto ab$, ayant les propriétés suivantes.

- L'ensemble A muni de l'addition est un groupe abélien. On note 0_A (ou simplement 0) son élément neutre.
- La multiplication est associative (c'est-à-dire $(ab)c = a(bc)$, $\forall a, b, c \in A$), elle possède un élément neutre noté 1_A (ou simplement 1) et elle est distributive par rapport à l'addition (c'est-à-dire $(a + b)c = ac + bc,\ a(b + c) = ab + ac$, $\forall a, b, c \in A$).

Si la multiplication est commutative, on dit que l'anneau est commutatif.

On exige donc d'un anneau l'existence d'un élément neutre 0_A pour l'addition, et aussi d'un élément neutre 1_A pour la multiplication.

Exercice I.1.2. Montrer que si $0_A = 1_A$, alors $A = \{0_A\}$.

Exemples I.1.3. Voici quelques exemples d'anneaux.

1. L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition et de la multiplication est un anneau commutatif.
2. Un corps est un anneau commutatif pour lequel tous les éléments non nuls sont inversibles pour la multiplication, par exemple l'ensemble $\mathbb{R}$ des nombres rationnels, l'ensemble $\mathbb{R}$ des nombres réels, l'ensemble $\mathbb{C}$ des nombres complexes, munis de l'addition et de la multiplication usuelles, sont des corps commutatifs, donc des anneaux commutatifs.
3. L'ensemble des classes de congruence modulo un nombre entier strictement positif donné n est un anneau commutatif pour la loi provenant la congruence ; il est noté $\mathbb{Z}/n\mathbb{Z}$.
4. Les quaternions d'Hamilton $\mathbb{H}$ constituent un anneau à division (c'est-à-dire que tout élément non nul est inversible). On adopte dans ce cours la terminologie moderne : un corps est forcément commutatif, et ce qui dans l'ancienne terminologie s'appelait corps non commutatif ou corps gauche s'appelle maintenant anneau à division).

5. Soit $P = a_0 + a_1 X + \ldots + X^n$ un polynôme à coefficients dans $\mathbb{Z}$ et ξ une racine complexe de P. Soit $\mathbb{Z}[\xi] = \{Q(\xi),\ Q \in \mathbb{Z}[X]\}$. On vérifie immédiatement que c'est un sous-anneau de $\mathbb{C}$. Ce type d'anneau joue un grand rôle en arithmétique.
6. L'ensemble des polynômes $A[X]$ à coefficients dans un anneau commutatif A est aussi un anneau commutatif.
7. Si X est un ensemble, et A un anneau, l'espace des fonctions sur X à valeurs dans A à une structure d'anneau, l'addition et la multiplication des fonctions étant induites par celles de A.
8. Les endomorphismes d'un espace vectoriel V sur un corps k forment un anneau noté $\mathrm{End}_k(V)$, où la première loi est l'addition de fonction pour la loi $+$ et la deuxième la composition. Il n'est pas commutatif en général.
9. On peut généraliser cette construction en remplaçant l'espace vectoriel V par un groupe abélien quelconque $(M, +)$. Soit $\mathrm{End}_{\mathbb{Z}}(M)$ l'ensemble des endomorphismes de M pour la structure de groupe abélien. Cet ensemble hérite de M d'une loi d'addition, que l'on note encore $+$, et d'un élément nul 0_M, qui en font un groupe abélien. Si l'on y ajoute la loi de multiplication $\circ$ donnée par la composition des endomorphismes (non commutative en général), et l'endomorphisme Id_M (l'identité de M), on obtient sur $\mathrm{End}_{\mathbb{Z}}(M)$ une structure d'anneau.
10. L'anneau $\mathcal{M}_n(A)$ des matrices carrées de taille n à coefficients dans un anneau commutatif A est lui-même un anneau unitaire (l'élément neutre multiplicatif étant la matrice identité I_n), il est non commutatif si $n > 1$. On peut aussi considérer des matrices à coefficients dans un anneau non commutatif, mais ce genre d'anneau est très difficile à manipuler.

Remarque I.1.4. On peut ranger les exemples ci-dessus en trois types : les anneaux de nombres (sous-anneaux d'un corps, anneaux de congruence), les anneaux de fonctions à valeurs dans un anneau, et les anneaux d'endomorphismes.

Certains anneaux ont une structure supplémentaire : ce sont aussi des espaces vectoriels sur un corps k. On parle alors de k-algèbre.

Définition I.1.5. Une k-algèbre A est un k-espace vectoriel et un anneau, la structure de groupe abélien sous-jacente étant la même pour ces deux structures. La multiplication dans A est de plus bilinéaire, c'est-à-dire que si l'on note $a \cdot b$ le produit de deux éléments a et b de A (structure d'anneau) et λa la multiplication d'un élément a de A par un scalaire λ de k (structure d'espace vectoriel), alors on a en plus quels que soient $a, b \in A$, $\lambda \in k$,

$$\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b). \tag{I.1.1}$$

Exemples I.1.6. Les espaces de polynômes à coefficients dans le corps k sont des k-algèbres : $k[X_1, \ldots, X_n]$. Pour un espace vectoriel V sur k, $\mathrm{End}_k(V)$ est une algèbre. L'espace $\mathcal{M}_n(k)$ des matrices carrées de taille n à coefficients dans k est une k-algèbre.

Remarque I.1.7. On peut aussi définir plus généralement des R-algèbres, où R est un anneau commutatif : une R-algèbre A est à la fois un anneau et un R-module (on verra la définition des modules au chapitre II) avec les mêmes condition de compatibilité (I.1.1).

On a parlé ci-dessus d'éléments inversibles, sans donner de définition. Réparons cet oubli.

Définition I.1.8. Un élément a de A est dit *inversible* s'il existe $b \in a$ tel que $ab = ba = 1_A$. L'ensemble des éléments inversible de A est noté $A^\times$. Un élément inversible est aussi appelé *une unité*.

Dans un anneau non commutatif, il est utile de définir les notions plus faibles d'inverse à gauche ou à droite :

- un élément a de A est dit inversible à gauche s'il existe $b \in a$ tel que $ba = 1_A$ (b s'appelle l'inverse à gauche de a).

- un élément a de A est dit inversible à droite s'il existe $b \in a$ tel que $ab = 1_A$ (b s'appelle l'inverse à droite de a).

Exercice I.1.9. Trouver un exemple d'anneau non commutatif A, et un élément a de A qui est inversible à gauche mais pas à droite, ou le contraire.

Exercice I.1.10. Le but de cet exercice est de calculer le groupe des unités de l'anneau $\mathbb{Z}[\sqrt{2}]$.

i) Vérifier que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | \, a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.

ii) Vérifier que $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}, \quad a + b\sqrt{2} \mapsto a^2 - 2b^2$ est multiplicative. En déduire que les unités de $\mathbb{Z}[\sqrt{2}]$ sont les $a + b\sqrt{2}$ tels que $N(a + b\sqrt{2}) = a^2 - 2b^2 = \pm 1$.

iii) Montrer que $(1 + \sqrt{2})^n$ est une unité pour tout $n \in \mathbb{Z}$.

iv) Montrer que $1 + \sqrt{2}$ est la plus petite (pour l'ordre usuel de $\mathbb{R}$) unité de $\mathbb{Z}[\sqrt{2}]$ qui soit > 1.

v) Soit u une unité de $\mathbb{Z}[\sqrt{2}]$, $u \neq \pm 1$. Montrer que dans l'ensemble $\{\pm u, \pm u^{-1}\}$, il y a un seul élément v tel que $v > 1$, puis qu'il existe un unique entier $k \in \mathbb{N}$ tel que

$$(1 + \sqrt{2})^k < v \leq (1 + \sqrt{2})^{k+1}$$

Conclure que $v = (1 + \sqrt{2})^{k+1}$.

Exercice I.1.11. Soit A un anneau tel que pour tout $x \in A$, $x^2 = x$. Montrer que $1_A + 1_A = 0_A$. Montrer que pour tout $x \in A$, $x + x = 0_A$. Montrer que A est commutatif. [1]

En mathématiques, un morphisme est une application entre deux ensembles préservant une certaine structure sur ces ensembles. Pour les anneaux, la définition est donc la suivante

Définition I.1.12 (Morphisme d'anneaux)**.** Soient A et B des anneaux. Un morphisme d'anneaux de A dans B est une application

$$\phi : \; A \longrightarrow B$$

vérifiant

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(0_A) = 0_B, \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(1_A) = 1_B.$$

Remarque I.1.13. La deuxième propriété découle de la première. On a choisi de la mettre dans la définition pour insister sur le fait que ce que l'on exige, c'est de préserver une structure.

Une autre notion évidente est celle de sous-anneau.

Définition I.1.14. Soit A un anneau. Une partie B de A est un sous-anneau si c'est une partie stable par addition et multiplication, qui contient 0_A et 1_A.

1. Un élément tel que $x^2 = x$ est appelé un idempotent, par exemple un projecteur dans l'anneau des endomorphismes d'un espace vectoriel.

I.1.2 Idéaux (à gauche, à droite, bilatères). Anneaux quotients.

Définition I.1.15. Soit A un anneau. Un idéal à gauche I de A est un sous-groupe abélien de A pour l'addition, et qui vérifie de plus $(\forall a \in A), (\forall x \in I),\ ax \in I$.

On peut définir de manière analogue les idéaux à droite. Dans un anneau commutatif, les deux notions coïncident, mais pas dans un anneau non commutatif. Une partie I de A qui est à la fois un idéal à gauche et à droite s'appelle un idéal bilatère.

Exercice I.1.16. Soit A un anneau, et I un idéal bilatère de A. Montrer que A/I admet une structure d'anneau et que la projection canonique $p : A \to A/I$ est un morphisme d'anneaux. (Exemple $\mathbb{Z}/n\mathbb{Z}$.)

Le noyau d'un morphisme d'anneaux $f : A \to B$ est un idéal bilatère de A noté $\ker(f)$ (mais l'image de f n'est en général pas un idéal de B). Plus généralement, l'image réciproque par f d'un idéal bilatère (resp. à gauche) de B est un idéal bilatère (resp. à gauche) de A. Si I est un idéal bilatère de A, le morphisme f se factorise par la projection $A \to A/I$ si et seulement si $I \subset \ker(f)$.

Exercice I.1.17. Soit I un idéal bilatère de l'anneau A. Montrer que $I = A$ si et seulement si I contient un élément inversible. En déduire que si l'anneau A est à division, alors ses seuls idéaux bilatères sont $\{0\}$ et A. La réciproque est-elle vraie ? On pourra regarder l'exemple de $\mathcal{M}_2(\mathbb{R})$. Et si A est commutatif ?

Proposition I.1.18 (Intersection d'idéaux)**.** *Soit A un anneau, et soit $(I_i)_{i\in I}$ une famille d'idéaux à gauche de M. Alors*

$$\bigcap_{i\in I} I_i \subset A$$

est un idéal à gauche de A.

On a bien sûr le même résultat avec des idéaux à droite ou bilatère.

Définition I.1.19 (Idéal engendré par une partie)**.** Soit A un anneau et soit X une partie de A. On appelle idéal à gauche engendré par X, et on note (X) le plus petit idéal à gauche de A contenant X, c'est-à-dire l'intersection de tous les idéaux à gauche J contenant X :

$$(X) = \bigcap_{X\subset J \text{ idéal}} J$$

où l'intersection est prise sur les idéaux à gauche.

Concrètement, $\langle X\rangle$ est l'image de

$$A^{(X)} \longrightarrow A, \quad (a_x)_{x\in X} \mapsto \sum_{x\in X} a_x \cdot x$$

(la somme est à support fini).

On définit de même cette notion pour les idéaux à droite ou bilatères.

Définition I.1.20 (Somme d'idéaux)**.** Soient $(I_i)_{i\in I}$ une famille d'idéaux à gauche de l'anneau A. On appelle somme des I_i dans M l'idéal M engendré par la réunion des I_i, et on le note $\sum_{i\in I} I_i$:

$$\sum_{i\in I} I_i = \langle \bigcup_{i\in I} I_i \rangle \subset A.$$

Définition I.1.21 (Idéal maximal)**.** Soit A un anneau et soit $\mathfrak{M}$ un idéal à gauche de A. On dit que $\mathfrak{M}$ est maximal si $\mathfrak{M} \neq A$ et si tout ideal I à gauche I de A contenant $\mathfrak{M}$ est soit égal à $\mathfrak{M}$, soit égal à A.

On définit de même les idéaux à droites ou bilatères maximaux.

Le théorème suivant est équivalent à l'axiome du choix. On l'admet (voir chapitre II.8). Introduisons la terminologie suivante : un idéal I de A est dit idéal propre s'il n'est pas égal à A.

Théorème I.1.22 (Krull)**.** *Soit Soit A un anneau et soit I un idéal à gauche propre de A. Alors il existe un idéal à gauche maximal $\mathfrak{M}$ de A contenant I.*

On a un énoncé similaire avec les idéaux à droite ou bilatère.

Exercice I.1.23. Soient A un anneau et I un idéal bilatère de A. Comment sont obtenus les idéaux bilatères de A/I à partir de ceux de A ?

Montrer que si A/I est un anneau à division alors I est maximal, que la réciproque est vraie si A et commutatif, et fausse en général.

Exercice I.1.24. Soit A un anneau commutatif. Montrer l'égalité

$$\bigcup_{\mathfrak{M} \text{ idéal maximal de} A} \mathfrak{M} = A \setminus A^{\times}.$$

Exercice I.1.25. Soit $\mathcal{C}$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$. Montrer que les idéaux maximaux de $\mathcal{C}$ sont les

$$I_x = \{f \in \mathcal{C} | f(x) = 0\},$$

pour chaque $x \in [0,1]$ (pour lesquels $\mathcal{C}/I_x \simeq \mathbb{R}$).

I.1.3 Anneaux intègres

Définition I.1.26 (Anneau intègre)**.** Un anneau A est dit intègre s'il est non réduit à $\{0\}$ et s'il vérifie la propriété suivante

$$(\forall a, b \in A), \quad [ab = 0] \implies [a = 0 \text{ ou } b = 0].$$

Exercice I.1.27. Parmi les exemples d'anneaux donnés ci-dessus (Exemple I.1.3), lesquels sont intègres ?

En anglais, un anneau commutatif intègre est appelé « integral domain », ou simplement « domain ».

Exercice I.1.28. Montrer que tout anneau commutatif intègre fini est un corps.

Exercice I.1.29. Soit A un anneau commutatif.

a) Si A est intègre, montrer que l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est aussi intègre.
b) Si A est intègre, quelles sont les unités de $A[X]$?
c) On rappelle qu'un élément a de A est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Soit a un élément nilpotent de A, et soit u une unité de A. Montrer que $u + a$ est inversible.
d) Soit $P = a_0 + a_1X + \ldots + a_NX^N$ un polynôme à coefficients dans A. On suppose que a_0 est inversible et que les éléments $a_1, \ldots, a_N$ sont nilpotents. Montrer que P est inversible dans $A[X]$.
e) Réciproquement, montrer que les les unités de $A[X]$ sont les polynômes $P = a_0 + a_1X + \ldots + a_NX^N$ avec a_0 inversible et $a_1, \ldots, a_N$ nilpotents

Exemple : dans $(\mathbb{Z}/4\mathbb{Z})[X]$, $(2X+1)^2 = 1$, donc $2X + 1$ est une unité dans cet anneau).

L'anneau $\mathbb{Z}$ occupe une place particulière parmi les anneaux. En effet

Théorème I.1.30 (Propriété universelle de l'anneau $\mathbb{Z}$)**.** *Pour tout anneau A, il existe un seul morphisme d'anneaux $\iota_A : \mathbb{Z} \to A$. Le noyau de ι_A est un idéal de $\mathbb{Z}$, il est donc de la forme (n) pour un entier $n \in \mathbb{N}$. Cet entier n s'appelle la caractéristique de A. Si A est intègre, p est un nombre premier ou bien 0.*

Démonstration. Comme ι_A est un morphisme d'anneaux, on a $\iota_A(1) = 1_A$ et $\iota_A(n) = n\iota_A(1) = n \cdot 1_A$, ce qui montre l'existence et l'unicité de ι_A. Le noyau de ι_A est un ideal de $\mathbb{Z}$, il est donc de la forme $(n) = n\mathbb{Z}$. Si A est un corps, et si $ab \in \ker \iota_A$, alors $ab \cdot 1_A = (a \cdot 1_A)(b \cdot 1_A) = 0$ et comme A est intègre, soit $b \cdot 1_A = 0$, soit c'est un inversible dans A, auquel cas $a \cdot 1_A = 0$. Donc soit $a \in \ker \iota_A$, soit $b \in \ker \iota_A$. L'idéal $\ker \iota_A$ est donc premier. On a un peu anticipé ici sur la notion d'idéal premier qui se trouve dans la section I.4. □

I.2 Corps des fractions d'un anneau commutatif intègre

Soit A un anneau commutatif intègre. On se demande si on peut inclure A dans un corps, et si oui quel est le plus petit corps pour lequel cela est possible. Par exemple, pour l'anneau $\mathbb{Z}$, la réponse est $\mathbb{Q}$. Pour l'anneau un anneau de polynômes $A[X]$, A commutatif intègre, la réponse est $A(X)$, le corps des fractions rationnelles à coefficients dans A. En général, on construit le corps des fractions $K(A)$ de la manière suivante :

On munit $A \times (A \setminus \{0_A\})$ de la relation

$$(a, b) \sim (c, d) \text{ si } ad = bc$$

et on vérifie immédiatement que c'est une relation d'équivalence. On note $K(A)$ l'ensemble des classes d'équivalence pour cette relation, et si $(a, b) \in A \times (A \setminus \{0_A\})$, on note $\frac{a}{b}$ la classe d'équivalence de (a, b) On munit $K(A)$ des lois d'addition et multiplication

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

On vérifie que c'est un anneau commutatif, l'élément neutre de l'addition est $\frac{0}{1}$ et l'élément neutre de la multiplication est $\frac{1}{1}$. Tout élément non nul de $K(A)$ est inversible, l'inverse de $\frac{a}{b}$ étant $\frac{b}{a}$, c'est donc un corps. On vérifie que

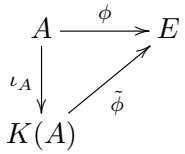
$$\iota_A : \ A \longrightarrow K(A), \quad a \mapsto \frac{a}{1}$$

est un morphisme d'anneaux injectif. En conséquence, on un élément de la forme $\frac{a}{1}$ simplement a.

En quel sens peut-on dire que $K(A)$ est le plus petit corps contenant A ? La réponse est la suivante : pour tout corps E et pour tout morphisme d'anneau,

$$\phi : \ A \longrightarrow E,$$

il existe un unique $\tilde{\phi} : \ K(A) \longrightarrow E$ tel que $\phi = \tilde{\phi} \circ \iota_A$:



C'est facile à vérifier car $\tilde{\phi}$ est déterminé par $\tilde{\phi}(\frac{a}{b}) = \phi(a)\phi(b)^{-1}$.

I.3 Lemme des restes chinois

Lemme I.3.1 (Lemme des restes chinois)**.** *Soit A un anneau commutatif et soient $\mathfrak{m}_i$, $i = 1, \ldots, r$ des idéaux de A tels que $\mathfrak{m}_i + \mathfrak{m}_j = A$ si $i \neq j$. Le morphisme canonique*

$$A/\bigcap_{i=1,\ldots,r} \mathfrak{m}_i \longrightarrow \prod_{i=1,\ldots,r} A/\mathfrak{m}_i$$

est un isomorphisme.

Démonstration. L'injectivité du morphisme est immédiate. On démontre la surjectivité par récurrence sur r, le cas $r = 1$ étant trivial. Si $r = 2$, il s'agit, quels que soient $a_1, a_2 \in A$ de trouver $a \in A$ et $\mu_1 \in \mathfrak{m}_1$, $\mu_2 \in \mathfrak{m}_2$ tels que $a + \mu_1 = a_1$, $a + \mu_2 = a_2$. Comme par hypothèse $\mathfrak{m}_1 + \mathfrak{m}_2 = A$, on prend $\mu_1 \in \mathfrak{m}_1$, $\mu_2 \in \mathfrak{m}_2$ tels que $\mu_1 - \mu_2 = a_1 - a_2$ et l'on pose $a = a_1 - \mu_1 = a_2 - \mu_2$, ce qui résout le problème. Si $r > 2$, par hypothèse de récurrence on a un isomorphisme

$$A/\bigcap_{i=1,\ldots,r-1} \mathfrak{m}_i \simeq \prod_{i=1,\ldots,r-1} A/\mathfrak{m}_i.$$

On applique le résultat pour $r = 2$ aux deux idéaux $\mathfrak{m}_r$ et $\bigcap_{i=1,\ldots,r-1} \mathfrak{m}_i$, ce qui permet de conclure, mais il faut pour cela vérifier que $\bigcap_{i=1,\ldots,r-1} \mathfrak{m}_i + \mathfrak{m}_r = A$. Par hyothèse, pour tout $i = 1, \ldots, r-1$, il existe $a_{r,i} \in \mathfrak{m}_r$ et a_i in $\mathfrak{m}_i$ tels que $a_i + a_{r,i} = 1$. En multipliant ces $r - 1$ égalités, on obtient

$$1 \in a_1 \ldots a_{r-1} + \mathfrak{m}_r \subset \bigcap_{i=1,\ldots,r-1} \mathfrak{m}_i + \mathfrak{m}_r$$

ce qui établit l'assertion. □

Ceci conclut la démonstration de la proposition. □

Exemple de Sun Zi (tiré de l'article Wikipedia sur lemme des restes chinois). La forme originale du théorème apparait sous forme de problème dans le livre de Sun Zi, le Sunzi suanjing, datant du iiie siècle. Il est repris par le mathématicien chinois Qin Jiushao dans son ouvrage le Shùshū Jiǔzhāng (≪ Traité mathématique en neuf chapitres ≫) publié en 1247. Le résultat concerne les systèmes de congruences.

Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ? Cette énigme est parfois associée au général Han Xin comptant son armée.

La résolution proposée par Sun Zi pour ce problème est la suivante :

Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105. Mais la solution n'explique qu'imparfaitement la méthode utilisée. On peut cependant remarquer que :

70 a pour reste 1 dans la division par 3 et pour reste 0 dans les divisions par 5 et 7 ;

21 a pour reste 1 dans la division par 5 et pour reste 0 dans les divisions par 3 et 7 ;

15 a pour reste 1 dans la division par 7 et pour reste 0 dans les divisions par 3 et 5.

Le nombre $2 \times 70 + 3 \times 21 + 2 \times 15$ a bien alors pour restes respectifs 2, 3 et 2 dans les divisions par 3, 5 et 7. Enfin, comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors de 23.

Exercice I.3.2. Quels sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$? Déterminer les $n \in \mathbb{N}$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit un groupe cyclique.

Exercice I.3.3. Soit A un anneau commutatif, et soit $e \in A$, $e \notin \{0_A, 1_A\}$ et tel que $e^2 = e$ (e est un idempotent). Considérons les idéaux engendrés par e et $1_A - e$ respectivement : $I = (e)$, $J = (1_A - e)$. Montrer que A est isomorphe à $A/I \times A/J$.

I.4 Divisibilité dans un anneau

Notre but est maintenant de généraliser l'arithmétique de l'anneau des entiers $\mathbb{Z}$ à un anneau commutatif quelconque. **Dans cette section, on ne considère que des anneaux commutatifs**.

Définition I.4.1. On dit que a divise b (dans l'anneau A), s'il existe $c \in A$ tel que $ac = b$. On note $a|b$ quand cela se produit. On dit aussi de manière équivalente que b est multiple de a.

Par exemple, dans $\mathbb{Z}$, $2|10$, $n|0$ pour tout $n \in \mathbb{Z}$, et si $0|n$, alors $n = 0$.

Reformulons cette définition en termes d'idéaux. Pour cela, on définit :

Définition I.4.2 (Idéal principal)**.** Un idéal engendré par un seul élément de A est appelé un idéal principal.

Pour tout $a \in A$, on note (a) l'idéal engendré par l'élément a (voir Définition I.1.19). On a $(a) = \{ac, c \in A\}$, c'est-à-dire l'ensemble des multiples de A.

On dit qu'un anneau est principal s'il est intègre et si tous ses idéaux sont principaux.

Proposition I.4.3. *Dans l'anneau A, a divise b si et seulement si $(b) \subset (a)$.*

Remarquons qu'une unité de l'anneau A divise tous les éléments de A.

Proposition I.4.4. *Soient a, b deux éléments de l'anneau A que l'on suppose intègre. On a $a|b$ et $b|a$ si et seulement s'il existe $u \in A^\times$ tel que $a = ub$. On dit alors que a et b sont* associés. *De manière équivalente, a et b sont associés si et seulement si $(a) = (b)$.*

Démonstration. On suppose que $a|b$ et $b|a$: il existe $c, d \in A$ tels que $b = ac$ et $a = bd$, d'où $b(1 - cd) = 0$ et donc si $b \neq 0$, on a $cd = 1$ (on utilise l'intégrité). Ainsi c et d sont inversibles, et a et b sont associés. La réciproque est évidente. □

Remarque I.4.5. Il est assez difficile de trouver un exemple d'anneau non intègre A et d'éléments $a, b \in A$ tels que $(a) = (b)$ et a et b ne sont pas associés. On peut prendre $A = \mathbb{R}[X, Y, Z]/(X(1 - YZ))$ et vérifier que les classes de X et XY engendrent le même idéal de A. Les inversibles dans A sont les classes des polynômes constants non nuls.

Il est facile de vérifier que « être associé avec » définit une relation d'équivalence sur A.

Nous allons maintenant définir les notions d'élément irréductible et d'élément premier dans un anneau commutatif intègre.

Définition I.4.6 (Eléments irréductibles et réductibles)**.** Soit A un anneau commutatif intègre. Un élément a de A est dit réductible si on peut écrire $a = xy$, avec x et y des éléments dans A non inversibles. Un élement qui n'est pas réductible est dit irréductible. Un élément a de A est irréductible si a est non nul et non inversible et, si $a = xy$, alors soit x, soit y est inversible. La seconde condition signifie que les seuls diviseurs de a sont ses associés et les unités de A.

Exemple I.4.7. Les éléments irréductibles de $\mathbb{Z}$ sont les $\pm p$, avec p nombre premier. Ceux de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Définition I.4.8 (Elément premier)**.** Soit A un anneau commutatif intègre. Un élément a de A est premier si a est non nul et non inversible et, si $a|xy$ dans A, alors soit $a|x$, soit $a|y$.

On peut relier ceci à la notion d'idéal premier.

Définition I.4.9 (Idéal premier)**.** Soit A un anneau commutatif. Un idéal I de l'anneau A est dit premier s'il est propre et s'il vérifie la propriété suivante. Si a, b sont deux éléments de A tels que $ab \in I$, alors $a \in I$ ou $b \in I$.

Proposition I.4.10. *Soit A un anneau commutatif intègre. Soit a un élément non nul de A. Alors l'idéal (a) est premier si et seulement si a est premier.*

Démonstration. Supposons que l'idéal (a) soit premier. Supposons aussi que a divise xy. On a alors $(xy) \subset (a)$, donc $xy \in (a)$ et donc soit $x \in (a)$, soit $(y) \in (a)$, c'est-à-dire, soit a divise x, soit a divise y. Donc a est premier.

Réciproquement, supposons a premier dans A, et supposons $xy \in (a)$, c'est-à-dire que a divise xy. On a donc a divise x ou a divise y, c'est-à-dire soit $x \in (a)$, soit $y \in (a)$. □

Proposition I.4.11. *Soient A un anneau commutatif et I un idéal de A. Alors I est un idéal premier si et seulement si A/I est un anneau intègre.*

Démonstration. Supposons I est premier, et soient $x, y \in A$ tels que $\bar{x}\bar{y} = 0$ dans A/I (on note $\bar{x}$ l'image de $x \in A$ par la projection canonique de A dans A/I. Ceci signifie que $xy \in I$, et comme I est premier, soit $x \in I$, c'est-à-dire $\bar{x} = 0$, soit $y \in I$, c'est-à-dire $\bar{y} = 0$, ce qui prouve que A/I est intègre. La réciproque se montre en inversant l'argument. □

Remarque I.4.12. Un idéal premier est propre car l'anneau nul $\{0\}$ n'est pas intègre.

Corollaire I.4.13. *Un idéal maximal est premier.*

En effet, on a vu dans l'exercice I.1.23 que si I est un idéal maximal, alors A/I est un corps, donc intègre.

Proposition I.4.14. *Soit a un élément non nul de A. Si a est premier, a est irréductible, mais la réciproque est fausse en général, comme le montre l'exercice I.4.16 ci-dessous.*

Démonstration. Supposons que a soit premier, et non irréductible. Alors il existe $x, y \in A$ non inversibles tels que $a = xy$. Donc $xy \in (a)$. Comme (a) est premier $x \in (a)$ ou $y \in (a)$. Disons que l'on est dans le premier cas. Alors $a|x$, mais on a aussi $x|a$, ce qui veut dire que x et a sont associés. On en déduit que y est inversible, car A est intègre et l'on aboutit à une contradiction. □

Exemple I.4.15. Si $n \geq 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. C'est alors un corps. On a

$$n \text{ est premier dans } \mathbb{Z} \Leftrightarrow \text{ l'idéal } (n) \text{ est premier } \Leftrightarrow \text{ l'idéal } (n) \text{ est maximal}$$

$$\Leftrightarrow \ n \text{ est irréductible} \Leftrightarrow n \text{ est un nombre premier}$$

Exercice I.4.16. Considérons le sous-anneau $\mathbb{Z}[i\sqrt{5}]$ de $\mathbb{C}$ et l'application « norme »

$$N : A \to \mathbb{N}, \quad a + i\sqrt{5}b \mapsto a^2 + 5b^2.$$

Montrer que $x \in A$ est une unité si et seulement si $N(x) = 1$. Montrer que le nombre 3 est irréductible mais l'idéal (3) n'est pas premier, car 3 divise le produit $(1 + i\sqrt{5})(1 - i\sqrt{5})$ mais aucun des facteurs.

Comme on le voit, les relations entre ces différentes notions sont subtiles. On a montré les implications suivantes dans un anneau commutatif intègre :

(I.4.1)
$$\begin{array}{ccc} & & a \text{ premier} \\ & & \Updownarrow \\ (a) \text{ maximal} & \Longrightarrow & (a) \text{ premier} \end{array} \qquad \Longrightarrow \ a \text{ irréductible}$$

Exercice I.4.17. Soient $f : A \to B$ un morphismes d'anneaux (commutatifs). Montrer que l'image réciproque d'un idéal premier de B est un idéal premier de A. Est-ce encore vrai pour un idéal maximal ?

Exercice I.4.18. Soient I et J deux idéaux d'un anneau commutatif A. On définit le produit d'idéaux

$$IJ = \left\{ \sum_i x_i y_i, \ x_i \in I, \ y_i \in J \right\}$$

Montrer que c'est un idéal de A contenu dans $I \cap J$. A-t-on toujours $I \cap J = IJ$?

Exercice I.4.19. Soit A un anneau commutatif.

(i) On suppose que A est intègre et ne possède qu'un nombre fini d'idéaux. Montrer que A est un corps.

(ii) On suppose que A ne possède qu'un nombre fini d'idéaux. Montrer que tout idéal premier est maximal.

(iii) On suppose que tout idéal propre de A est premier. Montrer que A est un corps.

I.5 Anneaux principaux, anneaux euclidiens

Dans cette section, comme la précédente, les anneaux sont supposés commutatifs.

Définition I.5.1. Un anneau A est *principal* (« principal ideal domain », ou « PID », en anglais) si A est intègre et si tout idéal de A est principal, c'est-à-dire qu'il peut être engendré par un élément.

L'anneau $\mathbb{Z}$ est donc principal (Exemple I.5.4), mais pas l'anneau $\mathcal{C}$ de l'exercice I.1.25, ni l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers, ni l'anneau $K[X,Y]$ des polynômes à deux indéterminées à coefficients dans un corps K.

Dans la pratique, on montre souvent qu'un anneau intègre est principal en exhibant une *division euclidienne* sur A.

Définition I.5.2. Soit A un anneau commutatif intègre. Une division euclidienne dans A est une fonction $\phi : A \setminus \{0\} \to \mathbb{N}$ vérifiant

(i) quels que soient $a, b \in A \setminus \{0\}$, $\phi(a) \leq \phi(ab)$,

(ii) quels que soient a et b dans $A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$, ou $r \neq 0$ et $\phi(r) < \phi(b)$.

Un anneau anneau commutatif intègre muni d'une division euclidienne s'appelle un anneau euclidien.

Proposition I.5.3. *Un anneau euclidien est principal.*

Il s'agit de montrer que tout idéal I est principal. Choisissons $x \in I$ avec $\phi(x) = \min_{y \in I} \phi(y)$ (ϕ étant à valeurs dans $\mathbb{N}$, ce minimum existe). Soit $y \in I$. on effectue la division euclidienne de x par y et l'on écrit $y = bx + r$ avec $r = 0$, ou $r \neq 0$ et $\phi(r) < \phi(x)$. Comme $r = bx - y \in I$, par minimalité de $\phi(x)$, on ne peut pas avoir $\phi(r) < \phi(x)$, donc $r = 0$ et $y = bx \in (x)$, ce qui montre que $I = (x)$. □

Les deux exemples fondamentaux sont :

Exemples I.5.4.
- l'anneau $\mathbb{Z}$ est euclidien pour la fonction $\phi(n) = |n|$;
- si K est un corps, l'anneau $K[X]$ est euclidien pour la fonction $\phi(P) = \deg(P)$.

On a verra en exercice d'autres exemples d'anneaux euclidiens : $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[j]$.

La proposition suivante montre que la situation entre les différentes notions vues en (I.8) est plus simple dans le cas des anneaux principaux.

Proposition I.5.5. *Soit A un anneau principal. Soit $0 \neq p \in A$. On a les équivalences suivantes*

(i) p est premier,

(ii) l'idéal (p) est premier,

(iii) p est irréductible,

(iv) l'idéal (p) est maximal.

Démonstration. Etant donnée les implications déjà démontrée en (I.8), il suffit de montrer que p est irréductible implique (p) maximal. Supposons p irréductible, et soit J un idéal contenant (p). On a $J = (q)$ pour un certain $q \in A$, et q divise p, donc en fait $(p) = (q) = J$ ou bien $(q) = A$. □

En particulier, l'anneau $\mathbb{Z}[i\sqrt{5}]$ de l'exercice I.4.16 n'est pas principal.

Définition I.5.6 (pgcd et ppcm dans un anneau principal)**.** Si a et b sont des éléments d'un anneau principal A, l'idéal (a, b) est engendré par un élément de A, uniquement déterminé à multiplication par un élément inversible de A près. On l'appelle un *pgcd* (« plus grand commun diviseur » ; « gcd » ou « greatest common divisor » en anglais) de a et b, parfois noté $a \wedge b$. De même, l'idéal $(a) \cap (b)$ est engendré par un élément de A, uniquement déterminé à multiplication par un élément inversible de A près, le *ppcm* (« plus grand commun multiple » ; « lcm » ou « least common multiple » en anglais) de a et b, parfois noté $a \vee b$. On peut de même définir le pgcd et le ppcm d'une famille quelconque d'élément de A.

Si $(a, b) = A$, ou de manière équivalente $a \wedge b = 1_A$, on dit que a et b sont premier entre eux.

Remarque I.5.7 (Théorème de Bézout)**.** Dans ce contexte, le « théorème de Bézout », qui dit que a et b sont premiers entre eux si et seulement s'il existe x et y dans A tels que

$$xa + yb = 1$$

est une tautologie.

Mentionnons comme conséquence un résultat classique

Lemme I.5.8 (Lemme de Gauss)**.** *Soit A un anneau principal. Si a, b et c sont des éléments de A tels que a divise bc mais est premier avec b, alors a divise c.*

Démonstration. Ecrivons $bc = ad$ et $xa + yb = 1$. On a alors $c = (xa + yb)c = xac + yad$, qui est bien divisible par a. □

Exercice I.5.9. Montrer que l'anneau des nombres décimaux (c'est-à-dire les nombres rationnels dont le développement décimal est fini) est principal. Quel est le pgcd de $0,6$ et de $30,4$?

Exercice I.5.10 (Anneau des entiers de Gauss). Montrer que l'anneau $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est euclidien, donc principal (i est l'élément de $\mathbb{C}$ tel que $i^2 = -1$). Posons $N(a+ib) = |a+ib|^2 = a^2 + b^2$. Que vaut N pour une unité ? Montrer que les unités de $\mathbb{Z}[i]$ sont ± 1, $\pm i$. Montrer que si un nombre premier impair p est réductible dans $\mathbb{Z}[i]$ alors $p \equiv 1 \mod 4$. Réciproquement, montrer que si $p \equiv 1 \mod 4$, alors p est réductible dans $\mathbb{Z}[i]$. On rappelle que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \mod 4$ (on pourra le redémontrer pour se rafraichir la mémoire), ce qui signifie qu'un nombre premier p tel que $p \equiv 1 \mod 4$ divise $m^2 + 1$ pour un certain entier m. On remarque alors que $m^2 + 1 = (m + i)(m - i)$ dans $\mathbb{Z}[i]$ et ainsi p n'est pas irréductible. Est-ce que 2 est irréductible dans $\mathbb{Z}[i]$? Montrer que si π est un irréductible dans $\mathbb{Z}[i]$, alors $(\pi) \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. En déduire que π divise un et un seul nombre premier p de $\mathbb{Z}$. Faire la liste des éléments irréductibles de $\mathbb{Z}[i]$.

Exercice I.5.11. Factoriser $-3 + 15i$ en irréductibles dans $\mathbb{Z}[i]$.

Exercice I.5.12 (Anneau des entiers d'Eisenstein). On considère l'ensemble $\mathbb{Z}[j] = \{a+bj \,|\, a, b \in \mathbb{Z}\}$, où $j = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$. On vérifie facilement que c'est un sous-anneau de $\mathbb{C}$ par exemple en utilisant le fait que $j^2 = -j - 1$. Posons $N(a + bj) = |a + bj|^2 = a^2 - ab + b^2$. Que vaut N pour une unité de $\mathbb{Z}[j]$? Déterminer le groupe des unités de $\mathbb{Z}[j]$. Montrer que $\mathbb{Z}[j]$ est un anneau euclidien. Montrer que si le nombre premier p est réductible dans $\mathbb{Z}[j]$, alors p s'écrit $p = x^2 - xy + y^2$, et que l'on a alors $p = (x + jy)(x + j^2y)$, puis $p = 3$ ou $p \equiv 1 \mod 3$. Pour la réciproque, on admettra un cas particulier du théorème de réciprocité quadratique de Gauss : si $p \equiv 1 \mod 3$, alors -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire que p divise $m^2 + 3$. Faire la liste des irréductibles de $\mathbb{Z}[j]$.

Exercice I.5.13. Montrer que les idéaux maximaux de l'anneau $\mathcal{C}$ des fonctions continues de $[0,1]$ dans $\mathbb{R}$ ne sont pas principaux (voir exercice. I.1.25). Que se passe-t-il si l'on remplace $\mathcal{C}$ par l'anneau des fonctions continues de classe $\mathcal{C}^\infty$ de $[0,1]$ dans $\mathbb{R}$?

Exercice I.5.14. Soit A un anneau intègre dans lequel tout idéal premier est principal. Montrer que l'anneau A est principal (*Indication :* on pourra considérer un élément maximal I dans la famille des idéaux non principaux de A, des éléments x et y de $A \setminus I$ tels que $xy \in I$, un générateur z de l'idéal $I + (x)$, un générateur w de l'idéal $\{a \in A \mid az \in I\}$, et montrer que zw engendre I).

Exercice I.5.15. Soit K un corps et considérons l'anneau des séries formelles $K[[X]]$. Montrer que c'est un anneau euclidien. Montrer que ses idéaux sont $\{0\}$ et les $I_m = (X^m)$ pour chaque $m \in \mathbb{N}$. (On pourra montrer que l'ensemble des éléments non inversibles de $K[[X]]$ est un idéal et que c'est donc le seul idéal maximal).

Exercice I.5.16. Soit p un nombre premier et soit $\alpha = i\sqrt{p}$. On considère l'anneau $A = \mathbb{Z}[\alpha]$. Montrer que l'idéal (α) de A est $\{a + b\alpha | a \in p\mathbb{Z},\ b \in \mathbb{Z}\}$. En déduire que α est premier dans A.

Algorithme d'Euclide. Soit A un anneau euclidien. En utilisant de manière répétée la division euclidienne, on peut trouver un algorithme qui calcule le pgcd de deux éléments de A. Soit a, b dans A, non nul. On écrit la division euclidienne de a par b :

$$a = bq_1 + r_1. \tag{I.5.1}$$

Puis celle de b par r_1,

$$b = r_1 q_2 + r_2 \tag{I.5.2}$$

Puis celle de r_1 par r_2,

$$r_1 = r_2 q_3 + r_3 \tag{I.5.3}$$

et ainsi de suite

$$r_i = r_{i+1} q_{i+2} + r_{i+2}. \tag{I.5.4}$$

Comme on a $\phi(b) > \phi(r_1) > \phi(r_2) > \cdots \phi(r_i) > \phi(r_{i+1}) \ldots$ il existe $N \in \mathbb{N}$ tel que $r_{N+1} = 0$. On s'arrête à ce moment là et la dernière équation que l'on écrit est

$$r_{N-1} = r_N q_{N+1}. \tag{I.5.5}$$

On a alors

$$(a, b) = (bq_1 + r_1, b) = (b, r_1) = (q_2 r_1 + r_2, r_1) = (r_1, r_2) = \ldots (r_i, r_{i+1}) = (r_N).$$

Ceci montre que r_N est un pgcd de a et b.

On peut aussi calculer des coefficients u et v d'une relation de Bézout

$$\mathrm{pgcd}(a, b) = ua + vb.$$

En effet

$$\mathrm{pgcd}(a, b) = r_N = r_{N-2} - q_N r_{N-1}$$

On remplace ensuite r_{N-1} dans cette formule par $r_{N-1} = r_{N-3} - r_{N-2} q_{N-1}$ et ainsi de suite jusqu'à obtenir r_N comme combinaison linéaire de a et b.

Exercice I.5.17. Terminer d'écrire complètement l'algorithme ci-dessus pour avoir une formule pour u et v en fonction des q_i. Implémenter cet algorithme sur une calculatrice ou un ordinateur.

Dans $\mathbb{Z}$ on peut donner un autre algorithme plus rapide que celui d'Euclide pour calculer le pgcd de deux entiers a et b. On peut supposer a et b strictement positifs. La première étape consiste à se ramener à des nombres impairs, on divise donc a et b par deux jusqu'à obtenir des nombres impairs a' et b' :

$$a = 2^{v_2(a)}a', \quad b = 2^{v_2(b)}b'.$$

On aura alors $\mathrm{pgcd}(a,b) = 2^{\min(v_2(a),v_2(b))}\mathrm{pgcd}(a',b')$. On peut supposer que $a' \geq b'$. On remarque que $a'-b'$ est pair. On a alors $\mathrm{pgcd}(a',b') = \mathrm{pgcd}(b',a'-b') = \mathrm{pgcd}(b', \frac{a'-b'}{2^{v_2(a'-b')}})$. On recommence le procédé en remplaçant (a',b') par $(b', \frac{a'-b'}{2^{v_2(a'-b')}})$ jusqu'à arriver à $\mathrm{pgcd}(d,0) = d$.

Exercice I.5.18. Trouver toutes les solutions entières de l'équation $999x - 49y = 5000$, puis celles de l'équation $147x + 258y = 369$.

Exercice I.5.19. Soit $P = X^3 + 1$ et $Q = X^2 + 1$. Montrer que P et Q sont premiers entre eux dans $\mathbb{Q}[X]$ et trouver $U, V \in \mathbb{Q}[X]$ tels que $UP + VQ = 1$.

I.6 Anneaux factoriels

Le théorème fondamental de l'arithmétique dit que tout élément de $\mathbb{Z}$ admet une décomposition en produit d'un facteur ± 1 et de nombres premiers, et que cette décomposition est unique, dans le sens où deux décompositions ne diffèrent que par une permutation des facteurs.

Un anneau factoriel est un anneau commutatif intègre où cette propriété, convenablement énoncée, est encore vraie. Dans cette section, même si on ne le précise pas à chaque fois, les anneaux sont tous commutatifs. Ce qui va jouer le rôle des nombres premiers de $\mathbb{Z}$, ce sont les éléments irréductibles de A, puisque ce sont les éléments qui n'admettent pas de décomposition « non triviale ». Evidemment, si u est une unité, on peut toujours écrire $x = uu^{-1}x$, mais ce n'est pas une décomposition très intéressante. Pour se débarrasser de ce problème avec les unités de l'anneau, rappelons que l'on dit que deux éléments a et b de A sont associés si $(a) = (b)$, ou de manière équivalente, s'il existe une unité $u \in A^\times$ tel que $b = ua$. Ceci définit une relation d'équivalence sur A, et il est facile de voir que cette relation préserve les éléments irréductibles. On peut donc choisir une fois pour toutes un système de représentants $\mathcal{P}$ des classes d'équivalence d'éléments irréductibles. Par exemple, dans $\mathbb{Z}$, les unités sont ± 1, et les classes les classes d'équivalence d'éléments irréductibles sont les $\{\pm p, p \text{ premier}\}$. On choisit naturellement comme système de représentants $\mathcal{P} = \{p \text{ premier}\}$. Dans un anneau quelconque, il n'y a pas forcément de choix naturel pour $\mathcal{P}$.

Définition I.6.1. Soit A un anneau commutatif intègre. Fixons un système de représentants $\mathcal{P}$ des classes d'équivalence d'éléments irréductibles. On dit alors que A est factoriel si tout élément non nul de A s'écrit comme produit d'une unité et d'éléments de $\mathcal{P}$, et que de plus, cette factorisation est unique à permutation des facteurs irréductibles près.

Tout élément non nul a de A s'écrit donc d'une manière unique

$$a = u \prod_{p \in \mathcal{P}} p^{n_p},$$

avec $u \in A^\times$, et où $(n_p)_{p\in\mathcal{P}}$ est une famille presque nulle d'entiers naturels. On note alors $v_p(a) := n_p$.

Remarque I.6.2. La plupart des anneaux intègres que l'on rencontre ont la propriété d'existence de la décomposition (voir Prop. I.6.7) ; la propriété forte est l'unicité.

Nous avons défini le pgcd de deux éléments d'un anneau principal (Définition I.5.6). On peut donner une autre définition pour deux éléments a et b d'un anneau factoriel : si $a = 0$, le pgcd $a \wedge b$ est par définition b ; de même $a \wedge 0 = a$. Si $ab \neq 0$, on pose

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}.$$

Cette définition dépend du choix de $\mathcal{P}$; on peut aussi déclarer que $a \wedge b$ est bien défini à association près. Dans tous les cas, le pgcd $a \wedge b$ est alors un diviseur commun de a et b, et tout diviseur commun à a et b divise $a \wedge b$ (mais l'inclusion d'idéaux $(a, b) \subset (a \wedge b)$ est en général stricte !).

Exercice I.6.3. Chercher un exemple d'anneau factoriel non principal et deux éléments a et b de cet anneau tel que l'inclusion d'idéaux $(a, b) \subset (a \wedge b)$ soit stricte.

On a une discussion analogue pour le ppcm, qui est laissée en exercice. On peut aussi parler du pgcd et du ppcm d'une famille finie quelconque d'éléments d'un anneau factoriel. Nous verrons plus tard qu'un anneau principal est toujours factoriel, et dans ce cas, les deux définitions coïncident.

Nous allons maintenant donner des critères pour qu'un anneau soit factoriel. Comme nous l'avons dit, l'existence d'une décomposition en produit d'irréductibles est une propriété assez faible. Elle est vérifiée pour une large classe d'anneaux, les anneaux noethériens. On reviendra plus tard (Section II.9) sur cette notion. Ici on se contente d'une définition pour les anneaux commutatifs.

Proposition I.6.4. *Soit A un anneau commutatif. Les trois propriétés suivantes sont équivalentes :*

(i) *tout idéal de A est engendré par un nombre fini d'éléments ;*

(ii) *toute suite croissante (pour l'inclusion) d'idéaux de A est stationnaire ;*

(iii) *toute famille non vide d'idéaux de A a un élément maximal pour l'inclusion.*

On dira que l'anneau A est noethérien *s'il vérifie ces propriétés*[2].

Démonstration. Montrons que (i) implique (ii). Soit (I_n) une telle suite ; la réunion I des I_n est encore un idéal car la famille (I_n) est totalement ordonnée pour l'inclusion. Par (i), il existe des éléments $x_1, \ldots, x_r$ de I qui l'engendrent. Chaque x_i est dans l'un des I_n, donc il existe n_0 (le plus grand des indices correspondants) tel que I_{n_0} les contienne tous. Alors $I = I_{n_0}$ et la suite (I_n) stationne à I_{n_0}.

Montrons que (ii) implique (iii). Si une famille non vide d'idéaux de A n'a pas d'élément maximal, on construit par récurrence une suite infinie strictement croissante d'idéaux de A, ce qui contredit (ii).

Montrons que (iii) implique (i). Soit I un idéal de A. La famille $\mathcal{E}$ des idéaux $J \subset I$ qui sont engendrés par un nombre fini d'éléments n'est pas vide (elle contient l'idéal (0)). Elle admet donc par hypothèse un élément maximal $J_0 \in \mathcal{E}$. Pour tout $x \in I$, l'idéal $J_0 + xA$ est aussi dans $\mathcal{E}$, donc $J_0 + xA = J_0$ par maximalité. Ceci signifie $x \in J_0$. Finalement $I = J_0$ et I est engendré par un nombre fini d'éléments. □

Exemples I.6.5 (et contre-exemples)**.**

2. Ces anneaux sont nommés ainsi en l'honneur d'Emmy Noether (1882–1935).

a) Tout anneau principal est noethérien ((i) est trivialement vérifié).
b) Si A est noethérien, tout quotient de A l'est encore (c'est immédiat à partir de la caractérisation (ii), vu que les idéaux de A/I sont les idéaux de A contenant I).
c) En revanche, un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien (voir exercice I.7.3).
d) Si K est un corps, l'anneau $K[(X_n)_{n\in\mathbb{N}}]$ n'est pas noethérien car

$$(X_0) \subset (X_0, X_1) \subset \cdots \subset (X_0, \ldots, X_n) \subset \cdots$$

forme une suite infinie strictement croissante d'idéaux.

Exercice I.6.6. Soit A un anneau tel que tout idéal *premier* de A est engendré par un nombre fini d'éléments. Montrer que A est noethérien (*Indication :* on pourra considérer un élément maximal I dans la famille des idéaux qui ne sont pas engendrés par un nombre fini d'éléments, des éléments x et y de $A \setminus I$ tels que $xy \in I$, des générateurs $x_1, \ldots, x_r, y$ de l'idéal $I + (y)$, avec $x_1, \ldots, x_r \in I$, des générateurs $a_1, \ldots, a_s$ de l'idéal $\{a \in A \mid ay \in I\}$, et montrer que $x_1, \ldots, x_r, a_1y, \ldots, a_sy$ engendrent I).

Proposition I.6.7. *Soit A un anneau intègre noethérien. On suppose fixé un système de représentants $\mathcal{P}$ des classes d'association d'irréductibles. Tout élément non nul de A peut s'écrire $up_1 \cdots p_r$ avec $u \in A^\times$ et $p_1, \ldots, p_r \in \mathcal{P}$.*

Démonstration. Soit $\mathcal{E}$ l'ensemble des idéaux de A de la forme (x), pour x ne s'écrivant pas comme demandé. Si $\mathcal{E}$ n'est pas vide, il admet un élément maximal (a) (par la Prop. I.6.4, ici on utilise que A est noethérien et pas le lemme de Zorn). En particulier a n'est alors pas irréductible. Comme il n'est pas inversible, il s'écrit $a = bc$ avec b et c non associés à a. Comme A est intègre, les idéaux (b) et (c) contiennent alors strictement (a), donc par maximalité, ils ne sont pas dans $\mathcal{E}$, de sorte que b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles. □

La proposition suivante donne un critère pour qu'un anneau soit factoriel quand on connaît déjà l'existence de la décomposition en irréductibles (par exemple, si l'anneau est noethérien, d'après ce qui précède). Nous avons donné la définition du fait que deux éléments a et b d'un anneau A sont premiers entre eux dans le cas d'un anneau principal, mais on peut étendre la définition à un anneau quelconque : a et b sont premiers entre eux si leurs seuls diviseurs communs sont les unités de A (par exemple, si p est irréductible, tout élément de A est ou bien premier avec p, ou bien divisible par p). Si A est un anneau principal ou factoriel, des éléments de A sont donc premiers entre eux si et seulement si leur pgcd est une unité.

Proposition I.6.8. *Soit A un anneau intègre tel que tout élément non nul de A soit produit d'irréductibles. Les propriétés suivantes sont équivalentes :*
(i) *A est factoriel ;*
(ii) *pour tout élément irréductible p de A, l'idéal (p) est premier*[3] *;*
(iii) *pour tous éléments non nuls a, b et c de A tels que a divise bc mais est premier avec b, a divise c.*

Démonstration. Montrons que (iii) implique (ii). Supposons p irréductible et $p|ab$. Si $ab = 0$, on a $a = 0$ ou $b = 0$ par intégrité de A, donc $p|a$ ou $p|b$. Si $ab \neq 0$ et que p ne divise pas a, alors p

3. Autrement dit, si a et b sont des éléments de A et que p divise ab, alors p divise a ou p divise b.

est premier avec a puisque p est irréductible, de sorte que p divise b d'après (iii). Ainsi l'idéal (p) est premier.

Montrons que (ii) implique (i). Soit $\mathcal{P}$ un système de représentants irréductibles. Si

$$u \prod_{p \in \mathcal{P}} p^{m_p} = v \prod_{p \in \mathcal{P}} p^{n_p}$$

sont des décompositions d'un élément non nul de A, la condition $m_q > n_q$ pour un certain $q \in \mathcal{P}$ implique, par intégrité de A, que q divise $v \prod_{p \in \mathcal{P},\ p \neq q} p^{n_p}$, donc l'un des facteurs d'après (ii). Mais q ne peut diviser un élément p de $\mathcal{P}$ distinct de q car $\mathcal{P}$ est un système de représentants irréductibles. Ainsi $m_p = n_p$ pour tout $p \in \mathcal{P}$, puis $u = v$ par intégrité de A.

Montrons que (i) implique (iii). On écrit $ad = bc$ et on décompose les éléments non nuls a, b, c et d comme ci-dessus. Alors pour tout $p \in \mathcal{P}$, on a (par unicité de la décomposition) $v_p(b) + v_p(c) = v_p(a) + v_p(d) \geq v_p(a)$. Si $v_p(b) = 0$, on a donc $v_p(a) \leq v_p(c)$. Si $v_p(b) > 0$, on a $v_p(a) = 0$ (car a est premier avec b) donc $v_p(a) \leq v_p(c)$. Ainsi a divise c. □

Exemple I.6.9. L'anneau $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$ est intègre mais n'est pas factoriel : 3 est irréductible mais l'idéal (3) n'est pas premier (voir exercice I.4.16).

Exercice I.6.10. Soit K un corps. Montrer que le sous-anneau $K[X^2, X^3]$ de $K[X]$ engendré par X^2 et X^3 n'est pas factoriel.

On déduit alors de la prop. I.6.8 les deux corollaires suivants.

Corollaire I.6.11. *Un anneau intègre noethérien est factoriel si et seulement si tout élément irréductible engendre un idéal premier.*

Il existe des anneaux factoriels non noetheriens (comme par exemple $K[(X_n)_{n\in\mathbb{N}}]$).

Corollaire I.6.12. *Tout anneau principal est factoriel.*

Exercice I.6.13. On a donc maintenant deux définitions du pgcd et du ppcm pour un anneau principal : celle de la définition I.5.6 pour les anneaux principaux, et celle donnée ci-dessus pour les anneaux factoriels. Montrer qu'elles coïncident.

Exercice I.6.14. Soit A un anneau factoriel. Le but de cet exercice est de montrer que A est principal si et seulement si tout idéal premier non nul de A est maximal.

On a déjà vu que tout idéal premier non nul d'un anneau principal est maximal (Prop. I.5.5). On veut donc démontrer la réciproque. On suppose donc que tout idéal premier non nul de A est maximal et on se propose de montrer que A est principal.

a) Montrer que tout idéal premier de A est principal. On pourra considérer un tel idéal I et la décomposition en irréductibles d'un élément x non nul de I.
b) En considérant l'ensemble $\mathcal{E}$ de tous les idéaux de A qui ne sont pas principaux, et dans le cas où cet ensemble est non vide, un élément maximal I de $\mathcal{E}$ (justifier l'existence), aboutir à une contradiction.

Exercice I.6.15. On considère l'anneau $A = \mathbb{Z}[i\sqrt{2}]$ et la norme $N(a+i\sqrt{2}b = a^2+2b^2)$. Montrer que A est un anneau euclidien. Montrer que les seules solutions entières de $y^2 + 2 = x^3$ sont $(x, y) = (3, \pm 5)$.

Exercice I.6.16. On considère l'anneau $A = \mathbb{Z}[i]$ de l'exercice I.5.10. Montrer que les seules solutions entières de $y^2 + 4 = x^3$ sont $(x, y) = (\pm 11, 5)$ ou $(\pm 2, 2)$.

Exercice I.6.17. On considère l'anneau $A = \mathbb{Z}[i\sqrt{3}]$. Le but de cet exercice est de montrer que ce n'est pas un anneau factoriel. On introduit la norme $N(a + bi\sqrt{3}) = a^2 + 3b^2$. Montrer que les unités de A sont ± 1. Montrer que 2 et $1 + i\sqrt{3}$ sont irréductibles dans A. Constater que $4 = 2.2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et conclure.

Exercice I.6.18. Soit A un anneau commutatif intègre et soit K son corps des fractions. On dit qu'un élément x de K est entier sur A s'il existe un polynôme $P = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n$ à coefficients dans A tels que $P(x) = 0$.

Montrer que si A est factoriel, les éléments de K entiers sur A sont les éléments de A. (Par exemple les éléments de $\mathbb{Q}$ entiers sur $\mathbb{Z}$ sont .... les entiers, c'est-à-dire les éléments de $\mathbb{Z}$.)

Montrer que $j = \frac{-1+i\sqrt{3}}{2}$est entier sur l'anneau $A = \mathbb{Z}[i\sqrt{3}]$ (qui n'est pas factoriel), mais que $j \notin A$.

Exercice I.6.19. Soit R un anneau euclidien qui n'est pas un corps.

a) Montrer que l'on peut trouver un élément non inversible x de R tel que la restriction à $R^\times \cup \{0\}$ de la projection canonique de R sur $R/(x)$ soit surjective. On pourra choisir x tel que $\phi(x)$ soit minimal parmi les éléments $x \notin R^\times$, où ϕ désigne le stathme d'une division euclidienne de R.

Soient $\alpha = \dfrac{1 + i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

b) En s'inspirant de 8.(a), déterminer $A^\times$.
c) Montrer que A n'est pas euclidien.
d) Si $a, b \in A \smallsetminus \{0\}$, montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.
e) Montrer que l'idéal engendré par 2 dans A est maximal.
f) Montrer que A est un anneau principal.

Exercice I.6.20. Soit k un corps.

a) Montrer que le sous-anneau $k[T^2, T^3]$ de $k[T]$ n'est pas factoriel.
b) Montrer que la k-algèbre $k[X, Y]/(X^2 - Y^3)$ est isomorphe à $k[T^2, T^3]$.
c) Montrer que la k-algèbre $k[X, Y]/(X^2 - Y)$ est isomorphe à $k[T]$.
d) Montrer que la k-algèbre $k[X, Y]/(XY - 1)$ n'est pas isomorphe à $k[T]$.

Exercice I.6.21. Soit A un anneau commutatif unitaire noethérien.

a) En raisonnant par l'absurde, montrer que, pour tout idéal I de A, il existe des idéaux premiers $\mathfrak{P}_i$ vérifiant $\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_{n_I} \subseteq I$.
b) Montrer que l'on peut exiger $I \subseteq \mathfrak{P}_i$ pour tout $1 \leq i \leq n_I$ dans la question précédente.
c) En déduire qu'il existe un nombre fini d'idéaux premiers minimaux.

Exercice I.6.22. [Théorème de Fermat pour $n = 3$]On rappelle que l'on a établi dans l'exercice I.5.12 que $A = \mathbb{Z}[j]$ est un anneau euclidien et que ses unités sont $\{\pm 1, \pm j, \pm j^2\}$. On a aussi vu que $\theta = i\sqrt{3}$ est premier dans A. Supposons qu'il existe des éléments non nuls x, y, z dans A tels que

$$x^3 + y^3 = z^3.$$

(i) Montrer que l'on peut supposer x, y, z premiers entre eux, ce que l'on suppose dans la suite.
(ii) Montrer que $\theta = i\sqrt{3}$ est premier dans A.
(iii) Montrer que tout élément de A est congru à $0, 1$ ou -1 modulo θ.

(iv) Soit ξ et η dans A non divisibles par θ. Montrer que

$$\begin{aligned} \xi \equiv 1 \mod \theta &\implies \xi^3 \equiv 1 \mod 9 \\ \xi \equiv -1 \mod \theta &\implies \xi^3 \equiv -1 \mod 9 \\ \xi^3 + \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9 \\ \xi^3 - \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9 \end{aligned}$$

(v) Montrer que θ divise et et un seul des entiers x, y, z.

(vi) On suppose qu'il existe x, y, z dans A tels que θ ne divise pas xyz, des unités ϵ_1, ϵ_2 et un entier $r > 0$ tels que

$$x^3 + \epsilon_1 y^3 + \epsilon_2 (\theta^r z)^3 = 0.$$

Montrer que $\epsilon_1 = \pm 1$ et $r \geq 2$.

(vii) Considérons x, y, z non nuls dans A vérifiant $x^3 + y^3 + \epsilon(\theta^r z)^3 = 0$, avec $r \geq 2$, ϵ une unité de A et θ ne divisant pas xyz. Supposons que $N(x^3 y^3 z^3 \theta^{3r})$ soit minimale dans $\mathbb{Z}$. Obtenir une contradiction en construisant un autre triplet (x', y', z') de norme strictement plus petite et conclure.

I.7 Anneaux de polynômes

Soit A un anneau commutatif. Dans cette section, on étudie les anneaux de polynômes à une ou plusieurs indéterminée à coefficients dans A. La question générale est la suivante : quelles sont les propriétés de A qui se transmettent à $A[X]$, ou plus généralement à $A[X_1, \ldots, X_n]$?

I.7.1 Théorème de Hilbert

On commence par la noethérianité avec le célèbre théorème de Hilbert.

Théorème I.7.1 (Hilbert)**.** *Soit A un anneau noethérien. Les anneaux $A[X_1, \ldots, X_n]$, $n \in \mathbb{N}$ sont noethériens.*

Démonstration. Il suffit de montrer que $A[X]$ est noethérien, car $A[X_1, \ldots X_n] = A[X_1, \ldots X_{N-1}][X_N]$. Soit I un idéal de $A[X]$. Pour chaque $k \in \mathbb{N}$, on note $D_k(I)$ le sous-ensemble de A constitué de 0 et des coefficients dominants des polynômes de degré k de I. Il est immédiat que $D_k(I)$ est un idéal de A et qu'une inclusion $I \subset J$ entraîne $D_k(I) \subset D_k(J)$. On a d'autre part les deux propriétés suivantes :

a) pour tout $k \in \mathbb{N}$, on a $D_k(I) \subset D_{k+1}(I)$: il suffit de remarquer que si $P \in I$, alors $XP \in I$;

b) si $I \subset J$, le fait que $D_k(I) = D_k(J)$ pour tout $k \in \mathbb{N}$ entraîne $I = J$: si $I \neq J$, on choisit un polynôme $P \in J \setminus I$ de degré r minimal ; comme $D_r(I) = D_r(J)$, l'idéal I contient un polynôme Q de degré r qui a même coefficient dominant que P, mais alors $P - Q$ est dans $J \setminus I$ et est de degré $< r$, contradiction.

Ceci étant établi, soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $A[X]$. Comme A est noethérien, la famille des $D_k(I_n)$ pour $k \in \mathbb{N}$ et $n \in \mathbb{N}$ admet un élément maximal $D_l(I_m)$. D'autre part, pour chaque $k \leq l$, la suite d'idéaux $(D_k(I_n))_{n\in\mathbb{N}}$ est croissante, donc elle est stationnaire, c'est-à-dire qu'il existe n_k tel que pour

$$\forall n \geq n_k \qquad D_k(I_n) = D_k(I_{n_k}).$$

Soit alors N le plus grand des entiers $m, n_0, n_1, \ldots, n_l$. Nous allons montrer que pour tout $n \geq N$ et tout k, on a $D_k(I_n) = D_k(I_N)$, ce qui suffira à conclure $I_n = I_N$ via la propriété b) ci-dessus. On distingue deux cas :

1) si $k \leq l$, on a $D_k(I_N) = D_k(I_{n_k}) = D_k(I_n)$ par définition de n_k puisque n et N sont tous deux $\geq n_k$;

2) si $k > l$, on a $D_k(I_N) \supset D_l(I_N) \supset D_l(I_m)$ (d'après la propriété a) ci-dessus, et puisque $N \geq m$) et $D_k(I_n) \supset D_l(I_n) \supset D_l(I_m)$ pour les mêmes raisons, donc par maximalité de $D_l(I_m)$, on a $D_k(I_N) = D_l(I_m) = D_k(I_n)$. □

Corollaire I.7.2. *Soit k un corps. Alors toute k-algèbre A de type fini est noethérienne. Plus généralement, soit R un anneau noethérien. Alors toute R-algèbre de type fini est noethérienne.*

Démonstration. Par définition, une k-algèbre A est de type fini si elle est engendrée (comme algèbre), par un nombre fini d'éléments $x_1, \ldots x_n$. Ceci signifie que le morphismes de k-algèbres :

$$k[X_1, \ldots, X_n] \to A, \quad P \mapsto P(x_1, \ldots x_n)$$

est surjectif. Si I est le noyau de ce morphisme, alors $A \simeq k[X_1, \ldots, X_n]/I$ qui est noetherien d'après l'exemple I.6.5. De même une R-algèbre engendrée par des éléments $x_1, \ldots, x_n$ est un quotient de l'anneau $R[X_1, \ldots, X_n]$, qui est noethérien par le Théorème I.7.1. C'est donc un anneau noethérien. □

Exercice I.7.3. Soit K un corps. Montrer que dans l'anneau noethérien $K[X, Y]$, le sous-anneau engendré par les $X^n Y$, pour $n \in \mathbb{N} \setminus \{0\}$, n'est pas noethérien.

Exercice I.7.4. Soit $A = \{P \in \mathbb{Q}[X] \,|P(0) \in \mathbb{Z}\}$. Vérifier que c'est un sous-anneau de $\mathbb{Q}[X]$. Quel est son corps des fractions ? Soit $p \in \mathbb{Z}$ un nombre premier. Montrer que p vu comme élément de A est irréductible. Montrer que X est divisible par p dans A, et en fait, que p est divisible par n'importe qu'elle puissance de p. En déduire que A ni factoriel ni noetherien. Montrer que si I est un idéal de type fini de A (engendré par un nombre fini d'éléments), alors I est un idéal principal.

I.7.2 Polynômes irréductibles, factorisation de polynômes

Supposons tout d'abord A intègre. Il est alors clair que quels que soient $P, Q \in A[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$. Nous avons vu que si k est un corps, $k[X]$ est un anneau euclidien, donc principal, et donc factoriels. Tout polynôme admet donc une factorisation essentiellement unique en produit d'irréductibles. La question de la détermination des irréductibles de $k[X]$ est l'un des problèmes les plus importants de l'arithmétique. Par exemple le théorème fondamental de l'algèbre :

Théorème I.7.5. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

se reformule en disant que les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.

De manière générale, les polynômes de degré un de $k[X]$ sont irréductibles, et les facteurs irréductibles de degré un d'un polynôme $P \in k[X]$ correspondent aux racines de P. En effet, $P(\alpha) = 0$ si et seulement si $(X - \alpha)|P$. On appelle multiplicité de la racine α dans P le plus grand entier m tel que $(X - \alpha)^m|P$. Pour détecter les racines multiples, on utilise la dérivation des polynômes.

Définition I.7.6. Soit A un anneau commutatif, et soit $P = a_0 + a_1 X + \ldots + a_n X^n$ un polynôme dans $A[X]$. La dérivée formelle de P est le polynôme

$$DP = \sum_{k=1}^{n} k a_k X^{k-1}.$$

(On note aussi souvent P' ce polynôme).

Remarque I.7.7. En analyse, la dérivée est définie par un procédé de limite. Ici c'est une opération purement algébrique, définie pour tout anneau A. C'est pour ça que l'on parle d'une dérivée formelle. Heureusement, si $P \in \mathbb{R}[X]$ est considéré comme une fonction de $\mathbb{R}$ dans $\mathbb{R}$, sa dérivée formelle et sa dérivée comme fonction d'une variable réelle coïncident.

La dérivée formelle vérifie les deux propriétés suivantes :

$$D(P+Q) = DP + DQ, \qquad D(PQ) = (DP)Q + P(DQ) \quad \text{(Règle de Leibniz)}.$$

Pour un corps k, rappelons que sa caractéristique est définie de la manière suivante. Il existe un unique morphisme d'anneaux $\iota : \mathbb{Z} \to k$. Le noyau de ce morphisme est un idéal premier de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ pour $p \in \mathbb{N}$ premier ou nul. Cet entier p est la caractéristique de k.

On a alors la proposition suivante.

Proposition I.7.8. *Soit k un corps de caractéristique 0, et soit $P \in k[X]$ non nul. Alors P est divisible par le carré d'un polynôme $Q \in k[X]$ de degré ≥ 1 si et seulement si $P \wedge DP \neq 1$ (c'est-à-dire P et sa dérivée formelle DP sont ne sont pas premiers entre eux).*

Démonstration. Supposons que $P = Q^2 R$ dans $k[X]$. Alors d'après le règle de Leibniz,

$$DP = 2(DQ)QR + Q^2(DR),$$

et Q un un diviseur commun non inversible de P et DP. Réciproquement, supposons que DP et P ont un diviseur commun non inversible L, et supposons que P n'a pas de facteurs carrés irréductibles. On écrit alors $P = LM$ dans $k[X]$, et L ne divise pas M. Or on a

$$DP = (DL)M + L(DM),$$

donc L divise $(DL)M$ et comme M est premier à L, L divise DL. Or le degré de DL est $\deg L - 1$ (c'est ici qu'on utilise l'hypothèse de caractéristique 0), on aboutit a une contradiction. □

Remarque I.7.9. L'implication $DP \wedge P = 1 \implies P$ n'a pas de facteurs carrés est encore vrai en caractéristique $p > 0$, comme on le voit par la démonstration donnée. Attention certains phénomènes en caractéristique $p > 0$. Par exemple, le polynôme X^p a pour dérivée 0. Considérons le corps $k = \mathbb{F}_p(Y^p)$ des fractions rationnelles en Y^p à coefficients dans le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p un nombre premier. Le polynôme $P = X^p - Y^p \in k[X]$ a pour dérivée 0, et l'on a donc $DP \wedge P = P \neq 1$, et pourtant P est un polynôme irréductible, donc sans facteurs carrés.

Exercice I.7.10. Démontrer que $P = X^p - Y^p \in k[X]$, $k = \mathbb{F}_p(Y^p)$, est irréductible (on peut se placer sur $K = \mathbb{F}_p(Y)$ et factoriser P dans $K[X]$.

Corollaire I.7.11. *Soit k un sous-corps de $\mathbb{C}$ (en particulier de caractéristique 0). Alors un polynôme irréductible dans $k[X]$ n'a pas de racines multiples dans $\mathbb{C}[X]$.*

Démonstration. Soit P un tel polynôme. Il vérifie donc $DP \wedge P = 1$ dans $k[X]$, et d'après le théorème de Bézout, on peut écrire $1 = UP + V(DP)$ dans $k[X]$, mais donc aussi dans $\mathbb{C}[X]$, ce qui signifie que $DP \wedge P = 1$ dans $\mathbb{C}[X]$. Il n'a donc pas de racine multiple dans $\mathbb{C}$. □

Passons maintenant au cas des anneaux factoriels : que peut-on alors dire des anneaux de polynômes à coefficients dans A ? Le lecteur est invité dans ce qui suit à avoir en tête l'exemple fondamental de l'anneau $\mathbb{Z}$. Son corps de fraction est bien sûr $\mathbb{Q}$.

Définition I.7.12. Soit A un anneau factoriel. Le *contenu,* noté $c(P)$, d'un polynôme $P \in A[X]$ est le pgcd de ses coefficients. Le polynôme P est dit *primitif* si $c(P) = 1$.

On notera que le contenu est défini à multiplication par une unité de A près. Le contenu d'un polynôme est nul si et seulement si le polynôme est nul.

Lemme I.7.13 (Gauss)**.** *Soit A un anneau factoriel. Quels que soient P et Q dans $A[X]$, on a*

$$c(PQ) = c(P)c(Q) \pmod{A^\times}.$$

Démonstration. Supposons d'abord P et Q primitifs et montrons que PQ est primitif. Soit p un irréductible de A. Comme P et Q sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_i (resp. b_j) le coefficient de P (resp. de Q) d'indice minimal non divisible par p. Alors le coefficient d'indice $i + j$ de PQ est somme de termes divisibles par p et de $a_i b_j$ donc il n'est pas divisible par p car (p) est premier vu que A est factoriel. Ceci montre qu'aucun élément irréductible de A ne divise tous les coefficients de PQ, qui est donc primitif.

Le cas général s'en déduit : si P ou Q est nul, il est évident ; sinon, on applique le résultat précédent à $P/c(P)$ et $Q/c(Q)$. □

Lemme I.7.14. *Soit A un anneau factoriel de corps des fractions K. Soient P et Q des éléments de $A[X]$, avec P primitif, et soit $R \in K[X]$ tel que $Q = PR$. Alors $R \in A[X]$.*

Démonstration. On peut écrire $R = R_1/r$, avec $r \in A$ et $R_1 \in A[X]$. On a alors $rQ = PR_1$, puis $rc(Q) = c(P)c(R_1) = c(R_1) \pmod{A^\times}$ par le lemme de Gauss, de sorte que r divise $c(R_1)$, donc aussi R_1, ce qui termine la démonstration. □

On a aussi l'important résultat suivant.

Théorème I.7.15. *Soit A un anneau factoriel de corps des fractions K. Les éléments irréductibles de $A[X]$ sont :*

a) *les polynômes constants p avec p irréductible dans A ;*

b) *les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.*

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans l'anneau $A[X]$ ou d'être irréductible dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident vu qu'il y a *a priori* plus de décompositions possibles dans $K[X]$).

Démonstration. Comme $(A[X])^\times = A^\times$ il est clair qu'un polynôme constant p est irréductible si et seulement si p est irréductible dans A.

Soit maintenant P un polynôme primitif de degré ≥ 1 de $A[X]$ qui est irréductible dans $K[X]$. Montrons qu'il est irréductible dans $A[X]$. Supposons donc qu'il s'écrive $P = QR$ avec Q et R dans $A[X]$. Le lemme de Gauss I.7.12 entraîne que $c(Q)$ et $c(R)$ sont inversibles. D'autre

part, l'un des polynômes Q ou R est constant (parce que P est irréductible dans $K[X]$), et c'est donc une constante inversible dans A, donc une unité de $A[X]$. Donc P, qui n'est pas inversible dans $A[X]$ car de degré au moins 1, est bien irréductible dans $A[X]$.

Montrons inversement qu'un polynôme P de degré ≥ 1 et irréductible dans $A[X]$ est primitif et irréductible dans K[X]. Comme $c(P)$ divise P dans $A[X]$ et ne lui est pas associé pour raison de degré, c'est une unité de $A[X]$, donc de A, et P est bien primitif. Il reste à montrer que P (qui n'est pas inversible dans $K[X]$) est irréductible dans $K[X]$. Or si $P = QR$ dans $K[X]$, on peut écrire $Q = Q_1/q$ et $R = R_1/r$ avec q et r dans A et Q_1 et R_1 dans $A[X]$. On obtient $qrP = Q_1R_1$ et, en passant aux contenus (lemme de Gauss), $qr = c(Q_1)c(R_1)$. Ainsi $P = Q_1R_1/qr = (Q_1/c(Q_1))(R_1/c(R_1))$ (mod $A^\times$). Comme P est irréductible dans $A[X]$, l'un des polynômes Q_1 ou R_1 de $A[X]$ est constant, et l'un des polynômes Q ou R est constant, ce qui achève la preuve. □

On a enfin le résultat fondamental suivant.

Théorème I.7.16. *Soit A un anneau factoriel. Les anneaux $A[X_1, \ldots, X_n]$ sont factoriels pour tout $n \in \mathbb{N}$.*

Remarque I.7.17. La conclusion reste vraie avec un nombre infini d'indéterminées (cela découle du cas fini).

Démonstration. Il suffit de montrer que $A[X]$ est factoriel. Montrons d'abord l'existence de la décomposition en produit d'irréductibles d'un polynôme P non nul. Après avoir écrit $P = c(P)(P/c(P))$ et décomposé $c(P)$ en produit d'irréductible dans A, on se ramène à P primitif non constant.

Soit K le corps des fractions A. On décompose alors P en produit d'irréductibles dans l'anneau factoriel $K[X]$ soit, en chassant les dénominateurs, $aP = P_1 \cdots P_r$ avec $a \in A$ et $P_i \in A[X]$ irréductible dans $K[X]$. écrivons $P_i = c(P_i)Q_i$, avec Q_i primitif, donc irréductible dans $A[X]$ d'après le théorème précédent. En passant aux contenus, on obtient qu'il existe $u \in A^\times$ tel que $ua = c(P_1) \cdots c(P_r)$, et $P = u \prod_{i=1}^r Q_i$ est une décomposition de P en produits d'irréductibles de $A[X]$.

Il suffit donc d'après la prop. I.6.8 de montrer que si $P \in A[X]$ est irréductible l'idéal (P) est premier. Si P est une constante irréductible p de $A[X]$, c'est clair (par vérification directe, ou encore en remarquant que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A, et que l'anneau des polynômes à coefficients dans un anneau integre est aussi intègre). Supposons maintenant P primitif de degré au moins 1, donc irréductible dans $K[X]$ d'après le théorème précédent. Si P divise le produit QR de polynômes dans $A[X]$, il divise alors Q ou R dans l'anneau principal $K[X]$ (prop. I.I.5.5), disons par exemple Q. Comme P est primitif, par le lemme I.7.14, le quotient Q/P est dans $A[X]$, de sorte que P divise Q dans $A[X]$. C'est ce que l'on voulait montrer. □

Remarque I.7.18. Si l'on reprend notre exemple fondamental $A = \mathbb{Z}$, on a donc obtenu que $\mathbb{Z}[X]$ est factoriel. Notons que $\mathbb{Z}[X]$ n'est pas principal. En effet, l'idéal $(2, X)$ n'est pas principal. On sait aussi que $\mathbb{Q}[X]$ est euclidien, donc principal, donc factoriel. Le théorème I.7.15 compare les irréductibles dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

Théorème I.7.19 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel, soit K son corps de fractions, soit $P(X) = \sum_{k=0}^n a_k X^k$ un polynôme non constant à coefficients dans A et soit p un élément irréductible de A. On suppose :*

- *p ne divise pas a_n ;*

- *p divise a_k pour chaque $k \in \{0, \ldots, n-1\}$;*
- *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ s'il est primitif).

Démonstration. Vu que $c(P)$ n'est pas divisible par p par le premier point, $P/c(P)$ vérifie les mêmes hypothèses que P. On peut donc supposer P primitif. Si P n'est pas irréductible, il s'écrit (d'après le th. I.7.15) $P = QR$ avec Q et R dans $A[X]$, non constants. Posons $Q(X) = b_r X^r + \cdots + b_0$ et $R(X) = c_s X^s + \cdots + c_0$, avec $r + s = n$, $r, s > 0$ et $a_n = b_r c_s$. L'anneau $B = A/(p)$ est intègre, et, comme on l'a remarqué dans la démonstration plus haut, $A[X]/(p)$ est isomorphe à $B[X]$. Dans cet anneau intègre, on a $\bar{a}_n X^n = \bar{Q}\bar{R}$, avec $\bar{a}_n \neq 0$, donc $\bar{Q}$ et $\bar{R}$ non nuls.

Supposons $\bar{Q}(0) \neq 0$ dans B et écrivons $\bar{R} = X^t R_1$ avec $R_1(0) \neq 0$ dans B et $0 \leq t \leq s$. On a alors $\bar{a}_n X^{n-t} = \bar{Q}R_1$. Comme $(\bar{Q}R_1)(0) \neq 0$, cela entraîne $t = n$, ce qui contredit $t \leq s = n - r < n$.

On a donc $\bar{Q}(0) = 0$ et de même, $\bar{R}(0) = 0$. Cela signifie que p divise b_0 et c_0, ce qui contredit le fait que a_0 n'est pas divisible par p^2. □

Par exemple, $X^{18} - 4X^7 - 2$ est irréductible dans $\mathbb{Q}[X]$ et $X^5 - XY^3 - Y$ est irréductible dans $\mathbb{C}[X, Y]$ (prendre $A = \mathbb{C}[Y]$ et $p = Y$).

Exercice I.7.20. Montrer que si p est un nombre premier, le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$ est irréductible dans $\mathbb{Q}[X]$ (*Indication :* on pourra poser $X = Y + 1$).

Une autre méthode pour prouver l'irréductibilité d'un polynôme dans $\mathbb{Z}[X]$ est de réduire modulo n. On établit facilement le critère suivant. Si $P = a_0 + a_1 X + \ldots + a_N X^N \in \mathbb{Z}[X]$, le polynôme obtenu en réduisant modulo n est $\bar{P} = \bar{a}_0 + \bar{a}_1 X + \ldots + \bar{a}_N X^N \in (\mathbb{Z}/n\mathbb{Z})[X]$, les coefficients $\bar{a}_j$ étant les réductions modulo n des coefficients a_j.

Théorème I.7.21. *Soit $P \in \mathbb{Z}[X]$ et soit $\bar{P}$ sa réduction modulo n. On suppose que* $\deg \bar{P} = \deg P$ *et que $\bar{P}$ est irréductible dans $(\mathbb{Z}/n\mathbb{Z})[X]$. Alors P est irréductible.*

Démonstration. En effet, si l'on suppose que $P = QR$ dans $\mathbb{Z}[X]$, aiors $\bar{P} = \bar{Q}\bar{R}$ dans $(\mathbb{Z}/n\mathbb{Z})[X]$, et comme

$$\deg P = \deg Q \times \deg R \geq \deg \bar{Q} \times \deg \bar{R} = \deg \bar{P} = \deg P,$$

on a nécessairement $\deg Q = \deg \bar{Q}$ et $\deg R = \deg \bar{R}$, et $\bar{P}$ est réductible, contradiction. □

Exercice I.7.22. Soit k un corps infini, et soit $A = k[X, Y]$ l'anneau des polynômes à deux variables à coefficients dans k.

1. Montrer qu'un idéal principal de A n'est pas maximal.
2. Montrer que si I est un idéal premier non principal de $k[X, Y]$, alors il existe un polynôme $P \in k[X] \cap I$ irréductible. On pourra utiliser l'inclusion $k[X, Y] \subset k(X)[Y]$.
3. Montrer que les idéaux premiers de $k[X, Y]$ sont (0), (P) avec $P \in k[X, Y]$ irréductible et les idéaux maximaux de $k[X, Y]$.
4. Si k est algébriquement clos, montrer que les idéaux maximaux de $k[X, Y]$ sont les idéaux $(X - a, Y - b)$ pour $(a, b) \in k^2$.
4. Les idéaux maximaux de $\mathbb{R}[X, Y]$ sont de la forme $(X - a, Y - b)$ avec $(a, b) \in \mathbb{R}^2$, ou (P, Q) avec $P \in \mathbb{R}[X] \cup \mathbb{R}[Y]$ irréductible de degré 2 et $Q \in \mathbb{R}[X, Y]$ avec $\deg(Q) = 1$.

Exercice I.7.23. Déterminer les idéaux premiers des anneaux suivants, ainsi que les morphismes de $\mathbb{R}$-algèbres de ces anneaux dans $\mathbb{R}$ ou $\mathbb{C}$. :

$$\mathbb{C}[X], \quad \mathbb{R}[X]/(X^2 + X + 1), \quad \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6), \quad \mathbb{R}[X]/(X^4 - 1)$$

Exercice I.7.24. Soit A un anneau commutatif. Montrer que si A n'est pas un corps, alors $A[X]$ n'est pas principal.

Exercice I.7.25. Soit k un corps. Montrer que l'anneau $k[X_1, X_2, \ldots, X_n \ldots]$ des polynômes à coefficients dans k à une infinité de variables est factoriel mais pas noethérien.

I.7.3 Propriété universelle de $k[X_1, \ldots, X_n]$

Le résultat suivant caractérise l'anneau des polynômes à n variables à coefficients dans A.

Théorème I.7.26. *Soit k un corps et $k[X_1, \ldots, X_n]$ l'anneau des polynômes à n variables à coefficients dans k. Pour toute k-algèbre B, et pour tout n-uplet $(b_1, \ldots, b_n)$ d'éléments de B, il existe un unique morphisme de k-algèbres $\phi : k[X_1, \ldots, X_n] \to B$ tel que pour tout $i = 1, \ldots, n$, $\phi(X_i) = b_i$.*

Démonstration. Pour tout $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, on note X^α le monôme $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. Il est clair que ϕ est unique, car si on écrit $P \in k[X_1, \ldots, X_n]$ sous la forme $P = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$ (somme à support fini), on a alors nécessairement $\phi(P) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha b_1^{\alpha_1} \cdots b_n^{\alpha_n}$. Mais, réciproquement, cette formule définit bien un morphisme de k-algèbres. En effet, on voit immédiatement que ϕ est k-linéaire. Il reste donc à vérifier que c'est un morphisme d'anneaux c'est-à-dire que $\phi(PQ) = \phi(P)\phi(Q)$. Pour cela, on remarque qu'il suffit de le vérifier lorsque P et Q sont des monômes, et cette vérification est immédiate. □

Remarque I.7.27. Plus généralement, le même résultat est vrai avec la même preuve si on remplace k par un anneau commutatif quelconque R, avec $R[X_1, \ldots, X_n]$ et B une R-algèbre.

On utilise ceci pour démontrer le résultat suivant, que l'on a utilisé de nombreuses fois sans justification (parce qu'il est évident, mais c'est quand même mieux d'avoir une démonstration).

Corollaire I.7.28. *On a un isomorphisme de R-algèbres $R[X_1, \ldots X_n] \simeq R[X_1, \ldots X_{n-1}][X_n]$.*

Démonstration. D'après la propriété universelle de $R[X_1, \ldots X_n]$, il existe un unique morphisme de R-algèbres $\phi : R[X_1, \ldots, X_n] \to R[X_1, \ldots X_{n-1}][X_n]$ tel que $\phi(X_i) = X_i$. Réciproquement, on remarque que $R[X_1, \ldots X_{n-1}]$ est un sous-anneau de $R[X_1, \ldots X_n]$, ce qui fait de $R[X_1, \ldots X_n]$ une $R[X_1, \ldots X_{n-1}]$-algèbre. D'après la propriété universelle de $R[X_1, \ldots X_{n-1}][X_n]$, il existe un unique morphisme de $R[X_1, \ldots X_{n-1}]$-algèbres $\psi : R[X_1, \ldots X_{n-1}][X_n] \to R[X_1, \ldots, X_n]$ tel que $\psi(X_n) = X_n$ (et $\psi(X_i) = X_i$ pour $i = 1, \ldots, n-1$). Ces deux morphismes de R-algèbres sont inverses l'un de l'autre. □

I.7.4 Résultant de deux polynômes et applications

Soit A un anneau intègre, soit $k = K(A)$ son corps des fractions et soit $\bar{k}$ une cloture algébrique de k. Pour tout $m \in \mathbb{N}$, on note $k_m[X]$ l'espace vectoriel des polynômes de degré au plus m à coefficients dans k. Il est muni de la base canonique $(1, X, \ldots, X^m)$. Soient $P, Q \in k[X]$ des polynômes de degré respectif p et q. On appelle *résultant* de P et Q, que l'on note $\mathcal{R}(P, Q)$ le déterminant de la matrice dans les bases canoniques de l'application :

$$\begin{array}{rccc} \Phi : & k_{q-1}[X] \times k_{p-1}[X] & \to & k_{p+q-1}[X] \\ & (A, B) & \mapsto & AP + BQ \end{array}.$$

De manière explicite, si $P = t_0 + t_1 X + \ldots + t^p X^p$ et $Q = u_0 + u_1 X + \ldots u t^q X^q$, on introduit la matrice de Sylvester :

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} t_0 & 0 & \dots & \dots & \dots & 0 & u_0 & 0 & \dots & 0 \\ t_1 & t_0 & \dots & \dots & \dots & 0 & u_1 & u_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{p-1} & t_{p-2} & \dots & \dots & \dots & 0 & u_{p-1} & u_{p-2} & \dots & u_0 \\ t_p & t_{p-1} & \dots & \dots & \dots & 0 & u_p & u_{p-1} & \dots & u_1 \\ 0 & t_p & \dots & \dots & \dots & 0 & u_{p+1} & u_p & \dots & u_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & t_0 & u_{q-1} & u_{q-2} & \dots & u_{q-p} \\ 0 & 0 & \dots & \dots & \dots & t_1 & u_q & u_{q-1} & \dots & u_{q-p+1} \\ 0 & 0 & \dots & \dots & \dots & t_2 & 0 & u_q & \dots & u_{q-p+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \dots & t_p & 0 & 0 & \dots & u_q \end{pmatrix}$$

et son déterminant $\mathcal{R}(P,Q) = \det(\mathrm{Syl}(P,Q))$.

On remarque que si P et Q sont dans $A[X]$ (resp. $k[X]$, resp. $\bar{k}[X]$), alors $\mathcal{R}(P,Q)$ est dans A (resp. k, resp. $\bar{k}$).

Proposition I.7.29. *Soient P et Q deux polynômes dans $k[X]$ de degré respectif p et q. On a $\mathcal{R}(P,Q) \neq 0$ si et seulement si P et Q sont premiers entre eux.*

Démonstration. On est dans l'anneau principal $k[X]$. Si P et Q sont premiers entre eux, alors $(P,Q) = k[X]$, ce qui signifie que tout polynôme R de $k[X]$ s'écrit sous la forme $R = AP + BQ$. Si $\deg(R) \leq p+q-1$, montrons que l'on peut prendre A avec $\deg(A) \leq q-1$ et $\deg(B) \leq p-1$. On peut remplacer A et B respectivement par par $A_1 = A + QS$ et $B_1 = B - PS$. Prenons alors B_1 et S comme étant le résultat de la division euclidienne de B par P. On a bien alors $\deg B_1 \leq p-1$. On a $R = A_1P + B_1Q$, et comme R et B_1Q sont de degré $\leq p+q-1$, on a $\deg A_1 \leq q-1$. Ceci montre que l'application Φ ci-dessus est une application linéaire surjective. Comme l'espace de départ et celui d'arrivée sont de même dimension, on en déduit que Φ est un isomorphisme, et ainsi son déterminant est non nul. On a donc $\mathcal{R}(P,Q) \neq 0$.

Au contraire, si P et Q ne sont pas premiers entre eux, alors $(P,Q) = (C)$ pour un certain polynôme $C \in k[X]$ non constant. Alors pour tout R dans l'image de Φ, C divise R, et donc Φ n'est pas surjective. Ce n'est donc pas un isomorphisme, et ainsi son déterminant est nul, c'est-à-dire $\mathcal{R}(P,Q) = 0$.

Corollaire I.7.30. *Le résultant $\mathcal{R}(P,Q)$ est nul si et seulement si P et Q ont une racine commune dans $\bar{k}$.*

Notre but est maintenant de montrer une formule pour le résultant en termes des racines de P et Q.

Théorème I.7.31. *Soient P et Q deux polynômes dans $k[X]$ de degré respectif p et q que l'on suppose scindé (on peut se placer sur $\bar{k}$). On peut donc écrire*

$$P = t_p \prod_{i=1}^{p} (X - \alpha_i), \quad Q = u_q \prod_{j=1}^{q} (X - \beta_j).$$

On a alors

$$\mathcal{R}(P,Q) = t_p^q u_q^p \prod_{i,j} (\alpha_i - \beta_j).$$

Démonstration. Remarquons que les coefficients $t'_0 = t_0/t_p$, $t'_1 = t_1/t_p$, ..., $t'_{p-1} = t_{p-1}/t_p$ sont des fonctions symétriques des α_i. Par exemple $t'_{p-1} = \pm(\alpha_1 + \ldots + \alpha_p)$, $t'_{p-2} = \pm\sum_{i<j}\alpha_i\alpha_j$,... $t'_0 = \alpha_1 \ldots \alpha_p$. Dans le déterminant qui donne $\mathcal{R}(P,Q)$, on met en facteur t_p sur les q premières colonnes, et u_q sur les p dernières et on obtient

$$\mathcal{R}(P,Q) = t_p^q u_q^p \, \mathcal{R}'(P,Q)$$

où $\mathcal{R}'(P,Q)$ est obtenu en remplaçant les t_i par les $t'_i = t_i/t_p$ et les u_j par $u'_j = u_j/u_q$. De même, on introduit la matrice de Sylvester modifiée de la même manière $\mathrm{Syl}'(P,Q)$.

Il s'agit donc de montrer que

$$\mathcal{R}'(P,Q) = \det(\mathrm{Syl}'(P,Q)) = \prod_{i,j}(\alpha_i - \beta_j).$$

Les deux termes sont donc des polynômes en les α_i et β_j. De manière équivalente, on peut supposer que les les polynômes P et Q sont unitaires, ce que l'on fait dans la suite. On va démontrer que la formule $\mathcal{R}(P,Q) = \det(\mathrm{Syl}(P,Q)) = \prod_{i,j}(\alpha_i - \beta_j)$ est valide dans l'anneau factoriel

$$\mathscr{A} = \mathbb{Z}[\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q],$$

où l'on considère maintenant les α_i et β_j comme des indéterminées. Remarquons que les $\alpha_i - \beta_j$ sont des polynômes irréductibles dans l'anneau factoriel $\mathscr{A}$. On en déduit que la formule est vraie pour des polynômes P et Q dans $k[X]$ comme ci-dessus par « spécialisation » c'est-à-dire en considérant le morphisme d'évaluation de $\mathscr{A}$ dans k qui envoie les indéterminées α_i ou β_j sur les éléments correspondants dans k.

Lemme I.7.32. *Dans un anneau de polynômes $A[X_1, \ldots X_r]$, un polynôme P qui s'annule lorsque $X_1 = X_2$ est divisible par $X_1 - X_2$.*

Démonstration. Dans $A[X]$, un polynôme P s'annule en 0 si et seulement si son coefficient constant est nul et ceci est le cas si et seulement si X divise P (c'est une conséquence de la construction de l'anneau des polynômes). Donc un polynôme P s'annule en $a \in A$ si et seulement si $(X - a)$ divise P (changement de variable $Y = X - a$). Le lemme en découle alors en utilisant l'isomorphisme $A[X_1, \ldots X_r] \simeq A[X_2, \ldots X_r][X_1]$. □

Revenons à la démonstration du théorème. On va utiliser un calcul de matrices assez miraculeux, en introduisant des matrices de Van Der Monde. Considérons la matrice carrée suivante, de taille N , à coefficient dans $\mathbb{Z}[y_1, \ldots, y_N]$:

$$V_N(y_1, \ldots, y_N) = \begin{pmatrix} 1 & y_1 & y_1^2 & \ldots & y_1^{N-1} \\ 1 & y_2 & y_2^2 & \ldots & y_2^{N-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & y_N & y_N^2 & \ldots & y_N^{N-1} \end{pmatrix}$$

Il est bien connu que le déterminant de cette matrice est $\prod_{1 \le j < i \le N}(y_i - y_j)$. Notons aussi $\mathrm{Diag_N}(y_1, \ldots, y_N)$ la matrice carrée diagonale de taille N dont les coefficients diagonaux sont $y_1, \ldots, y_N$.

Effectuons maintenant le produit

$$V_{p+q}(\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q)\mathrm{Syl}(P,Q).$$

Comme les α_i sont racines de P et les β_j racines de Q, on trouve que ce produit est de la forme

$$\left(\begin{array}{c|c} \mathbf{0} & \mathrm{Diag_p}(Q(\alpha_1), \ldots, Q(\alpha_p))\ V_p(\alpha_1, \ldots, \alpha_p)) \\ \hline \mathrm{Diag_q}(P(\beta_1), \ldots, P(\beta_q))\ V_q(\beta_1, \ldots, \beta_q) & \mathbf{0} \end{array}\right).$$

En prenant le déterminant on obtient

$$\begin{aligned}&\det(V_{p+q}(\alpha_1,\dots,\alpha_p,\beta_1,\dots,\beta_q))\mathcal{R}'(P,Q)\\ =&(-1)^{pq}\det(\mathrm{Diag_p}(Q(\alpha_1),\dots,Q(\alpha_p)))\det(V_p(\alpha_1,\dots,\alpha_p))\\ &\times\det(\mathrm{Diag_q}(P(\beta_1),\dots,P(\beta_q))\ \det(V_q(\beta_1,\dots,\beta_q))\end{aligned}$$

Ce qui donne en simplifiant les déterminants de Van der Monde (ceux du terme de droite divisent celui du terme de gauche) on est dans l'anneau intègre $\mathbb{Z}[\alpha_1,\dots,\alpha_p,\beta_1,\dots,\beta_q]))$

$$\prod_{i,j}(\beta_j-\alpha_i)\times\mathcal{R}(P,Q)=(-1)^{pq}\prod_i Q(\alpha_i)\times\prod_j P(\beta_j)$$

En simplifiant à nouveau, on a finalement

$$\mathcal{R}(P,Q)=(-1)^{pq}\prod_i Q(\alpha_i)=\prod_j P(\beta_j)=\prod_{i,j}(\beta_j-\alpha_i).$$

□

Exercice I.7.33. Montrer que l'ensemble $\bar{\mathbb{Q}}$ des nombres algébriques sur $\mathbb{Q}$ est un corps. On pourra utiliser les propriétés du résultant.

Exercice I.7.34 (Anneau des entiers algébriques). On rappelle qu'un nombre complexe x est un *nombre algébrique* (sur $\mathbb{Q}$) s'il existe un polynôme $P\in\mathbb{Z}[X]$ tel que l'on ait $P(x)=0$ et on dit que 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 $\bar{\mathbb{Q}}$ le corps des nombres algébriques (voir exercice précédent) et $\bar{\mathbb{Z}}$ l'ensemble des entiers algébriques.

a) Montrer que $\bar{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$ (On pourra utiliser les propriétés du résultant).
b) Montrer que le corps des fractions de $\bar{\mathbb{Z}}$ est $\bar{\mathbb{Q}}$.
c) Montrer que $\bar{\mathbb{Z}}\cap\mathbb{Q}=\mathbb{Z}$.
d) Montrer que $\bar{\mathbb{Z}}$ n'est pas noethérien.

Exercice I.7.35. Montrer que le corps $\bar{\mathbb{Q}}$ des nombres algébriques sur $\mathbb{Q}$ est algébriquement clos.

I.8 Résumé du chapitre I

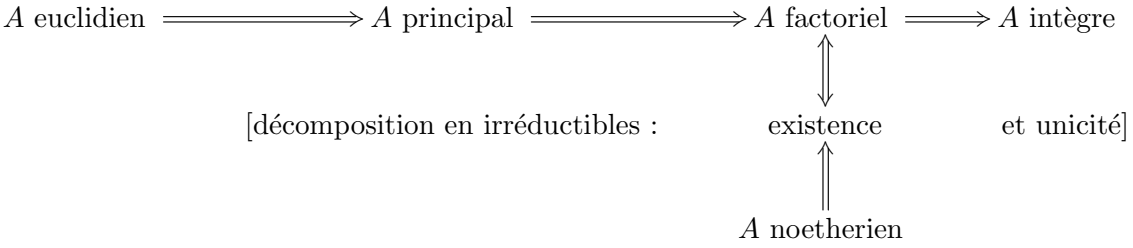
On peut étudier certaines questions mathématiques en les plaçant dans le cadre d'un anneau A et en étudiant les propriétés de cet anneau. L'exemple typique est le théorème des deux carrés que l'on résout en étudiant l'anneau des entiers de Gauss $\mathbb{Z}[i]$ (exercice I.5.10). Voir aussi l'exercice I.6.16 pour une autre application, l'exercice I.6.15 qui utilise l'anneau $\mathbb{Z}[i\sqrt{2}]$, et les exercices I.5.12 et I.6.22 qui utilisent l'anneau des entiers d'Eisenstein $\mathbb{Z}[j]$. Ces exemples sont dans le domaine de la théorie des nombres, mais les applications de l'étude des anneaux existent dans tous les domaines des mathématiques. Un autre domaine important basé sur la théorie des anneaux commutatifs est la géométrie algébrique, c'est-à-dire l'étude des ensembles de points définis par des équations polynomiales. Les anneaux que l'on étudie sont les anneaux de polynômes de la section I.7.

Les propriétés d'un anneau commutatif qui donnent les informations les plus intéressantes sont le fait d'être un anneau principal ou un anneau factoriel. Les exemples donnés ci-dessus sont des anneaux principaux et c'est ce qu'on utilise. Mais il est intéressant de connaître des exemples d'anneaux qui ne sont pas principaux, ou même factoriels. En effet, dans le passé, de

grands mathématiciens du 18ème siècle ont produits des démonstrations fausses du théorème de Fermat, ou de cas particuliers de celui-ci, en croyant que certains anneaux étaient factoriels (c'est comme cela que l'on interprète leur erreur aujourd'hui, à l'époque, la notion d'anneau factoriel n'était pas encore dégagée. En fait c'est en raison de ces tâtonnements que l'importance de cette notion est apparue ...).

Rappelons les principales notions introduites dans ce chapitre pour un anneau commutatif A et les implications entre elles :

(I.8.1)



Exemples d'anneaux euclidiens : $\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $\mathbb{Z}[i\sqrt{2}]$, l'anneau $\mathbb{D}$ des nombres décimaux (exercice I.5.9), $k[X]$ si k est un corps, l'anneau des séries formelles $k[[X]]$ (exercice I.5.15).

Exemple d'anneau principal non euclidien : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ (exercice I.6.19).

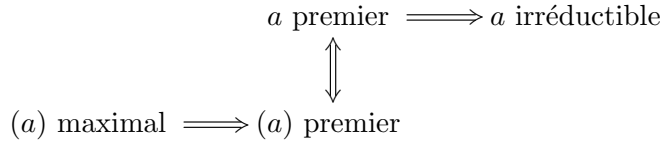
Exemple d'anneaux factoriels non principaux : ($\mathbb{Z}[X]$ Remarque I.7.18), $k[X,Y]$ (exercice I.7.22).

Exemple d'anneaux noethériens intègres non factoriels : $\mathbb{Z}[i\sqrt{5}]$ (Exemple I.6.9), $\mathbb{Z}[i\sqrt{3}]$ (Exercice I.6.17), $k[X^2,X^3]$ (Exercice I.6.10).

Exemple d'anneau factoriel non noethérien : $k[X_1,\ldots,X_n,\ldots]$ (Exercice I.7.25).

Autres exemples d'anneaux non noethériens : Voir Exercice I.7.3, Exercice I.7.4.

On a des critères portant sur les idéaux pour établir certaines de ces propriétés. Rappelons que dans tout anneau intègre on a



Dans un anneau principal, ces quatre propriétés sont équivalentes (Proposition I.5.5).

On a montré que si A est factoriel, alors A est principal si et seulement si tout idéal premier est maximal (Exercice I.6.14).

On a aussi vu que si A est noethérien et intègre, alors il est factoriel si et seulement si tout élément irréductible est premier (Proposition I.6.8).

Pour aller plus loin dans les applications la théorie des anneaux à l'arithmétique, on peut lire des livres sur la « théorie algébrique des nombres » (in english "algebraic number theory"), en particulier la théorie des anneaux de Dedekind ("Dedekind domains")

Chapitre II

Modules

II.1 Définitions et exemples

De même que la notion de groupe est inséparable de la notion d'action de groupe, la notion d'anneau est inséparable de celle de module sur un anneau. Si l'anneau est un corps, un module n'est alors rien d'autres qu'un espace vectoriel sur ce corps. Par généralité décroissante, on a donc les théories suivantes :

- Groupes / Actions de groupes
- Anneaux / Modules sur un anneau
- Corps / Espaces vectoriels.

L'objet de ce chapitre est donc le deuxième point, en supposant que le lecteur possède une certaine connaissance des deux autres.

Introduisons maintenant la notion de modules. Pour cela, repartons de l'exemple où M est un groupe abélien et $A = \mathrm{End}_{\mathbb{Z}}(M)$ est l'ensemble des endomorphismes de M pour la structure de groupe abélien (si l'on préfère, on suppose que M est un k-espace vectoriel et on prend $A = \mathrm{End}_k(M)$).

Considérons maintenant l'action naturelle de $\mathrm{End}_{\mathbb{Z}}(M)$ sur M :

$$\mathrm{End}_{\mathbb{Z}}(M) \times M \longrightarrow M, \quad (\phi, m) \mapsto \phi \cdot m = \phi(m). \tag{II.1.1}$$

C'est une action de groupe pour la structure de groupe abélien sur $\mathrm{End}_{\mathbb{Z}}(M)$, c'est-à-dire que l'on a

$$(\phi_1 + \phi_2) \cdot m = \phi_1 \cdot m + \phi_2 \cdot m, \quad (\phi_1, \phi_2 \in \mathrm{End}_{\mathbb{Z}}(M),\, m \in M), \tag{II.1.2}$$

ce qui implique en particulier que

$$0 \cdot m = 0, \quad (m \in M), \tag{II.1.3}$$

On a en plus une propriété de compatibilité avec la structure de groupe abélien de M car les éléments de $\mathrm{End}_{\mathbb{Z}}(M)$ sont des morphismes de groupes abéliens :

$$\phi \cdot (m_1 + m_2) = \phi \cdot m_1 + \phi \cdot m_2, \quad (\phi \in \mathrm{End}_{\mathbb{Z}}(M),\, m_1, m_2 \in M). \tag{II.1.4}$$

Enfin, on a l'associativité de la composition :

$$(\phi_1 \circ \phi_2) \cdot m = \phi_1 \cdot (\phi_2 \cdot m), \quad (\phi_1, \phi_2 \in \mathrm{End}_{\mathbb{Z}}(M),\, m \in M), \tag{II.1.5}$$

et par définition de Id_M,

$$\mathrm{Id}_M \cdot m = m, \quad (m \in M). \tag{II.1.6}$$

On prend ces propriétés comme axiomes de la structure de A-module, où A est un anneau.

Définition II.1.1. Soient A un anneau et $(M, +)$ un groupe abélien. On dit que M est un A-module (à gauche) si l'on a une application

$$A \times M \longrightarrow M, \quad (a, m) \mapsto a \cdot m \tag{II.1.7}$$

vérifiant les propriétés suivantes :

$$(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m, \quad (a_1, a_2 \in A,\ m \in M), \tag{II.1.8}$$ (distributivité)

$$a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2, \quad (a \in \mathrm{End}(M),\ m_1, m_2 \in M), \tag{II.1.9}$$ (linéarité)

$$a_1 \cdot (a_2 \cdot m) = (a_1 a_2) \cdot m, \quad (a_1, a_2 \in \mathrm{End}(M),\ m \in M), \tag{II.1.10}$$ (associativité)

$$1_A \cdot m = m, \quad (m \in M). \tag{II.1.11}$$ (élément neutre)

Nous laissons le lecteur dégager de lui-même la notion (non équivalente si l'anneau n'est pas commutatif) de module à droite. Lorsque l'on ne précise pas, A-module veut dire A-module à gauche.

De manière équivalente, M est un A-module si et seulement si l'application

$$A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M), \quad a \mapsto (m \mapsto a \cdot m)$$

est un morphisme d'anneaux.

Définition II.1.2. Soient A un anneau commutatif, et $\mathscr{B}$ un A-module, qui est en plus muni d'une structure d'anneau. En particulier $\mathscr{B}$ a une structure de groupe abélien qui vient du fait que c'est un A-module, et une structure de groupe abélien qui vient du fait que c'est un anneau. On dit que $\mathscr{B}$ est un A-algèbre si ces deux structures de groupes abéliens sont les mêmes, et de plus, quels que soient $\lambda \in A$, $x, y \in \mathscr{B}$, en notant λx l'action de λ sur x (structure de module) et $x \cdot y$ le produit dans l'anneau $\mathscr{B}$

$$\lambda(x \cdot y) = (\lambda x) \cdot y = x \cdot (\lambda y) \tag{II.1.12}$$

Exemples II.1.3. Donnons quelques exemples importants.

1 - Tout groupe abélien M est naturellement un $\mathbb{Z}$-module. La structure d'anneau de $\mathbb{Z}$ est tellement simple qu'être un $\mathbb{Z}$-module n'apporte aucune information supplémentaire au fait d'être un groupe abélien

2 - Soit k un corps. Un k-module n'est rien d'autre qu'un k-espace vectoriel. La théorie des modules est donc une généralisation de l'algèbre linéaire, mais il faut prendre garde que certains résultats de l'algèbre linéaire ne se généralisent pas aux modules. Par exemple, les notions de famille libre et famille génératrice ont un sens pour les modules, mais ceux-ci n'admettent pas en général de base.

3 - L'anneau A est un A-module à gauche (A agit sur lui-même par multiplication à gauche). On appelle ce module le module régulier.

4 - Soit I un ensemble, et A un anneau. Alors A^I (l'ensemble des familles indexées par I d'éléments de A, où encore l'ensemble des application de I dans A) est naturellement un A-module.

5 - Le sous-ensemble $A^{(I)}$ de A^I des suites $(a_i)_{i\in I}$ à support fini, c'est-à-dire telles que tous les a_i sauf un nombre fini sont nuls, est un A-module. Le module $A^{(I)}$ s'appelle le A-module libre de base I (nous verrons plus loin le pourquoi de cette terminologie). Si $I = \{1, \dots, n\}$, on note alors simplement ce module A^n.

6 - Soient k un corps, V un espace vectoriel sur k, et u un endomorphisme de V. Alors V est muni d'une structure de $k[X]$-module par

$$P \cdot v = P(u)(v), \quad (P \in k[X],\, v \in V).$$

Réciproquement, si V est un $k[X]$-module, c'est en particulier un k-module, et donc un k-espace vectoriel, et $v \mapsto X \cdot v$ définit un endomorphisme de V. Les deux notions sont donc équivalentes. Nous verrons que la théorie de la réduction des endomorphismes se déduit de théorèmes généraux sur la structure des $k[X]$-modules.

7 - On peut généraliser l'exemple précédent : la donnée de n endomorphimes $u_1, \dots, u_n$ d'un k-espace vectoriel V qui commutent deux à deux est équivalente à la donnée d'une structure de $k[X_1, \dots, X_n]$-module sur V (par $X_i \cdot v = u_i(v)$). La théorie de la réduction simultanée des endomorphismes $u_1, \dots, u_n$ découle de la théorie générale des $k[X_1, \dots, X_n]$-modules.

8 - On peut encore généraliser. Si G est un groupe, et k un corps, on forme l'algèbre $k[G]$ dont les éléments sont les combinaisons linéaires formelles $\sum_{g\in G} c_g\,[g]$ (à support fini, seul un nombre fini de c_g sont non nuls). Le produit est défini par

$$\left(\sum_{g\in G} c_g\,[g]\right)\left(\sum_{g\in G} d_h\,[h]\right) = \sum_{g,h\in G} c_g d_h\,[gh].$$

Un $k[G]$-module V n'est alors rien d'autre qu'une représentation de G dans le k-espace vectoriel V, les deux notions sont équivalentes.

Exercice II.1.4. Montrer que tout anneau A est isomorphe à un sous-anneau d'un anneau $\mathrm{End}_{\mathbb{Z}}(M)$ pour un certain groupe abélien M.

Ayant définis les *objets* qui nous intéressent (les A-modules), il s'agit maintenant de définir les *morphismes* entre les objets.

Définition II.1.5. Soient A un anneau et M, N, deux A-modules. Un morphisme de A-modules

$$f : M \longrightarrow N$$

est un morphisme de groupes abéliens vérifiant de plus :

$$f(a \cdot m) = a \cdot f(m), \quad (a \in A,\, m \in M).$$

On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N. Il est muni d'une structure évidente de groupe abélien. On note aussi $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$ et $\mathrm{Aut}_A(M)$ le sous-groupe des inversibles de l'anneau $\mathrm{End}_A(M)$.

Exercice II.1.6. Trouver un isomorphisme entre $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$ et $\mathbb{Z}$. Trouver un isomorphisme entre $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$ et $\mathbb{Z}/n\mathbb{Z}$.

Exercice II.1.7. Soit $n \in \mathbb{Z}$. Montrer qu'il n'existe aucun morphisme de $\mathbb{Z}$-modules non nul de $\mathbb{Q}$ vers $\mathbb{Z}/n\mathbb{Z}$. Existe-il des morphismes de $\mathbb{Z}$-modules non nul de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Q}$?

Exercice II.1.8. Déterminer, pour chaque $m, n \in \mathbb{N}$, le $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

Exercice II.1.9. Soient k un corps et M, N deux $k[X]$-modules correspondants respectivement aux endomorphismes u et v des k-espaces vectoriels M et N (*cf.* Exemples II.1.3, 6.). Comment caractériser les éléments de $\mathrm{Hom}_{k[X]}(M, N)$? Ceux de $\mathrm{Aut}_{k[X]}(M)$?

La théorie des modules est donc une généralisation de la théorie des espaces vectoriels. Il faut faire très attention car des résultats bien connus en algèbre linéaire ne sont plus vrais pour les modules. Mais certains aspects de la théorie se généralisent sans problème et nous allons commencer par en voir quelques uns.

On définit la notion de sous-module. Cela marche comme pour la notion de sous-espace vectoriel, ou de sous-groupe.

Définition II.1.10 (Sous-modules)**.** Soit M un A-module. On dit que $N \subset M$ est un sous A-module si N est un sous-groupe du groupe abélien M qui reste stable sous-l'action de A, c'est-à-dire que pour tout $a \in A$ et tout $n \in N$, $a \cdot n \in N$.

Exemple II.1.11. Soit A un anneau. On peut voir A comme un module sur lui-même par multiplication (à gauche). Un sous-module s'appelle alors un idéal à gauche. Un idéal à gauche I de A est donc un sous-groupe abélien de A pour l'addition, et qui vérifie de plus $(\forall a \in A), (\forall x \in I),\ ax \in I$.

On a le même résultat pour les idéaux à droite.

Exemple II.1.12 (Noyau et image)**.** Soit $f : M_1 \to M_2$ un morphisme de A-modules. Alors

$$\ker(f) = \{m \in M_1 \,|\, f(m) = 0\}$$

est un sous-A-module de M_1 que l'on appelle le noyau de f, et

$$\mathrm{Im}\,(f) = \{f(m) |\, m \in M_1\}$$

est un sous-A-module de M_2 que l'on appelle l'image de f.

Si N_1 est un sous-module de M_1, $f(N_1)$ est un sous-module de M_2, et si N_2 est un sous-module de M_2, $f^{-1}(N_2)$ est un sous-module de M_1.

Exemple II.1.13 (Intersection de sous-modules)**.** Soit M un A-module, et soit $(M_i)_{i \in I}$ une famille de sous-modules de M. Alors

$$\bigcap_{i \in I} M_i \subset M$$

est un sous-A-module de M.

Définition II.1.14 (Sous-module engendré par une partie)**.** Soit M un A-module, et soit X une partie de M. On appelle sous-module engendré par X, et on note $\langle X \rangle$ le plus petit sous-module de M contenant X, c'est-à-dire l'intersection de tous les sous-modules contenant X :

$$\langle X \rangle = \bigcap_{X \subset M' \subset M} M'$$

Concrètement, on a un morphisme de A-module :

$$A^{(X)} \longrightarrow M, \quad (a_x)_{x \in X} \mapsto \sum_{x \in X} a_x \cdot x$$

(la somme est à support fini) et $\langle X \rangle$ est l'image de ce morphisme.

Définition II.1.15 (Somme de sous-modules)**.** Soient $(M_i)_{i\in I}$ une famille de sous-modules d'un A-module M. On appelle somme des M_i dans M le sous-module de M engendré par la réunion des M_i, et on le note $\sum_{i\in I} M_i$:

$$\sum_{i\in I} M_i = \langle \bigcup_{i\in I} M_i \rangle \subset M.$$

Définition II.1.16 (Modules quotients)**.** Soit M un A-module et soit N un sous-module de M. On munit le groupe quotient M/N d'une structure de A-module par

$$a \cdot \bar{m} = \overline{a \cdot m}, \quad (\bar{m} \in M/N),\ (a \in A).$$

On vérifie immédiatement que la définition de cette action ne dépend pas du représentant choisi $m \in M$ de $\bar{m}$. La projection canonique $\pi : M \to M/N$ est un morphisme de A-modules.

Exemple II.1.17. Soit $f : M_1 \to M_2$ un morphisme de A-modules. Alors

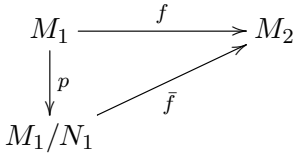
$$\mathrm{coker}(f) = M_2/\mathrm{Im}\,(f)$$

est un module quotient de M_2, appelé *conoyau* de f et

$$\mathrm{coim}(f) = M_1/\ker(f)$$

est un module quotient de M_1, appelé *coimage* de f.

Proposition II.1.18 (Propriété universelle du noyau)**.** *Soit $f : M_1 \to M_2$ un morphisme de A-modules et soit N_1 un sous-module de M_1 contenu dans* $\ker(f)$*. Alors on peut factoriser f de manière unique par la projection canonique $p : M_1 \to M_1/N_1$ en $f = \bar{f} \circ p$, $\bar{f} : M_1 \to M_1/N_1 \to M_2$.*



Si f est surjective, alors $\bar{f}$ aussi. Si $N_1 = \ker f$ alors $\bar{f}$ est injective.

Démonstration. Tout cela se vérifie de manière élémentaire.

Proposition II.1.19. *Soit M un A-module et soit I un idéal bilatère de A. On note IM le sous-module engendré par les éléments de la forme $a\cdot m$, $a \in I$, $m \in M$. L'idéal I est inclus dans le noyau du morphisme d'anneaux de A dans* $\mathrm{End}_{\mathbb{Z}}(M/IM)$*, ce dernier se factorise donc en un morphisme d'anneaux de A/I dans* $\mathrm{End}_{\mathbb{Z}}(M/IM)$*. Autrement dit M/IM est naturellement muni d'une structure de A/I-module.*

En particulier, si I annule M, c'est-à-dire si $a \cdot m = 0$ pour tout $m \in M$ et tout $a \in I$, alors M devient naturellement un A/I-module.

Définition II.1.20 (Produits)**.** Soit $(M_i)_{i\in I}$ une famille de A-modules. On munit le produit des groupes abéliens $\prod_{i\in I} M_i$ d'une structure de A-module par

$$a\cdot(m_i)_{i\in I}=(a\cdot m_i)_{i\in I},\quad (a\in A),\ (m_i)_{i\in I}\in\prod_{i\in I}M_i$$

Les projections $p_j:\prod_{i\in I}M_i\to M_j$ sont des morphismes de A-modules.

La *propriété universelle* du produit est : étant donné pour tout $i\in I$, un morphisme de A-modules $f_i:N\to M_i$, il existe un unique morphisme $f:N\to\prod_{i\in I}M_i$ tel que $f_j=p_j\circ f$, pour tout $j\in I$, ou autrement dit

$$\mathrm{Hom}_A(N,\prod_{i\in I}M_i)\simeq\prod_{i\in I}\mathrm{Hom}_A(N,M_i).$$

Définition II.1.21 (Sommes directes)**.** Soit $(M_i)_{i\in I}$ une famille de A-modules. La somme directe des groupes abéliens $\bigoplus_{i\in I}M_i$ est le sous-groupe du produit $\prod_{i\in I}M_i$ dont les éléments sont les familles $(m_i)_{i\in I}$ dont seul un nombre fini d'éléments sont non nuls. On vérifie facilement que $\bigoplus_{i\in I}M_i$ est un sous-A-module de $\prod_{i\in I}M_i$. Les injections $\iota_j:M_j\to\prod_{i\in I}M_i$ sont des morphismes de A-modules.

La *propriété universelle* de la somme directe est : étant donné pour tout $i\in I$, un morphisme de A-module $f_i:M_i\to N$, il existe un unique morphisme $f:\bigoplus_{i\in I}M_i\to N$ tel que $f_i=f\circ\iota_j$, pour tout $j\in I$, ou autrement dit

$$\mathrm{Hom}_A(\bigoplus_{i\in I}M_i,N)\simeq\prod_{i\in I}\mathrm{Hom}_A(M_i,N).$$

Remarque II.1.22. Les deux notions, produit et somme directe, sont proches mais non équivalentes : c'est évident lorsqu'on considère des sommes et produits infinis, mais même lorsque l'ensemble d'indices est fini et que l'on a $\prod_{i\in I}M_i=\bigoplus_{i\in I}M_i$, le produit vient avec les projections canoniques p_i, tandis que la somme vient avec les injections canonique ι_i.

Remarque II.1.23 (Sommes directes internes)**.** On a vu plus haut la notion de somme d'une famille $(M_i)_{i\in I}$ de sous-modules d'un A-module M : c'est un sous-module que l'on a noté $\sum_{i\in I}M_i$. C'est une notion interne au module M. On a aussi défini la somme directe d'une famille $(M_i)_{i\in I}$, qui ne suppose pas que les $(M_i)_{i\in I}$ soient des sous-modules d'un module commun. A posteriori, les M_i sont des sous-modules de leur somme directe $\bigoplus_{i\in I}M_i$.

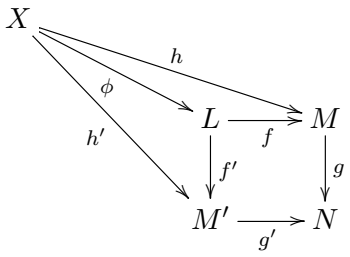
Revenons au premier cas, où les M_i sont des sous-modules d'un module M. On a une application

$$\bigoplus_{i\in I}M_i\longrightarrow\sum_{i\in I}M_i\ (\subset M),\quad (m_i)_{i\in I}\mapsto\sum_i m_i$$

(seul un nombre fini de m_i sont non nuls, ceci est bien défini). Ce morphisme est surjectif. S'il est aussi injectif, c'est-un isomorphisme. On dit alors que les M_i sont en somme directe dans M, et l'on écrit aussi $\bigoplus_{i\in I}M_i$ pour le sous-module $\sum_{i\in I}M_i$ dans ce cas (somme directe interne).

Exercice II.1.24 (Pull-back). Soient $g:M\to N$, $g':M'\to N$ deux morphismes de A-modules. On veut construire un objet L (le pull-back de g,g'), muni de deux morphismes $f:L\to M$, $f':L\to M'$, vérifiant la propriété universelle suivante :

- pour tout couple de morphisme $h : X \to M$, $h' : X \to M'$, tels que $g' \circ h' = g \circ h$, il existe un unique morphisme $\phi : X \to L$ rendant le diagramme suivant commutatif

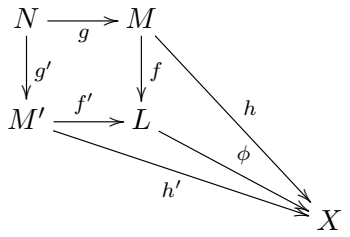


1- Montrer l'existence et l'unicité d'un tel objet (deux tels objets sont isomorphes par un isomorphisme uniquement déterminé).

2- Montrer que f' induit un isomorphisme de $\ker f$ sur $\ker g'$ et que si g' est injectif, alors f aussi.

Exercice II.1.25 (Push-out). Soient $g : N \to M$, $g' : N \to M'$ deux morphismes de A-modules. On veut construire un objet L (le push-out de g, g'), munit de deux morphismes $f : M \to L$, $f' : M' \to L$, vérifiant la propriété universelle suivante :

- pour tout couple de morphisme $h : M \to X$, $h' : M' \to X$, tels que $h' \circ g' = h \circ g$, il existe un unique morphisme $\phi : L \to X$ rendant le diagramme suivant commutatif



1- Montrer l'existence et l'unicité d'un tel objet.

2 - Montrer que f induit un isomorphisme de $\mathrm{coker} g$ sur $\mathrm{coker} f'$ et que si g est surjectif, alors f' aussi.

II.2 Théorèmes d'isomorphisme

Soit $f \in \mathrm{Hom}_A(M, M'')$ et soit M' un sous-module de M contenu dans $\ker f$. Alors f est constante sur les classes de M' dans M et induit donc $\bar{f} : M/M' \to M''$. On vérifie immédiatement que $\bar{f}$ est un morphisme de A-modules. On peut appliquer ceci à $M' = \ker f$. On obtient

$$\bar{f} : M/\ker f \to M'',$$

ce morphisme $\bar{f}$ ayant maintenant la propriété d'être injectif. On a évidemment $\mathrm{Im}\,(\bar{f}) = \mathrm{Im}\,(f)$, et l'on obtient le

Théorème II.2.1 (premier théorème d'isomorphisme)**.** *Soit $f : M \to M''$ un morphisme de A-module. On a*

$$\mathrm{coim}(f) = M/\ker f \simeq \mathrm{Im}\,(f)$$

l'isomorphisme étant réalisé par $\bar{f}$.

Puisqu'il y a un premier théorème d'isomorphisme, c'est qu'il y en a un deuxième.

Théorème II.2.2 (deuxième théorème d'isomorphisme)**.** *Soient $M'' \subset M'$ deux sous-modules d'un A-module M. Alors M'/M'' est un sous-module de M/M'' et l'on a un isomorphisme canonique*

$$\big(M/M''\big) \,/\, \big(M'/M''\big) \simeq M/M'.$$

Démonstration. La projection canonique $\pi : M \to M/M'$, de noyau M', induit $\bar{\pi} : M/M'' \to M/M'$, dont le noyau est M'/M''. On applique le premier théorème d'isomorphisme en remarquant que π étant surjective, $\bar{\pi}$ aussi. □

Remarque II.2.3. On a une bijection entre sous-modules de M contenant M'' et sous-modules de M/M'', donnée par $M' \mapsto M'/M''$.

Il y a aussi un troisième théorème d'isomorphisme :

Théorème II.2.4 (troisième théorème d'isomorphisme)**.** *Soient M', M'' deux sous-modules d'un A-module M. Alors on a un isomorphisme canonique*

$$M'/(M' \cap M'') \simeq (M' + M'')/M''.$$

Démonstration. On considère le morphisme

$$M' \longrightarrow M' + M'' \longrightarrow (M' + M'')/M''.$$

Il est surjectif, de noyau $M' \cap M''$, et on applique le premier théorème d'isomorphisme. □

II.3 Suites exactes

On dit qu'une suite de morphisme de A-modules

$$M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \longrightarrow \cdots \longrightarrow M_n \xrightarrow{f_n} M_{n+1}$$

est exacte si et seulement si pour tout $i = 0, \ldots, n-1$, $\mathrm{Im}\,(f_i) = \ker(f_{i+1})$ Une suite exacte courte est une suite exacte de la forme

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

en particulier f est injective et g est surjective.

La notion de suite exacte est au coeur de l'étude des modules, la raison en étant qu'en un certain sens, le module M peut s'analyser en termes de son sous-module $\mathrm{Im}\,(f)$ isomorphe à M' et de son module quotient $M/\ker g$ isomorphe à M''.

Exercice II.3.1. Soit la suite exacte courte de A-modules :

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Montrer que les conditions suivantes sont équivalentes :

(*i*) Il existe un morphisme de A-modules $s : M'' \to M$ tel que $g \circ s = \mathrm{Id}_{M''}$.

(*ii*) Il existe un morphisme de A-modules $t : M \to M'$ tel que $t \circ f = \mathrm{Id}_{M'}$.

(*iii*) Il existe un isomorphisme de A-modules $\phi : M \simeq M' \oplus M''$ tels que, si $\iota_{M'}$ est l'injection canonique de M' dans $M' \oplus M''$ et $p_{M''}$ la projection canonique de $M' \oplus M''$ sur M'', $\iota_{M'} = \phi \circ f$ et $g = p_{M''} \circ \phi$.

On dit qu'une suite exacte courte vérifiant l'une de ces conditions est *scindée*. Une telle suite réduit l'étude du module M à celle d'une somme directe de deux modules « plus petits ». Si $A = k$ est un corps, une suite exacte courte de k-espaces vectoriels est toujours scindée (tout sous-espace admet un supplémentaire). Ce n'est pas le cas en général pour des A-modules.

Exercice II.3.2. Montrer que la suite exacte

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n\times} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

n'est pas scindée si $n \geq 2$.

Exercice II.3.3. On munit $\mathbb{Z}^2$ de structures de $\mathbb{Z}[X]$-modules par

(a) $X \cdot (a, b) = (b, a)$

(b) $X \cdot (a, b) = (a + b, b)$.

Dans le cas (a), quelles sont les structures de $\mathbb{Z}[X]$-modules sur $\mathbb{Z}$ qui font de

$$0 \longrightarrow \mathbb{Z} \xrightarrow{a\mapsto(a,a)} \mathbb{Z}^2 \longrightarrow \mathbb{Z} \longrightarrow 0$$

une suite exacte courte ? Est-elle alors scindée ?

Mêmes questions dans le cas (b) avec

$$0 \longrightarrow \mathbb{Z} \xrightarrow{a\mapsto(a,0)} \mathbb{Z}^2 \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Exercice II.3.4 (Exactitude à gauche des foncteurs Hom_A). Soit A un anneau.

(i) Soient M et N deux A-modules. Montrer que $\mathrm{Hom}_{\mathbb{A}}(M, N)$ est un $\mathbb{Z}$-module, mais qu'il n'a pas de structure de A-module, à moins que A ne soit commutatif. Montrer que $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ possède une structure de A-module à gauche et une structure de A-module à droite qui coïncident si A est commutatif.

(ii) Soit N un A-module et soit $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M''$ une suite exacte de A-modules. Montrer que l'on a la suite exacte (de groupes abéliens)

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \xrightarrow{u\circ\cdot} \mathrm{Hom}_A(N, M) \xrightarrow{v\circ\cdot} \mathrm{Hom}_A(N, M'').$$

(iii) Soit $M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ une suite exacte de A-modules. Montrer que l'on a la suite exacte (de groupes abéliens)

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{\cdot\circ v} \mathrm{Hom}_A(M, N) \xrightarrow{\cdot\circ u} \mathrm{Hom}_A(M', N).$$

Exercice II.3.5 (Lemme des 5 court). On considère un diagramme commutatif de morphismes de A-modules de la forme suivante, où les deux lignes forment des suites exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

Montrer que si, parmi les trois morphismes f, g et h, deux sont des isomorphismes, alors le troisième est aussi un isomorphisme.

Exercice II.3.6 (Lemme du serpent). On considère un diagramme commutatif de morphismes de A-modules de la forme suivante, où les deux lignes forment des suites exactes :

$$\begin{array}{ccccccccc} & & L & \xrightarrow{u} & M & \xrightarrow{v} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \xrightarrow{u'} & M' & \xrightarrow{v'} & N' & & \end{array}$$

Montrer qu'il existe une suite exacte canonique

$$\ker f \to \ker g \to \ker h \xrightarrow{\delta} \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h.$$

(Indication : les deux premières flèches sont induites par u et v ; les deux dernières par u' et v'. Soit $x \in \ker h$; on peut écrire $x = v(y)$, avec $y \in M$; il existe alors un unique $z \in L'$ tel que $u'(z) = g(y)$. On vérifie que la classe $z + \mathrm{Im}\, f$ ne dépend que de x et pas du choix de y, ce qui autorise à poser $\delta(x) = z$. L'homomorphisme δ étant ainsi défini, il faut vérifier que la suite obtenue est exacte).

Note : δ est appelé homomorphisme de liaison. Ce lemme joue un grand rôle en algèbre homologique, il est la base des suites exactes longues de groupes d'homologie ou de cohomologie.

II.4 Idéal annulateur. Torsion

Soit M un A-module, et soit $m \in M$. On pose

$$\mathrm{Ann}_A(m) = \{a \in A |\, a \cdot m = 0\}.$$

Plus généralement, pour toute partie $E \subset M$, on pose

$$\mathrm{Ann}_A(E) = \{a \in A |\, a \cdot m = 0,\ (\forall m \in E)\} = \bigcap_{m \in E} \mathrm{Ann}_A(m).$$

C'est un idéal (à gauche) de A, appelé *idéal annulateur de* E. Remarquons que $\mathrm{Ann}_A(M)$ est un idéal bilatère de A.

Un élément $m \in M$ est dit *de torsion* si $\mathrm{Ann}_A(m) \neq \{0\}$. L'ensemble des éléments de torsion de M est noté $\mathrm{Tor}_A(M)$.

Remarque II.4.1. La possibilité d'avoir des éléments de torsion dans un module est un des faits qui distingue la théorie générale des modules de la théorie des espaces vectoriels.

L'ensemble $\mathrm{Tor}_A(M)$ n'est pas en général un sous-module de M. Par exemple, si $M = A$, les éléments de torsion sont les diviseurs (à droite) de zéro, qui ne forment pas un idéal en général. Pour avoir cette propriété, il faut des hypothèses supplémentaires, par exemple :

Proposition II.4.2. *Soit M un A-module, où A est anneau commutatif, intègre. Alors* $\mathrm{Tor}_A(M)$ *est un sous-module de M.*

Démonstration. La stabilité par l'action de A est claire, grâce à la commutativité de A. Si m_1, $m_2 \in \mathrm{Tor}_A(M)$, il existe a_1 et a_2 dans A, non nuls, tels que $a_1 \cdot m_1 = 0$ et $a_2 \cdot m_2 = 0$, et l'on en déduit facilement que $(a_1 a_2) \cdot (m_1 + m_2) = 0$. De plus $a_1 a_2 \neq 0$ car A est intègre. □

Proposition II.4.3. *Soit M un A-module, où A est anneau commutatif, intègre. Alors*

$$\mathrm{Tor}_A(\mathrm{Tor}_A(M)) = \mathrm{Tor}_A(M) \text{ et } \mathrm{Tor}_A(M/\mathrm{Tor}_A(M)) = 0.$$

Démonstration. La première assertion est évidente. Pour la seconde, soit $m \in M$ et supposons qu'il existe $a \in A$ non nul tel que $a \cdot \bar{m} = 0 \in M/\mathrm{Tor}_A(M)$. Alors il existe $m_1 \in \mathrm{Tor}_A(M)$ tel que $a \cdot m = m_1$, et comme $m_1 \in \mathrm{Tor}_A(M)$, il existe $b \in A$ non nul tel que $b \cdot m_1 = 0$. On a alors $ab \cdot m = 0$ et $ab \neq 0$ car A est intègre. Donc $m \in \mathrm{Tor}_A(M)$ et $\bar{m} = 0$. Ainsi $\mathrm{Tor}_A(M/\mathrm{Tor}_A(M)) = 0$.

II.5 Familles génératrices, familles libres, bases

Définition II.5.1. Soit M un A-module et soit $(x_i)_{i\in I}$ une famille d'éléments de M. Considérons le morphisme

$$A^{(I)} \longrightarrow M, \quad (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i \cdot x_i \tag{II.5.1}$$

On dit que la famille $(x_i)_{i\in I}$ est *génératrice* si ce morphisme est surjectif, c'est-à-dire que le sous-module engendré par les x_i (voir section II.1.14) est M tout entier. Si M admet une famille génératrice finie, on dit que M est de type fini.

Les éléments du noyau de ce morphisme s'appellent les *relations* entre les x_i. On dit que la famille $(x_i)_{i\in I}$ est *libre* si ce noyau est trivial.

Si le morphisme (II.5.1) est un isomorphisme, le famille $(x_i)_{i\in I}$ est à la fois libre et génératrice, et l'on dit que c'est une *base* de M.

On dit que le module M est libre s'il admet une base, c'est-à-dire s'il est isomorphe à un $A^{(I)}$.

Exercice II.5.2. Quelles sont les bases du A-module A ?

Remarque II.5.3. Le vocabulaire ci-dessus est cohérent avec le vocabulaire usuel de la théorie des espaces vectoriels, mais de nombreuses propriétés valides pour les espaces vectoriels ne sont plus vraies en général.

1 - Un A-module M n'admet pas nécessairement de base. Par exemple, si A est commutatif et si I est un idéal de A non nul et non égal à A, alors tous les éléments de A/I sont de torsion : $\mathrm{Tor}(A/I) = A/I$ et A/I n'admet aucune famille libre non vide.

2 - Si M est un module libre, un sous-module de M n'est pas nécessairement libre. Par exemple, si A est commutatif et si I est un idéal de A non nul et non égal à A, alors deux éléments de I sont liés, et les familles libres de I ont au plus un élément. Les idéaux I ne sont libres que si A est principal, et même cette condition n'est pas suffisante, il faut en plus supposer A intègre.

3 - Une famille libre maximale n'est pas nécessairement une base : dans le $\mathbb{Z}$-module $\mathbb{Z}$, la famille à un élément (2) est libre et maximale (elle n'est strictement contenue dans aucune autre famille libre).

4 - Une famille génératrice minimale n'est pas nécessairement une base : dans le $\mathbb{Z}$-module $\mathbb{Z}$, la famille à deux élément $(2, 3)$ est génératrice et minimale (elle ne contient aucune sous-famille génératrice), mais ce n'est pas une base.

II.5.1 Modules libres

Théorème II.5.4. *Soit A un anneau commutatif, et soit M un A-module admettant une base finie $(x_1, \ldots, x_n)$ ayant n éléments. Alors toute base de M est de cardinal n. De manière équivalente, si A^n et A^m sont isomorphes, alors $n = m$. On appelle alors rang de M le cardinal d'une de ses bases.*

Ce qui est surprenant dans cet énoncé, c'est que la condition A commutatif est nécessaire. En effet il existe un anneau non commutatif A tel que A^n et A^m soient isomorphes, avec $n \neq m$. En voici un exemple. Considérons un espace vectoriel V de dimension infinie dénombrable sur un corps k. Soit $(e_i)_{i\in\mathbb{N}}$ une base de V. Alors V est isomorphe à $V \oplus V$, par exemple en définissant

un isomorphisme ϕ envoyant e_{2i} sur $e_i, 0$ et e_{2i+1} sur $(0, e_i)$. On a donc

$$\mathcal{E} := \mathrm{End}_k(V) = \mathrm{Hom}_k(V,V) = \mathrm{Hom}_k(V \oplus V, V) \simeq \mathrm{Hom}_k(V,V) \times \mathrm{Hom}_k(V,V) = \mathcal{E} \times \mathcal{E},$$

$$f \mapsto (f \circ \phi \circ \iota_1, f \circ \phi \circ \iota_2).$$

Il est immédiat de vérifier que c'est un isomorphisme de A-modules (à gauche).

Démonstration. Nous esquissons deux démonstrations. La première est basée sur le théorème de Krull (voir chapitre II.8). Soit I un idéal maximal de A. Alors A/I est un corps. Supposons que l'on ait un isomorphisme $f : A^n \to A^m$. Soit $(e_1, \ldots, e_n)$ la base canonique de A^n, et soit $(i_1, \ldots, i_n) \in I^n$. On a $f(i_1, \ldots, i_n) = \sum_{i=1}^n i_i f(e_i) \in I^m$ car I est un idéal. Le morphisme f induit donc un morphisme

$$\bar{f} : \ (A^n/I^n) \simeq (A/I)^n \longrightarrow (A^m/I^m) \simeq (A/I)^m \, .$$

On vérifie facilement que $\bar{f}$ reste un isomorphisme. On est donc ramené au cas des espaces vectoriels sur un corps, que l'on suppose connu, et l'on obtient $n = m$.

La seconde démonstration utilise la théorie des matrices à coefficients dans A. On suppose que M admet deux bases, la première $(e_1, \ldots, e_n)$, et la seconde $(f_1, \ldots, f_m)$, avec $m > n$. On écrit $f_i = \sum_{j=1}^n a_{ij} e_j$, et $e_j = \sum_{k=1}^m b_{jk} f_k$, ce qui en substituant donne pour $i = 1, \ldots, m$

$$f_i = \sum_{j=1}^n a_{ij} \left(\sum_{k=1}^m b_{jk} f_k \right) = \sum_{k=1}^m \left(\sum_{j=1}^n a_{ij} b_{jk} \right) f_k$$

En terme matriciel, avec $\mathcal{A} = (a_{ij}) \in \mathcal{M}_{m,n}(A)$ et $\mathcal{B} = (b_{k,\ell}) \in \mathcal{M}_{n,m}$, ceci équivaut à $\mathcal{A}\mathcal{B} = I_m$. On complète les matrices rectangulaires $\mathcal{A}$ et $\mathcal{B}$ en des matrices carrées $\tilde{\mathcal{A}}$, $\tilde{\mathcal{B}}$ dans $\mathcal{M}_m(A)$ en ajoutant $m - n$ lignes nulles à $\mathcal{B}$ (en bas), et $m - n$ colonnes nulles à $\mathcal{A}$ (à droite). On a encore $\tilde{\mathcal{A}}\tilde{\mathcal{B}} = I_m$, et l'on peut montrer en utilisant la théorie des déterminants, que $\tilde{\mathcal{A}}$ et $\tilde{\mathcal{B}}$ sont inversibles. En effet la formule $\det(M) I_n = M \times {}^t\mathrm{Com}(M)$ (transposée de la comatrice) reste valable sur un anneau commutatif, et $\det(\tilde{\mathcal{A}}\tilde{\mathcal{B}}) = 1 = \det(\tilde{\mathcal{A}}) \det(\tilde{\mathcal{B}})$, donc $\det(\tilde{\mathcal{A}})$, $\det(\tilde{\mathcal{B}})$ sont inversibles dans A, ce qui montre l'assertion. On a ainsi $\tilde{\mathcal{B}}\tilde{\mathcal{A}} = I_m$, ce qui est en contradiction avec la forme de ces matrices. □

Remarque II.5.5. Attention aux habitudes issues de la théorie des espaces vectoriels ! Par exemple, une famille libre à n éléments dans un module libre de rang n n'est pas nécessairement une base (par exemple, 2 n'est pas une base du $\mathbb{Z}$-module libre $\mathbb{Z}$, de rang 1). En revanche, si A est commutatif, toute famille génératrice à n éléments d'un A-module libre de rang n en est bien une base (cor. III.3.5).

Exercice II.5.6. Soient A un anneau commutatif et I un idéal non nul de A. Montrer que I est un A-module libre si et seulement si I est un idéal principal engendré par un non diviseur de zéro.

Exercice II.5.7. Soit A un anneau commutatif non nul, soit M un A-module libre et soit N un sous-module *libre* de M. Montrer $\mathrm{rg}(N) \leq \mathrm{rg}(M)$.

Exercice II.5.8. Montrer que le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas libre.

Exercice II.5.9. Soit A un anneau intègre et soit K son corps des fractions. Tout espace vectoriel sur K peut être aussi vu comme un A-module.

1) Soit V un K-espace vectoriel. Montrer qu'une famille libre $(v_i)_{i\in I}$ est libre dans le K-espace vectoriel V si et seulement si elle est libre dans le A-module V.
2) Montrer qu'une famille génératrice $(v_i)_{i\in I}$ dans le A-module V est génératrice dans K-espace vectoriel V. La réciproque est-elle vraie ?
3) Montrer que K est un A-module libre si et seulement si $A = K$.
4) Montrer que K est un A-module de type fini si et seulement si $A = K$.
5) Soit V et W deux K-espaces vectoriels. Montrer que tout morphisme de A-modules de V vers W est une application K-linéaire.

Exercice II.5.10. 1) Soient M un A-module et N un sous-module. Montrer que si N et M/N sont libres, alors M aussi.
2) Montrer que toute somme directe de A-modules libres est libre, ainsi que tout produit direct fini (un produit direct infini de modules libres n'est pas toujours libre comme le montre l'exemple de $\mathbb{Z}^{\mathbb{N}}$ dans l'exrcice suivant).
3) Ici $A = \mathbb{Z}/6\mathbb{Z}$. Montrer que les A-modules $3A$ et $2A$ ne sont pas libre, mais que $3A \oplus 2A = A$ (et donc est libre).

Exercice II.5.11. Tout espace vectoriel est libre. En particulier le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^{\mathbb{N}}$ des suites de nombres rationnels a une base (mais il faut l'axiome du choix pour montrer son existence). Nous allons montrer cependant que le $\mathbb{Z}$-module $M := \mathbb{Z}^{\mathbb{N}}$ n'est pas libre. Supposons par l'absurde qu'il admet une base $\mathcal{B}$.
a) Montrer que $\mathcal{B}$ n'est pas dénombrable.
b) Soit $e_n \in M$ la suite dont tous les termes sont nuls, sauf le n-ième qui vaut 1. On écrit e_n comme combinaison linéaire d'une partie finie $\mathcal{B}_n$ de $\mathcal{B}$ et on considère le sous-module (libre) $N \subset M$ engendré par la partie dénombrable $\bigcup_{n\in\mathbb{N}} \mathcal{B}_n$ de $\mathcal{B}$. Montrer que si $x \in M/N$ n'est pas nul, il existe au plus un nombre fini d'entiers $k \in \mathbb{Z}$ tels que l'on puisse écrire $x = ky$, avec $y \in M/N$.
c) Montrer que la partie $S = \{(\epsilon_n n!)_{n\in\mathbb{N}} \mid \epsilon_n \in \{-1, 1\}\}$ de M n'est pas dénombrable. En déduire qu'il existe $s \in S$ tel que $s \notin N$.
d) Montrer que pour chaque $k \in \mathbb{Z}$, il existe $y \in M/N$ tel que $\bar{s} = ky$. Conclure.

Exercice II.5.12. Soit M un A-module. On appelle *présentation par générateurs et relations* de M la donnée d'une famille génératrice $(x_i)_{i\in I}$ de A et d'une famille génératrice $(r_j)_{j\in J}$ du noyau du morphisme

$$A^{(I)} \longrightarrow M, \quad (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i \cdot x_i.$$

Pour $A = \mathbb{Z}[Z]$, donner une présentation du A-module $I = (2, X) \subset A$.

Exercice II.5.13. 1) Soient M un A-module de type fini. Montrer que toute famille génératrice de M contient une sous-famille génératrice finie.
2) Ici $A = \mathbb{Z}^{\mathbb{N}}$. Alors $M = A$ est un A-module de type fini. Montrer que $N = \mathbb{Z}^{(\mathbb{N})}$ est un sous-A-module de M qui n'est pas de type fini.
3) Soient M un A-module et N un sous-module. Montrer que si N et M/N sont de type fini, alors M aussi.

Exercice II.5.14. On considère le $\mathbb{Z}$-module $\mathbb{Q}$.
1) Montrer que tout sous-module N de type fini est libre de rang 1. En déduire que $\mathbb{Q}$ n'est pas de type fini sur $\mathbb{Z}$.
2) Montrer que si $(x_i)_{i\in I}$ est une famille génératrice du $\mathbb{Z}$-module $\mathbb{Q}$, alors pour tout $j \in I$, la famille $(x_i)_{i\in I\setminus\{j\}}$ est encore génératrice.

II.5.2 Propriété universelle des modules libres

Nous avons vu dans l'exemple II.1.3 la définition du A-module libre de base I, noté $A^{(I)}$. La propriété universelle satisfaite par ce module est la suivante. Pour deux ensembles X et Y, notons $\mathrm{Hom}_{\mathcal{E}ns}(X,Y)$ l'ensemble des applications de X dans Y. On peut voir un A-module N simplement comme un ensemble. Pour tout module N, on a un isomorphisme « naturel » :

$$\Phi_{I,N} : \mathrm{Hom}_{\mathcal{E}ns}(I,N) \simeq \mathrm{Hom}_A(A^{(I)},N).$$

En effet, la définition de cet isomorphisme est « naturelle », dans le sens usuel de cet adjectif en français : pour tout $j \in I$ l'on note δ_j l'élément de $A^{(I)}$ défini par $\delta_j(i) = 1_A$ si $i = j$ et 0_A sinon. Si $\phi \in \mathrm{Hom}_A(A^{(I)},N)$, on définit un élément de $\mathrm{Hom}_{\mathcal{E}ns}(I,N)$ par $i \mapsto \phi(\delta_i)$, et réciproquement $f \in \mathrm{Hom}_{\mathcal{E}ns}(I,N)$, on définit $\phi(\delta_i) = f(i)$ et ceci s'étend de manière unique par linéarité en un morphisme $\phi \in \mathrm{Hom}_A(A^{(I)},N)$. Ces deux opérations sont inverses l'une de l'autre et définissent l'isomorphisme (de $\mathbb{Z}$-modules) cherché. La « naturalité » de cet isomorphisme a aussi un sens technique, que nous n'explicitons pas totalement (c'est un concept de la théorie des catégories).

Disons simplement que tout élément $g \in \mathrm{Hom}_{\mathcal{E}ns}(I,J)$ définit par composition

$$g_N^* : \mathrm{Hom}_{\mathcal{E}ns}(J,N) \longrightarrow \mathrm{Hom}_{\mathcal{E}ns}(I,N), \quad f \mapsto f \circ g,$$

et aussi un morphisme de A-modules :

$$g^{(.)} : A^{(I)} \longrightarrow A^{(J)}, \quad \delta_i \mapsto \delta_{g(i)}$$

qui définit à son tour par composition

$$g_N^* = \mathrm{Hom}_A(A^{(J)},N) \longrightarrow \mathrm{Hom}_A(A^{(I)},N), \quad \phi \mapsto \phi \circ g^{(.)}.$$

La première condition de naturalité consiste alors en la commutativité du diagramme

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{E}ns}(J,N) & \xrightarrow{\Phi_{J,N}} & \mathrm{Hom}_{\mathcal{G}r}(A^{(J)},N) \\ \downarrow{\scriptstyle .\circ g} & & \downarrow{\scriptstyle .\circ g^{()}} \\ \mathrm{Hom}_{\mathcal{E}ns}(I,N) & \xrightarrow{\Phi_{I,N}} & \mathrm{Hom}_{\mathcal{G}r}(A^{(I)},N). \end{array}$$

De même, tout morphisme de A-modules $\psi \in \mathrm{Hom}_A(M,N)$ définit par composition

$$\psi_*^I = \mathrm{Hom}_A(A^{(I)},M) \longrightarrow \mathrm{Hom}_A(A^{(I)},N), \quad \phi \mapsto \psi \circ \phi,$$

et

$$\psi_*^I : \mathrm{Hom}_{\mathcal{E}ns}(I,M) \longrightarrow \mathrm{Hom}_{\mathcal{E}ns}(I,N), \quad f \mapsto \psi \circ f,$$

La deuxième condition de naturalité consiste alors en la commutativité du diagramme

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{E}ns}(I,M) & \xrightarrow{\Phi_{I,M}} & \mathrm{Hom}_{\mathcal{G}r}(A^{(I)},M) \\ \downarrow{\scriptstyle \psi\circ.} & & \downarrow{\scriptstyle \psi\circ.} \\ \mathrm{Hom}_{\mathcal{E}ns}(I,N) & \xrightarrow{\Phi_{I,N}} & \mathrm{Hom}_{\mathcal{G}r}(A^{(I)},N). \end{array}$$

Exercice II.5.15. Montrer que tout module est quotient d'un module libre.

II.5.3 Groupe libre. Présentation d'un groupe

Dans cette section, nous allons définir la notion de groupe libre sur un ensemble, du point de vue de la théorie des catégories, mais conformément à la philosophie de ce cours, sans introduire le formalisme complet de celle-ci. Nous faisons ceci ici pour insister sur la ressemblance avec la notion de module libre vue dans la section précédente.

Nous considérons deux catégories. La première est celle des ensembles, $\mathcal{E}ns$. Etant donnés deux ensembles X et Y, on considère l'ensemble des applications de X dans Y, que l'on va noter

$$\mathrm{Hom}_{\mathcal{E}ns}(X, Y).$$

On note typiquement

$$X \xrightarrow{f} Y$$

un élément de $\mathrm{Hom}_{\mathcal{E}ns}(X, Y)$.

La deuxième est la catégorie des groupes $\mathcal{G}r$. Etant donnés deux groupes G et H, on considère l'ensemble des morphisme de groupes de G dans H, que l'on va noter

$$\mathrm{Hom}_{\mathcal{G}r}(G, H).$$

Idem pour la notation

$$G \xrightarrow{\phi} H$$

pour un élément de $\mathrm{Hom}_{\mathcal{G}r}(G, H)$.

Remarquons que étant donné une flèche $G \xrightarrow{\phi} H$ dans $\mathcal{G}r$, on peut oublier qu'on a affaire à des groupes et à un morphisme de groupes, et voir cette flèche comme une flèche dans $\mathcal{E}ns$. En terme technique, on a un « foncteur » de $\mathcal{G}r$ dans $\mathcal{E}ns$, le foncteur d'oubli. On peut penser que ce foncteur n'est pas passionnant, mais il n'est pas aussi bête qu'il n'y paraît, comme nous allons le voir.

Ce qui semblerait plus intéressant, c'est de définir un foncteur dans l'autre sens, de $\mathcal{E}ns$ vers $\mathcal{G}r$. Comment, à partir d'un ensemble I, fabriquer un groupe, disons F_I, et ceci de manière naturelle ? Et pour toute application ensembliste $I \xrightarrow{f} J$, on doit aussi fabriquer un morphisme de groupes $F_I \xrightarrow{F_f} F_J$.

Il faut préciser un peu le problème. Ce qu'on cherche c'est une construction telle que pour tout ensemble I, et pour tout groupe G, on ait un isomorphisme

$$\mathrm{Hom}_{\mathcal{E}ns}(I, G) \xrightarrow{\Psi_{I,G}} \mathrm{Hom}_{\mathcal{G}r}(F_I, G). \tag{II.5.2}$$

Remarquons l'analogie formelle avec la notion d'opérateur adjoint dans un espace euclidien ou hermitien. Pour cette raison, un foncteur $I \mapsto F_I$ vérifiant (II.5.2) est dit adjoint à gauche du foncteur d'oubli.

Mais l'existence d'isomorphismes (II.5.2) pour tout groupe G n'est pas la seule condition que l'on s'impose. Ces isomorphismes doivent être « naturels ». Ceci signifie la chose suivante. Remarquons que toute flèche $G \xrightarrow{\phi} H$ dans $\mathcal{G}r$ définit par composition des applications une flèche

$$\mathrm{Hom}_{\mathcal{E}ns}(I, G) \xrightarrow{\phi\circ\cdot} \mathrm{Hom}_{\mathcal{E}ns}(I, H)$$

et de même dans $\mathcal{G}r$, par compostion des morphismes de groupes :

$$\mathrm{Hom}_{\mathcal{G}r}(F_I, G) \xrightarrow{\phi\circ\cdot} \mathrm{Hom}_{\mathcal{G}r}(F_I, H).$$

La première condition de naturalité que l'on exige est la commutativité du diagramme

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{E}ns}(I,G) & \xrightarrow{\Psi_{I,G}} & \mathrm{Hom}_{\mathcal{G}r}(F_I,G) \\ \downarrow{\scriptstyle \phi\circ.} & & \downarrow{\scriptstyle \phi\circ.} \\ \mathrm{Hom}_{\mathcal{E}ns}(I,H) & \xrightarrow{\Psi_{I,H}} & \mathrm{Hom}_{\mathcal{G}r}(F_I,H) \end{array}$$

On a une deuxième condition similaire portant sur les flèches $I \xrightarrow{f} J$ dans $\mathcal{E}ns$, qui donne $F_I \xrightarrow{F_f} F_J$ dans $\mathcal{G}r$, et par composition

$$\mathrm{Hom}_{\mathcal{E}ns}(J,G) \xrightarrow{\cdot\circ f} \mathrm{Hom}_{\mathcal{E}ns}(I,G)$$

et

$$\mathrm{Hom}_{\mathcal{G}r}(F_J,G) \xrightarrow{\cdot\circ F_f} \mathrm{Hom}_{\mathcal{G}r}(F_I,G).$$

La deuxième condition de naturalité que l'on exige est la commutativité du diagramme

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{E}ns}(J,G) & \xrightarrow{\Psi_{J,G}} & \mathrm{Hom}_{\mathcal{G}r}(F_J,G) \\ \downarrow{\scriptstyle .\circ f} & & \downarrow{\scriptstyle .\circ F_f} \\ \mathrm{Hom}_{\mathcal{E}ns}(I,G) & \xrightarrow{\Psi_{I,G}} & \mathrm{Hom}_{\mathcal{G}r}(F_I,G). \end{array}$$

Le problème est maintenant bien posé. Avant de discuter de la construction de F_I et des isomorphismes Ψ_G (c'est-à-dire du problème de l'existence d'une solution), considérons le problème de l'unicité de celle-ci. Supposons que nous ayons deux solutions, un groupe F_I et des isomorphismes Ψ_G, et un groupe F'_I et des isomorphismes Ψ'_G. Nous allons exhiber un isomorphisme naturel, déterminé uniquement, entre F_I et F'_I qui permet d'identifier ces deux groupes. Ceci est un point important, qui nous permettra de parler « du » groupe F_I (par abus de langage).

Pour construire un isomorphisme entre F_I et F'_I, on part de la suite d'isomorphismes

$$\mathrm{Hom}_{\mathcal{G}r}(F'_I,F_I) \xleftarrow{\Psi_{F'_I}} \mathrm{Hom}_{\mathcal{E}ns}(I,F_I) \xrightarrow{\Psi_{F_I}} \mathrm{Hom}_{\mathcal{G}r}(F_I,F_I)$$

et l'on exploite le fait qu'à droite, on un élément privilégié, à savoir Id_{F_I}. Ceci nous donne un élément $F'_I \xrightarrow{\eta'} F_I$. De manière symétrique, on obtient $F_I \xrightarrow{\eta} F'_I$. Par naturalité on obtient un diagramme commutatif

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathcal{G}r}(F'_I,F_I) & \xleftarrow{\Psi'_{F_I}} & \mathrm{Hom}_{\mathcal{E}ns}(I,F_I) & \xrightarrow{\Psi_{F_I}} & \mathrm{Hom}_{\mathcal{G}r}(F_I,F_I) \\ \downarrow{\scriptstyle \eta\circ.} & & \downarrow{\scriptstyle \eta\circ.} & & \downarrow{\scriptstyle \eta\circ.} \\ \mathrm{Hom}_{\mathcal{G}r}(F'_I,F'_I) & \xleftarrow{\Psi'_{F'_I}} & \mathrm{Hom}_{\mathcal{E}ns}(I,F'_I) & \xrightarrow{\Psi_{F'_I}} & \mathrm{Hom}_{\mathcal{G}r}(F_I,F'_I) \end{array}$$

Si on part de l'élément Id_{F_I} en haut à droite, on obtient au quatre coins du rectangle

$$\begin{array}{ccc} \eta' & \longleftarrow & \mathrm{Id}_{F_I} \\ \downarrow & & \downarrow \\ \eta\circ\eta' & \longleftarrow & \eta \end{array}$$

Mais par définition, η est aussi l'élément qui correspond à $\mathrm{Id}_{F'_I}$ via les isomorphismes

$$\mathrm{Hom}_{\mathcal{G}r}(F_I, F'_I) \xleftarrow{\Psi_{F'_I}} \mathrm{Hom}_{\mathcal{E}ns}(I, F'_I) \xrightarrow{\Psi'_{F'_I}} \mathrm{Hom}_{\mathcal{G}r}(F'_I, F'_I)$$

On a donc $\eta \circ \eta' = \mathrm{Id}_{F'_I}$. De même, on obtient $\eta' \circ \eta = \mathrm{Id}_{F_I}$.

Ainsi F_I et F'_I sont isomorphes, l'isomorphisme entre les deux étant déterminé par les propriétés qu'ils satisfont et donne une manière bien définie de les identifier.

Remarque II.5.16. Comme nous l'avons vu, ce type de résultat d'unicité est typique d'objets satisfaisant une « propriété universelle », comme celle ci-dessus en (II.5.2). Nous avons vu ou nous verrons d'autres exemples : produits et coproduits, modules libres, produits tensoriels, etc.

Ce problème d'unicité étant réglé, passons à l'existence. Nous allons être bref et expliquer l'idée sans formalisme excessif. Il s'agit de donner une construction de F_I. Considérons l'alphabet $\mathcal{A}$ dont les lettres sont les x, x^{-1} avec $x \in I$. On forme ensuite l'ensemble des mots dans l'alphabet $\mathcal{A}$, c'est-à-dire des suites finies de lettres. Mais lorsque dans un mot, les lettres x et x^{-1} apparaissent consécutivement (dans un ordre ou l'autre), on obtient un mot équivalent en les enlevant du mot. Par exemple les mots $yx^{-1}xz$ et yz sont équivalents. Ceci définit une relation d'équivalence sur les mots. Le groupe F_I a pour élément les classes d'équivalence de mots. La loi de groupe est donnée par la concaténation des mots, et l'élément neutre est le mot vide. Il est immédiat de donner l'inverse d'un élément de F_I. Par exemple, l'inverse de $xyx^{-1}z^{-1}$ est $zxy^{-1}x^{-1}$. Le groupe F_I étant construit, donnons les isomorphismes Ψ_G. Si $I \xrightarrow{f} G$, on définit un morphisme de groupes $F_I \xrightarrow{\phi} G$ par $\phi(\emptyset) = e_G$, $\phi(x) = f(x)$, $x \in I$, et $\phi(x^{-1}) = f(x)^{-1}$ pour les mots de plusieurs lettres, on utilise la propriété des morphismes de groupes. Réciproquement un morphisme de groupes $F_I \xrightarrow{\phi} G$ définit $I \xrightarrow{f} G$ par $f(x) = \phi(x)$. On effectue ensuite facilement les vérifications nécessaires pour montrer que nos constructions vérifient les propriétés voulues.

Le groupe F_I construit ci-dessus, ou tout autre vérifiant la propriété universelle (II.5.2), s'appelle le groupe libre sur I.

Soit maintenant $\mathcal{R}$ une partie de F_I. Soit $N(\mathcal{R})$ le plus petit sous-groupe distingué de F_I contenant $\mathcal{R}$ (c'est le sous-groupe engendré par tous les éléments de $\mathcal{R}$ et leur conjugués). On a alors un groupe quotient $F_I/N(\mathcal{R})$. Ce groupe admet I comme système de générateurs, et on dit que les éléments de $\mathcal{R}$ sont les relations satisfaites par ces générateurs. Remarquons que tout morphisme de groupe $F_I \xrightarrow{\phi} G$ qui s'annule sur $\mathcal{R}$ s'annule sur $N(\mathcal{R})$ et définit un morphisme de groupes

$$F_I/N(\mathcal{R}) \xrightarrow{\bar{\phi}} G$$

(et réciproquement, $\bar{\phi}$ définit ϕ qui s'annule sur $N(\mathcal{R})$ donc sur $\mathcal{R}$).

Une présentation d'un groupe G est la donnée d'un ensemble I, et d'une partie $\mathcal{R}$ de F_I et d'un isomorphisme $F_I/N(\mathcal{R}) \xrightarrow{\bar{\phi}} G$. Les éléments de I donnent un système de générateurs $(g_i)_{i\in I}$ de G, et les éléments de $\mathcal{R}$ donnent les relations entre ceux-ci.

Proposition II.5.17. *Tout groupe admet une présentation.*

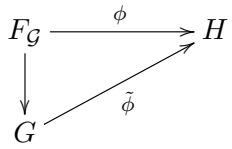
Démonstration. Il suffit de trouver un morphisme surjectif $F_I \to G$, et de prendre le noyau pour $\mathcal{R}$. Il est clair par construction que l'on a un morphisme surjectif $F_G \xrightarrow{\phi} G$. Remarquons que par la propriété universelle, ce morphisme est celui qui correspond à $\mathrm{Id}_G \in \mathrm{Hom}_{\mathcal{E}ns}(G, G)$. Une

démonstration plus élégante consiste à utiliser la propriété universelle plutôt que la construction explicite de F_G. Or ϕ est surjectif si et seulement lorsque pour deux morphismes

$$\psi_1, \psi_2 : G \to H$$

on a $\psi_1 \circ \phi = \psi_2 \circ \phi$, alors $\psi_1 = \psi_2$. Remarquons que l'on a là une définition « catégorielle » de la surjectivité, c'est-à-dire en terme de flèches plutôt qu'en terme d'éléments d'un ensemble. Or le fait que $\psi_1 \circ \phi = \psi_2 \circ \phi$ implique $\psi_1 = \psi_2$. est conséquence immédiate de la propriété universelle (II.5.2) pour F_G. □

Comment montre t-on en pratique qu'un groupe admet une présentation donnée ? Supposons que l'on nous donne un groupe G avec système de générateurs, disons $\mathcal{G}$, et un ensemble de relations $\mathcal{R}$ satisfaites par ces générateurs. Un groupe avec la présentation $(\mathcal{G}, \mathcal{R})$ vérifie la propriété universelle suivante : pour tout morphisme de groupes $F_{\mathcal{G}} \xrightarrow{\phi} H$ qui est trivial sur les élément de $\mathcal{R}$, il existe un unique $G \xrightarrow{\tilde{\phi}} H$ qui rend le diagramme



commutatif. L'idée est que l'image de ϕ dans H est un groupe qui admet $\mathcal{G}$ comme système de générateurs, et que les relations $\mathcal{R}$ y sont vérifiées, mais il se peut qu'il y ait d'autres relations qui ne soient pas engendrées par $\mathcal{R}$. Le groupe avec la présentation $(\mathcal{G}, \mathcal{R})$ est le plus gros quotient de $F_{\mathcal{G}}$ qui vérifie les relations $\mathcal{R}$. Remarquons que l'unicité de $\tilde{\phi}$ est automatique, car $\tilde{\phi}$ est imposé sur $\mathcal{G}$. L'exercice suivant donne un exemple non trivial de présentation.

Exercice II.5.18. — 1. Quel est le groupe libre sur l'ensemble à un élément. Les groupes engendrés par un éléments sont dits monogènes. Quels sont leurs présentations avec un seul générateur ?

— 2. Soit $\mathbb{F}$ un corps. Considérons les éléments suivants de $\mathbf{SL}(2, \mathbb{F})$:

$$t(y) = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix},\ y \in \mathbb{F}^\times, \quad n(z) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},\ z \in \mathbb{F}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Posons

$$\mathcal{G} = \{t(y),\ y \in \mathbb{F}^\times,\ n(z),\ z \in \mathbb{F}, w\},$$

et soit $\mathcal{R}$ l'ensemble des relations suivantes :

$$\begin{aligned} t(y_1)t(y_2) &= t(y_1y_2) & n(z_1)n(z_2) &= n(z_1 + z_2) \\ t(y)n(z)t(y)^{-1} &= n(y^2z) & wt(y)w^{-1} &= t(y^{-1}) \end{aligned}$$

$$n(z)wn(z^{-1})w^{-1}n(z) = t(z)w, \quad (z \neq 0).$$

Montrer que $(\mathcal{G}, \mathcal{R})$ est une présentation de $\mathbf{SL}(2, \mathbb{F})$.

Indication. Constater que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = n(a/c)t(-c^{-1})wn(d/c) \quad \text{si } c \neq 0, \quad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = t(a)n(b/a).$$

II.5.4 Modules projectifs

Cette notion est présentée ici sous forme d'exercice.

Exercice II.5.19 (Modules projectifs). Nous avons vu dans l'exercice II.3.4 que si

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

est une suite exacte courte de A-modules, alors pour tout A-module N

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \xrightarrow{u\circ\cdot} \mathrm{Hom}_A(N, M) \xrightarrow{v\circ\cdot} \mathrm{Hom}_A(N, M'')$$

est exacte.

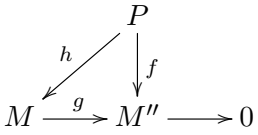
Le but de cet exercice est de caractériser les modules N tels que l'on obtienne une suite exacte courte complète :

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \xrightarrow{u\circ\cdot} \mathrm{Hom}_A(N, M) \xrightarrow{v\circ\cdot} \mathrm{Hom}_A(N, M'') \to 0$$

Les modules vérifiant cette propriété (P1) sont appelés *modules projectifs*.

1. Montrer que P est projectif si et seulement si :

(P2) pour tout morphisme $P \xrightarrow{f} M''$ et pour tout morphisme $M \xrightarrow{g} M''$ surjectif, il existe un morphisme $P \xrightarrow{h} M$ tel que $f = g \circ h$. On illustre cela par le diagramme commutatif



2. Montrer qu'un module libre est projectif.

3. Montrer qu'un module est projectif si et seulement s'il vérifie l'une des deux propriétés suivantes :

(P3) Toute suite exacte $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} P \longrightarrow 0$ est scindée.

(P4) Il existe un A-module K et un module libre L tels que $L = P \oplus K$.

Remarque II.5.20. Si on inverse le sens des flèches dans (P1), (P2), (P3), on obtient la définition de *module injectif* qui est la notion duale à celle de projectif.

Exercice II.5.21. Dans cet exercice, nous allons exhiber un exemple de module projectif non libre. On considère l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ et son idéal $I = (2, 1 + i\sqrt{5})$.

1 Montrer que I n'est pas un idéal principal. En déduire que I n'est pas un A-module libre (*cf.* Exercice II.5.6).

2 On considère le morphisme de A-modules

$$\phi : A^2 \longrightarrow I, \qquad (z, z') \mapsto 2z + (1 + i\sqrt{5})z'.$$

Il est surjectif par définition de I, on en déduit donc une suite exacte

$$0 \longrightarrow \ker\phi \longrightarrow A^2 \xrightarrow{\phi} I \longrightarrow 0.$$

Montrer que cette suite exacte est scindée. En déduire que I est un A-module projectif.

II.5.5 Modules cycliques

Définition II.5.22. On dit qu'un A-module M est cyclique (ou monogène) s'il est engendré par un seul élément.

Soit $x \in M$ un élément engendrant M, c'est-à-dire $M = A \cdot x$. Le morphisme

$$A \to M, \quad a \mapsto a \cdot x$$

est surjectif, et son noyau est $I = \mathrm{Ann}_A(x)$ qui est un idéal à gauche de A. On a donc $M \simeq A/I$, et réciproquement, si I est un idéal à gauche de A, A/I est un A-module cyclique.

Exercice II.5.23. On suppose A commutatif. Soit M un A-module monogène engendré par un élément $x \in M$. Montrer que l'idéal annulateur $I = \mathrm{Ann}_A(x)$ est en fait indépendant du générateur x choisi.

II.6 Produits tensoriels

II.6.1 Produits tensoriels sur un anneau commutatif

Dans cette section, les anneaux sont supposés commutatifs. On remarque que pour un anneau commutatif A, et deux modules N, M, $\mathrm{Hom}_A(M, N)$ est muni d'une structure de A-module (par multiplication à la source *ou* au but).

Applications multilinéaires.

Soit A un anneau commutatif et soient M, $M_1, \ldots, M_r$ des A-modules. Notons

$$\mathcal{L}_A(M_1, \ldots, M_r;\, M)$$

l'ensemble des applications de $M_1 \times \ldots \times M_r$ dans M, linéaires en chacune des variables.

Définition par propriété universelle.

On dit qu'un A-module N muni de $\iota \in \mathcal{L}_A(M_1, \ldots M_r;\, N)$ est le *produit tensoriel* de $M_1, \ldots, M_r$ s'il vérifie la propriété suivante : pour toute application multilinéaire $f \in \mathcal{L}_A(M_1, \ldots, M_r;\, M)$, il existe un unique morphisme de A-modules $\tilde{f} : N \to M$ tel que $\tilde{f} \circ \iota = f$.

Comme tous les objets définis par propriété universelle, on a unicité à un unique isomorphisme près.

Proposition II.6.1. *Soient*

$$\iota_1 \in \mathcal{L}_A(M_1, \ldots, M_r;\, N_1), \quad \iota_2 \in \mathcal{L}_A(M_1, \ldots, M_r;\, N_2)$$

vérifiant la propriété universelle ci-dessus. Alors N_1 et N_2 sont isomorphes, par un unique isomorphisme $\varphi : N_1 \simeq N_2$ vérifiant $\varphi \circ \iota_1 = \iota_2$.

Démonstration. On applique la propriété universelle de ι_1 à $f = \iota_2$: on obtient un A-morphisme $\tilde{\iota_2} : N_1 \to N_2$, vérifiant $\tilde{\iota_2} \circ \iota_1 = \iota_2$, et idem en échangeant les rôles de 1 et 2, on obtient $\tilde{\iota_1}$ tel que $\tilde{\iota_1} \circ \iota_2 = \iota_1$. On a donc $\tilde{\iota_2} \circ \tilde{\iota_1} \circ \iota_2 = \iota_2$,

On applique la propriété universelle de ι_2 à lui-même et par unicité ceci implique que $\tilde{\iota_2} \circ \tilde{\iota_1} = \mathrm{Id}_{N_2}$. De même on obtient $\tilde{\iota_1} \circ \tilde{\iota_2} = \mathrm{Id}_{N_2}$. Les modules N_1 et N_2 sont donc isomorphes, l'isomorphisme entre les deux étant $\tilde{\iota_2}$ d'inverse $\tilde{\iota_1}$. □

L'unicité à isomorphisme près justifie d'appeler N *le* produit tensoriel des M_i. On le note

$$M_1 \otimes_A M_2 \otimes_A \ldots \otimes_A M_r \text{ ou encore } \bigotimes_{i=1}^{r} M_i.$$

Il reste à montrer *l'existence* du produit tensoriel. On le réalise comme quotient du module libre $A^{(M_1 \times \cdots \times M_r)}$. Les éléments de $A^{(M_1 \times \cdots \times M_r)}$ sont les familles d'éléments de A indexées par $M_1 \times \cdots \times M_r$ et à support fini, et une base de ce module libre est donnée par les $(\delta_{(m_1,\ldots,m_r)})_{(m_1,\ldots,m_r) \in M_1 \times \cdots \times M_r}$, où $\delta_{(m_1,\ldots,m_r)}$ est la famille valant 1_A sur l'élément $(m_1, \ldots, m_r)$ et 0_A sur tous les autres éléments. On considère le sous-module $\mathcal{N}_0$ de $A^{(M_1 \times \cdots \times M_r)}$ engendré par les éléments de la forme

$$\delta_{(m_1,\ldots,m_{i-1},a\cdot m_i + a'\cdot m_i', m_{i+1},\ldots,m_r)} - a \cdot \delta_{(m_1,\ldots,m_{i-1},m_i,m_{i+1},\ldots,m_r)} - a' \cdot \delta_{(m_1,\ldots,m_{i-1},m_i',m_{i+1},\ldots,m_r)}$$

et l'on pose $N = A^{(M_1 \times \cdots \times M_r)}/\mathcal{N}_0$. L'application

$$\begin{aligned} \iota : M_1 \times \cdots \times M_r &\longrightarrow N = A^{(M_1 \times \cdots \times M_r)}/\mathcal{N}_0, \\ (m_1, \ldots, m_r) &\mapsto \delta_{(m_1,\ldots,m_r)} \mod \mathcal{N}_0 \end{aligned}$$

est multilinéaire. On note $m_1 \otimes \cdots \otimes m_r$ l'élément $\delta_{(m_1,\ldots,m_r)} \mod \mathcal{N}_0$ de N.

Soit $f \in \mathcal{L}_A(M_1, \ldots M_r; M)$. On peut oublier que f est multilinéaire, et la considérer comme une application ensembliste, c'est-à-dire comme un élément de $\mathrm{Hom}_{\mathcal{E}ns}(M_1 \times \ldots \times M_r, M)$. Par la propriété universelle du module libre $A^{(M_1 \times \cdots \times M_r)}$, il correspond à f un unique $\tilde{\tilde{f}}$ dans $\mathrm{Hom}_A(A^{(M_1 \times \cdots \times M_r)}, M)$. La multilinéarité de f se traduit sur $\tilde{\tilde{f}}$ exactement par le fait que $\mathcal{N}_0$ est dans le noyau de $\tilde{\tilde{f}}$, et ainsi $\tilde{\tilde{f}}$ induit un morphisme de A-modules $\tilde{f} : N \to M$. On vérifie que $f = \tilde{f} \circ \iota$. L'unicité de $\tilde{f}$ découle de celle de $\tilde{\tilde{f}}$. □

Remarque II.6.2. On note donc $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_r$ le produit tensoriel des M_i, muni de l'application multilinéaire $\iota : M_1 \times \cdots \times M_r \to M_1 \otimes_A \otimes_A \cdots \otimes_A M_r$, et l'on note $m_1 \otimes \cdots \otimes m_r$ l'élément $\iota(m_1, \ldots, m_r)$ de $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_r$. Il est important d"être conscient que cette dernière notation est ambigüe, par exemple, supposons que N_1 et N_2 sont des sous-modules respectivement de M_1 et M_2. Si $n_1 \in N_1$ et $n_2 \in N_2$, alors $n_1 \otimes n_2$ peuvent désigner soit un élément de $N_1 \otimes N_2$ ou bien de $M_1 \otimes M_2$. Or il se peut que le second soit nul et pas le premier ! Cette assertion outrageuse mérite une illustration qui la démontre : considérons $A = \mathbb{Z}$, $M_1 = \mathbb{Z}$, $N_1 = 2\mathbb{Z}$, $M_2 = N_2 = \mathbb{Z}/2\mathbb{Z}$ et l'élément $2 \otimes \bar{1}$. Dans $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, on a $2 \otimes \bar{1} = 1 \otimes 2 \cdot \bar{1} = 1 \otimes 0 = 0$, mais $2 \otimes \bar{1} \neq 0$ dans $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

D'autre part, pour effectuer des calculs, on se rappellera que tout élément de $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_r$ s'écrit comme une combinaison linéaire de tenseurs purs $m_1 \otimes \cdots \otimes m_r$ et que l'action de $a \in A$ sur un tenseur pur est

$$a \cdot (m_1 \otimes \cdots \otimes m_r) = (a \cdot m_1) \otimes \cdots \otimes m_r = m_1 \otimes (a \cdot m_2) \otimes \cdots \otimes m_r = \ldots$$

On vérifie de manière formelle les propriétés suivantes du produit tensoriel.

Proposition II.6.3. *1. Soient $M_1, \ldots, M_r$, M des A-modules. Alors on a un isomorphisme canonique*

$$M \otimes_A \left(\bigoplus_{i=1,\ldots,r} M_i \right) \simeq \bigoplus_{i=1,\ldots,r} (M \otimes_A M_i), \quad (m \otimes (m_1, \ldots, m_r) \mapsto (m \otimes m_1, \ldots, m \otimes m_r)$$

2. Soient M, N, L des A-modules, alors on a un isomorphisme canonique

$$(M \otimes_A N) \otimes_A L \simeq M \otimes_A (N \otimes_A L), \quad (m \otimes n) \otimes \ell \mapsto m \otimes (n \otimes \ell).$$

3. Soient M, N des A-modules, alors on a un isomorphisme canonique

$$M \otimes_A N \simeq N \otimes_A M, \quad (m \otimes n) \mapsto n \otimes m.$$

4. Soient M, N, L des A-modules, alors on a un isomorphisme canonique

$$\mathrm{Hom}_A(L, \mathrm{Hom}_A(M, N)) \simeq \mathrm{Hom}_A(L \otimes_A M, N) \simeq \mathcal{L}_A(L \times M; N)$$

5. On a canoniquement $A \otimes_A M \simeq M$.

Corollaire II.6.4. *Si $A = k$ est un corps et si $M_1, \ldots, M_r$ sont des k-espaces vectoriels de dimension finie, alors $M_1 \otimes_A M_2 \otimes_A \ldots \otimes_A M_r$ est de dimension finie égale à* $\dim_k(M_1) \times \cdots \times \dim_k(M_r)$.

Produit tensoriel de morphismes. Soient $f : M \to M'$, $g : N \to N'$ des morphismes de A-modules. Définissons

$$h : M \times N \longrightarrow M' \otimes_A N', \quad h(x, y) = f(x) \otimes g(y).$$

On vérifie facilement la bilinéarité de h et l'on en déduit un morphisme de A-modules

$$f \otimes g : M \otimes_A N \longrightarrow M' \otimes_A N',$$

tel que $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$, $(x \in M, y \in N)$. Soient $f' : M' \to M$" and $g' : N' \to N$" des morphismes de A-modules. Alors on a clairement $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.

Exercice II.6.5. Calculer $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z})$. Plus généralement, pour m,n entiers positifs, calculer $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$.

Exercice II.6.6. Soient k un corps, M et N des k-espaces vectoriels et M^*, N^* leur dual respectif. Etudier l'injectivité et la surjectivité des morphismes

$$M^* \otimes_k N \longrightarrow \mathrm{Hom}_k(M, N), \quad f \otimes n \mapsto (m \mapsto f(m)\, n).$$

$$M^* \otimes_k N^* \longrightarrow (M \otimes_k N)^*, \quad f \otimes g \mapsto (m \otimes n \mapsto f(m) \otimes g(n)).$$

$$\mathrm{End}_k(M) \otimes_k \mathrm{End}_k(N) \longrightarrow \mathrm{End}_k(M \otimes_k N), \quad f \otimes g \mapsto (m \otimes n \mapsto f(m) \otimes g(n)).$$

Exercice II.6.7 (Exactitude à droite du foncteur $\bullet \otimes N$). Soit M un A-module. Supposons que l'on ait une suite exacte

$$N' \xrightarrow{\phi} N \xrightarrow{\psi} N'' \longrightarrow 0.$$

Montrer que la suite

$$N' \otimes_A M \overset{\phi\otimes \mathrm{Id}_M}{\longrightarrow} N \otimes_A M \overset{\psi\otimes \mathrm{Id}_M}{\longrightarrow} N'' \otimes_A M \longrightarrow 0$$

est exacte.

On pourra pour cela utiliser le critère suivant : supposons que

$$(*) \quad L' \overset{\phi}{\longrightarrow} L \overset{\psi}{\longrightarrow} L'' \longrightarrow 0.$$

soit une suite de A-modules, que l'on ne suppose pas exacte. Alors $(*)$ est exacte si et seulement si pour tout A-module K,

$$(**) \quad 0 \longrightarrow \mathrm{Hom}_A(L'', K) \overset{\psi}{\longrightarrow} \mathrm{Hom}_A(L, K) \overset{\phi}{\longrightarrow} \mathrm{Hom}_A(L', K).$$

est exacte

Remarque II.6.8. Un A-module M tel que le foncteur $\bullet \otimes_A M$ is exact est dit plat.

Remarque II.6.9. Supposons qu'un problème nous demande de construire un morphisme f de A-module de la forme

$$M_1 \otimes_A M_2 \otimes_A \otimes M_r \longrightarrow N,$$

et que l'on ait une formule à proposer pour $f(m_1 \otimes \cdots \otimes m_r)$. Il faut alors donner un argument pour montrer que f est bien définie. La bonne manière de faire est d'utiliser la propriété uiverselle du produit tensoriel, et d'éviter la construction explicite de celui-ci. Il s'agit donc par exemple ici de définir une application multilinéaire $\bar{f} : M_1 \times M_2 \times M_r \longrightarrow N$, la vérification de la multilinéarité étant en général sans problème. A titre d'illustration, voir les exercices qui suivent.

Exercice II.6.10. Soient $A \to B$ et $A \to C$ des morphismes d'anneaux commutatifs. Montrer que le produit tensoriel $B \otimes_A C$ est muni canoniquement d'une structure de A-algèbre.

Exercice II.6.11. Soient $I, J \subset A$ deux idéaux de l'anneau commutatif A. Montrer que l'on a un isomorphisme de A-algèbres

$$(A/I) \otimes_A (A/J) \simeq A/(I + J).$$

En déduire $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$ pour tout couple d'entiers naturels non nuls (m, n).

Exercice II.6.12. Soient M un A-module et I un idéal de l'anneau commutatif A. Montrer que

$$M/IM \simeq M \otimes_A (A/I).$$

II.6.2 Restriction/Extension des scalaires

Soit $f : A \to B$ un morphisme d'anneaux commutatifs. L'application

$$A \times B \to B, \quad (a, b) \mapsto f(a)b$$

munit B d'une structure de A-module.

On peut donc, étant donné un A-module M, former le produit tensoriel $B \otimes_A M$ pour cette structure de A-module sur B (f a disparu de la notation, ce qui est ambigu mais plus léger). On munit alors $B \otimes_A M$ d'une structure de B-module par

$$B \times (B \otimes_A M) \longrightarrow B \otimes_A M, \quad (b, c \otimes m) \mapsto bc \otimes m.$$

et on appelle ce B-module l'extension des scalaires de A à B de M.

Exemple II.6.13. Soit V un $\mathbb{R}$ espace vectoriel. On prend pour morphisme f l'inclusion de $\mathbb{R}$ dans $\mathbb{C}$. La construction ci-dessus fournit un $\mathbb{C}$-espace vectoriel $V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V$ que l'on appelle la complexification de l'espace vectoriel V. Si $(e_i)_{i\in I}$ est une base du $\mathbb{R}$ espace vectoriel V, $(1 \otimes e_i)$ est une base du $\mathbb{C}$ espace vectoriel $V_{\mathbb{C}}$.

Dans l'autre sens, toujours grâce à $f : A \to B$, on peut munir un B-module N d'une structure de A-module par

$$A \times N \longrightarrow N, \qquad (a, n) \mapsto f(a) \cdot n$$

et l'on appelle ce A-module la restriction des scalaires de B à A du module N. On le note $\mathrm{res}^B_A(N)$ pour le plaisir d'être lourd.

Proposition II.6.14. *Soit M un A-module et N un B-module. On un un isomorphisme naturel*

$$\mathrm{Hom}_A(M, \mathrm{res}^B_A(N)) \simeq \mathrm{Hom}_B(B \otimes_A M, N)$$

Démonstration. Si $g \in \mathrm{Hom}_A(M, \mathrm{res}^B_A(N))$, définissons $G : B \times M \to N$ par $G(b, m) = b \cdot g(m)$. C'est une application bilinéaire, qui s'étend donc au produit tensoriel $B \otimes_A M$. Il est immédiat de voir que ceci réalise l'isomorphisme voulu. □

Exercice II.6.15. Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs et soit $P \in A[X]$. On note encore $\phi : A[X] \to B[X]$ le morphisme induit par ϕ en l'appliquant aux coefficients des polynômes. Montrer que l'on a un isomorphisme de B-algèbres

$$B \otimes_A (A[X]/(P)) \simeq B[X]/(\phi(P)).$$

Calculer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Est-ce un corps ? Même question avec $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

Exercice II.6.16. Soient A et B des anneaux commutatifs, soient M un A-module, P un B-module et N un (A, B)-bimodule (c'est-à-dire que N est is simultanément un A-module et un B-module et que les actions de A et B sur N commutent. Montrer que $M \otimes_A N$ est naturellement un B-module, et $N \otimes_B P$ un A-module, et que

$$(M \otimes_A N) \otimes_B P \simeq M \otimes_A (N \otimes_B P).$$

II.6.3 Produits tensoriels sur un anneau non commutatif

Le produit tensoriel sur un anneau non commutatif est plus délicat à définir. On y arrive tout de même, au prix de quelques adaptations.

Définition II.6.17. Soient M un A-module à droite et N un A-module à gauche et Z un $\mathbb{Z}$-module. On dit que $f \in \mathcal{L}_{\mathbb{Z}}(M \times N; Z)$ est *balancée* si $f(m \cdot a, n) = f(m, a \cdot n)$ quels que soient $a \in A$, $m \in M$ et $n \in N$.

On appelle produit tensoriel de M et N, et l'on note $M \otimes_A N$ un $\mathbb{Z}$-module et une application $\iota \in \mathcal{L}_{\mathbb{Z}}(M \times N; M \otimes_A N)$ bien balancée telle que toute application $f \in \mathcal{L}_{\mathbb{Z}}(M \times N; Z)$ se factorise en $\tilde{f} \circ \iota$ pour un unique $\tilde{f} \in \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, Z)$.

Comme dans le cas commutatif, et comme pour tout objet défini par une propriété universelle, $M \otimes_A N$ est caractérisé par cette propriété à isomorphisme près. La construction de $M \otimes_A N$ se fait comme dans le cas commutatif, en prenant le quotient de $\mathbb{Z}^{(M\times N)}$ par le sous-module engendré par les relations voulues. On passe les détails.

Proposition II.6.18. *Soient M un A-module à droite et N et L des A-modules à gauche. Le $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}}(N, L)$ est un A-module à droite par $(f \cdot a)(n) = f(a \cdot n)$. On a un isomorphisme naturel de $\mathbb{Z}$-modules*

$$\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbb{Z}}(N, L)) \simeq \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, L).$$

II.7 Lemme de Yoneda

Le lemme de Yoneda est un résultat de théorie des catégories. On en donne ici une version faible appliquée aux modules sur un anneau A, qui peut se révéler utile.

Théorème II.7.1 (Yoneda (version faible))**.** *Soit X et Y deux A-modules et supposons que pour tout A-module Z, on ait un isomorphisme naturel*

$$\Psi_Z : \mathrm{Hom}_A(X, Z) \simeq \mathrm{Hom}_A(Y, Z).$$

Alors X et Y sont isomorphes.

On a le même résultat avec des isomorphismes naturels

$$\Phi_Z : \mathrm{Hom}_A(Z, X) \simeq \mathrm{Hom}_A(Z, Y).$$

La naturalité des Ψ_Z signifie que si on a un morphisme $\eta : Z_1 \to Z_2$, alors on a un diagramme commutatif

$$\begin{array}{ccc} \mathrm{Hom}_A(X, Z_1) & \xrightarrow{\Psi_{Z_1}} & \mathrm{Hom}_A(Y, Z_1) \\ \downarrow{\scriptstyle \eta\circ\bullet} & & \downarrow{\scriptstyle \eta\circ\bullet} \\ \mathrm{Hom}_A(X, Z_2) & \xrightarrow{\Psi_{Z_2}} & \mathrm{Hom}_A(Y, Z_2) \end{array}$$

<u>*Démonstration*</u>. On utilise les isomorphismes

$$\Psi_X : \mathrm{Hom}_A(X, X) \simeq \mathrm{Hom}_A(Y, X), \quad \Psi_Y : \mathrm{Hom}_A(X, Y) \simeq \mathrm{Hom}_A(Y, Y).$$

et l'on note $\Psi_X(\mathrm{Id}_X) = f : Y \to X$ et $\Psi_Y^{-1}(\mathrm{Id}_Y) = g : X \to Y$.

La naturalité des Ψ_Z nous donne

$$\begin{array}{ccc} \mathrm{Hom}_A(X, X) & \xrightarrow{\Psi_X} & \mathrm{Hom}_A(Y, X) \\ \downarrow{\scriptstyle g\circ\bullet} & & \downarrow{\scriptstyle g\circ\bullet} \\ \mathrm{Hom}_A(X, Y) & \xrightarrow{\Psi_Y} & \mathrm{Hom}_A(Y, Y) \end{array}$$

et en partant de Id_X en haut à gauche, on obtient $\mathrm{Id}_Y = g \circ f$ en bas à droite. On obtient de même $\mathrm{Id}_X = f \circ g$. □

II.8 Interlude culturel : axiome du choix, lemme de Zorn, théorème de Krull

Dans cette section, nous rappelons l'énoncé de l'axiome du choix et nous donnons deux énoncés équivalents souvent utilisé en algèbre, le lemme de Zorn et le théorème de Krull.

Axiome du choix. L'axiome du choix est un axiome de la théorie des ensembles. Voici quelques formulations équivalentes.

(a) Pour tout ensemble X d'ensembles non vides, il existe une fonction de choix f sur X, c'est-à-dire qu'à tout ensemble E de X est associé un élément $f(E)$ de E.

(b) Pour toute ensemble E, il existe une fonction f sur $\mathcal{P}(E) \setminus \{\emptyset\}$ (l'ensemble des parties non vide de E) telle que pour tout $A \in \mathcal{P}(E) \setminus \{\emptyset\}$, $f(A) \in A$.

(c) Pour toute relation d'équivalence sur un ensemble, il existe un ensemble de représentants des classes.

(d) Toute surjection $p : X \to Y$ possède une section, c'est-à-dire une application $s : Y \to X$ telle que $p \circ s = \mathrm{Id}_Y$.

(e) Le produit $\prod_i X_i$ d'une famille d'ensembles non vide est non vide.

Lemme de Zorn. Un ensemble partiellement ordonné E est dit inductif quand toute partie S de E totalement ordonnée (ou chaîne) de E admet un majorant (c'est-à-dire un élément $M \in E$ tel que pour tout $s \in S$, $s \leq M$).

Le lemme de Zorn dit que tout ensemble inductif E admet un élément maximal, c'est-à-dire un élément $m \in E$ tel que si $x \geq m$ dans E, alors $x = m$.

Rappelons les définitions suivantes : un idéal (à gauche) d'un anneau A est propre s'il n'est pas égal à A. Un idéal (à gauche) est dit maximal si c'est idéal propre qui n'est contenu dans aucun autre idéal propre que lui-même.

Théorème de Krull. Tout idéal à gauche propre d'un anneau est contenu dans un idéal maximal.

On a des énoncés similaires avec les idéaux à droite, ou bilatères. Pour illustrer la façon dont on utilise le lemme de Zorn, donnons une preuve de ce théorème, dans le cas des idéaux à gauche par exemple, les autres cas étant similaires.

Démonstration. Fixonx un idéal propre J et considérons l'ensemble $\mathcal{P}$ des idéaux propres de A contenant J, ordonné par l'inclusion. Montrons que c'est un ensemble inductif. C'est un ensemble non vide car $J \in \mathcal{P}$. Soit $(I_j)_{j\in J}$ une chaîne dans $\mathcal{P}$. Il s'agit de montrer que $(I_j)_{j\in J}$ admet un majorant dans $\mathcal{P}$. Un majorant de la chaîne vide est l'idéal $\{0\}$. Si la chaîne n'est pas vide, le candidat pour être un majorant est $\mathscr{I} = \bigcup_{j\in J} I_j$. Montrons que c'est bien un élément de $\mathcal{P}$. Soient $x_1, x_2 \in \mathscr{I}$ et $x \in A$. Il existe $j_1, j_2 \in J$ avec $x_1 \in I_{j_1}$ et $x_2 \in I_{j_2}$. La propriété de chaîne dit que l'on a $I_{j_1} \subset I_{j_2}$ ou $I_{j_2} \subset I_{j_1}$. Disons que l'on est dans le premier cas. Alors $x_1 + x_2 \in I_{j_2} \subset \mathscr{I}$. Ceci montre que $\mathscr{J}$ est un sous-groupe additif de A. On a aussi $ax_1 \in I_{j_1} \subset \mathscr{I}$, ce qui montre que $\mathscr{I}$ est un idéal. Il est clair qu'il contient J. Le point crucial est bien sûr de montrer que $\mathscr{I}$ est un idéal propre. Si tel n'est pas le cas, alors $1 \in \mathscr{I}$. Mais alors Il existe $j_0 \in J$ avec $1 \in I_{j_0}$, ce qui contredit le fait que I_{j_0} est propre. Nous avons donc montré que $\mathscr{I} = \bigcup_{j\in J} I_j$ est un majorant de $(I_j)_{j\in J}$ dans $\mathcal{P}$, et cet ensemble est donc inductif. Par le lemme de Zorn, il contient un élément maximal $\mathfrak{m}$. □

Outre le théorème de Krull, des énoncés très importants en algèbre nécessitent l'axiome du choix.

Théorème de la base incomplète. Toute famille libre dans un espace vectoriel peut être complétée en une base, et de toute famille génératrice, on peut extraire une base.

Clôture algébrique d'un corps. Tout corps admet une clôture algébrique.

II.9 Modules noethériens, artiniens

II.9.1 Conditions de finitude

Définition II.9.1. Soit M un A-module. Si M admet une famille génératrice finie, on dit que M est *de type fini*.

Exercice II.9.2. Le but de cet exercice est de donner une définition équivalente de module de type fini qui ne fasse pas appel aux notions ensemblistes (éléments d'un ensemble) mais seulement aux notions « catégorielles » (les A-modules et leur morphismes).

Montrer que M est un module de type fini si et seulement si la propriété suivante est vérifiée.

(i) Soit $(M_i)_{i\in I}$ une famille de sous-modules de M telle que $\sum_{i\in I} M_i = M$. Alors il existe une partie finie $J \subset I$ telle que $\sum_{i\in J} M_j = M$.

On remarquera l'analogie de (i) avec la définition des compacts en topologie.

On appelle *chaîne* dans M une famille $(M_i)_{i\in I}$ de sous-modules totalement ordonnée pour l'inclusion (c'est-à-dire que pour $i, j \in I$, soit on a $M_i \subset M_j$, soit $M_j \subset M_i$). Considérons la propriété suivante :

(ii) Pour toute chaîne de sous-modules propres $(M_i)_{i\in I}$, $\sum_{i\in I} M_i$ est encore un sous-module propre.

Montrer que si M est de type fini, M vérifie (ii). La réciproque est vraie aussi, mais difficile.

Exercice II.9.3. Soit M un A-module de type fini et soit L un sous-module propre de M. Montrer qu'il existe un sous-module propre N de M contenant L et maximal pour l'inclusion avec ces deux propriétés. Indication : Zorn.

Définition II.9.4. Un A-module M est dit *noetherien* si tout ensemble non vide $\mathcal{U}$ de sous-modules de M admet un élément maximal, c'est-à-dire qu'il existe $M_0 \in \mathcal{U}$ tel que si $M_1 \in \mathcal{U}$ vérifie $M_0 \subset M_1$, alors $M_0 = M_1$.

Voici d'autres définitions équivalentes de cette notion.

Proposition II.9.5. *Le A-module M est noethérien si et seulement si l'une des deux conditions suivantes est vraie :*

(i) *tout sous-module de M est de type fini,*

(ii) *Toute suite croissante*

$$M_1 \subset M_2 \subset \ldots \subset M_n \subset \ldots$$

de sous-modules de M est stationnaire à partir d'un certain rang.

Démonstration. Montrons que (ii) implique que M est noethérien, en supposant que (ii) est vrai et qu'il existe un ensemble $\mathcal{U}$ non vide de sous-modules de M qui ne contient pas d'élément maximal pour l'inclusion. Prenons $M_1 \in \mathcal{U}$. Comme M_1 n'est pas maximal pour l'inclusion, il existe $M_2 \in \mathcal{U}$ tel que $M_1 \subsetneq M_2$. Mais M_2 n'est pas non plus maximal pour l'inclusion... On construit donc une suite infinie strictement croissante de sous-modules de M, ce qui contredit (ii).

Supposons M noethérien et montrons (i) : Soit M' un sous-module de M. Considérons l'ensemble $\mathcal{U}$ de tous les sous-module de type fini de M'. Cet ensemble admet un élément maximal, disons M_0. Pour tout $m \in M'$, le sous-module $M_0 + A \cdot m$ (le module engendré par M_0 et m) est de type fini, et donc par maximalité de M_0, on a $M_0 + A \cdot m = M_0$, c'est-à-dire $m \in M_0$, ce qui prouve que $M_0 = M'$, et M' est de type fini.

Supposons maintenant (i) et montrons (ii). Soit

$$M_1 \subset M_2 \subset \ldots \subset M_n \subset \ldots$$

une suite croissante de sous-modules. La réunion $M_\infty = \bigcup_{n\in\mathbb{N}_{>0}} M_n$ est un sous-module de M, donc de type fini. Soit $(m_1, \ldots, m_r)$ une famille finie génératrice de M_∞, et pour chaque m_i,

soit M_{n_i} l'un des sous-module de la suite avec $m_i \in M_{n_i}$. On a alors $M_\infty = \bigcup_{i=1,\dots,r} M_{n_i}$ ce qui montre que la suite de sous-modules est stationnaire à partir de $\max_{i=1,\dots,r} n_i$. □

Si l'on remplace le mot « maximal » par « minimal » dans la définition d'un module noethérien ci-dessus, on obtient la notion de module *artinien*. La caractérisation (ii) de la proposition se traduit en remplaçant « suite croissante de sous-modules » par « suite décroissante ».

Définition II.9.6. Un A-module M est dit artinien si tout ensemble non vide $\mathcal{U}$ de sous-modules de M admet un élément minimal, c'est-à-dire qu'il existe $M_0 \in \mathcal{U}$ tel que si $M_1 \in \mathcal{U}$ vérifie $M_1 \subset M_0$, alors $M_0 = M_1$.

De manière équivalente, un module est artinien si toute suite décroissante

$$M_1 \supset M_2 \supset \dots \supset M_n \supset \dots$$

de sous-modules de M est stationnaire à partir d'un certain rang.

L'équivalence se montre comme dans la proposition.

Exemples II.9.7. 1. Le $\mathbb{Z}$-module $\mathbb{Z}$ est noethérien, mais pas artinien,

2. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est ni noethérien, ni artinien.

3. Tout $\mathbb{Z}$-module de cardinal fini est noethérien et artinien.

4. Soit k un corps et A une k-algèbre. Tout A-module est aussi un k-espace vectoriel, et si M est un A-module de dimension finie comme k-espace vectoriel, alors M est noethérien et artinien.

Exercice II.9.8. 1. Montrer qu'un produit direct fini de A-modules noethériens (resp. artiniens) est noethérien (resp. artinien).

2. Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de A-modules. Montrer que M est noethérien (resp. artinien) si et seulement si M' et M'' sont noethériens (resp. artiniens).

Définition II.9.9. Un anneau A est noetherien, s'il est noetherien en tant que A-module à gauche. Autrement dit, toute suite croissante d'idéaux à gauche de A est stationnaire.

Théorème II.9.10. *Tout module de type fini sur un anneau noethérien est noethérien.*

Démonstration. Soit A un anneau noethérien, et soit M un A-module de type fini : Il existe $r \in \mathbb{N}_{>0}$ et un morphisme surjectif $A^r \to M$. Le module M est donc isomorphe à un module quotient de A^r. Or A^r est noethérien d'après l'exercice II.9.8, (1) et donc M est noethérien d'après le (2) du même exercice. □

Une classe importante d'anneaux noethériens est celle des anneaux commutatifs principaux, c'est-à-dire tel que tout idéal I de A est monogène (engendré par un seul élément). C'est le cas de $\mathbb{Z}$. On rappelle aussi le théorème de la base de Hilbert, déjà démontré (*cf.* Thm. I.7.1).

Théorème II.9.11 (Hilbert)**.** *Soit A un anneau commutatif noethérien. Alors l'anneau des polynômes $A[X]$ est noethérien.*

Exercice II.9.12. Soit $f : M \to M$ un endomorphisme de A-modules.

(a) On suppose M noethérien. Montrer que si f est surjectif, alors c'est un isomorphisme.

(b) On suppose M artinien. Montrer que si f est injectif, alors c'est un isomorphisme.

(c) (Lemme de Fitting) On suppose M noethérien et artinien. Montrer qu'il existe une décomposition

$$M = M_{-\infty} \oplus M_\infty$$

de M en somme directe de deux sous-modules stables par f, tels que la restriction de f à M_∞ soit un automorphisme, et la restriction de f à $M_{-\infty}$ soit nilpotente.

Remarque II.9.13. On peut particulariser le lemme de Fitting au cas où $A = k$ est un corps et $M = V$ est un k-espace vectoriel de dimension finie. Pour tout endomorphisme f de V, il existe une décomposition de V en somme directe

$$V = V_{-\infty} \oplus V_\infty$$

telle que la restriction de f à $V_{-\infty}$ soit nilpotente et la restriction à V_∞ inversible.

II.10 Modules indécomposables

Définition II.10.1. Un A-module M est décomposable s'il peut s'écrire comme somme directe $M = M' \oplus M''$ de deux sous-modules non nuls. Un A-module M non nul qui n'est pas décomposable est dit *indécomposable*. Un A-module M est dit *totalement décomposable* s'il peut s'écrire comme somme directe (éventuellement infinie) de sous-modules indécomposables.

Nous allons donner un critère pour qu'un module M soit indécomposable qui s'exprime par une propriété de l'anneau $\mathrm{End}_A(M)$.

Définition II.10.2. Un anneau E est dit *local* si $\mathscr{I} = E \setminus E^\times$ est un idéal bilatère.

Remarque II.10.3. On voit facilement que $\mathscr{I} = E \setminus E^\times$ contient tout idéal propre de E (un idéal propre ne contient pas d'inversible). Si $\mathscr{I} = E \setminus E^\times$ est un idéal bilatère, il est donc maximal, et c'est l'unique idéal bilatère maximal de E. La réciproque n'est pas vraie en général. Par exemple, si V est un espace vectoriel de dimension finie sur un corps k, alors les seuls idéaux bilatères de $\mathrm{End}_k(V)$ sont $\{0\}$ et $\mathrm{End}_k(V)$. Le seul idéal maximal est donc $\{0\}$ et $\mathrm{End}_k(V) \setminus \mathbf{GL}(V)$ n'est pas un idéal bilatère.

En revanche, si A est commutatif, alors tout élément non inversible engendre un idéal propre, et donc si A admet un seul idéal maximal $\mathfrak{M}$, on a $\mathfrak{M} = A \setminus A^\times$. Pour un anneau commutatif, on prend souvent cette caractérisation comme définition d'un anneau local.

Théorème II.10.4. *Soit M un A-module noethérien ou artinien. Si $\mathrm{End}_A(M)$ est un anneau local, alors M est indécomposable. Si l'on suppose M noethérien et artinien, la réciproque est vraie. Plus précisément, on a alors les équivalences suivantes :*

(i) le module M est indécomposable.

(ii) l'anneau $E = \mathrm{End}_A(M)$ est local.

Démonstration. Supposons que M ne soit pas indécomposable, on va montrer que $E = \mathrm{End}_A(M)$ n'est pas local. On a par hypothèse l'existence d'une décomposition non triviale $M = M' \oplus M''$. On a alors une décomposition

$$E = \mathrm{End}_A(M) = \begin{pmatrix} \mathrm{End}_A(M') & \mathrm{Hom}_A(M', M'') \\ \mathrm{Hom}_A(M'', M') & \mathrm{End}_A(M'') \end{pmatrix}$$

Posons $e' = \begin{pmatrix} \mathrm{Id}_{M'} & 0 \\ 0 & 0 \end{pmatrix}$ (c'est l'opérateur de projection sur M', il vérifie $e^2 = e$). De même $e'' = \mathrm{Id}_M - e'$ est l'opérateur de projection sur M''. Comme les décomposition sont non triviales, e' et e'' ne sont pas inversibles, mais leur somme l'est, puisque $\mathrm{Id}_M = e' + e''$. Ainsi $E \setminus E^\times$ n'est pas un idéal bilatère et E est non local. On a donc montré que $(ii) \implies (i)$.

Supposons M noethérien, artinien et indécomposable. D'après le lemme de Fitting, (exercice II.9.12), tout élément non nul de $E = \mathrm{End}_A(M)$ est soit nilpotent, soit inversible, et ainsi l'ensemble $\mathfrak{M} = E \setminus E^\times$ est l'ensemble des nilpotents de E. Montrons que c'est un idéal bilatère : soit $e \in \mathfrak{M}$ et $a \in E$. Comme e est nilpotent, on a d'après l'exercice II.9.12, $\ker(e) \neq \{0\}$ et $\mathrm{Im}\,(e) \neq E$, d où $\ker(ae) \neq \{0\}$ et $\mathrm{Im}\,(ea) \neq E$. Ainsi ea et ae ne sont pas inversibles, ils sont donc nilpotents, et $\mathfrak{M}$ est stable par multiplication à gauche et à droite par un élément de E. Il reste à montrer que $\mathfrak{M}$ est un sous-groupe additif de E. Si $e, e' \in \mathfrak{M}$ sont tels que $e + e'$ est inversible, il existe $c \in E$ avec $ec = 1_E - e'c$, et comme $ec' \in \mathfrak{M}$, il est nilpotent, et donc $1 - ec' = ec$ est inversible (d'inverse $\sum_{j=0}^{\infty}(ec')^j$) ce qui constitue une contradiction avec le fait que e soit nilpotent. □

On note $\mathrm{Indec}(A)$ l'ensemble des classes d'isomorphisme de A-modules indécomposables.

Théorème II.10.5 (Krull-Schmidt)**.** *Soit M un A-module noethérien ou artinien. Alors il existe une application à support fini*

$$\kappa : \mathrm{Indec}(A) \longrightarrow \mathbb{N}$$

tel que M soit isomorphe à la somme directe

$$\bigoplus_{N \in \mathrm{Indec}(A)} N^{\kappa(N)}.$$

Si M est à la fois noethérien et artinien, cette application κ est unique. On la note alors κ_M, et $\kappa_M(N)$ est la multiplicité du module indécomposable N dans M.

Démonstration. Montrons l'existence de la décomposition, par l'absurde. On suppose donc que M n'est pas totalement décomposable. En particulier, il n'est pas indécomposable, et il existe donc une décomposition

$$M = M_1^{(0)} \oplus M_2^{(0)}$$

où $M_1^{(0)}$ et $M_2^{(0)}$ ne sont pas tous les deux totalement décomposables, disons que $M_1^{(0)}$ ne l'est pas... on itère alors l'argument et l'on obtient des décompositions successives

$$M = M_1^{(1)} \oplus M_2^{(1)} \oplus M_2^{(0)}$$

$$\cdots$$

$$M = M_1^{(n+1)} \oplus M_2^{(n+1)} \oplus M_2^{(n)} \oplus \cdots \oplus M_2^{(1)} \oplus M_2^{(0)}$$

On obtient ainsi en particulier une suite strictement croissante de sous-modules

$$M_2^{(0)} \subset M_2^{(0)} \oplus M_2^{(1)} \subset \cdots \subset M_2^{(0)} \oplus M_2^{(1)} \oplus \cdots \oplus M_2^{(n)},$$

et une suite strictement décroissante de sous-modules

$$M_1^{(0)} \supset M_1^{(1)} \supset \cdots \supset M_1^{(n)},$$

ce qui contredit l'hypothèse faite sur M.

Supposons maintenant M noethérien et artinien, et montrons l'unicité de la décomposition.

Il suffit grâce à une récurrence simple de montrer le résultat suivant : si M, M', $N_1, \ldots, N_t$ sont des A-modules, avec M et les N_i indécomposables, et que l'on a un isomorphisme

$$M \oplus M' \simeq N = N_1 \oplus \cdots \oplus N_t$$

alors il existe un indice s entre 1 et t tel que

$$M \simeq N_s \text{ et } M' \simeq \bigoplus_{j \neq s} N_j.$$

Soit $\Phi = (\phi, \phi') : M \oplus M' \to N$ l'isomorphisme de l'énoncé, écrit sous forme matricelle, et $\Psi = \begin{pmatrix} \psi \\ \psi' \end{pmatrix} : N \to M \oplus M'$ son inverse. On note ι_i l'injection canonique de N_i dans N et p_i la projection canonique de N sur N_i. On a

$$\mathrm{Id}_N = \phi \circ \psi + \phi' \circ \psi', \quad \begin{pmatrix} \psi \circ \phi \\ \psi' \circ \phi' \end{pmatrix} = \begin{pmatrix} \mathrm{Id}_M \\ \mathrm{Id}_{M'} \end{pmatrix}$$

$$\mathrm{Id}_M = \psi \circ \phi = \sum_{i=1}^{t} \psi \circ \iota_i \circ p_i \circ \phi$$

D'après le théorème II.10.4, $E = \mathrm{End}_A(M)$ est un anneau local, et donc $E \setminus E^\times$ est un idéal bilatère. Ainsi au moins l'un des $\psi \circ \iota_i \circ p_i \circ \phi$ est inversible, disons $\chi = \psi \circ \iota_s \circ p_s \circ \phi \in E^\times$. On en déduit que $\psi \circ \iota_s$ est une surjection de N_s sur M et $p_s \circ \phi$ est une injection de M dans N_s. De plus $N_s = \mathrm{Im}\,(p_s \circ \phi) \oplus \ker(\psi \circ \iota_s)$. Comme N_s est indécomposable, on a donc $N_s = \mathrm{Im}\,(p_s \circ \phi)$ et $\ker(\psi \circ \iota_s) = \{0\}$, ce qui fournit l'isomorphisme entre N_s et M.

On a $\chi^{-1} \circ \psi \circ \iota_s \circ p_s \circ \phi = \mathrm{Id}_M$ et $p_s \circ \phi \circ \chi^{-1} \circ \psi \circ \iota_s = \mathrm{Id}_{N_s}$. On définit pour $j \neq s$, $\iota'_j : N_j \to M'$ et $p'_j : M' \to N_j$ par

$$\iota'_j = \psi' \circ \iota_j, \quad p'_j = p_j \circ (\mathrm{Id}_N - \phi \circ \chi^{-1} \circ \psi \circ \iota_s \circ p_s) \circ \phi'.$$

On vérifie que $p'_j \circ \iota'_j = \mathrm{Id}_{N_j}$:

$$p'_j \circ \iota'_j = p_j \circ (\mathrm{Id}_N - \phi \circ \chi^{-1} \circ \psi \circ \iota_s \circ p_s) \circ \phi' \circ \psi' \circ \iota_j.$$

On utilise $\phi' \circ \psi' = \mathrm{Id}_N - \phi \circ \psi$, ce qui donne

$$p'_j \circ \iota'_j = p_j \circ (\mathrm{Id}_N - \phi \circ \chi^{-1} \circ \psi \circ \iota_s \circ p_s) \circ (\mathrm{Id}_N - \phi \circ \psi) \circ \iota_j.$$

$$= p_j \circ \iota_j - p_j \circ \phi \circ \psi \circ \iota_j - p_j \circ \phi \circ \chi^{-1} \circ \psi \circ \iota_s \circ p_s \circ \iota_j + p_j \circ \phi \circ \chi^{-1} \circ \psi \circ \iota_s \circ p_s \circ \phi \circ \psi \circ \iota_j$$

Comme $p_j \circ \iota_j = \mathrm{Id}_{N_j}$, $p_s \circ \iota_j = 0$, $\chi^{-1} \circ \psi \circ \iota_s \circ p_s \circ \phi = \mathrm{Id}_M$, on obtient le résultat voulu. De même on vérifie que $p'_j \circ \iota'_i = 0$ si $i \neq j$. Enfin, on a

$$\sum_{j \neq s} \iota'_j \circ p'_j = \mathrm{Id}_{M'},$$

qui se vérifie de même en utilisant $\sum_{j \neq s} \iota_j \circ p_j = \mathrm{Id}_N - \iota_s \circ p_s$ et $\psi' \circ \phi = 0$. On en déduit aisément que $M' \simeq \bigoplus_{j \neq s} N_j$. □

Ce théorème présente un aspect satisfaisant : l'étude des A-modules se ramène à celle des modules indécomposables. Ceux-ci sont les blocs de base grâce auxquels tous les autres modules sont obtenus par somme directe. L'aspect moins satisfaisant est que les modules indécomposables peuvent avoir une structure interne compliquée, difficile à analyser. D'autre part, on ne connait une classification des modules indécomposables que dans très peu de cas, par exemple les anneaux semi-simples (voir exercice II.11.10), ou les anneaux de Dedekind, dont nous verrons un cas particulier, celui des anneaux principaux.

Exercice II.10.6. Soit F un corps fini, de cardinal disons q. On rappelle que pour chaque entier naturel n, le groupe $\mathbf{GL}_n(F)$ est d'ordre

$$\alpha_n = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}).$$

(i) Soient $k \leq n$ deux entiers naturels. Montrer qu'il y a exactement $\alpha_n/\alpha_k\alpha_{n-k}$ paires (X, Y) formées de deux sous-espaces vectoriels supplémentaires de F^n, tels que $\dim X = k$ et $\dim Y = n - k$.

(ii) Pour chaque entier naturel n, on note β_n le nombre de matrices nilpotentes dans $\mathcal{M}_n(F)$ (on convient que $\beta_0 = 1$). Montrer que

$$\sum_{k=0}^{n} \beta_k/\alpha_k = q^{n^2}/\alpha_n.$$

Indication : regardons les éléments de $\mathcal{M}_n(F)$ comme des endomorphismes de l'espace vectoriel $V = F^n$. D'après le lemme de Fitting, chaque élément $u \in \mathcal{M}_n(F)$ détermine une unique décomposition $V = V_\infty \oplus V_{-\infty}$ en somme directe de deux sous-espaces, sur lesquels u agit de façon respectivement inversible et nilpotente. Ainsi on atteint chaque élément $u \in \mathcal{M}_n(F)$ une et une seule fois en prenant une décomposition $V = X \oplus Y$, un endomorphisme nilpotent de X, et un élément de $\mathbf{GL}(Y)$.

(iii) En déduire que $\beta_n = q^{n(n-1)}$.

Exercice II.10.7. [Lemme de Nakayama]

a) Soit A un anneau commutatif et I un idéal qui est inclus dans tous les idéaux maximaux de A. Soit M un A-module de type fini. Supposons que $IM = M$. Montrer que l'on a $M = 0$.

b) Soient A un anneau commutatif local, $\mathscr{I}$ son ideal maximal, M un A-module de type fini et N un sous-module. Montrer que si $M = N + \mathscr{I} \cdot M$, alors $M = N$. En déduire que si $x_1, \dots, x_n$ sont des éléments de M tels que $\bar{x}_1, \dots, \bar{x}_n$ engendrent $M/\mathscr{I} \cdot M$, alors $x_1, \dots, x_n$ engendrent M.

c) Soient A un anneau commutatif local et M un A-module projectif de type fini. Montrer que M est libre.

II.11 Module simple. Suites de Jordan-Hölder

Définition II.11.1. On dit qu'un A-module M est simple s'il est non nul et si ses seuls sous-modules sont $\{0\}$ et M. Notons $\widehat{A}$ l'ensemble des classes d'isomorphisme de A-modules simples.

On dit qu'un module est complètement réductible s'il peut s'écrire comme une somme directe de sous-modules simples.

Les modules simples sont faciles à caractériser en termes d'idéaux maximaux. En effet, soit M un module simple et soit $0 \neq m \in M$. Considérons

$$p : A \to M, \quad a \mapsto a \cdot m.$$

Ce morphisme doit être surjectif, donc M est monogène, engendré par m. Si l'on pose $\mathfrak{M} = \ker(p)$, on a $A/\mathfrak{M} \simeq M$, et $\mathfrak{M}$ est un idéal à gauche maximal de A. En effet, si I est un idéal à gauche de A avec $\mathfrak{m} \subset I$, alors $I \cdot m$ est un sous-module de M, donc $I \cdot m = 0$, ou bien $I \cdot m = M$. Dans le premier cas, $I \subset \ker p$ donc $I = \mathfrak{m}$ et dans le second, il existe $a \in I$ tel que $a \cdot m = m$, d'où $1_A - a \in \mathfrak{m} \subset I$, donc $1_A \in I$, et $I = A$.

Définition II.11.2. On dit qu'un anneau E non nul est un anneau à division si tout élément non nul est inversible ($E \setminus \{0\} = E^\times$).

Un anneau à division est en particulier local, $\{0\} = A \setminus A^\times$ étant son unique idéal bilatère maximal.

Lemme II.11.3 (Lemme de Schur)**.** *Si M et M' sont deux A-modules simples, alors on est dans l'une des deux situations suivantes :*

- M et M' ne sont pas isomorphes, et alors $\mathrm{Hom}_A(M, M') = \{0\}$.

- M et M' sont isomorphes : on fixe un isomorphisme $\phi : M \simeq M'$. Tout morphisme $\psi \in \mathrm{Hom}_A(M, M')$ est alors de la forme $\psi = \chi \circ \phi$ avec $\chi \in \mathrm{End}_A(M)$, ce qui fournit un isomorphisme de groupes abéliens

$$\mathrm{Hom}_A(M, M') \simeq \mathrm{End}_A(M).$$

De plus, $E = \mathrm{End}_A(M)$ est un anneau à division.

Si A est une k-algèbre sur un corps k algébriquement clos et si M est un A-module simple avec $\dim_k M$ *finie, alors* $\mathrm{End}_A(M) = \{\lambda \times \mathrm{Id}_M,\ \lambda \in k\}$.

<u>*Démonstration*</u>. L'image et le noyau d'un morphisme de A-module sont des sous-modules, et tout se déduit facilement de là. Pour le second point, on utilise le fait qu'un endomorphisme k-linéaire d'un espace vectoriel de dimension finie admet une valeur propre et un sous-espace propre non trivial si k est algébriquement clos. □

Exercice II.11.4. Montrer que si E est une k-algèbre à division de k-dimension finie, k algébriquement clos, alors $E = k$.

Corollaire II.11.5. *Soit $M = \bigoplus_{i=1}^t M_i^{\oplus n_i}$ un A-module somme directe de modules simples M_i deux à deux non isomorphes. On a alors un isomorphisme canonique d'anneaux*

$$\mathrm{End}_A(M) \simeq \prod_{i=1}^t \mathcal{M}_{n_i}(\mathrm{End}_A(M_i)).$$

On retiendra les implication suivantes, avec pour la flèche verticale de droite, l'hypothèse supplémentaire que M est artinien ou noetherien :

$$\begin{array}{ccc} M \text{ simple} & \Longrightarrow & M \text{ indécomposable} \\ \Downarrow & & \Uparrow \\ \mathrm{End}_A(M) \text{ anneau à division} & \Longrightarrow & \mathrm{End}_A(M) \text{ anneau local} \end{array}$$

Proposition II.11.6. *Soit M un A-module. Alors M admet deux sous-modules $M_1 \subset M_2$ tels que le quotient M_2/M_1 soit simple. Si M est de type fini, alors M admet un quotient simple.*

<u>*Démonstration*</u>. Supposons M de type fini. Considérons l'ensemble $\mathcal{P}$ des sous-modules propres de M, ordonné par inclusion. Pour pouvoir appliquer le lemme de Zorn, vérifions que si $(N_i)_{i\in I}$ est une chaîne dans $\mathcal{P}$, alors leur union $\cup_i N_i$ est encore un sous-module propre, qui est bien sûr un majorant de $(N_i)_{i\in I}$ (un majorant de la chaîne vide est le sous-module $\{0\}$). Il est facile de vérifier que $\cup_i N_i$ est un sous-module (grâce à la propriété de chaîne). Supposons $M = \cup_i N_i$. Comme M est de type fini, tout ses générateurs sont dans un certain N_{i_0} (encore grâce à la

propriété de chaîne), et l'on a alors $M = \cup_i N_i = N_{i_0}$, ce qui contredit le fait que N_{i_0} est propre. Ainsi S est inductif. Il admet un élément maximal N. Le quotient M/N est alors simple.

Si M n'est pas de type fini, on considère un sous-module M_2 de type fini de M, et l'on vient de montrer qu'il existe un sous-module M_1 de M_2 tel que M_2/M_1 est simple. □

Lemme II.11.7. *Soit M un A-module. Les conditions suivantes sont équivalentes :*

(i) il existe des modules simples M_i, $i \in I$, tels que $M = \sum_{i\in I} M_i$,

(ii) il existe des modules simples M_j, $j \in J$, tels que $M = \bigoplus_{j\in J} M_j$ (cette propriété est la complète réductibilité),

(iii) pour tout sous-module M' de M, il existe un sous-module M'' tel que $M = M' \oplus M''$ (cette propriété est la semi-simplicité).

On dit alors que M est semi-simple ou complètement réductible, ces deux propriétés étant équivalentes.

Démonstration. Il est clair que $(ii) \implies (i)$. Supposons (i) et montrons (iii). Soit M' un sous-module de M. On peut, d'après l'hypothèse, écrire M comme une somme (mais pas directe) de sous-objets,

$$M = \sum_{i\in I} M_i$$

pour un certain ensemble d'indices I.

Considérons l'ensemble $\mathcal{S}$ des sous-modules N de M de la forme $N = \sum_{k\in K} M_k$, $K \subset I$, tel que la somme $F = M' + \sum_{k\in K} M_k$ soit directe. Constatons que $\mathcal{S}$ contient le sous-module trivial $\{0\}$. Ordonnons $\mathcal{S}$ par l'inclusion, et montrons que c'est un ensemble inductif. Soit $(N_j)_{j\in J}$ une chaîne non vide dans $\mathcal{S}$ et montrons que $\mathcal{N} = \bigcup_j N_j$ est un majorant de cette chaîne dans $\mathcal{S}$. (la chaîne vide est majoré par $\{0\} \in \mathcal{S}$). On montre facilement en utilisant la propriété de chaîne que $\mathcal{N}$ est un sous-module, et il est bien de la forme $\mathcal{N} = \sum_{k\in\mathscr{K}} M_k$ (l'ensemble $\mathscr{K}$ est la réunion des ensembles d'indices K_j dans les écritures $N_j = \sum_{k\in K_j} M_k$, $j \in J$). Le point crucial est de montrer que $M' + \sum_{k\in\mathscr{K}} M_k$ est une somme directe. Supposons que l'on ait une relation

$$m' + \sum_{k\in\mathscr{K}} m_k = 0,$$

où $m' \in M'$ et $m_k \in M_k$, $k \in \mathscr{K}$ tous nuls sauf un nombre fini. Chaque m_k non nul est dans un N_{j_k} pour un $j_k \in J$ et la propriété de chaîne fait que ils sont tous dans un $N_{j_0} = \sum_{k\in K_{j_0}} M_k$ fixé. La relation est donc dans $M' + N_{j_0}$ et comme la somme $M' + \sum_{k\in K_{j_0}} M_k$ est directe, $m' = 0$ et $\sum m_k = 0$. Ceci montre que $\mathcal{N}$ est un majorant de la chaîne $(N_j)_{j\in J}$ dans $\mathcal{S}$. On peut donc appliquer le lemme de Zorn : un sous-module de M de la forme $\sum_{j\in J} M_j$, $J \subset I$, maximal pour l'inclusion et tel que la somme $F = M' + \sum_{j\in J} M_j$ soit directe. Alors cette somme est égale à M. En effet, il suffit de voir que chaque M_i, $i \in I$, est dans $F = M' \oplus (\bigoplus_{j\in J} M_j)$. Comme l'intersection de F avec M_i est un sous-module de M_i, cette intersection est M_i ou 0 puisque M_i est simple. Si cette intersection était nulle, on pourrait adjoindre i à J ce qui contredit la maximalité de J. Donc $M_i \subset F$. Montrons maintenant que (iii) implique (ii). Commençons par voir que M admet alors un sous-module simple. Soit M' un sous-module de M de type fini. Considérons l'ensemble S des sous-modules propres de M', ordonné par l'inclusion. Nous avons vu dans la démonstration de la proposition II.11.6 que cet ensemble est inductif, et donc qu'il admet d'après le lemme de Zorn un élément maximal N. Cet N est un sous-module de M. D'après l'hypothèse, on peut écrire $M = N \oplus F$, pour un certain sous-module F. On a alors

$$M' = N \oplus (M' \cap F).$$

Comme N est maximal dans M', $M' \cap F$ est simple. Ceci montre que M admet un sous-module simple. Soit maintenant M_0 une somme directe maximale de sous-modules simples de M. Si $M \neq M_0$, on écrit $M = M_0 \oplus F$. On applique maintenant la remarque précédente à F : il existe un sous-objet simple de F. Ceci contredit la définition de M_0. □

Corollaire II.11.8. *Tout sous-quotient d'un module complètement réductible est complètement réductible.*

Démonstration. Soit M un A-module complètement réductible et soit N un sous-module. Soit L un sous-module de N. D'après le lemme, L admet un supplémentaire dans M, disons $M = L \oplus F$, et on a alors $N = L \oplus (F \cap N)$. Ceci montre que tout sous-module de N admet un supplémentaire, et par le lemme, on sait que N est alors complètement réductible.

D'autre part l'image de tout module simple de M par la projection canonique $p : M \to M/N$ est soit un module simple, soit 0. Comme M est complètement réductible, on en déduit que M/N aussi. L'énoncé général avec un sous-quotient est conséquence immédiate des énoncés pour un sous-module et un module quotient. □

Exercice II.11.9. Soit $0 \to M' \to M \to M''' \to 0$ une suite exacte courte de A-modules. Montrer que si M est semi-simple, il en est de même de M' et M''. La réciproque est-elle vraie ?

Exercice II.11.10. Montrer que les conditions suivantes sur l'anneau A sont équivalentes :

(a) tout A-module M est semi-simple,

(b) le A-module régulier A est semi-simple.

On dit alors que A est un anneau semi-simple.

Exercice II.11.11. Soit A un anneau à division. Montrer que le seul A-module simple est le module régulier A. En déduire que tout A-module est libre et semi-simple.

Exercice II.11.12 (Théorème de Maschke). Soit G un groupe fini et k un corps dont la caractéristique ne divise pas $|G|$. Montrer que tout $k[G]$-module est semi-simple. Ceci reste-il vrai sans l'hypothèse sur la caractéristique de k ?

II.11.1 Suites de composition et théorème de Jordan-Hölder

Soit M un A-module. On appelle *filtration* de M une suite décroissante finie de sous-modules

$$M = F_0(M) \supset F_1(M) \supset \cdots \supset F_n(M) \supset F_{n+1}(M).$$

Le *gradué associé* à cette filtration est le module :

$$\mathrm{Gr}_F(M) = \bigoplus_{i=1}^{n} F_i(M)/F_{i+1}(M).$$

On dit que la filtration $F_\bullet(M)$ comme ci-dessus est une *suite de composition* de M si les quotients $F_i(M)/F_{i+1}(M)$ sont simples. Le module gradué $\mathrm{Gr}_F(M)$ est alors semi-simple.

On associe à une telle suite de composition une fonction de multiplicité.

$$m_F : \widehat{A} \to \mathbb{N}$$

définie comme suit : on se rappelle que $\widehat{A}$ est l'ensemble des classes d'isomorphisme de A-modules simples. Si $S \in \widehat{A}$, $m_F(S)$ est le nombre de modules simples $F_i(M)/F_{i+1}(M)$ dans le gradué qui sont dans la classe S.

Théorème II.11.13 (Jordan-Hölder)**.** *Soit M un A-module noethérien et artinien. Alors M admet une suite de composition. De plus, deux suites de composition $F_\bullet(M)$ et $F'_\bullet(M)$ ont même fonction de multiplicité : $m_F = m_{F'}$.*

Puisque la fonction multiplicité m_F et le gradué $\mathrm{Gr}_F(M)$ ne dépendent pas de la suite de composition choisie, on les note plutôt respectivement m_M et $\mathrm{Gr}(M)$. La longueur de la suite de composition ne dépend pas non plus de celle-ci, on dit que le module M est de longueur finie, cette longueur étant celle d'une de ses suites de composition, ou encore la somme des multiplicités des modules simples dans M.

Le théorème dit que M est formé à partir des modules simples (avec leur multiplicité) dans une suite de composition, mais la structure de M est en général bien plus compliquée qu'une somme directe. On peut comparer le résultat avec le théorème de Krull-Schmidt : dans ce théorème nous avions obtenu une décomposition dont la structure est transparente (une somme directe), mais les modules indécomposables peuvent eux avoir une structure assez compliquée, en particulier ils peuvent être assez gros et on ne dispose que de peu de résultats de classification des indécomposables. En revanche, dans le théorème de Jordan-Hölder, les modules simples (au sens mathématiques) sont des objets dont la structure est accessible, mais la façon dont un module M est constitué de module simples peut être subtile.

Exemple II.11.14. Considérons la k-algèbre A des matrices triangulaires supérieures dans $\mathcal{M}_n(k)$ (k est un corps), et pour M, prenons le module k^n. Notons $(e_1, \ldots, e_n)$ la base canonique de k^n. On a une filtration de k^n donnée par $F_{n-i+1}(k^n) = \langle e_1, \ldots, e_i \rangle$, et les quotients successifs, étant de dimension 1, sont simples. C'est donc une suite de composition, dont le gradué associé est encore isomorphe à k^n. Mais l'action d'une matrice de A sur un élément du gradué ne se fait que par sa diagonale (le passage aux quotients successifs tue l'action des coefficients au dessus de la diagonale).

Remarque II.11.15. Les hypothèses du théorème de Jordan-Hölder sont importantes : le $\mathbb{Z}$-module $\mathbb{Z}$ n'est pas artinien et il n'admet pas de suite de composition finie.

Lemme II.11.16 (du papillon)**.** *Soit M un A-module et soient $M_2 \subset M_1$ et $N_2 \subset N_1$ des sous-modules de M. On a alors un isomorphisme canonique :*

$$\frac{M_2 + (M_1 \cap N_1)}{M_2 + (M_1 \cap N_2)} \simeq \frac{N_2 + (N_1 \cap M_1)}{N_2 + (N_1 \cap M_2)}.$$

Démonstration. Considérons la restriction de la projection canonique

$$\pi : M \longrightarrow \frac{M}{M_2 + (M_1 \cap N_2)}$$

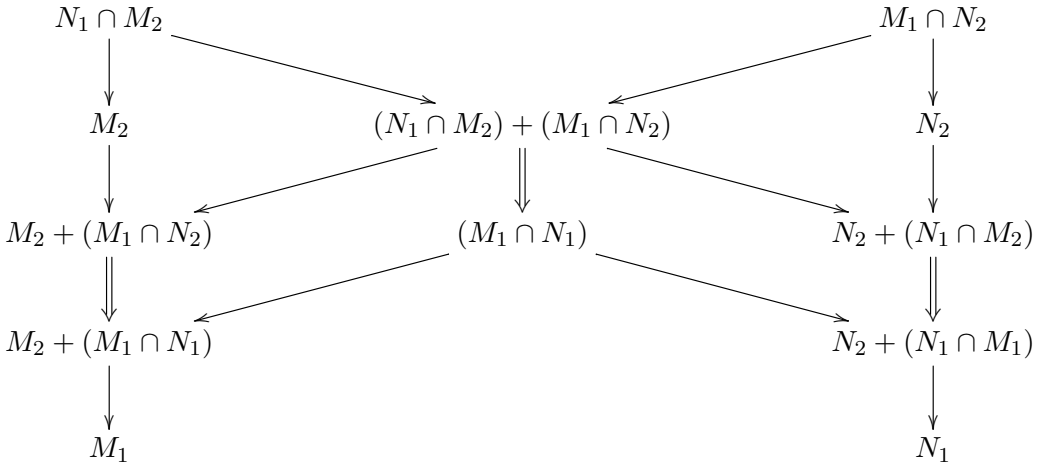
à $M_1 \cap N_1$. Le noyau est $M_1 \cap N_1 \cap (M_2 + (M_1 \cap N_2)) = (M_2 \cap N_1) + (M_1 \cap N_2)$ et l'image est $\dfrac{M_2 + (M_1 \cap N_1)}{M_2 + (M_1 \cap N_2)}$. On obtient donc par le premier théorème d'isomorphisme

$$\frac{M_1 \cap N_1}{(M_2 \cap N_1) + (N_1 \cap M_2)} \simeq \frac{M_2 + (M_1 \cap N_1)}{M_2 + (M_1 \cap N_2)}.$$

On conclut en échangeant le rôle des M_i et des N_i qui est symétrique. □

Le diagramme suivant explique le nom du lemme et montre que les mathématiciens sont

parfois des poètes. Les doubles flèches indiquent les inclusions donnant des quotients isomorphes.



On passe maintenant à la démonstration du théorème.

Démonstration. Montrons l'existence d'une suite de composition. Notons $\mathcal{S}$ l'ensemble des sous A-modules de M possédant une suite de composition. L'ensemble $\mathcal{S}$ est non-vide puisqu'il contient 0. Comme M est noethérien, $\mathcal{S}$ possède donc un élément M_0, maximal pour l'inclusion. Supposons $M_0 \neq M$. L'ensemble $\mathcal{S}_0$ des sous A-modules de M contenant strictement M_0 est non-vide puisqu'il contient M. Comme M est artinien, $\mathcal{S}_0$ possède donc un élément M_{00}, minimal pour l'inclusion. Mais par construction M_{00}/M_0 est un A-module simple donc, comme M_0 possède une suite de composition, M_{00} aussi : cela contredit la maximalité de M_0.

Soient $F_\bullet(M)$ et $F'_\bullet(M)$ deux suites de composition de M. Posons

$$F_{i,j} = (F_i(M) \cap F'_j(M)) + F_{i+1}, \quad F'_{j,i} = (F'_j(M) \cap F_i(M)) + F'_{j+1},$$

On a

$$\cdots \supset F_{i-1,n'+1} = F_i(M) = F_{i,0} \supset F_{i,1} \supset \cdots \supset F_{i,j} \supset F_{i,j+1} \supset \ldots \supset F_{i,n'+1} = F_{i+1}(M) = F_{i+1,0} \supset \cdots$$

$$\cdots \supset F'_{j-1,n+1} = F'_j(M) = F'_{j,0} \supset F'_{j,1} \supset \cdots \supset F'_{j,i} \supset F'_{j,i+1} \supset \ldots \supset F'_{j,n+1} = F'_{j+1}(M) = F'_{j+1,0} \supset \cdots$$

Comme $F_i(M)/F_{i+1}(M)$ est simple, il existe un unique $j = j(i) \in \{0, \ldots, n'\}$ tel que $F_{i,j}/F_{i,j+1} = F_i(M)/F_{i+1}(M)$, les autres quotients étant nuls, et idem pour la seconde filtration, chaque j détermine un unique $i = i(j)$. On voit facilement que ceci détermine deux bijections inverses l'une de l'autre entre les ensembles $\{0, , \ldots, n\}$ et $\{0, , \ldots, n'\}$ On a alors $F_i(M) = F_{i,j}$ et $F_{i+1}(M) = F_{i,j+1}$. En outre, le lemme du papillon donne alors

$$F_i(M)/F_{i+1}(M) = F_{i,j}/F_{i,j+1} = F'_{j,i}/F'_{j,i+1} = F'_j(M)/F'_{,j+1}(M).$$

□

Chapitre III

Modules de type fini sur un anneau principal

Dans ce chapitre nous allons décrire, à isomorphisme près, tous les A-modules de type fini sur un anneau principal (donc en particulier commutatif et intègre).

Nous allons donner deux approches différentes de ce résultat. La première est basée sur le théorème de Krull-Schmidt II.10.5, un résultat d'injectivité pour l'analyse de la partie de torsion et une réduction à la partie de torsion.

La seconde approche, plus élémentaire, passe par un théorème de réduction des matrices (Théorème III.4.1) et le théorème de la base adaptée. Remarquons que dans la première approche, on déduit le théorème de la base adaptée et celui de réduction des matrices du théorème de classification des modules. Ces trois résultats sont donc essentiellement équivalents.

On peut lire indépendamment les deux approches, c'est-à-dire les sections III.1 et III.2 d'une part, ou bien les sections III.3, III.4,III.5 et III.6 d'autre part. Il est intéressant de comparer les deux approches et de voir dans quel ordre sont démontrés les résultats intermédiaires.

On passe ensuite aux applications : structure des groupes abéliens de type fini (section III.7) et algèbre linéaire (section III.8).

III.1 Décomposition des modules de type fini I

Soit M un module de type fini sur l'anneau principal A. Rappelons que nous avons introduit en II.4 le sous-module $\mathrm{Tor}_A(M)$ des éléments de torsion de M. On a donc une suite exacte courte

$$1 \longrightarrow \mathrm{Tor}_A(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}_A(M) \longrightarrow 0 \tag{III.1.1}$$

où le module $M/\mathrm{Tor}_A(M)$ est sans torsion et de type fini.

Nous allons montrer que cette suite se scinde, et donne une décomposition

$$M = \mathrm{Tor}_A(M) \oplus L$$

où $L \simeq M/\mathrm{Tor}_A(M)$ est sans torsion. Nous montrerons aussi qu'un module sans torsion sur un anneau principal est libre. Ainsi M est somme directe d'un module libre et de son module de torsion. Dans la section suivante, nous analyserons la structure de $\mathrm{Tor}_A(M)$.

Lemme III.1.1. *Soit A un anneau commutatif intègre et soit M un module de type fini sans torsion. Alors M est sous-module d'un module libre.*

Démonstration. Soit $(m_1, \ldots, m_r)$ un système de générateur de M. Le morphisme

$$A^r \longrightarrow M, \quad (a_1, \ldots, a_r) \mapsto \sum_{i=1}^{r} a_i \cdot m_i$$

est donc surjectif. Soit $\mathcal{S}$ l'ensemble des parties $I \in \{1, \ldots, r\}$ telles que le morphisme

$$A^{(I)} \to M, \quad (a_i)_{i \in I} \mapsto \sum_{i \in I} a_i \cdot m_i$$

soit injectif. Remarquons que $\mathcal{S}$ contient les singletons, puisque M est supposé sans torsion. Il existe donc un élément maximal pour l'inclusion dans $\mathcal{S}$, disons J. Soit N le sous-module engendré par les m_j, $j \in J$. Par construction $N \simeq A^{(J)}$ est libre. Si $i \notin J$, il existe $a_i \in A \setminus \{0\}$ tel que $a_i \cdot m_i \in N$. En effet, si tel n'était pas le cas, on pourrait rajouter i à l'ensemble J et contredire la maximalité de J dans $\mathcal{S}$. On pose alors $a = \prod_{i \notin J} a_j$, et a est non nul car A est intègre. Considérons

$$M \to M, \quad m \mapsto a \cdot m$$

Ce morphisme est injectif car M est sans torsion. De plus il est à valeurs dans N. En effet on écrit $m = \sum_{k=1}^{r} b_k \cdot m_k = \sum_{k \in J} b_k \cdot m_k + \sum_{k \notin J} b_k \cdot m_k$ et

$$a \cdot m = \sum_{k \in J} (ab_k) \cdot m_k + \sum_{k \notin J} (ab_k) \cdot m_k$$

la première somme est dans le sous-module N, et chaque terme de la seconde aussi. Ainsi M s'injecte dans le module libre N. □

Théorème III.1.2. *Soit A un anneau principal, et soit M un module libre de rang n sur A. Alors tout sous-module N de M est libre de rang plus petit ou égal à n.*

Démonstration. Par convention, le module $\{0\}$ est libre de rang 0. Si $n = 0$, le résultat est donc vrai. On raisonne par récurrence sur n. On suppose donc $n > 0$ et le résultat vrai pour les modules libres de rang $\leq n - 1$. Soit M libre de rang n, de base $(e_1, \ldots, e_n)$. Soit M' le sous-module engendré par $(e_2, \ldots, e_n)$: il est libre de rang $n-1$. Soit N un sous-module de M. Si $N \subset M'$, on applique l'hypothèse de récurrence : N est libre de rang $\leq n-1$. Sinon, il existe $y \in N$, $y \notin M'$. Soit $\mathscr{I}$ l'ensemble des $b \in A$ tels qu'il existe $x \in M'$ avec $be_1 + x \in N$. Il est clair que c'est un idéal de A et il est non nul. On a donc $\mathscr{I} = (d)$ pour un certain $d \in A$ non nul et il existe $f_1 = de_1 + x_1 \in N$ avec $x_1 \in M'$. Considérons $N \cap M'$: c'est un sous-module de M', par hypothèse de récurrence, il est libre, disons de base $(f_2, \ldots, f_m)$ avec $m - 1 \leq n - 1$. Montrons que $(f_1, f_2, \ldots, f_m)$ est une base de N. Tout élément de N s'écrit $be_1 + y$ avec $b \in (d)$ et $y \in M'$. On écrit $b = kd$. On a

$$(be_1 + y) - kf_1 = kde_1 + y - k(de_1 + x_1) = y - kx_1 \in (M' \cap N)$$

et donc $(be_1 + y) - kf_1$ est dans le sous-module engendré par $(f_2, \ldots f_m)$ et $be_1 + y$ est dans le sous-module engendré par $(f_1, \ldots f_m)$. Autrement dit $(f_1, \ldots, f_m)$ engendre N. Montrons que $(f_1, f_2, \ldots, f_m)$ est une famille libre : supposons $\sum_{i=1}^{n} k_i f_i = 0$ On a donc

$$k_1 de_1 + k_1 x_1 + \sum_{i=2}^{n} k_i f_i = 0$$

avec $k_1 x_1 + \sum_{i=2}^{n} k_i f_i \in M'$, donc une combinaison linéaire des $e_2, \ldots, e_n$. Ceci donne une relation entre les e_i, d'où l'on déduit que $k_1 d = 0$, d'où $k_1 = 0$. On a alors $\sum_{i=2}^{n} k_i f_i = 0$ et donc tous les k_i sont nuls. □

Revenons à un module de type fini M sur l'anneau principal A. Les deux résultats précédents nous disent que le module $M/\mathrm{Tor}_A(M)$ est libre, disons de rang r, donc isomorphe à A^r. Un module libre étant projectif (voir exercice II.5.19), la suite exacte courte (III.1.1) est scindée, et ainsi on a bien

$$M = \mathrm{Tor}_A(M) \oplus L,$$

où $L \simeq M/\mathrm{Tor}_A(M) \simeq A^r$ est un module libre de rang r.

Exercice III.1.3. Soit A un anneau principal et soient M un module libre de type fini sur A, et N un sous-module. Montrer que N admet un supplémentaire dans M si et seulement si M/N est sans torsion.

III.2 Décomposition des modules de type fini II

Il reste à analyser le module $\mathrm{Tor}_A(M)$. Remarquons deux choses. Premièrement, A est principal, donc noethérien, et M est de type fini sur un anneau noethérien, donc noethérien (*cf.* Théorème II.9.10), et le sous-module $\mathrm{Tor}_A(M)$ est de type fini. Pour la suite de l'étude, on peut donc supposer sans perdre de généralité que $M = \mathrm{Tor}_A(M)$.

Proposition III.2.1. *Supposons M de type fini et de torsion sur l'anneau principal A. Alors M est artinien.*

Démonstration. En effet, soit $(m_1, \ldots, m_n)$ une famille génératrice finie de M. Pour chaque $i \in \{1, \ldots, n\}$ il existe un élément non-nul $a_i \in A$ tel que $a_i \cdot m_i = 0$. Alors $a = a_1 \ldots a_n$ annule chaque m_i, donc annule tous les éléments de M. Le morphisme surjectif de A-modules

$$A^n \to M, \quad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i \cdot m_i$$

se factorise par A^n/aA^n. Nous allons voir juste après que A/aA est artinien. Ainsi M est un quotient du module artinien A^n/aA^n ; c'est donc un module artinien (*cf.* exercice II.9.8).

Il reste à voir que A/aA est artinien. Les sous-modules de A/aA sont donnés par les idéaux bA de A contenant aA, c'est-à-dire par les diviseurs de a. L'anneau A étant factoriel, il n'y a qu'un nombre fini d'idéaux bA contenant aA. □

Corollaire III.2.2. *Soit M un A-module de type fini et de torsion sur l'anneau principal A. Alors M admet une décomposition en somme directe de modules indécomposables (et encore de torsion et de type fini).*

Démonstration. Les hypothèses du théorème de Krull-Schmidt sont en effet satisfaites. Un sous-module d'un module de torsion est encore de torsion, ceci découle immédiatement de la définition, et A est principal donc noethérien, et tout sous-module est de type fini. □

Les modules de type fini, de torsion indécomposables sur un anneau principal admettent une caractérisation explicite.

Proposition III.2.3. *Soit M un module de type fini, de torsion et indécomposable. Alors il existe un unique idéal premier non-nul $\mathfrak{p}$ de A et un unique entier $n \geq 1$ tels que $M \simeq A/\mathfrak{p}^n$. Réciproquement, les modules de la forme $A/\mathfrak{p}^n$ avec $\mathfrak{p}$ idéal premier sont de type fini, de torsion et indécomposables.*

Démonstration. Rappelons que l'annulateur d'un A-module M est l'idéal $\mathrm{Ann}(M) = \{a \in A \,|\, \forall m \in M,\, a \cdot m = 0\}$ de A. Pour chaque $m \in M$, notons μ_m un générateur de l'idéal $\mathrm{Ann}(m) = \{a \in A \,|\, a \cdot m = 0\}$.

Lemme III.2.4. *Il existe un élément $m \in M$ tel que $\mathrm{Ann}(M) = (\mu_m) = \mathrm{Ann}(m)$.*

Démonstration. Dans un anneau factoriel, on définit facilement grâce à la décomposition en facteurs irréductibles ce qu'est le *plus petit commun multiple* (PPCM) d'une famille finie d'éléments $a_1, \dots a_r$. Il est unique et défini à un inversible près. En termes d'idéaux, un tel plus petit commun multiple est un générateur de l'idéal $\bigcap_{i=1,\dots,r}(a_i)$. On choisit un système de générateurs fini $m_1, \dots m_r$ de notre module M, et l'on a donc une famille finie $\mu_{m_1}, \dots, \mu_{m_r}$ d'éléments de A, et il est clair que

$$\mathrm{Ann}(M) = \bigcap_{i=1,\dots,r} \mathrm{Ann}(m_i) = \bigcap_{i=1,\dots,r} (\mu_{m_i}) = \mathrm{PPCM}((\mu_{m_i})_{i=1,\dots r}).$$

Il reste à montrer que l'on peut trouver un élément $m \in M$ tel que μ_m soit un PPCM des μ_{m_i}. Par une récurrence évidente, il suffit de montrer que si m', $m'' \in M$, il existe $m \in M$ tel que μ_m soit un PPCM de $\mu_{m'}$ et $\mu_{m''}$. Pour cela, on utilise la décomposition en produit d'éléments irréductibles de $\mu_{m'}$ et $\mu_{m''}$ pour trouver des factorisations $\mu_{m'} = c'd'$ et $\mu_{m''} = c''d''$ de sorte que c' et c'' soient premiers entre eux et que leur produit soit un PPCM de $\mu_{m'}$ et $\mu_{m''}$. Écrivons une égalité de Bézout $b'c' + b''c'' = 1$ et posons $m = d'm' + d''m''$. Tout multiple commun de $\mu_{m'}$ et $\mu_{m''}$ annule m. Réciproquement, si a annule m, alors $ad'm' = -ad''m''$, et donc $ad'm' = (b'c' + b''c'')ad'm' = b'c'ad'm' - b''c''ad''m'' = ab'\mu_{m'}m' - ab''\mu_{m''}m'' = 0$, ce qui montre que ad' est un multiple de $\mu_{m'}$ et que ad'' est un multiple de $\mu_{m''}$. Ainsi a est un multiple commun de c'et c'', donc est un multiple de leur produit, lequel est un PPCM de $\mu_{m'}$ et $\mu_{m''}$ par construction. Les éléments de A annulant m sont donc les multiples communs de $\mu_{m'}$ et de $\mu_{m''}$: nous avons bien $\mu_m = \mathrm{PPCM}(\mu_{m'}, \mu_{m''})$. □

Regardons maintenant l'homomorphisme $A \mapsto a \cdot m$ du A-module à gauche régulier dans M. Son image est le sous-module $A \cdot m$ engendré par m, son noyau est $(\mu_m) = \mathrm{Ann}(M)$. Nous disposons ainsi d'une suite exacte courte

$$0 \longrightarrow A/\mathrm{Ann}(M) \longrightarrow M \longrightarrow M/A \cdot m \longrightarrow 0.$$

Appelons B l'anneau quotient $A/\mathrm{Ann}(M)$ et notons $a \mapsto \bar{a}$ la projection canonique. Le A-module M peut être vu comme un B-module, car l'homomorphisme de A dans $\mathrm{End}_{\mathbb{Z}}(M)$ définissant la structure de A-module de M se factorise à travers B ; le sous-module de M engendré par m est le même, que l'on regarde M comme un module sur A ou sur B et la suite exacte ci-dessus peut donc être vue comme une suite exacte de B-modules

$$0 \longrightarrow B \longrightarrow M \longrightarrow M/B \cdot m \longrightarrow 0. \tag{III.2.1}$$

La suite exacte ci dessus est scindée, en effet, plus généralement, on a le résultat suivant :

Lemme III.2.5. *Soit A un anneau principal et $B = A/I$ où I est un idéal non nul de A, Alors toute suite exacte de B-modules*

$$0 \longrightarrow B \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

est scindée.

Autrement dit, le B-module régulier B est *injectif*. Cette notion est duale de celle de module projectif étudiée en II.5.4.

Démonstration. Introduisons l'ensemble $\mathcal{E}$ des couples (u, N) où N est un sous-B-module de M contenant $m = f(1)$, et u est un morphisme de B-modules de N dans B tel que $u(m) = 1$. On munit $\mathcal{E}$ de la relation d'ordre définie par $(u_1, N_1) \leq (u_2, N_2)$ si $N_1 \subset N_2$ et si la restriction de u_2 à N_1 est égale à u_1. Remarquons que $\mathcal{E}$ est non vide. En effet, le morphisme $B \to B \cdot m$ induit un isomorphisme $v : B \simeq B \cdot m$, et l'on a $(v^{-1}, B \cdot m) \in \mathcal{E}$. Par définition, $\mathcal{E}$ est un ensemble ordonné inductif, et d'après le lemme de Zorn, il contient un élément maximal, disons (u_0, N_0). On raisonne par l'absurde en supposant que $N_0 \neq M$. On prend alors $y \in M \setminus N_0$, et l'on étend u_0 en

$$u_1 : N_0 + B \cdot y \to B$$

en fixant judicieusement la valeur de $u_1(y)$, ce qui contredira la maximalité de (u_0, N_0). On identifie B-modules et A-modules annulés par I.

On introduit l'idéal

$$J = \{\bar{b} \in B | \, \bar{b} \cdot y \in N_0\}.$$

Soit $\mu \in A$ un générateur de l'idéal I, de sorte que $B = A/(\mu)$. On a donc $J = (b_0)/(\mu)$, avec b_0 diviseur de μ : il existe $\alpha \in A$ avec $\alpha b_0 = \mu$. Comme $\bar{b}_0 \cdot y \in N_0$, on pose $u_0(b_0 \cdot y) = \bar{c} \in B$. On a $u_0(\mu.y) = 0 = \alpha\bar{c}$, et ainsi $\alpha c = q\mu = q\alpha b_0$ pour un certain q dans A. Comme A est intègre, on a $c = qb_0$. On a donc obtenu

$$u_0(\bar{b}_0 \cdot y) = \bar{c} = \bar{q}\bar{b}_0.$$

Il est donc naturel de poser $u_1(y) = \bar{q}$ et donc par linéarité

$$u_1(n + \bar{b} \cdot y) = u_0(n) + \bar{b}\bar{q}, \quad (\bar{b} \in B,\, n \in N_0).$$

Il s'agit maintenant de voir que u_1 est bien défini et ne dépend pas de la décomposition dans $N_0 + B \cdot y$. On suppose donc que l'on a deux écritures $n_1 + \bar{b}_1 \cdot y = n_2 + \bar{b}_2 \cdot y$. On veut donc vérifier que $u_1(n_1 + \bar{b}_1 \cdot y) = u_1(n_2 + \bar{b}_2 \cdot y)$, ou encore $u_1(n_1 - n_0) = u_1((\bar{b}_2 - \bar{b}_1) \cdot y)$ c'est-à-dire, si $n = \bar{b} \cdot y \in N_0 \cap B \cdot y$, alors $u_0(n) = \bar{b}\bar{q}$. Or $\bar{b} \in J$, donc $\bar{b} = \beta\bar{b}_0$ et $\bar{b}\bar{q} = \beta\bar{b}_0\bar{q} = \beta u_0(b_0 \cdot y) = u_0(\beta\bar{b}_0 \cdot y) = u_0(n)$. Ceci montre que u_1 est bien défini. Nous sommes parvenu à la contradiction voulue. On a donc $N_0 = M$ et l'existence du morphisme $u_0 : M \to B$ avec $u_0(m) = 1$ montre que la suite (III.2.1) est scindée (*cf.* exercice II.3.1). □

Revenons à la démonstration de la proposition. On a donc, en tant que B-modules, $M \simeq B \oplus (M/B \cdot m)$, et en tant que A-module,

$$M \simeq A/\mathrm{Ann}(M) \oplus (M/A \cdot m).$$

Cela montre que si M est un A-module de torsion, de type fini et décomposable, alors $M \simeq A/\mathrm{Ann}(M)$. Nous avons ainsi montré qu'un A-module M de type fini, de torsion et indécomposable est nécessairement isomorphe à un module A/I, où I est un idéal non-nul de A. De plus, la donnée de M détermine I, car $I = \mathrm{Ann}(M)$.

Lemme III.2.6. *Le module A/I est indécomposable si et seulement si I est une puissance strictement positive d'un idéal premier.*

Si $a = up_1^{\alpha_1} \dots p_n^{\alpha_n}$ est la décomposition d'un élément non-nul $a \in A$ en produit d'un élément inversible u et de puissances $p_i^{\alpha_i}$ d'éléments irréductibles distincts, alors il y a un isomorphisme de A-modules (lemme des restes chinois)

$$A/(a) \simeq A/(p_1^{\alpha_1}) \oplus \dots \oplus A/(p_n^{\alpha_n}).$$

Pour que $A/(a)$ soit un A-module indécomposable, il est donc nécessaire que la décomposition de a en produit de puissances d'éléments irréductibles fasse intervenir exactement un facteur. La condition est aussi suffisante. De fait, soit (p) un idéal premier et $n \geq 1$ un entier. Soit B l'anneau $A/(p^n)$. C'est un anneau local, car il possède un unique idéal maximal, à savoir $(p)/(p^n)$. Identifiant le A-module $A/(p^n)$ au B-module régulier, nous obtenons l'égalité $\mathrm{End}_A(A/(p^n)) = \mathrm{End}_B(B) \simeq B$. L'anneau des endomorphismes du module $A/(p^n)$ est donc local : le module est indécomposable (*cf.* théorème II.10.4). Ceci conclut la démonstration de la proposition. □

Corollaire III.2.7. *Soit M un A-module de type fini et de torsion. Alors il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ de A et des entiers strictement positifs $\alpha_1, \ldots, \alpha_s$ tels que*

$$M \simeq \bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{\alpha_i}.$$

Si l'on préfère, on écrit ceci en prenant des générateurs irréductibles p_i des idéaux premiers $\mathfrak{p}_i$ et l'on a

$$M \simeq \bigoplus_{i=1}^{s} A/(p_i^{\alpha_i}).$$

A permutation près, la suite $((\mathfrak{p}_i, \alpha_i)_{i=1,\ldots s})$ est unique.

L'unicité provient du théorème de Krull-Schmidt. On peut en utilisant le lemme des restes chinois mettre le résultat sous la forme suivante

Corollaire III.2.8. *Soit M un A-module de type fini. Alors il existe une suite unique d'idéaux propres*

$$I_1 \supset I_2 \supset \cdots \supset I_k$$

de A tels que

$$M \simeq \bigoplus_{i=1}^{s} A/I_k.$$

Si l'on préfère, on écrit ceci en prenant des générateurs $d_i \in A$ des idéaux $\mathfrak{p}_i$ et l'on a

$$M \simeq \bigoplus_{i=1}^{s} A/(d_i),$$

avec d_i divisant d_{i+1} pour tout $i = 1, \ldots, k-1$.

La suite d'idéaux $I_1 = (d_1) \supset \cdots \supset I_k = (d_k)$ s'appelle la suite des invariants du A-module M. Remarquons que nous n'avons pas supposé M de torsion. La partie libre de M est obtenue en prenant la somme des facteurs avec $(d_i) = I_i = 0$ apparaissant à la fin de la suite des invariants.

<u>Démonstration</u>. On peut supposer que M est de torsion et partir de la décomposition du corollaire III.2.7. Notons $\mathcal{P}(M)$ l'ensemble des idéaux premiers $\mathfrak{p}$ de A contribuant non trivialement à la décomposition de M. La composante $\mathfrak{p}$-primaire $M_\mathfrak{p}$ de M est la somme

$$M_\mathfrak{p} \simeq \bigoplus_{j|\mathfrak{p}_j=\mathfrak{p}} A/\mathfrak{p}_j^{\alpha_j} \subset \bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{\alpha_i} \simeq M$$

et M est somme directe de ses composantes $\mathfrak{p}$-primaires. Ecrivons la composante $\mathfrak{p}$-primaire sous la forme

$$M_\mathfrak{p} \simeq \bigoplus_{j \leq r_\mathfrak{p}} A/\mathfrak{p}^{\beta_{\mathfrak{p},j}}$$

avec une suite finie $(\beta_{\mathfrak{p},j})$ décroissante d'entiers strictement positifs.

On pose alors $J_1 = \bigcap_{\mathfrak{p}\in\mathcal{P}(M)} \mathfrak{p}^{\beta_{\mathfrak{p},1}}$ (c'est-à-dire que si pour chaque $\mathfrak{p} \in \mathcal{P}(M)$, on choisit un générateur $p \in A$ irréductible ($\mathfrak{p} = (p)$), J_1 est l'idéal engendré par le PPCM des $p^{\beta_{\mathfrak{p},1}}$ et comme ils sont premiers entre eux, ce PPCM est leur produit). On pose ensuite $J_2 = \bigcap_{\mathfrak{p}\in\mathcal{P}(M),\, r_\mathfrak{p}\geq 2} \mathfrak{p}^{\beta_{\mathfrak{p},2}}$, et ainsi de suite, $J_\ell = \bigcap_{\mathfrak{p}\in\mathcal{P}(M),\, r_\mathfrak{p}\geq \ell} \mathfrak{p}^{\beta_{\mathfrak{p},\ell}}$, jusqu'à épuisement de tous les facteurs indécomposables. On obtient ainsi une suite croissante d'idéaux

$$J_1 \subset J_2 \subset \cdots \subset J_s$$

avec

$$A \simeq \bigoplus_{i=1}^{s} A/J_k,$$

et l'on pose $I_i = J_{s-i+1}$. L'unicité vient de l'unicité dans le théorème de Krull-Schmidt.

Exercice III.2.9. Soit A un anneau commutatif principal. Soient $(p_1), \ldots, (p_r)$ des idéaux premiers distincts et $n_1, \ldots, n_r$ des entiers strictement positifs. Montrer que $A/(p_1^{n_1} \cdots p_r^{n_r})$ est semi-simple si et seulement si tous les n_i sont égaux à 1.

Exercice III.2.10. Soit M un module de type fini et de torsion sur l'anneau principal A. Pour tout idéal premier $\mathfrak{p} = (p)$, notons $M_\mathfrak{p} = \{m \in M | \, \exists n \in \mathbb{Z}_{>0}, p^n \cdot m = 0\}$. Montrer que $M_\mathfrak{p}$ est la composante $\mathfrak{p}$-primaire de M définie dans la démonstration du corollaire III.2.8 Montrer que M est somme directe des $M_\mathfrak{p}$ lorsque $\mathfrak{p}$ décrit tous les idéaux premiers (seuls un nombre fini de $M_\mathfrak{p}$ sont non-nuls).

Exercice III.2.11. (Théorème de la base adaptée). Soit M un A-module libre de rang n (A principal). Soit N un sous-module. Le but est de montrer qu'il existe une unique suite d'idéaux $I_1 = (d_1) \supset \cdots \supset I_s = (d_s)$, $s \leq n$, de A et une base $(m_1, \ldots, m_n)$ de M tels que $(d_1 \cdot m_1, \ldots, d_s \cdot m_s)$ soit une base de N.

1. Montrer l'unicité dans l'énonce ci-dessus (en admettant l'existence).

Nous allons montrer le résultat d'existence par récurrence sur n.

2. Traiter le cas $n = 1$. Traiter aussi le cas $N = \{0\}$ pour n quelconque.

On suppose maintenant $n > 1$ et $N \neq \{0\}$.

3. Notons $\mathcal{E} = \{\lambda(N),\ \lambda \in \mathrm{Hom}_A(M, A)\}$. Montrer que $\mathcal{E}$ admet un élément $I_1 = (d_1)$ maximal pour l'inclusion, avec d_1 non nul.

4. Fixons $\lambda_1 \in \mathrm{Hom}_A(M, A)$ avec $\lambda_1(N) = I_1 = (d_1)$ et n_1 in N avec $\lambda_1(n_1) = d_1$. Montrer que pour tout $\mu \in \mathrm{Hom}_A(M, A)$, $\mu(n_1) \in I_1 = \lambda_1(N)$.

5. Fixons une base $(e_i)_i$ de M et écrivons $n_1 = \sum_i \alpha_i \cdot e_i$. Montrer que tous les α_i sont divisibles par d_1.

En déduire qu'il existe $m_1 \in M$ avec $d_1 \cdot m_1 = n_1$ et $\lambda_1(m_1) = 1$. En déduire que $M = A \cdot m_1 \oplus \ker \lambda_1$ et $N = A \cdot d_1 \cdot m_1 \oplus (\ker \lambda_1 \cap N)$.

6. Appliquer l'hypothèse de récurrence à $M' = \ker \lambda_1$ et $N' = M' \cap N$, et conclure.

III.3 Matrices à coefficients dans A

Nous allons maintenant exposer la seconde approche, basée sur un théorème de réduction des matrices. On commence par des considérations générales. Ici A est un anneau commutatif. On note $\mathcal{M}_{m,n}(A)$ l'espace des matrices à coefficients dans A à m lignes et n colonnes. On note simplement $\mathcal{M}_n(A)$ pour $\mathcal{M}_{n,n}(A)$ (matrices carrées). Nous allons énoncer quelques faits simples. Les démonstrations sont évidentes où identiques à celles où $A = k$ est un corps.

— $\mathcal{M}_{m,n}(A)$ est un module libre de rang mn sur l'anneau A.
— La multiplication des matrices

$$\mathcal{M}_{m,n}(A) \times \mathcal{M}_{n,k}(A) \longrightarrow \mathcal{M}_{m,k}(A), \quad (M,N) \mapsto MN$$

est définie par les mêmes formules que dans le cas des corps. Cette multiplication est associative : si $M \in \mathcal{M}_{m,n}(A)$, $N \in \mathcal{M}_{n,k}(A)$, $P \in \mathcal{M}_{k,\ell}(A)$ alors $(MN)P = M(NP) \in \mathcal{M}_{m,\ell}(A)$.
— $\mathcal{M}_n(A)$, muni de l'addition et de la multiplication des matrices est un anneau, l'élément neutre de la multiplication est I_n, la matrice identité.
— Le déterminant d'une matrice M de $\mathcal{M}_n(A)$ est défini par la même formule algébrique que dans le cas des corps. Pour une matrice $M = (m_{i,j})_{1\leq i,j\leq n}$,

$$\det M = \sum_{\sigma\in\mathfrak{S}_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)} \right)$$

— La transposée d'une matrice $M = (m_{i,j}) \in \mathcal{M}_{m,n}(A)$ est la matrice $N = (n_{ij}) \in \mathcal{M}_{n,m}(A)$ où quels que soient i, j, $n_{ij} = m_{ji}$. On la note ${}^tM$.
— La comatrice d'une matrice M de $\mathcal{M}_n(A)$ est défini par la même formule algébrique que dans le cas des corps, avec les déterminants mineurs extraits. On la note $\operatorname{Com}(M)$.
— Si M est une matrice de $\mathcal{M}_n(A)$, on a la formule

$$M\ {}^t\operatorname{Com}(M) = \det(M) \cdot I_n$$

En particulier, M est inversible dans $\mathcal{M}_n(A)$ si et seulement si $\det(M)$ est une unité dans A, l'inverse étant donnée par

$$M^{-1} = (\det M)^{-1} \quad {}^t\operatorname{Com}(M)$$

Le groupe (multiplicatif) des matrices inversibles d'ordre n à coefficients dans A est noté $\mathbf{GL}(n, A)$. Le sous-groupe distingué formé des matrices de déterminant 1 est noté $\mathbf{SL}(n, A)$.
— Deux matrices M et N de $M \in \mathcal{M}_{m,n}(A)$ sont dites équivalentes s'il existe $P \in \mathbf{GL}(m, A)$ et $Q \in \mathbf{GL}(n, A)$ telles que $N = PMQ$. Ceci définit une relation d'équivalence sur $M \in \mathcal{M}_{m,n}(A)$.

On démontre maintenant le théorème célèbre suivant :

Théorème III.3.1 (Cayley-Hamilton)**.** *Soit M un A-module de type fini et soit $u : M \to M$ un endomorphisme.*

Si $m_1, \ldots, m_n$ sont des générateurs de M, on peut écrire $u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$, où la matrice $R = (a_{ij})_{1\leq i,j\leq n}$ est dans $\mathcal{M}_n(A)$. Posons $\chi_u(X) = \det(XI_n - R) \in A[X]$. Alors $\chi_u(u) = 0$ dans $\operatorname{End}_A(M)$.

Remarque III.3.2. Attention à la terminologie toutefois, on aimerait appeler χ_u le polynôme caractéristique de u, mais si M n'est pas un A-module libre de base $(m_1, \ldots, m_n)$, il n'y a pas unicité des a_{ij} (la famille $(m_1, \ldots, m_n)$ n'est pas libre), donc χ_u n'est pas uniquement déterminé. Bien sûr, si M est un A-module libre de base $(m_1, \ldots, m_n)$ (par exemple si $A = k$ est un corps, alors il n'y a pas de problème, et on appelle χ_u le polynôme caractéristique de u.

Démonstration. Munissons M d'une structure de $A[X]$-module en posant

$$\forall Q \in A[X], \quad \forall m \in M, \qquad Q \cdot m := Q(u)(m).$$

On a alors

$$(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

où $XI_n - R$ est une matrice carrée d'ordre n à coefficients dans $A[X]$. En multipliant cette égalité à gauche par ${}^t\mathrm{Com}(XI_n - R)$, on obtient

$$\det(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

ce qui implique que $\chi_u(X) = \det(XI_n - R)$ annule le $A[X]$-module M, ou encore que $\chi_u(u)$ est nul sur M. □

Remarque III.3.3. Il est important de remarquer que si I est un idéal de A tel que $u(M) \subset IM$, on peut prendre les a_{ij} dans I (le choix des a_{ij} n'est en général pas unique et on verra dans les applications qu'il est parfois crucial de le faire de façon astucieuse !). En effet par hypothèse, $u(m_i) \in IM$, c'est-à-dire que $u(m_i) = \sum_{k=1}^{\ell} c_{ik} y_k$, avec $c_k \in I$ et $y_k \in M$. On écrit ensuite les y_k comme combinaison linaire des m_j, c'est-à-dire $y_k = \sum_{j=1}^{n} b_{kj} m_j$. On a alors

$$u(m_i) = \sum_{k=1}^{\ell} \sum_{j=1}^{n} c_{ik} b_{kj} m_j = \sum_{j=1}^{n} a_{ij} m_j$$

où $a_{ij} = \sum_{k=1}^{\ell} c_{ik} b_{kj} \in I$. D'après le théorème de Cayley-Hamilton $\chi_u = \det(XI_n - R)$ annule u. Mais si on développe le déterminant, il s'écrit $q_0 + q_1 X + \ldots q_{n-1} X^{n-1} + q_n X^n$, avec les q_j dans I (et on a même $q_j \in I^{n-j}$).

Corollaire III.3.4. *Soit M un A-module de type fini. Tout endomorphisme surjectif de M est bijectif*[1].

Démonstration. Soit $f : M \to M$ un endomorphisme surjectif. Comme dans la preuve du théorème, on munit M d'une structure de $A[X]$-module en posant $X \cdot m = f(m)$. Comme f est surjectif, on a $M = IM$, où $I = (X)$. On applique alors le théorème de Cayley-Hamilton à $u = \mathrm{Id}_M$ vu comme endomorphisme de $A[X]$-modules (et non pas de A-modules), sous la forme de la remarque III.3.3. On a alors l'existence d'un polynôme $q_0 + q_1 Y + \ldots q_{n-1} Y^{n-1} + q_n Y^n$, avec les q_j dans I, qui annule u (Attention, c'est un polynôme en Y à coefficients dans $A[X]$).

On en déduit l'égalité suivante dans $\mathrm{End}_A(M)$:

$$0 = P(u) = u^n + q_{n-1} u^{n-1} + \cdots + q_1 u + q_0 \mathrm{Id}_M,$$

avec $q_j \in I^{n-j} = (X^{n-j})$. En écrivant $q_j = X r_j$, on obtient

$$\begin{aligned} \forall m \in M \qquad 0 &= (u^n + q_{n-1} u^{n-1} + \cdots + q_1 u + q_0 \mathrm{Id}_M)(m) \\ &= m + q_{n-1} \cdot m + \cdots + q_1 \cdot m + q_0 \cdot m \\ &= m + q_{n-1}(f)(m) + \cdots + q_1(f)(m) + q_0(f)(m) \\ &= m + f \circ (r_{n-1}(f) + \cdots + r_1(f) + r_0(f))(m), \end{aligned}$$

1. Comparer avec exercice II.9.12

c'est-à-dire $\mathrm{Id}_M + f \circ r(f) = 0$ pour un polynôme $r \in A[X]$. L'endomorphisme $-r(f)$ de M est l'inverse de f. □

Corollaire III.3.5. *Soit M un A-module libre de rang n. Toute famille génératrice de M à n éléments est une base de M.*

Démonstration. On peut supposer $M = A^n$. Une famille génératrice $\mathcal{B}$ à n éléments définit un endomorphisme surjectif $A^n \to A^n$. Le cor. III.3.4 dit qu'il est bijectif, donc $\mathcal{B}$ est une base de M. □

Exercice III.3.6. Soit M un A-module de type fini et soit I un idéal tel que $IM = M$. Montrer qu'il existe $a \in I$ tel que $a \cdot m = m$ pour tout $m \in M$.

Exercice III.3.7. Soit A un anneau. Soit I un idéal de type fini de A tel que $I^2 = I$. Montrer que I est engendré par un élément $e \in A$ tel que $e^2 = e$ (on dit que e est un *idempotent* de A).

III.4 Réduction des matrices à coefficients dans un anneau principal

Dans cette section, A est un anneau principal. Etant donnée une matrice M à coefficients dans A, le problème que nous nous posons est celui de trouver une matrice équivalente à M la plus simple possible. On sait qu'une matrice M de rang r à coefficients dans un corps est équivalente à la matrice par blocs

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Le théorème qui suit est une version de ce résultat pour les matrices à coefficients dans A.

Théorème III.4.1. *Soit M une matrice (non nécessairement carrée) à coefficients dans un anneau principal A. Il existe des matrices inversibles P et Q à coefficients dans A et des éléments non nuls $d_1, \ldots, d_r$ de A vérifiant $d_1 \mid \cdots \mid d_r$, tels que*

$$PMQ = \begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & 0 & & \\ & & d_r & & & & \\ & & & 0 & & & \\ & 0 & & & \ddots & & \\ & & & & 0 & \cdots & 0 \end{pmatrix}.$$

L'entier r est uniquement déterminé. Les éléments $d_1, \ldots, d_r$ de A sont aussi uniquement déterminés, à multiplication par une unité de A près ; on les appelle les facteurs invariants *de la matrice M.*

Bien sûr, l'entier r est le rang de la matrice M vue comme matrice à coefficients dans le corps des fractions de A. On peut voir ce théorème comme la description des *classes d'équivalence* des matrices à coefficients dans un anneau principal. Il est beaucoup plus difficile de déterminer les *classes de similitude* (on sait le faire lorsque A est un corps grâce aux invariants de similitude, on verra ça plus loin).

Avant de commencer la preuve de ce théorème, faisons quelques rappels sur les *opérations élémentaires.* Par « opération élémentaire » sur les lignes (resp. sur les colonnes), nous entendrons uniquement ici « ajouter un multiple d'une ligne (resp. d'une colonne) à une autre ».

Cela correspond à multiplier à gauche (resp. à droite) la matrice d'origine par une *matrice élémentaire,* c'est-à-dire une matrice qui ne diffère de la matrice identité que par un seul coefficient, situé hors de la diagonale. Une matrice élémentaire est inversible (son déterminant est 1) donc on obtient après des opérations élémentaires une matrice équivalente à la matrice d'origine (et de même déterminant). Nous noterons

$$E(n, A) < \mathbf{SL}(n, A)$$

le sous-groupe engendré par les matrices élémentaires.

Avec des opérations élémentaires, on peut aussi échanger deux lignes, l'une d'elles étant changée en son opposé :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \longrightarrow \begin{pmatrix} L_i \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix}$$

(On ne peut pas juste échanger deux lignes, puisque le déterminant est inchangé par nos opérations élémentaires).

Lemme III.4.2. *Soit A un anneau principal et soient $a_1, \ldots, a_s$ des éléments de A. Il existe une matrice carrée d'ordre s à coefficients dans A dont la première ligne est $\begin{pmatrix} a_1 & \cdots & a_s \end{pmatrix}$ et dont le déterminant est un pgcd de $a_1, \ldots, a_s$.*

<u>Démonstration</u>. (du lemme) On raisonne par récurrence sur s, le cas $s = 1$ étant évident. Supposons $s \geq 2$. Par hypothèse de récurrence, il existe donc une matrice carrée N d'ordre $s-1$ de première ligne $\begin{pmatrix} a_2 & \cdots & a_s \end{pmatrix}$ et de déterminant $d = a_2 \wedge \cdots \wedge a_s$. Soient x et y des éléments de A tels que

$$a_1 \wedge a_2 \wedge \cdots \wedge a_s = a_1 \wedge d = a_1 x + dy.$$

La matrice

$$\begin{pmatrix} a_1 & & & \\ 0 & & N & \\ \vdots & & & \\ 0 & & & \\ (-1)^{s-1} y & (-1)^s a_2 x/d & \cdots & (-1)^s a_s x/d \end{pmatrix}$$

convient alors. □

On remarquera que la construction d'une matrice obéissant aux conditions du lemme est le seul endroit où la preuve du théorème III.4.1 n'est pas « algorithmique » (sauf dans le cas où A est un anneau euclidien ; voir exercice. III.4.4).

<u>Démonstration</u>. (du théorème) Le lemme entraîne facilement le théorème dans le cas où M est une matrice ligne (ou colonne), que l'on peut supposer non nulle : si $M = \begin{pmatrix} m_1 & \cdots & m_s \end{pmatrix}$ et $d = m_1 \wedge \cdots \wedge m_s$ (non nul), il existe $a_1, \ldots, a_s$ dans A tels que $d = a_1 m_1 + \cdots + a_s m_s$ et $a_1, \ldots, a_s$ sont premiers entre eux dans leur ensemble. Il existe donc d'après le lemme une matrice inversible Q dont la première colonne est $\begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix}$. Le produit MQ s'écrit alors

$$MQ = \begin{pmatrix} d & b_2 & \cdots & b_s \end{pmatrix},$$

où d divise chacun des b_i. En effectant des opérations élémentaires sur les colonnes de MQ, on arrive à la matrice

$$\begin{pmatrix} d & 0 & \cdots & 0 \end{pmatrix},$$

ce qui montre l'existence d'une réduction dans ce cas. On raisonne de même en transposant tout dans le cas où M est une matrice colonne.

Traitons le cas général, en raisonnant par récurrence sur la taille de la matrice. Par le processus décrit ci-dessus, on se ramène à une matrice dont la première ligne est du type $\begin{pmatrix} d^{(1)} & 0 & \cdots & 0 \end{pmatrix}$ puis, en procédant de façon analogue, on peut aussi supposer que la première colonne est de ce type. Cela détruit la forme de la première ligne, donc on recommence le processus. On obtient ainsi alternativement des matrices de première ligne ou de première colonne de ce type, avec des premiers coefficients $d^{(i)}$ qui vérifient $d^{(i+1)} \mid d^{(i)}$. Comme l'anneau A est principal, cette suite se stabilise (voir prop. III.I.6.4), ce qui veut dire que l'on arrive après un nombre fini d'opérations à une matrice disons de première ligne $\begin{pmatrix} d^{(m)} & 0 & \cdots & 0 \end{pmatrix}$ telle que le pgcd des coefficients de la première colonne soit associé à $d^{(m)}$. Cela signifie que $d^{(m)}$ divise chacun de ces coefficients. On peut alors, par opérations élémentaires sur les lignes, se ramener à une matrice du type :

$$\begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}.$$

Appliquant l'hypothèse de récurrence à N, nous sommes ramenés à une matrice du type

$$\begin{pmatrix} d & & & \\ & d_2 & 0 & \\ & 0 & \ddots & \\ & & & d_r \end{pmatrix}$$

(où nous n'avons écrit que les r premières lignes et colonnes de la matrice, tous les autres coefficients étant nuls) avec $d_2 \mid \cdots \mid d_r$, mais il reste à montrer la condition que d divise d_2. Par une opération élémentaires sur les lignes, on arrive à la matrice

$$\begin{pmatrix} d & d_2 & 0 & 0 \\ 0 & d_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & d_r \end{pmatrix}.$$

En appliquant le lemme III.4.2 encore une fois, on peut remplacer d par $d_1 := d \wedge d_2$. La coefficient d_1 divise maintenant $d_2, d_3, \ldots, d_r$, mais le nouveau d_2 peut ne plus diviser d_3. Le même procédé nous permet de le remplacer par $d_2 \wedge d_3$. On conclut facilement en procédant de proche en proche.

Pour montrer l'unicité, le plus rapide est de considérer

$$\delta_k(M) = \text{pgcd}(k \times k \text{ mineurs de } M)$$

et de montrer que $\delta_k(M)$ *divise* $\delta_k(PM)$ *pour toute matrice carrée* P *de taille convenable.* Lorsque P est inversible, on a alors $\delta_k(PM) \mid \delta_k(P^{-1}PM) = \delta_k(M)$, de sorte que $\delta_k(M)$ et $\delta_k(PM)$ sont associés. On en déduit en considérant les matrices transposées que si Q est aussi inversible, $\delta_k(M)$ et $\delta_k(MQ)$ sont associés, donc finalement que $\delta_k(M)$ et $\delta_k(PMQ)$ sont associés. Si PMQ a la forme donnée dans le théorème, on a de plus

$$\delta_k(PMQ) = d_1 \cdots d_k,$$

ce qui exprime les d_k en fonction d'éléments de A qui ne dépendent que de M (à multiplication par une unité de A près).

Il reste à démontrer cette propriété. Elle résulte du fait que les lignes de PM sont combinaisons linéaires des lignes de M. Plus précisément, si l'on appelle L_i^k le k-vecteur formé des k premiers coefficients de la $i$ème ligne de M et que l'on note $P = (b_{i,j})_{1\leq i,j\leq p}$, le premier $k \times k$ mineur de PM est

$$\det(b_{1,1}L_1^k + \cdots + b_{1,p}L_p^k, \ldots, b_{k,1}L_1^k + \cdots + b_{k,p}L_p^k)$$

qui est une combinaison linéaire des $k \times k$ mineurs extraits des k premières colonnes de M. Il est donc divisible par $\delta_k(M)$. □

Exercice III.4.3. Soit A un anneau principal et soient a et b des éléments non nuls de A. Quelle est la forme réduite que l'on obtient en appliquant le théorème à la matrice $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$?

Exercice III.4.4. Soit A un anneau *euclidien.*

a) Montrer que dans la conclusion du théorème, on peut choisir les matrices P et Q (qui ne sont pas uniquement déterminées) produits de matrices élémentaires.

b) Si $M \in \mathbf{GL}(n, A)$, montrer qu'il existe $P \in E(n, A)$ telle que

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

En déduire $\mathbf{SL}(n, A) = E(n, A)$.

Exercice III.4.5. Soit A un anneau.

a) Soit M un élément de $\mathbf{GL}(n, A)$. Utiliser l'identité

$$\begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix} = \begin{pmatrix} I_n & M \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -M^{-1} & I_n \end{pmatrix} \begin{pmatrix} I_n & M \\ 0 & I_n \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$

pour montrer que la matrice $\begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix}$ est dans $E(2n, A)$.

b) Soient M et N des éléments de $\mathbf{GL}(n, A)$. Utiliser l'identité

$$\begin{pmatrix} MNM^{-1}N^{-1} & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} MN & 0 \\ 0 & N^{-1}M^{-1} \end{pmatrix} \begin{pmatrix} M^{-1} & 0 \\ 0 & M \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & N \end{pmatrix}$$

pour montrer que la matrice $MNM^{-1}N^{-1}$ est dans $E(2n, A)$.

III.5 Théorème de la base adaptée

On revient à l'étude des modules sur l'anneau principal A.

Théorème III.5.1 (Théorème de la base adaptée)**.** *Soit A un anneau principal, soit M un A-module libre de type fini et soit N un sous-A-module de M. Alors N est un A-module libre de type fini et il existe une base $(e_1, \ldots, e_n)$ de M et des éléments non nuls $d_1, \ldots, d_r$ de A, avec $0 \leq r \leq n$, tels que $d_1 \mid \cdots \mid d_r$ et que $(d_1e_1, \ldots, d_re_r)$ soit une base de N.*

Il est facile de montrer que N est de type fini (voir la preuve ci-dessous). Si on savait déjà que N était libre, le fait que son rang soit plus petit que celui de M résulterait de l'exercice

II.5.7, mais c'est bien la liberté de N qui est le point difficile, et qui ne marche pas dès que A n'est pas principal.

Attention aux erreurs habituelles : le théorème de la base adaptée ne dit pas que N admet un supplémentaire, ni que l'on peut compléter une base de N en une base de M.

Enfin, il est clair que pour un anneau A « général », un sous-A-module, même de type fini, d'un A-module libre de type fini n'est pas nécessairement libre (c'est le cas, par l'exercice II.5.6, pour les idéaux non principaux d'un anneau non principal), et qu'un sous-A-module d'un A-module libre de type fini n'est pas nécessairement de type fini (c'est le cas, dans un anneau non noethérien, pour les idéaux qui ne sont pas de type fini (voir prop. III.I.6.4)).

Démonstration. On peut supposer $M = A^n$. Montrons par récurrence sur n que N est un A-module de type fini. Pour $n = 0$, il n'y a rien à démontrer. Si $n > 0$, on considère la projection $p : A^n \to A$ sur un facteur. Le noyau $Q = N \cap A^{n-1}$ du morphisme $N \to p(N)$ est un sous-module de A^{n-1} donc est de type fini par hypothèse de récurrence. L'image $p(N) \simeq N/Q$ est un idéal de A donc est engendrée (en tant qu'idéal, donc aussi en tant que A-module) par un élément. Il en résulte que N est de type fini (exercice II.9.8).

Choisissons une base de M et un système fini de générateurs de N, dont on écrit la matrice des coordonnées dans la base de M. Multiplier à gauche cette matrice par une matrice inversible revient à changer de base pour M. Multiplier à droite cette matrice par une matrice inversible revient à changer de système de générateurs pour N. Le théorème III.4.1 donne immédiatement le résultat. □

III.6 Structure des modules de type fini sur un anneau principal

On déduit du théorème de la base adaptée le résultat fondamental suivant :

Théorème III.6.1. *Soit M un module de type fini sur un anneau principal A. Il existe des éléments non nuls et non inversibles $d_1, \dots, d_s$ de A, avec $s \geq 0$, tels que $d_1 \mid \cdots \mid d_s$, et un entier $r \geq 0$, tels que*

$$M \simeq A^r \oplus A/(d_1) \oplus \cdots \oplus A/(d_s).$$

Les entiers r et s, et les d_i à association près, ne dépendent que de M. On appelle ces derniers les facteurs invariants *de M.*

Démonstration. Comme M est de type fini, il est engendré par n éléments, qui définissent un morphisme surjectif $A^n \to M$ de A-modules. Il suffit d'appliquer le cor. III.5.1 à son noyau N, en ne gardant que les d_i non inversibles.

Pour l'unicité, il ne semble pas que l'on puisse facilement appliquer l'énoncé analogue qui apparaît dans le théorème III.4.1. Nous allons donc procéder directement. Tout d'abord, dans une telle décomposition, on a

$$T(M) \simeq A/(d_1) \oplus \cdots \oplus A/(d_s)$$

donc ce A-module ne dépend que de M et pas de la décomposition. De plus, l'entier r ne dépend aussi que de M : c'est le rang du A-module libre $M/T(M)$. Supposons que l'on ait un isomorphisme

$$A/(d_1) \oplus \cdots \oplus A/(d_s) \simeq A/(e_1) \oplus \cdots \oplus A/(e_t). \tag{III.6.1}$$

où les d_i et les e_j ne sont ni nuls ni inversibles, $d_1 \mid \cdots \mid d_s$ et $e_1 \mid \cdots \mid e_t$. Nous allons montrer $s = t$ puis, par récurrence sur s, que e_i est associé à d_i pour chaque i. Si T est le A-module

apparaissant dans (III.6.1), l'astuce est de regarder ce que deviennent les deux membres lorsque l'on considère dT et T/dT, pour $d \in A$ bien choisi.

On commence donc par la remarque suivante : soient d et e des éléments de A ; on a

$$d\big(A/(e)\big) \simeq A/(e/d \wedge e); \tag{III.6.2}$$

$$\big(A/(e)\big)\Big/d\big(A/(e)\big) \simeq A/(d \wedge e). \tag{III.6.3}$$

Le A-module de gauche dans (III.6.2) est l'image de la multiplication $A \xrightarrow{\times d} A/(e)$. Un élément x de A est dans le noyau si et seulement si e divise dx, c'est-à-dire $e/d \wedge e$ divise x (utiliser le lemme de Gauss I.5.8). On a bien l'isomorphisme cherché par factorisation canonique.

Pour (III.6.3), regardons la surjection canonique $A \to \big(A/(e)\big)/d\big(A/(e)\big)$. Un élément x de A est dans le noyau si et seulement s'il existe $y \in A$ avec $\bar{x} = d\bar{y}$ dans $A/(e)$, c'est-à-dire si et seulement s'il existe $y, z \in A$ avec $x = dy + ez$. Cela signifie $x \in (d, e) = (d \wedge e)$.

En particulier, si p est un élément irréductible de A, de sorte que $A/(p)$ est un corps (prop. I.5.5), on a par (III.6.3) :

$$A/(e)/p(A/(e)) \simeq \begin{cases} 0 & \text{si } p \wedge e = 1; \\ A/(p) & \text{si } p \mid e. \end{cases}$$

Si on choisit $p \mid d_1$, on voit que la dimension du $A/(p)$-espace vectoriel T/pT est s, tandis que c'est aussi le nombre ($\leq t$) de e_j divisibles par p. On a donc $s \leq t$, puis égalité par symétrie.

Considérons maintenant le A-module d_1T. On a par (III.6.2)

$$d_1T \simeq A/(d_2/d_1) \oplus \cdots \oplus A/(d_s/d_1) \simeq A/(e_1/d_1 \wedge e_1) \oplus \cdots \oplus A/(e_s/d_1 \wedge e_s).$$

Le nombre de facteurs non nuls de chaque côté devant être le même (comme on vient de le démontrer), on en déduit que $e_1/d_1 \wedge e_1$ est inversible, donc que e_1 divise d_1. Par symétrie, ils sont associés, et on obtient des isomorphismes

$$d_1T \simeq A/(d_2/d_1) \oplus \cdots \oplus A/(d_s/d_1) \simeq A/(e_2/d_1) \oplus \cdots \oplus A/(e_s/d_1).$$

On conclut par l'hypothèse de récurrence que soit d_i/d_1 et e_i/d_1 sont inversibles, soit ils sont associés, donc que d_i et e_i sont toujours associés. Ceci termine la démonstration. □

Corollaire III.6.2. *Soit A un anneau principal. Un A-module de type fini est libre si et seulement s'il est sans torsion.*

Attention : $\mathbb{Q}$ est un $\mathbb{Z}$-module sans torsion, mais pas libre (pourquoi ?).

Corollaire III.6.3. *Soit M un A-module de type fini. Alors il existe un entier r, des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ de A et des entiers strictement positifs $\alpha_1, \ldots, \alpha_s$ tels que*

$$M \simeq A^r \oplus \left(\bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{\alpha_i} \right).$$

Si l'on préfère, on écrit ceci en prenant des générateurs irréductibles p_i des idéaux premiers $\mathfrak{p}_i$ et l'on a

$$M \simeq \bigoplus_{i=1}^{s} A/(p_i^{\alpha_i}).$$

A permutation près, la suite $((\mathfrak{p}_i, \alpha_i)_{i=1,\ldots s})$ est unique.

Le corollaire se déduit du théorème par lemme des restes chinois I.3.1.

Exercice III.6.4. a) Soit A un anneau principal et soient M, P et Q des A-modules de type fini. On suppose que les A-modules $M \oplus P$ et $M \oplus Q$ sont isomorphes. Montrer que les A-modules P et Q sont isomorphes (on dit que M est *simplifiable*).

b) Soit A un anneau et soient P et Q des A-modules non isomorphes. Soit M le A-module $(P \oplus Q)^{(\mathbb{N})}$. Montrer que les A-modules $M \oplus P$ et $M \oplus Q$ sont isomorphes (M n'est donc pas simplifiable).

c) Soit A l'anneau $\mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$. Soit P le noyau du morphisme de A-modules $A^3 \to A$ défini en envoyant les vecteurs de la base canonique de A^3 sur $\bar{X}$, $\bar{Y}$ et $\bar{Z}$ respectivement. Montrer que l'on a $A \oplus P \simeq A^3 \simeq A \oplus A^2$, mais que P n'est pas isomorphe à A^2 (A n'est donc pas simplifiable) (*Indication :* on pourra utiliser des résultats sur la topologie de la sphère $\mathbf{S}^2$).

III.7 Application aux groupes abéliens de type fini

Un groupe abélien de type fini (c'est-à-dire engendré par un nombre fini d'éléments) n'est autre qu'un $\mathbb{Z}$-module de type fini. On déduit donc du théorème. III.6.1et de son corollaire le théorème de structure suivant.

Théorème III.7.1. *Soit M un groupe abélien de type fini. On se donne un système de représentants des éléments irréductibles $\mathcal{P}(M)$.*

Il existe alors une suite (unique) $d_1 | \dots | d_s$ d'entiers strictement positifs et un entier r (unique) tels que M est isomorphe à

$$\mathbb{Z}^r \oplus \left(\bigoplus_{i=1}^{s} \mathbb{Z}/(d_i) \right).$$

Il existe un ensemble fini (unique) de nombres premiers $p_i, \dots, p_s \in \mathcal{P}(M)$ et pour chaque p_i, une suite décroisante finie (unique) d'entiers strictement positifs $\beta_{i,j}, \dots \beta_{i,r_i}$ tels que M est isomorphe à

$$\mathbb{Z}^r \oplus \left(\bigoplus_{i=1\dots,s} \bigoplus_{j=1}^{r_i} \mathbb{Z}/(p_i^{\beta_{i,j}}) \right).$$

Bien entendu, M est fini si et seulement si $r = 0$.

Exercice III.7.2. Donner la liste des groupes abéliens de cardinal 6, 16, 18, 24, 36.

Exercice III.7.3. Soit $M = \mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})$. Donner la liste de tous les suplémentaires du facteur $\mathbb{Z}/3\mathbb{Z}$ dans M.

Exercice III.7.4. Soit $M = \mathbb{Z}^r \oplus (\bigoplus_{i=1}^{s} \mathbb{Z}/(d_i))$. Quel est l'annulateur dans $\mathbb{Z}$ de M ?

III.8 Application à la réduction des endomorphismes d'espaces vectoriels

Soit V un k-espace vectoriel de dimension finie, et u un endomorphisme de V. Nous avons vu que V est alors muni d'une structure de $k[X]$-module. Or $k[X]$ est principal et V est de type fini et de torsion, car de dimension finie sur k.

Théorème III.8.1. *Soient V un k-espace vectoriel de dimension finie, et u un endomorphisme de V. Il existe alors une suite (unique) $P_1|\dots|P_s$ de polynômes unitaires tels que, comme $k[X]-$modules,*

$$V \simeq \left(\bigoplus_{i=1}^{s} k[X]/(P_i)\right).$$

On dit que les P_i sont les invariants de similitude de u.

Exercice III.8.2. Quels sont les $k[X]$-modules cycliques ? Si l'on voit un $k[X]$-module de k-dimension finie comme un un k-espace vectoriel V muni d'un endomorphisme u, comment cette notion se traduit sur u ?

Exercice III.8.3. Soit V un k-espace vectoriel de dimension finie, et u un endomorphisme de V. soit $P_1|\dots|P_s$ la suite des invariants de similitude de u. Quels sont les polynômes caractéristiques et minimal de u ?

Montrer qu'il existe une base de V telle que la matrice de u dans cette base soit une matrice diagonale par bloc, dont les blocs sont les matrices compagnons des P_i.

Exercice III.8.4. Soit V un k-espace vectoriel de dimension finie, et soit $u, v \in \mathrm{End}_k(V)$ deux endomorphismes. Montrer que u et v sont conjugués (par un élément de $\mathbf{GL}(V)$ si et seulement si les suites des invariants de similitude associées respectivement aux $k[X]$-modules V_u et V_v sont les mêmes.

Exercice III.8.5. Soit q une puissance d'un nombre premier et notons $\mathbb{F}_q$ le corps fini à q éléments. Calculer le nombre de classes de conjugaison (sous $\mathbf{GL}_n(\mathbb{F}_q)$) dans $\mathcal{M}_n(\mathbb{F}_q)$ et dans $\mathbf{GL}_n(\mathbb{F}_q)$).

Exercice III.8.6. Soit A un anneau principal. Considérons l'action de $\mathbf{GL}_n(A) \times \mathbf{GL}_m(A)$ sur $\mathcal{M}_{n,m}(A)$ donné par $(P, Q, M) \mapsto PMQ^{-1}$. Montrer que l'ensemble des orbites est classifié par les suites

$$(d_1) \supset (d_2) \supset \cdots \supset (d_r)$$

d'idéaux de A. En déduire que lorsque $A = k$ est un corps commutatif, on retrouve le théorème de classification des classes d'équivalences par le rang.

Exercice III.8.7. Soient P et Q des polynômes. Calculer les invariants de similitude de la matrice par blocs

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

Exercice III.8.8. Soit u un endomorphisme d'un k-espace vectoriel E de dimension finie. On pose

$$\begin{aligned} \mathrm{Com}(u) &= \{v \in \mathrm{End}(E) \mid uv = vu\}, \\ \mathcal{P}(u) &= \{P(u) \mid P \in K[X]\} \subset \mathrm{Com}(u) \subset \mathrm{End}(E). \end{aligned}$$

La dimension du k-espace vectoriel $\mathcal{P}(u)$ est le degré du polynôme minimal de u.

a) Montrer $\mathcal{P}(u) = \bigcap_{v \in \mathrm{Com}(u)} \mathrm{Com}(v)$.

b) Si K est infini [2], montrer que les propriétés suivantes sont équivalentes :
   (i) u est cyclique ;
   (ii) le polynôme minimal de u est égal à son polynôme caractéristique ;
   (iii) $\mathrm{Com}(u) = \mathcal{P}(u)$;
   (iv) l'espace vectoriel E n'a qu'un nombre fini de sous-espaces vectoriels stables par u.

2. Cette hypothèse n'est pas nécessaire pour toutes les implications.