Algèbre Commutative

R. Taillefer

7 novembre 2012

Table des matières

I Ensembles ordonnés et lemme de Zorn

Nous aurons besoin de ce lemme pour faire certaines démonstrations où une récurrence est impossible (si l'ensemble d'indices n'est pas dénombrable). Il est équivalent à l'axiome du choix (indépendant des autres axiomes, Cohen 1963).

Axiome du choix. Un produit d'une famille non vide d'ensembles non vides est non vide.
Autrement dit, si $(A_i)_{i\in I}$ est une famille non vide d'ensembles non vides, on peut choisir $x_i \in A_i$ pour tout $i \in I$.

Nous nous contenterons d'énoncer le lemme de Zorn, et admettrons qu'il est équivalent à l'axiome du choix.

A Lemme de Zorn

Définition A.1. *Soit E un ensemble. Un* ordre sur *E est une relation binaire $\preccurlyeq$, réflexive, antisymétrique et transitive, c'est-à-dire telle que :*

- $\forall\, x \in E,\ x \preccurlyeq x$;
- $\forall\, x, y \in E$, *si* $x \preccurlyeq y$ *et* $y \preccurlyeq x$, *alors* $x = y$;
- $\forall\, x, y, z \in E$, *si* $x \preccurlyeq y$ *et* $y \preccurlyeq z$ *alors* $x \preccurlyeq z$.

On dit alors que l'ensemble $(E, \preccurlyeq)$ est un ***ensemble ordonné****.*

Remarque A.2. Il est clair que, si F est un sous-ensemble de l'ensemble E et si $\preccurlyeq$ est un ordre sur E, alors $\preccurlyeq$ induit un ordre sur F.

Définition A.3. *Si $(E, \preccurlyeq)$ est un ensemble ordonné et si, pour tous $x, y \in E$, on a $x \preccurlyeq y$ ou $y \preccurlyeq x$, on dit que $\preccurlyeq$ est un* ***ordre total*** *ou que $(E, \preccurlyeq)$ est un* ***ensemble totalement ordonné****.*

Définition A.4. *Soit $(E, \preccurlyeq)$ un ensemble ordonné.*

- *Un* ***élément maximal*** *de $(E, \preccurlyeq)$ est un élément $x \in E$ tel que, pour tout $y \in E$, si $x \preccurlyeq y$, alors $x = y$.*
- *Soit F un sous ensemble de E. Un* majorant de F dans E *est un élément m de E tel que pour tout $x \in F$, $x \preccurlyeq m$.*
- *On dit que $(E, \preccurlyeq)$ est un* ***ensemble inductif*** *si tout sous-ensemble non-vide F de E tel que $(F, \preccurlyeq)$ soit totalement ordonné admet un majorant dans E.*

Lemme A.5 (Lemme de Zorn)**.** Soit $(E, \preccurlyeq)$ un ensemble ordonné, inductif et non vide. Alors il existe un élément maximal dans E.

Démonstration. (admis) A.5

B Applications

Théorème B.1. Soit $\mathbb{K}$ un corps. Tout espace vectoriel non nul sur $\mathbb{K}$ a une base.

Démonstration. Soit E un espace vectoriel sur $\mathbb{K}$. Soit $\mathcal{S}$ l'ensemble des parties libres de E muni de l'ordre fourni par l'inclusion. Comme $E \neq \{0\}$, on a $\mathcal{S} \neq \varnothing$.

$\mathcal{S}$ muni de cet ordre est inductif : soit $(S_i)_{i\in I}$ une partie totalement ordonnée de $\mathcal{S}$. Alors $\cup_{i\in I} S_i$ est libre. En effet, soit $\sum_{j\in J} \lambda_j x_j = 0$ une relation de dépendance avec J une partie finie de I, $x_j \in S_j$ et $\lambda_j \in \mathbb{K}$. Puisque J est fini et $(S_i)_{i\in I}$ est totalement ordonné, on peut choisir $i_0 \in J$ tel que $S_j \subset S_{i_0}$ pour tout $j \in J$. Alors $x_j \in S_{i_0}$ pour tout $j \in J$. Or S_{i_0} est libre, donc $\lambda_j = 0$ pour tout $j \in J$.

D'après le lemme de Zorn, il existe une partie libre maximale dans $\mathcal{S}$, notons-la B. Il reste à montrer que B est un système générateur : sinon, il existe $y \in E$ tel que $\{y\} \cup B$ est libre, ce qui contredit la maximalité de B. B.1

Théorème B.2 (Théorème de Krull)**.** Soit A un anneau commutatif unitaire. Alors tout idéal de A distinct de A est contenu dans un idéal maximal.

Démonstration. Nous la donnerons dans le chapitre suivant. B.2

II Rappels et compléments sur les anneaux

Dans toute la suite du cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.

A Idéaux premiers et maximaux.

Définition A.1. *Soient A un anneau et I un idéal de A.*

(1) *L'idéal I est dit **premier** s'il est distinct de A et vérifie la condition suivante : pour tous $a, b \in A$, $ab \in I \Longrightarrow a \in I$ ou $b \in I$.*

(2) *L'idéal I est dit **maximal** s'il est distinct de A et vérifie la condition suivante : pour tout idéal J de A, $I \subset J \subset A \Longrightarrow J = I$ ou $J = A$.*

Remarque A.2. Soient A un anneau et $\mathcal{E}$ l'ensemble de tous les idéaux de A distincts de A. L'inclusion définit une relation d'ordre sur $\mathcal{E}$ et on note $(\mathcal{E}, \subset)$ l'ensemble ordonné ainsi obtenu. Alors, I est un idéal maximal de A si et seulement si I est un élément maximal de $(\mathcal{E}, \subset)$.

On peut caractériser la primalité ou la maximalité de l'idéal I d'un anneau A à l'aide de l'anneau quotient A/I.

Proposition A.3. Soient A un anneau et I un idéal de A.

(1) L'idéal I est premier si et seulement si l'anneau A/I est intègre.

(2) L'idéal I est maximal si et seulement si l'anneau A/I est un corps.

Démonstration. Exercice. A.3

Remarque A.4.
- ✦ Il est clair d'après la proposition **A.3** que tout idéal maximal est premier.
- ✦ Par contre, il est facile de montrer que $\{0\}$ est un idéal premier et non maximal de l'anneau $\mathbb{Z}$. (En effet, $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ est intègre mais n'est pas un corps).

Remarque A.5. Soient A un anneau, I un idéal de A et $\pi : A \longrightarrow A/I$ la projection canonique. On note $\mathbf{I}_{A/I}$ l'ensemble de tous les idéaux de A/I et $\mathbf{I}_{A,I}$ l'ensemble de tous les idéaux de A contenant I.

(1) On sait alors que les applications

$$\begin{array}{ccc} \mathbf{I}_{A,I} & \xrightarrow{\alpha} & \mathbf{I}_{A/I} \\ K & \mapsto & \pi(K) \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbf{I}_{A/I} & \xrightarrow{\beta} & \mathbf{I}_{A,I} \\ \mathcal{K} & \mapsto & \pi^{-1}(\mathcal{K}) \end{array}$$

sont des bijections réciproques l'une de l'autre et qu'elles établissent donc une correspondance bijective entre idéaux de A/I et idéaux de A contenant I.

(2) De plus, le troisième théorème d'isomorphisme précise que pour tout idéal K de A contenant I, on a un isomorphisme d'anneaux

$$A/K \cong (A/I)/\pi(K).$$

Ainsi, d'après la proposition **A.3**, pour tout idéal K de A contenant I, K est premier (resp. maximal) dans A si et seulement si $\pi(K)$ est premier (resp. maximal) dans A/I. On en déduit que

la correspondance bijective entre idéaux de A/I et idéaux de A contenant I induit une correspondance bijective entre idéaux premiers (resp. maximaux) de A/I et idéaux premiers (resp. maximaux) de A contenant I.

Il est clair par définition que l'anneau nul ne contient pas d'idéaux premiers (et donc pas d'idéaux maximaux). La première question légitime est alors la suivante : étant donné un anneau non nul A, existe-t-il toujours des idéaux premiers, des idéaux maximaux, dans A ? La réponse est donnée par le *théorème de Krull*.

Théorème A.6 (Théorème de Krull)**.** Soit A un anneau unitaire. Alors tout idéal de A distinct de A est contenu dans un idéal maximal.

Démonstration. Soit I un idéal de A distinct de A. Soit $\mathcal{S}$ l'ensemble des idéaux de A qui contiennent I et qui sont distincts de A, ordonné par l'inclusion. Puisque $I \in \mathcal{S}$, cet ensemble est non vide. De plus, $\mathcal{S}$ muni de cet ordre est inductif : soit $(I_j)_{j\in J}$ une famille totalement ordonnée d'idéaux qui contiennent I et qui sont distincts de A. Alors $\cup_{j\in J} I_j$ est encore un idéal distinct de A et contenant I. En effet, $1 \notin \cup_{j\in J} I_j$ donc $\cup_{j\in J} I_j \neq A$. Il est clair que $I \subset \cup_{j\in J} I_j$. De plus, si x et y sont dans $\cup_{j\in J} I_j$, il existe j_0 tel que x et y soient dans I_{j_0} (puisque la famille des I_j est totalement ordonnée). Alors $x + y \in I_{j_0} \subset \cup_{j\in J} I_j$ et $ax \in I_{j_0} \subset \cup_{j\in J} I_j$ pour tout $a \in A$, donc c'est bien un idéal.

D'après le lemme de Zorn, $\mathcal{S}$ contient un élément maximal. C'est un idéal maximal de A contenant I. A.6

B Nilradical, radical de Jacobson.

Définition B.1. *Soit A un anneau. Un élément $x \in A$ est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$. L'ensemble de tous les éléments nilpotents, noté $\mathcal{N}(A)$, est appelé le nilradical de A.*

Proposition B.2. Soit A un anneau ; le nilradical de A est un idéal.

Démonstration. Il est clair que $\mathcal{N}(A)$ contient 0, qu'il est stable par passage à l'opposé (*ie.* si $x \in \mathcal{N}(A)$, alors $-x \in \mathcal{N}(A)$) et qu'il est stable par multiplication par les éléments de A (*ie.* si $a \in A$ et $x \in \mathcal{N}(A)$, alors $ax \in \mathcal{N}(A)$). Par ailleurs, soient $x, y \in \mathcal{N}(A)$; il existe $m, n \in \mathbb{N}^*$ tels que $x^n = 0 = y^m$. La formule du binôme donne alors

$$(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}.$$

Mais, pour $0 \leqslant i \leqslant m+n-1$, on a soit $i \geqslant n$ et donc $x^i = 0$, soit $m+n-1-i \geqslant m$ et donc $y^{m+n-1-i} = 0$. Donc $(x+y)^{m+n-1} = 0$. Ainsi, $\mathcal{N}(A)$ est stable par somme. B.2

Le théorème suivant explique l'importance du nilradical d'un anneau.

Théorème B.3. Soit A un anneau non nul. Le nilradical de A est l'intersection de tous les idéaux premiers de A.

Démonstration. On note I l'intersection de tous les idéaux premiers de A. Soit $x \in \mathcal{N}(A)$. Il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$. Par suite, pour tout idéal premier P de A, $x^n \in P$ et donc $x \in P$. Ainsi, $\mathcal{N}(A) \subset I$. L'inclusion réciproque est plus délicate ; elle utilise le lemme de Zorn. Soit x un élément non nilpotent de A. On note $\mathcal{E}$ l'ensemble des idéaux J de A tels que, $\forall n \in \mathbb{N}^*$, $x^n \notin J$. L'ensemble $\mathcal{E}$ est non vide puisque, x n'étant pas nilpotent, $\{0\} \in \mathcal{E}$. On montre facilement que l'ensemble $\mathcal{E}$ muni de l'ordre donné par l'inclusion est inductif. Par le lemme de Zorn, $(\mathcal{E}, \subset)$ possède donc un élément maximal ; on le note P. En fait, l'idéal P est premier. En effet, $P \neq A$ puisque $x \notin P$. De plus, soient $y, z \in A \setminus P$. Les idéaux $P + (y)$ et $P + (z)$ ne sont pas dans $\mathcal{E}$ puisque P est maximal pour $(\mathcal{E}, \subset)$. Ainsi, il existe $n, m \in \mathbb{N}^*$ tels que $x^n \in P + (y)$ et $x^m \in P + (z)$. Il s'ensuit facilement que $x^{n+m} \in$

$(P+(y))(P+(z)) = P+(yz)$. Donc, $P+(yz) \notin \mathcal{E}$, et par suite $yz \notin P$. Ceci montre que l'idéal P est premier. Ainsi, il existe un idéal premier qui ne contient pas x. On a montré que le complémentaire dans A de $\mathcal{N}(A)$ est inclus dans le complémentaire de I, c'est-à-dire que $I \subset \mathcal{N}(A)$. B.3

On définit maintenant le radical de Jacobson d'un anneau.

Définition B.4. *Soit A un anneau. Le **radical de Jacobson** de A, noté $\mathcal{J}(A)$, est l'intersection des idéaux maximaux de A.*

Le radical de Jacobson peut être caractérisé de la façon suivante.

Proposition B.5. Soient A un anneau et $x \in A$. Alors, x est dans le radical de Jacobson de A si et seulement si, pour tout y de A, $1-xy$ est un élément inversible de A.

Démonstration. ($\Longleftarrow$) Supposons qu'il existe un idéal maximal $\mathfrak{m}$ de A tel que $x \notin \mathfrak{m}$ et soit $\pi : A \longrightarrow A/\mathfrak{m}$ la projection canonique. Alors $\pi(x)$ est un élément non nul du corps $A/\mathfrak{m}$ et par suite il est inversible : il existe $y \in A$ tel que $\pi(1_A) = \pi(x)\pi(y)$, c'est-à-dire tel que $1-xy \in \mathfrak{m}$. On a montré qu'il existe $y \in A$ tel que $1-xy$ ne soit pas inversible dans A.

($\Longrightarrow$) Supposons qu'il existe $y \in A$ tel que $1-xy$ ne soit pas un élément inversible de A. Alors, d'après le théorème de Krull **A.6**, il existe un idéal maximal $\mathfrak{m}$ de A qui contient $1-xy$. Comme 1 ne peut être dans $\mathfrak{m}$, il s'ensuit que x n'est pas dans $\mathfrak{m}$. B.5

Remarque B.6. Soit A un anneau ; il est clair que $\mathcal{N}(A) \subset \mathcal{J}(A)$.

C Arithmétique.

Dans cette partie, on étudie les propriétés arithmétiques des anneaux, c'est-à-dire les propriétés des anneaux liées à la divisibilité.

Dans tout cette partie, sauf mention expresse du contraire, A désigne un anneau (commutatif, unitaire) intègre (et donc non nul). On note alors $A^\times$ le groupe des éléments inversibles de A.

C.1 Divisibilité.

Définition C.1. *Soient $a, b \in A$.*

(1) *On dit que a **divise** b, et on note $a|b$, s'il existe un élément c de A tel que $b = ac$.*

(2) *On dit que a et b sont **associés** si $a|b$ et $b|a$.*

Remarque C.2. Soient $a, b \in A$. Les points suivants sont clairs :

(1) a divise b si et seulement si $(b) \subset (a)$;

(2) a et b sont associés si et seulement si $(a) = (b)$;

(3) a et b sont associés si et seulement s'il existe $u \in A^\times$ tel que $a = ub$.

Définition C.3. *Soit p dans A. On dit que p est **irréductible** s'il satisfait aux conditions suivantes :*

(i) *$p \notin A^\times$;*

(ii) *$p = ab$ avec $a, b \in A$ entraîne que a ou b est un élément inversible.*

Remarque C.4. **(1)** Le produit d'un irréductible par un élément inversible est un irréductible.

(2) L'élément 0 n'est pas irréductible car $0 = 0.0$. Ainsi, un corps n'a pas d'éléments irréductibles.

(3) Soit p dans A ; p est irréductible si et seulement si :

(i) $p \notin A^\times$;

(ii) $p \neq 0$ et les seuls diviseurs de p sont les élément inversibles de A et les éléments de A associés à p.

(4) Soit $p \in A$; si (p) est premier, alors p est irréductible.

Définition C.5. *Soient I un ensemble non vide et $(a_i)_{i\in I}$ une famille d'éléments de A non tous nuls.*

(1) *On dit que $a \in A$ est un **diviseur** (resp. **multiple**) **commun** de $(a_i)_{i\in I}$ si, pour tout $i \in I$, $a|a_i$ (resp. $a_i|a$).*

(2) *On dit que $d \in A$ est un **plus grand commun diviseur** (en abrégé p.g.c.d.) de $(a_i)_{i\in I}$ si c'est un divieur commun de $(a_i)_{i\in I}$ et si tout diviseur commun de $(a_i)_{i\in I}$ divise d.*

(3) *On dit que $m \in A$ est un **plus petit commun multiple** (en abrégé p.p.c.m.) de $(a_i)_{i\in I}$ si c'est un multiple commun de $(a_i)_{i\in I}$ qui divise tout multiple commun de $(a_i)_{i\in I}$.*

(4) *On dit que les a_i, $i \in I$ sont **premiers entre eux** si 1 est un p.g.c.d. de $(a_i)_{i\in I}$.*

Remarque C.6. Soit I un ensemble non vide et $\mathcal{A} = (a_i)_{i\in I}$ une famille d'éléments de A non tous nuls. On montre facilement que si $a \in A$ est un p.g.c.d. (resp. p.p.c.m.) de $\mathcal{A}$, un élément b est un p.g.c.d. (resp. p.p.c.m.) de $\mathcal{A}$ si et seulement si c'est un associé de a.

Remarque C.7. Soit $a \in A \setminus \{0\}$; a et 0 sont premiers entre eux si et seulement si a est un élément inversible de A.

Proposition C.8. Soit a un élément irréductible de A et b un élément de A. Alors, a et b sont premiers entre eux si et seulement si a ne divise pas b.

Démonstration. Exercice. C.8

C.2 Anneaux factoriels

Anneaux factoriels.

Définition C.9. (1) *On dit que A satisfait la condition (E) si tout élément non nul et non inversible $a \in A$ admet une décomposition en produit d'irréductibles, c'est-à-dire qu'il existe $r \in \mathbb{N}^*$ et des éléments irréductibles $p_1, \dots, p_r$ tels que $a = p_1 \dots p_r$.*

(2) *On dit que A satisfait la condition (U) si pour tout élément non nul et non inversible de A, une décomposition en produit d'irréductibles (si elle existe) est essentiellement unique, c'est-à-dire que, si $a = p_1 \dots p_r = q_1 \dots q_s$ où $r, s \in \mathbb{N}^*$ et $p_1, \dots, p_r, q_1, \dots, q_s$ sont des éléments irréductibles de A alors $r = s$ et, il existe $\sigma \in \mathfrak{S}_r$ tel que, pour $1 \leqslant i \leqslant r$, p_i et $q_{\sigma(i)}$ soient associés.*

(3) *On dit que A est **factoriel** s'il satisfait les conditions (E) et (U) (et s'il est intègre).*

Exemple C.10. Tout corps est un anneau factoriel.

Proposition C.11 (Existence de p.g.c.d. et de p.p.c.m. dans les anneaux factoriels)**.** Supposons A factoriel. Si $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) sont des éléments non nuls de A, alors ils admettent un p.g.c.d. et un p.p.c.m.

Démonstration. Exercice (en utilisant les décompositions en facteurs irréductibles des a_i). C.11

Théorème C.12. Soit A un anneau intègre satisfaisant la condition (E). Alors les assertions suivantes sont équivalentes :

(a) A satisfait la condition (U).

(b) Pour tout triplet (a, b, c) d'éléments de A tel que a ou b est non nul, si a et b sont premiers entre eux et si $a|bc$, alors $a|c$ (condition de Gauss).

(c) Pour tout triplet (a, b, c) d'éléments de A, si a est irréductible et divise bc, alors a divise b ou a divise c (condition d'Euclide).

(d) Pour p dans A, (p) est premier si et seulement si p est irréductible (condition de primalité).

Démonstration. **(a)⇒(b)** Soient a et b premiers entre eux divisant bc. Si un des éléments parmi a, b et c est nul, alors le résultat est clair (voir la remarque **C.7**). Si l'un d'eux est inversible, le résultat est clair. Sinon, puisque A est factoriel, on peut décomposer a, b et c de manière essentiellement unique. Notons $a = u\prod_{i=1}^{n} p_i^{\alpha_i}$, $b = v\prod_{i=1}^{n} p_i^{\beta_i}$ et $c = w\prod_{i=1}^{n} p_i^{\gamma_i}$ avec les p_i irréductibles et u, v, w inversibles (on choisit les mêmes p_i quitte à avoir des exposants nuls et à multiplier par des éléments inversibles). Alors, puisque a et b sont premiers entre eux, on a $\alpha_i\beta_i = 0$ pour tout i. Puisque a divise bc on a $\alpha_i \leqslant \beta_i + \gamma_i$ pour tout i. On en déduit facilement que $\alpha_i \leqslant \gamma_i$ pour tout i et donc que a divise c.

(b)⇒(c) Soit a un irréductible divisant bc. Si a ne divise pas b, alors d'après la proposition **C.8** a et b sont premiers entre eux, donc d'après la condition de Gauss a divise c.

(c)⇒(d) C'est clair.

(d)⇒(a) Soit $a \in A$ et supposons que $a = p_1 \dots p_m = q_1 \dots q_n$ avec $m \leqslant n$. On raisonne par récurrence sur m.

- Si $m = 1$, on a $a = p_1 = q_1 \dots q_n$. Donc $q_1 \mid p_1$, p_1 est irréductible et $q_1 \notin A^\times$, donc $q_1 = up_1$ avec $u \in A^\times$. Donc $uq_2 \dots q_n \in A^\times$ et donc $n = 1$.
- Supposons que le résultat soit vrai jusqu'au rang $m-1$ et montrons-le au rang m. On a $p_1(p_2, \dots, p_m) = q_1 \dots q_n$. Puisque p_1 est irréductible, (p_1) est premier d'après **(d)**, et il divise $q_1 \dots q_n$, donc il existe i tel que $p_1 \mid q_i$: on a $q_i = u_1 p_1$ avec $u_1 \in A$. Puisque q_i est irréductible, $u_1 \in A^\times$.

  On a donc $p_1(p_2 \dots p_m) = u_1 p_1(q_1 \dots q_{i-1}q_{i+1} \dots q_n)$, donc $p_2 \dots p_m = u_1 q_1 \dots q_{i-1}q_{i+1} \dots q_n$ et par hypothèse de récurrence on a $m - 1 = n - 1$, donc $m = n$, et on a $u_j \in A^\times$ pour tout $j = 2 \dots m$ et $\tau \in \mathfrak{S}_{m-1}$ tels que $p_j = u_j q_{\tau(j)}$ pour tout $j = 2, \dots, m$. On conclut en définissant $\sigma \in \mathfrak{S}_m$ par $\sigma(1) = i$ et $\sigma(j) = \tau(j)$ pour $j = 2, \dots, m$. C.12

Exemples d'anneaux factoriels.

Dans cette sous-section, on étudie les anneaux principaux et les anneaux euclidiens. Ce sont des exemples d'anneaux factoriels.

On commence par l'étude des anneaux principaux. On rappelle que dans un anneau A quelconque (*ie.* non nécessairement intègre), un idéal I est dit **principal** s'il existe $a \in A$ tel que $I = (a)$.

Définition C.13. *L'anneau A est dit **principal** s'il est intègre et si tout idéal de A est principal.*

Lemme C.14. Soit A un anneau principal et soit $I_0 \subset I_1 \subset \dots \subset I_n \subset \dots A$ une suite croissante d'idéaux de A. Alors cette suite stationne, c'est-à-dire qu'il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$ on ait $I_n = I_N$.

Démonstration. Posons $I = \cup_{n\in\mathbb{N}} I_n$. Alors I est un idéal de A (exercice), donc comme A est principal il existe $a \in A$ tel que $I = (a)$. Alors $a \in \cup_{n\in\mathbb{N}} I_n$, donc il existe $N \in \mathbb{N}$ tel que $a \in I_N$. Alors $(a) \subset I_N \subset I = (a)$, donc $I = I_N$. De plus, pour tout $n \geqslant N$, on a $I_N \subset I_n \subset I = I_N$ donc $I_n = I_N$. C.14

Lemme C.15. Soit A un anneau principal. Alors la condition de primalité est vérifiée.

Démonstration. Soit a un élément irréductible de A. Nous devons montrer que (a) est premier. Puisque a n'est pas inversible, on a $(a) \neq A$. D'après le théorème de Krull, il existe un idéal maximal I tel que $(a) \subset I$. Puisque A est principal, on a $I = (b)$ pour un $b \in A$. On a donc $a = bc$ pour un $c \in A$. Puisque a est irréductible et b non inversible ($(b) = I \neq A$), a et b sont associés donc $(a) = (b) = I$ est maximal donc premier. C.15

Théorème C.16. Si A est principal, il est factoriel.

Démonstration. Si A est un corps, il est factoriel (voir l'exemple **C.10**). Supposons donc que A n'est pas un corps.

D'après le lemme **C.15**, la condition de primalité est satisfaite par A. Il suffit donc d'après le théorème **C.12** de montrer que tout élément non nul et non inversible de A est un produit d'éléments irréductibles.

Soit $\mathcal{S}$ l'ensemble des idéaux (a) engendrés par les éléments a non nuls, non inversibles et n'admettant pas de factorisation en produit d'éléments irréductibles. Supposons par l'absurde que $\mathcal{S} \neq \varnothing$.

Démontrons que $\mathcal{S}$ admet un élément maximal. Si ce n'est pas le cas, soit $(a_1) \in \mathcal{S}$. Alors (a_1) n'est pas maximal dans $\mathcal{S}$ donc il existe $(a_2) \in \mathcal{S}$ tel que $(a_1) \subsetneq (a_2)$. De même, (a_2) n'est pas maximal donc il existe $(a_3) \in \mathcal{S}$ tel que $(a_2) \subsetneq (a_3)$. En procédant ainsi, on construit une suite strictement croissante d'idéaux dans A, contredisant ainsi le lemme **C.14**.

Donc $\mathcal{S}$ admet un élément maximal, notons-le (a_0). En particulier, comme $(a_0) \in \mathcal{S}$, l'élément a_0 n'est pas irréductible, donc on peut écrire $a_0 = bc$ avec b et c non nuls et non inversibles. On a alors $(a_0) \subsetneq (b)$ et $(a_0) \subsetneq (c)$ donc par maximalité de (a_0) dans $\mathcal{S}$, on a $(b) \notin \mathcal{S}$ et $(c) \notin \mathcal{S}$. Par définition de $\mathcal{S}$ il existe donc des éléments irréductibles $p_1, \dots, p_r$ et $q_1, \dots, q_s$ tels que $b = p_1 \cdots p_r$ et $c = q_1 \cdots q_s$. Mais alors $a_0 = p_1 \cdots p_r q_1 \cdots q_s$ ce qui contredit le fait que $(a_0) \in \mathcal{S}$.

Finalement, $\mathcal{S} = \varnothing$ et donc la propriété (E) est bien vérifiée. C.16

Remarque C.17. On suppose A principal.

(1) Si A est un corps, son unique idéal premier est $\{0\}$.

(2) Si A n'est pas un corps, ses idéaux premiers sont $\{0\}$ et les idéaux (p) où p est irréductible. Ses idéaux maximaux sont les idéaux (p) où p est irréductible. *[En effet, tout idéal maximal est premier et $\{0\}$ n'est pas maximal puisqu'il existe $a \in A$ non nul et non inversible et alors $\{0\} \subsetneq (a) \subsetneq A$; enfin, si p est irréductible, alors (p) est maximal : si $(p) \subsetneq I \subset A$, on pose $I = (a)$ puisque A est principal, donc a divise p et n'est pas associé à p, donc puisque p est irréductible a est inversible et donc $I = A$.]*

Le théorème **C.16** a pour conséquence que toute famille finie d'éléments non tous nuls de A admet un p.g.c.d. et un p.p.c.m. (voir proposition **C.11**) ; on peut les caractériser au moyen d'idéaux.

Proposition C.18. Supposons A principal et soient $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) des éléments non tous nuls de A. Un élément de A est p.g.c.d. (resp. p.p.c.m.) de $\{a_1, \dots, a_r\}$ si et seulement s'il engendre l'idéal $a_1A + \cdots + a_rA = (a_1, \dots, a_r)$ (resp. $a_1A \cap \cdots \cap a_rA = (a_1) \cap \cdots \cap (a_r)$).

Démonstration. Exercice. C.18

Corollaire C.19. Supposons A principal et soient $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) des éléments non tous nuls de A. Alors, les éléments $a_1, \dots, a_r$ sont premiers entre eux si et seulement s'il existe $x_1, \dots, x_r \in A$ tels que $a_1x_1 + \cdots + a_rx_r = 1$.

Démonstration. C'est une conséquence immédiate de la proposition **C.18**. C.19

On passe maintenant au cas des anneaux euclidiens. Ce sont des exemples d'anneaux principaux.

Définition C.20. *L'anneau A est dit* ***euclidien*** *s'il est intègre et s'il existe une application $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que, pour tout couple (a, b) d'éléments de A tel que $b \neq 0$, il existe un couple (q, r) d'éléments de A tel que $a = bq + r$ et ou bien $r = 0$, ou bien $\varphi(r) < \varphi(b)$.*

Théorème C.21. Si A est euclidien, il est principal.

Démonstration. cf. TD. C.21

Exemple C.22.
- ✦ L'anneau $\mathbb{Z}$ est euclidien (considérer $\mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$, $n \mapsto |n|$).
- ✦ Si K est un corps, l'anneau $K[X]$ est euclidien (considérer $K[X] \setminus \{0\} \longrightarrow \mathbb{N}$, $P \mapsto \deg P$).
- ✦ L'anneau $\mathbb{Z}[i] = \{a + ib; a \in \mathbb{Z}, b \in \mathbb{Z}\}$ des entiers de Gauss est un anneau euclidien (considérer $\mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$).

Corollaire C.23. Soit A un anneau commutatif unitaire quelconque (*ie.* non nécessairement intègre). L'anneau $A[X]$ est principal si et seulement si A est un corps.

Démonstration. D'après le théorème **C.21** et l'exemple **C.22**, si A est un corps, alors $A[X]$ est principal.

Réciproquement, supposons que $A[X]$ est principal. Alors A est intègre car c'est un sous-anneau de $A[X]$ qui est principal donc intègre.

Considérons l'idéal (X) de $A[X]$. Puisque $A[X]/(X) \cong A$ est intègre, (X) est premier, donc maximal puisque $A[X]$ est principal, et donc $A \cong A[X]/(X)$ est un corps. C.23

III Modules

A Modules

Définition A.1. *Soit A un anneau (commutatif, unitaire). Un* ***module sur*** *A ou* ***A-module*** *est la donnée d'un groupe abélien M muni d'une loi externe* $\begin{array}{ccc} A \times M & \to & M \\ (a,m) & \mapsto & am \end{array}$ *(on parle d'**action** de A sur M) vérifiant, pour tout $(a,b) \in A \times A$ et tout $(x,y) \in M \times M$,*

(i) $(a+b)x = ax + bx$

(ii) $a(x+y) = ax + ay$

(iii) $a(bx) = (ab)x$

(iv) $1x = x$.

Un module ressemble donc à un espace vectoriel, mais le corps de base est remplacé par un anneau. Les modules ne vérifieront pas toutes les mêmes propriétés qu'un espace vectoriel, puisque les scalaires ne sont pas inversibles.

Remarque A.2. Il n'est pas indispensable d'avoir un anneau *commutatif* pour définir un module sur cet anneau. Lorsque A n'est pas commutatif, la définition ci-dessus est celle d'un **A-module à gauche**, et on peut définir de manière similaire un A-module à droite. Nous aurons rapidement besoin dans ce cours de supposer que A est commutatif, donc pour simplifier nous ne considérerons que des anneaux commutatifs.

Exemple A.3. **(1)** L'anneau A est un module sur lui-même (l'action de A sur A est donnée par la multiplication dans A).

(2) Les $\mathbb{Z}$-modules sont précisément les groupes abéliens.

(3) Un idéal d'un anneau A est un module sur A (l'action de A sur l'idéal est donnée par la multiplication dans A).

(4) Si S est un ensemble et si M est un module sur un anneau A, notons M^S l'ensemble des applications de S dans M. Alors M^S est un module sur A, dont la loi interne est donnée par

$$\begin{array}{ccc} M^S \times M^S & \to & M^S \\ (f,g) & \mapsto & f+g = [s \mapsto f(s)+g(s)] \end{array}$$

et dont la loi externe est donnée par

$$\begin{array}{ccc} A \times M^S & \to & M^S \\ (a,f) & \mapsto & af = [s \mapsto af(s)] \end{array}$$

pour $f \in M^S$, $g \in M^S$ et $a \in A$.

Remarque A.4. Soit M un module sur un anneau A.

- $a0 = 0$ pour tout $a \in A$. *[En effet, $a0 = a(0+0) = a0 + a0$ donc $a0 = a0 + (-a0) = 0$].*
- $0x = 0$ pour tout $x \in M$. *[En effet, $0x = (0+0)x = 0x + 0x$ etc.].*
- $(-a)x = -(ax)$ pour tout $a \in A$ et tout $x \in M$. *[En effet, $(-a)x + ax = (-a+a)x = 0x = 0$ donc $(-a)x = -(ax)$].*

B Sous-modules

Définition B.1. *Soit M un A-module. Un **sous-module** de M est un sous-groupe N de M qui est stable par la loi externe.*

Proposition B.2. Une partie non vide N d'un A-module M est un sous-module de M si et seulement si

- ✦ pour tous $x \in N$, $y \in N$ on a $x - y \in N$, et
- ✦ pour tous $a \in A$, $x \in N$ on a $ax \in N$.

Démonstration. En exercice. B.2

Proposition B.3. Soit M un A-module, et soient N et N' deux sous-modules de M. Alors $N \cap N'$ est un sous-module de M. (Plus généralement, une intersection quelconque de sous-modules est un sous-module).

Démonstration. En exercice. B.3

Exemple B.4. Soit M un A-module et soient I un idéal de A et N un sous-module de M. Alors $IN := \left\{\sum_{i=1}^{p} a_i y_i ; p \in \mathbb{N}^*, a_i \in I, y_i \in N\right\}$ est un sous-A-module de M. (Exercice).

Définition B.5. *Soit M un A-module et soit S une partie non vide de M. Une **combinaison linéaire** d'éléments de S est un élément de M qui s'écrit $x = \sum_{s \in S} a_s s$ où les a_s sont des éléments de A qui sont tous nuls sauf un nombre fini d'entre eux (donc la somme est finie).*

On note $\langle S \rangle$ (ou AS) l'ensemble des combinaisons linéaires d'éléments de S.

Définition-Proposition B.6. Soit M un A-module et soit S une partie non vide de M. Alors $\langle S \rangle$ est un sous-module de M ; c'est l'intersection de tous les sous-modules de M contenant S. Il est appelé **sous-module de M engendré par S**.

Démonstration. En exercice. B.6

Définition B.7. *Soit M un A-module et soient M_i, $i \in I$, des sous-modules de M. On appelle **somme** des sous-modules M_i et on note $\sum_{i \in I} M_i$ le sous-module de M engendré par $\cup_{i \in I} M_i$. C'est donc l'ensemble des sommes finies d'éléments de $\cup_{i \in I} M_i$.*

Définition B.8. *Soit M un A-module. Une **partie génératrice** de M est une partie non vide S de M telle que $M = \langle S \rangle$. On dit alors que S **engendre** M.*

*S'il existe une partie finie S de M qui engendre M, on dit que M est de **type fini**.*

*S'il existe une partie S de M à un élément qui engendre M, on dit que M est **cyclique**, ou **monogène**.*

Remarque B.9. Tout module a une partie génératrice : il est clair que $M = \langle M \rangle$.

B.1 Somme directe de *sous-modules*

Définition B.10. *Soit M un A-module, soit N un sous-module de M et soient $N_1, \ldots, N_p$ des sous-modules de M. On dit que N est la **somme directe** (on précise parfois **interne**) des sous-modules $N_1, \ldots, N_p$, notée $N = \bigoplus_{i=1}^{n} N_i$, si les deux conditions suivantes sont vérifiées :*

(i) $N = \sum_{i=1}^{p} N_i$

(ii) *Pour tout* j, $1 \leqslant j \leqslant p$, *on a* $N_j \cap \left(\sum_{\substack{1 \leqslant i \leqslant p \\ i \neq j}} N_i \right) = \{0\}$.

Remarque B.11. Dans le cas où $p = 2$ on retrouve la définition que vous connaissez bien.

Remarque B.12. Cette définition n'est valable que pour des *sous-modules* d'un module donné.

Proposition B.13. Soit M un A-module, soit N un sous-module de M et soient $N_1, \ldots, N_p$ des sous-modules de N. Alors $N = \bigoplus_{i=1}^{n} N_i$ si et seulement si tout élément $x \in N$ s'écrit de manière unique sous la forme $x = \sum_{i=1}^{p} x_i$ avec $x_i \in N_i$ pour tout i.

Démonstration.

✦ Supposons que $N = \bigoplus_{i=1}^{n} N_i$, et soit $x \in N$. Il est clair d'après la propriété **(i)** que l'on peut écrire $x = \sum_{i=1}^{p} x_i$ avec $x_i \in N_i$ pour tout i. Supposons que l'on puisse aussi écrire $x = \sum_{i=1}^{p} y_i$ avec $y_i \in N_i$ pour tout i. Fixons j avec $1 \leqslant j \leqslant p$. Alors $x_j - y_j \in N_j$. Mais $x_j - y_j = \sum_{\substack{1 \leqslant i \leqslant p \\ i \neq j}} (y_i - x_i) \in \sum_{\substack{1 \leqslant i \leqslant p \\ i \neq j}} N_i$. Donc d'après l'hypothèse **(ii)** on a $x_j - y_j = 0$, d'où $x_j = y_j$. C'est valable pour tout j, donc l'écriture de x est unique.

✦ Supposons que tout élément $x \in N$ s'écrive de manière unique sous la forme $x = \sum_{i=1}^{p} x_i$ avec $x_i \in N_i$ pour tout i. Il est alors clair que **(i)** est vérifiée.

Soit maintenant $x \in N_j \cap \left(\sum_{\substack{1 \leqslant i \leqslant p \\ i \neq j}} N_i \right)$. On peut donc l'écrire $x = 0 + \cdots + 0 + x + 0 + \cdots + 0$ avec $x \in N_j$ et $0 \in N_i$ pour tout $i \neq j$. On peut aussi l'écrire $x = x_1 + \cdots + x_{j-1} + 0 + x_{j+1} + \cdots + x_p$ avec $x_i \in N_i$ pour $i \neq j$ et $0 \in N_j$. On a donc deux écritures de x dans $\sum_{i=1}^{p} N_i$. Puisque l'écriture est unique, cela impose en particulier que $x = 0$. Donc $N_j \cap \left(\sum_{\substack{1 \leqslant i \leqslant p \\ i \neq j}} N_i \right) = \{0\}$. B.13

C Modules quotient

Soit M un A-module et soit N un sous-module de M. On sait que M/N est un groupe abélien. Pour tout $x \in M$, on note $\overline{x}$ sa classe dans M/N. On rappelle que l'addition dans M/N est donnée par $\overline{x} + \overline{y} = \overline{x+y}$ pour tout $(\overline{x}, \overline{y}) \in M/N \times M/N$.

Définition-Proposition C.1. M/N est un A-module pour la loi externe définie par $a\overline{x} = \overline{ax}$ pour tout $a \in A$ et tout $\overline{x} \in M/N$. Ce A-module est appelé **module quotient** de M par N.

Démonstration. Montrons tout d'abord que l'application $(a, \overline{x}) \mapsto \overline{ax}$ ci-dessus est bien définie : si on choisit deux représentants x et x' dans M d'un même élément de M/N (donc $\overline{x} = \overline{x'}$), il nous faut montrer que $\overline{ax} = \overline{ax'}$. Or $x - x'$ est dans N, donc $a(x - x')$ est dans N (sous-module), et donc $ax - ax' \in N$ et $\overline{ax} = \overline{ax'}$.

Maintenant vérifions que M/N est un A-module. Nous savons déjà que c'est un groupe abélien. De plus,

(i) $(a+b)\overline{x} = \overline{(a+b)x} = \overline{ax+bx} = \overline{ax} + \overline{bx} = a\overline{x} + b\overline{x}$ pour tout $(a, b) \in A \times A$ et tout $\overline{x} \in M/N$.

(ii) $a(\overline{x} + \overline{y}) = a\,\overline{x+y} = \overline{a(x+y)} = \overline{ax+ay} = \overline{ax} + \overline{ay} = a\overline{x} + a\overline{y}$ pour tout $a \in A$ et tout $(\overline{x}, \overline{y}) \in M/N \times M/N$.

(iii) $a(b\overline{x}) = a\,\overline{bx} = \overline{a(bx)} = \overline{(ab)x} = (ab)\overline{x}$ pour tout $(a,b) \in A \times A$ et tout $\overline{x} \in M/N$.

(iv) $1\overline{x} = \overline{1x} = \overline{x}$ pour tout $\overline{x} \in M/N$. C.1

Exercice C.2. Soit A un anneau et soit M un A-module. Soit I un idéal de A. Alors M/IM est un module sur l'anneau A/I.

[Il est clair que M/IM est un groupe abélien. Il reste à vérifier que $\overline{a}\,\overline{m} := \overline{am}$ définit bien une structure de A/I-module sur M/IM].

D Morphismes

D.1 Généralités

Définition D.1. *Un **(homo)morphisme de A-modules** (ou **application A-linéaire**) de M dans N est une application $f : M \to N$ vérifiant :*

- ✦ *$f(x+y) = f(x) + f(y)$ pour tout $(x,y) \in M \times M$, et*
- ✦ *$f(ax) = af(x)$ pour tout $a \in A$ et tout $x \in M$.*

*Si $M = N$, un morphisme de A-modules de M dans M est aussi appelé un **endomorphisme** de M.*

Exemple D.2. **(1)** $\mathrm{id}_M : M \to M$ et l'application nulle $0 : M \to N$ sont des morphismes de A-modules.

(2) Si N est un sous-module de M, alors l'inclusion naturelle $N \hookrightarrow M$ est un morphisme de A-modules.

(3) La **projection canonique** $M \to M/N$ qui à x associe $\overline{x}$ est un morphisme de A-modules.

(4) Les morphismes de $\mathbb{Z}$-modules sont les morphismes de groupes abéliens.

(5) Soient M un A-module, S un ensemble et fixons s_0 dans S. Alors l'application $\varphi : M^S \to M$ qui à $f \in M^S$ associe $\varphi(f) := f(s_0)$ est un morphisme de A-modules.

Définition D.3. *Soit $f : M \to N$ un morphisme de A-modules. On définit le noyau et l'image de f par*

$$\mathrm{Ker}\, f := \{x \in M; f(x) = 0\} \quad \textit{et} \quad \mathrm{Im}\, f := \{f(x); x \in M\}\,.$$

Proposition D.4. Soit $f : M \to N$ un morphisme de A-modules. Alors

- ✦ Pour tout sous-module N' de N, $f^{-1}(N')$ est un sous-module de M. En particulier, $\mathrm{Ker}\, f = f^{-1}(\{0\})$ est un sous-module de M.
- ✦ Pour tout sous-module M' de M, $f(M')$ est un sous-module de N. En particulier, $\mathrm{Im}\, f = f(M)$ est un sous-module de N.

Démonstration. En exercice. D.4

Remarque D.5. Soit $f : M \to N$ un morphisme de A-modules. Alors f est injectif si et seulement si $\mathrm{Ker}\, f = \{0\}$, et f est surjectif si et seulement si $\mathrm{Im}\, f = N$. *[Exercice].*

Proposition D.6. La composée de deux morphismes de A-modules est un morphisme de A-modules.

Démonstration. En exercice. D.6

Proposition D.7. Si $f : M \to N$ est un morphisme de A-modules qui est bijectif, alors $f^{-1} : N \to M$ est un morphisme de A-modules.

Démonstration. En exercice. D.7

Définition D.8. *Un **isomorphisme** de A-modules est un morphisme de A-modules qui est bijectif.*

Proposition D.9. La projection canonique $\pi : M \to M/N$ induit une bijection entre les sous-modules de M/N et les sous-modules de M contenant N.

Démonstration. Notons $\mathcal{S}_{M,N}$ l'ensemble des sous-modules de M qui contiennent N, et $\mathcal{S}_{M/N}$ l'ensemble des sous-modules de M/N. On définit une application $\varphi : \mathcal{S}_{M,N} \to \mathcal{S}_{M/N}$ en posant $\varphi(P) = \pi(P)$ et une application $\psi : \mathcal{S}_{M/N} \to \mathcal{S}_{M,N}$ en posant $\psi(\bar{P}) = \pi^{-1}(\bar{P})$. Ces applications ont bien un sens : on sait que $\pi(P)$ est un sous-module de M/N, et que $\pi^{-1}(\bar{P})$ est un sous-module de M. De plus, puisque $\{0\} \subset \bar{P}$, on a $N = \operatorname{Ker}\pi = \pi^{-1}(\{0\}) \subset \pi^{-1}(\bar{P})$.

On a bien $\varphi \circ \psi = \mathrm{id}_{\mathcal{S}_{M/N}}$ car π est surjectif.

Pour $\psi \circ \varphi$: on a toujours $\pi^{-1}(\pi(P)) \supset P$. Pour l'autre inclusion, soit $x \in \pi^{-1}(\pi(P))$. Alors $\pi(x) \in \pi(P)$, donc il existe $y \in P$ tel que $\pi(x) = \pi(y)$. Mais alors $x - y = n \in \operatorname{Ker}\pi = N \subset P$, donc $x = y + n \in P$. On a donc bien $\psi \circ \varphi = \mathrm{id}_{\mathcal{S}_{M,N}}$. D.9

D.2 Théorèmes d'isomorphisme

Théorème D.10 (Premier théorème d'isomorphisme)**.** Soit $f : M \to N$ un morphisme de A-modules. Alors il existe un isomorphisme $\bar{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$.

Démonstration. Notons $\overline{x}$ la classe dans $M/\operatorname{Ker} f$ d'un élément de M. Posons $\bar{f}(\overline{x}) = f(x)$ pour tout $\overline{x} \in M/\operatorname{Ker} f$, et montrons que cela définit bien une application $\bar{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$. Si on choisit un autre représentant $y \in M$ de $\overline{x}$, alors $x - y$ est dans $\operatorname{Ker} f$, donc $f(x - y) = 0$ et donc $f(x) = f(y)$. Donc $\bar{f}$ est une application bien définie. Il faut démontrer que c'est un morphisme (exercice).

Montrons que $\bar{f}$ est injectif. Si $\bar{f}(\overline{x}) = 0$ alors $f(x) = 0$, donc $x \in \operatorname{Ker} f$ et donc $\overline{x} = \overline{0}$. Donc $\operatorname{Ker}\bar{f} = \{\overline{0}\}$.

Si $y \in \operatorname{Im} f$, il existe $x \in M$ tel que $y = f(x)$ et donc $y = \bar{f}(\overline{x}) \in \operatorname{Im}\bar{f}$. Donc $\bar{f}$ est surjectif. D.10

Plus généralement :

Théorème D.11 (Passage au quotient)**.** Soient M et M' deux A-modules, soit N un sous-module de M et soit N' un sous-module de M'. On note $\pi : M \to M/N$ et $\pi' : M' \to M'/N'$ les projections. Soit $f : M \to M'$ un morphisme de A-modules tel que $f(N) \subset N'$.
Alors il existe un unique morphisme de A-modules $\bar{f} : M/N \to M'/N'$ tel que $\bar{f} \circ \pi = \pi' \circ f$.

Démonstration. La condition $\bar{f} \circ \pi = \pi' \circ f$ nous impose de définir $\bar{f}(\overline{x}) = \overline{f(x)}$ pour tout $\overline{x} \in M/N$. Donc si $\bar{f}$ existe, il est unique.

Montrons que la formule ci-dessus définit bien une application : si on choisit un autre représentant $y \in M$ de $\overline{x}$, on a donc $x - y \in N$, donc $f(x - y) \in f(N) \subset N'$, et donc $\overline{f(x - y)} = \overline{0}$ dans M'/N'. On a donc $\overline{f(x)} = \overline{f(y)}$.

Il reste à démontrer que $\bar{f}$ est un morphisme de A-modules. *(Exercice).* D.11

Corollaire D.12 (Deuxième théorème d'isomorphisme)**.** Soit M un A-module, et soient N et N' deux sous-modules de M. Alors $N/(N \cap N') \cong (N + N')/N'$ (isomorphisme de A-modules).

Démonstration. N' est un sous-module de $N+N'$. La composée de l'inclusion $N \to N+N'$ suivie de la projection $N+N' \to (N+N')/N'$ nous donne donc un morphisme $N \to (N+N')/N'$ qui est surjectif *(exercice)* et dont le noyau est $N \cap N'$ *(exercice)*, donc il induit un isomorphisme $N/(N\cap N') \cong (N+N')/N'$ d'après le premier théorème d'isomorphisme. D.12

Corollaire D.13 (Troisième théorème d'isomorphisme)**.** Soit M un A-module, M' un sous-module de M et M'' un sous-module de M' ($M'' \subset M' \subset M$). Alors $(M/M'')/(M'/M'') \cong M/M'$ (isomorphisme de A-modules).

Démonstration. Le théorème de passage au quotient appliqué à id_M nous permet de définir un morphisme de A-modules $M/M'' \to M/M'$. Cet morphisme est clairement surjectif, et son noyau est M'/M''. Donc d'après le premier théorème d'isomorphisme il induit un isomorphisme de A-modules $(M/M'')/(M'/M'') \cong M/M'$. D.13

Définition-Proposition D.14. Soient M et N deux A-modules. L'ensemble $\mathrm{Hom}_A(M,N)$ des morphismes de A-modules de M dans N est un A-module pour les opérations suivantes :

- ✦ Si f et g sont dans $\mathrm{Hom}_A(M,N)$, alors $f+g \in \mathrm{Hom}_A(M,N)$ est défini par $(f+g)(x) = f(x)+g(x)$ pour tout $x \in M$.
- ✦ Si f est dans $\mathrm{Hom}_A(M,N)$ et si $a \in A$, alors $af \in \mathrm{Hom}_A(M,N)$ est défini par $(af)(x) = af(x)$ pour tout $x \in M$.

Démonstration. En exercice. Attention, on se sert ici du fait que A est commutatif. D.14

D.3 Produit direct, somme directe de *modules*

Définition-Proposition D.15. Soit $(M_i)_{i\in I}$ une famille non-vide de A-modules.

- ✦ Le **produit** des M_i, noté $\prod_{i\in I} M_i$, est l'ensemble des familles $(x_i)_{i\in I}$ avec $x_i \in M_i$ pour tout $i \in I$. C'est un A-module, pour les opérations suivantes :
  - ✧ $(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i+y_i)_{i\in I}$
  - ✧ $a(x_i)_{i\in I} = (ax_i)_{i\in I}$.

  Pour chaque $j \in I$, on définit la projection $\pi_j : \prod_{i\in I} M_i \to M_j$ qui à $(x_i)_{i\in I}$ associe x_j. C'est un morphisme de A-modules.
- ✦ La **somme directe** (on précise parfois *externe*) des M_i, noté $\bigoplus_{i\in I} M_i$, est le sous-A-module de $\prod_{i\in I} M_i$ formé des familles $(x_i)_{i\in I}$ dont tous les x_i sont nuls sauf un nombre fini d'entre eux. Pour chaque $j \in I$, on définit l'injection $\sigma_j : M_j \to \bigoplus_{i\in I} M_i$ qui à x_j associe la famille $(m_i)_{i\in I}$ avec $m_j = x_j$ et $m_i = 0$ pour tout $i \neq j$. C'est un morphisme de A-modules.

Démonstration. En exercice. D.15

Remarque D.16. Si I est fini, c'est-à-dire qu'il n'y a qu'un nombre fini de M_i, alors $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Notation D.17. $\prod_{i=1}^2 M_i$ est aussi noté $M_1 \times M_2$. Lorsque tous les M_i sont égaux à un même module M, on note $M^I = \prod_{i\in I} M_i$ et $M^{(I)} := \bigoplus_{i\in I} M_i$. De plus, si I est fini de cardinal n, on note $M^n = M^{(I)} = M^I$.

Remarque D.18. Puisqu'il y a un nombre fini de M_i, on a $M \cong \prod_{i=1}^n M_i = \bigoplus_{i=1}^n M_i$.

Proposition D.19. Soient M un A-module, $n \in \mathbb{N}^*$, et $\varphi_i : M \to M$ un morphisme de A-modules pour chaque i, $1 \leqslant i \leqslant n$ vérifiant

- ✦ $\varphi_i \circ \varphi_j = 0$ si $i \neq j$
- ✦ $\sum_{i=1}^n \varphi_i = \mathrm{id}_M$.

Alors

(i) pour tout $i = 1, \ldots, n$ on a $\varphi_i^2 = \varphi_i$

(ii) si on pose $M_i = \mathrm{Im}\, \varphi_i$, l'application $\begin{array}{rcl} \varphi : M & \to & \prod_{i=1}^n M_i \\ x & \mapsto & (\varphi_1(x), \ldots, \varphi_n(x)) \end{array}$ est un isomorphisme de A-modules.

Démonstration. ✦ $\varphi_j = \varphi_j \circ \mathrm{id}_M = \varphi_j \circ \sum_{i=1}^n \varphi_i = \sum_{i=1}^n \varphi_j \circ \varphi_i = \varphi_j \circ \varphi_j = \varphi_j^2$.

✦ Montrons que φ est injectif : si $x \in \mathrm{Ker}\, \varphi$, alors $\varphi_i(x) = 0$ pour tout $i = 1, \ldots, n$, donc $0 = \sum_{i=1}^n \varphi_i(x) = \mathrm{id}_M(x) = x$. Donc $\mathrm{Ker}\, \varphi = \{0\}$.

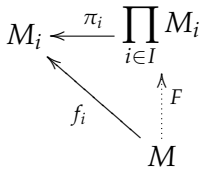
✦ Montrons que φ est surjectif : soit $y = (y_i)_{i=1,\ldots,n} \in \prod_{i=1}^n M_i$. Puisque $M_i = \mathrm{Im}\, \varphi_i$, pour chaque $i = 1, \ldots, n$ il existe $x_i \in M$ tel que $y_i = \varphi_i(x_i)$. On a alors $y_i = \varphi_i(x_i) = \varphi_i^2(x_i) = \varphi_i(y_i)$: on peut donc choisir $x_i = y_i$.
Posons $x = \sum_{i=1}^n y_i$. Fixons $j \in \{1, \ldots, n\}$. Alors $\varphi_j(x) = \sum_{i=1}^n \varphi_j(y_i) = \sum_{i=1}^n \varphi_j(\varphi_i(y_i)) = \varphi_j(\varphi_j(y_j)) = \varphi_j(y_j) = y_j$. Donc $y = (y_i)_{i=1,\ldots,n} = (\varphi_i(x))_{i=1,\ldots,n} = \varphi(x)$. D.19

Corollaire D.20. Soit M un A-module, et soient $N_1, \ldots, N_p$ des sous-modules de M. On suppose que M est égal à la somme directe (interne) des *sous-modules* N_i. Alors M est isomorphe à la somme directe (externe) des *modules* N_i.

Démonstration. On suppose que M est la somme directe interne de ses sous-modules N_i. On peut donc écrire tout élément de M de manière unique comme somme d'éléments des N_i. Définissons donc $\varphi_i : M \to M$ pour $1 \leqslant i \leqslant p$ de la façon suivante : si $x = \sum_{i=1}^n x_i \in M$ avec $x_i \in N_i$, on pose $\varphi(x) = x_i$. Il est facile de voir que φ_i est bien défini (puisque l'écriture de x est unique), que c'est un morphisme, que son image est N_i, que $\varphi_i \circ \varphi_j = 0$ si $i \neq j$ et que $\sum_{i=1}^p \varphi_i = \mathrm{id}_M$. D'après la proposition précédente, on a donc des isomorphismes $M \cong \prod_{i=1}^p N_i = \bigoplus_{i=1}^p N_i$ où la dernière somme directe est externe. D.20

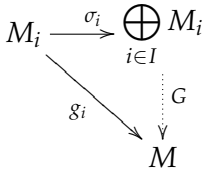
Remarque D.21. Ce corollaire explique l'abus de notation que nous faisons en notant les sommes directes de sous-modules (interne) et de modules (externe) de la même manière.

Proposition D.22 (Propriété universelle du produit)**.** Soit M un A-module, soient M_i, $i \in I$, des A-modules et, pour tout $i \in I$, soit $f_i \in \mathrm{Hom}_A(M, M_i)$. Alors il existe un unique $F \in \mathrm{Hom}_A(M, \prod_{i\in I} M_i)$ tel que pour tout $i \in I$ le diagramme suivant soit commutatif :



Démonstration. Exercice. D.22

Proposition D.23 (Propriété universelle de la somme directe)**.** Soit M un A-module, soient M_i, $i \in I$, des A-modules et, pour tout $i \in I$, soit $g_i \in \mathrm{Hom}_A(M_i, M)$. Alors il existe un unique $G \in \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, M)$ tel que pour tout $i \in I$ le diagramme suivant soit commutatif :



Démonstration. En TD. D.23

Proposition D.24. Soit $(M_i)_{i\in I}$ une famille de A-modules et soit N un A-module. Alors nous avons les isomorphismes de A-modules suivants :

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

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

Démonstration. **(i)** Notons $\sigma_i : M_i \hookrightarrow \bigoplus_{i\in I} M_i$ les inclusions naturelles.

Soit $f \in \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N)$. Alors pour tout $i \in I$, $f \circ \sigma_i \in \mathrm{Hom}_A(M_i, N)$.

Posons donc $\varphi(f) = (f \circ \sigma_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$, et montrons que l'application φ ainsi définie est un isomorphisme de A-modules.

φ morphisme : exercice.

Soit $(g_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$. La propriété universelle de la somme directe nous donne un unique $G \in \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N)$ tel que $G \circ \sigma_i = g_i$ pour tout $i \in I$, c'est-à-dire tel que $\varphi(G) = (g_i)_{i\in I}$. Donc φ est bijectif.

(ii) L'isomorphisme $\psi : \mathrm{Hom}_A(N, \prod_{i\in I} M_i) \cong \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$ est donné par $\psi(f) = (\pi_i \circ f)_{i\in I}$, la démonstration est similaire au cas précédent en utilisant la propriété universelle du produit. D.24

D.4 Suites exactes

Définition D.25. *Une **suite exacte** de A-modules est une suite d'morphismes de A-modules $M' \xrightarrow{f} M \xrightarrow{g} M''$ vérifiant* $\mathrm{Ker}\, g = \mathrm{Im}\, f$.

En particulier, une suite $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *est exacte si*

- f *est injectif*
- $\mathrm{Ker}\, g = \mathrm{Im}\, f$
- g *est surjectif.*

Théorème D.26. Soit $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ une suite exacte de A-modules. Alors, pour tout A-module N, la suite $0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\tilde{g}} \mathrm{Hom}_A(M, N) \xrightarrow{\tilde{f}} \mathrm{Hom}_A(M', N)$ où $\tilde{f}(\varphi) = \varphi \circ f$ et $\tilde{g}(\varphi) = \varphi \circ g$ est exacte.

Démonstration.

- Il est facile de vérifier que $\tilde{f}$ et $\tilde{g}$ sont A-linéaires.
- Montrons que $\tilde{g}$ est injectif : si $\psi \in \mathrm{Ker}\, \tilde{g}$, alors $\psi \circ g = 0$, c'est-à-dire que ψ est nul sur l'image de g. Mais g est surjectif par hypothèse, donc $\mathrm{Im}\, g = M''$, et donc ψ est nul sur M'', c'est-à-dire que ψ est nul.
- Montrons que $\mathrm{Im}\, \tilde{g} \subset \mathrm{Ker}\, \tilde{f}$: soit $\varphi \in \mathrm{Im}\, \tilde{g}$. Alors il existe $\psi \in \mathrm{Hom}_A(M'', N)$ tel que $\varphi = \tilde{g}(\psi) = \psi \circ g$. Donc $\tilde{f}(\varphi) = \varphi \circ f = \psi \circ g \circ f = 0$ puisque $\mathrm{Im}\, f = \mathrm{Ker}\, g$ par hypothèse.

✦ Montrons que $\operatorname{Ker}\tilde{f} \subset \operatorname{Im}\tilde{g}$: soit $\varphi \in \operatorname{Ker}\tilde{f}$. On a donc $0 = \tilde{f}(\varphi) = \varphi \circ f$. On cherche à construire $\psi \in \operatorname{Hom}_A(M'', N)$ tel que $\varphi = \tilde{g}(\psi) = \psi \circ g$.

Soit donc $x'' \in M''$. Puisque g est surjectif, il existe $x \in M$ tel que $x'' = g(x)$. Alors $\varphi(x) \in N$. Posons donc $\psi(x'') = \varphi(x)$. Il faut vérifier que cela définit bien une application ψ : soit $x_1 \in M$ un autre élément tel que $x'' = g(x_1)$. Alors $x - x_1 \in \operatorname{Ker} g = \operatorname{Im} f$, donc il existe $x' \in M'$ tel que $x - x_1 = f(x')$. On a donc $\varphi(x) - \varphi(x_1) = \varphi(x - x_1) = \varphi(f(x')) = \varphi \circ f(x') = 0$, donc $\varphi(x) = \varphi(x_1)$.

Il est facile de voir que l'application ψ ainsi construite est un morphisme de A-modules, et on a bien $\varphi = \tilde{g}(\psi) \in \operatorname{Im}\tilde{g}$.

On en déduit donc que $\operatorname{Ker}\tilde{f} = \operatorname{Im}\tilde{g}$. D.26

Remarque D.27. Si la suite $0 \to M' \to M$ est exacte, on n'a pas nécessairement une suite exacte $\operatorname{Hom}_A(M, N) \to \operatorname{Hom}_A(M', N) \to 0$. Par exemple, si $M = \mathbb{Z}$, $M' = 2\mathbb{Z}$ et $N = \mathbb{Z}$, et si on choisit $\varphi \in \operatorname{Hom}_A(M', N) = \operatorname{Hom}_{\mathbb{Z}}(2\mathbb{Z}, \mathbb{Z})$ l'morphisme de groupes abéliens défini par $\varphi(2) = 1$, alors φ n'a pas d'antécédent dans $\operatorname{Hom}_A(M, N) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$. En effet, si φ a un antécédent $\psi \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$, alors $1 = \varphi(2) = \psi(2) = 2\psi(1)$ donc 2 est inversible dans $\mathbb{Z}$: contradiction.

Théorème D.28. Soit $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ une suite exacte de A-modules. Alors, pour tout A-module M, la suite $0 \to \operatorname{Hom}_A(M, N') \xrightarrow{\tilde{f}} \operatorname{Hom}_A(M, N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N'')$ où $\tilde{f}(\varphi) = f \circ \varphi$ et $\tilde{g}(\varphi) = g \circ \varphi$ est exacte.

Démonstration. ✦ Il est facile de vérifier que $\tilde{f}$ et $\tilde{g}$ sont A-linéaires.

✦ Montrons que $\tilde{f}$ est injectif : soit $\varphi \in \operatorname{Ker}\tilde{f}$. Alors $\tilde{f}(\varphi) = 0$, c'est-à-dire $f \circ \varphi = 0$, et donc $\operatorname{Im}\varphi \subset \operatorname{Ker} f$. Or f est injectif, donc $\operatorname{Ker} f = \{0\}$ et donc $\operatorname{Im}\varphi = \{0\}$, c'est-à-dire que $\varphi = 0$.

✦ Montrons que $\operatorname{Im}\tilde{f} \subset \operatorname{Ker}\tilde{g}$: soit $\psi \in \operatorname{Im}\tilde{f}$, il existe donc $\varphi \in \operatorname{Hom}_A(M, N')$ tel que $\psi = \tilde{f}(\varphi) = f \circ \varphi$. Donc $\tilde{g}(\psi) = g \circ \psi = g \circ f \circ \varphi = 0$ puisque $\operatorname{Im} f \subset \operatorname{Ker} g$ par hypothèse. Donc $\psi \in \operatorname{Ker}\tilde{g}$.

✦ Montrons que $\operatorname{Ker}\tilde{g} \subset \operatorname{Im}\tilde{f}$: soit $\psi \in \operatorname{Ker}\tilde{g}$, on a donc $g \circ \psi = 0$. On veut construire $\varphi \in \operatorname{Hom}_A(M, N')$ tel que $\psi = \tilde{f}(\varphi) = f \circ \varphi$. Soit donc $x \in M$. Alors $\psi(x) \in N$. De plus, $g(\psi(x)) = g \circ \psi(x) = 0$, donc $\psi(x) \in \operatorname{Ker} g = \operatorname{Im} f$. Comme de plus f est injectif, il existe un unique $y' \in N'$ tel que $\psi(x) = f(y')$. Posons donc $\varphi(x) = y'$. On voit facilement que l'application φ ainsi construite est un morphisme de A-modules. D.28

Remarque D.29. Une suite exacte $N \xrightarrow{g} N'' \to 0$ n'induit pas nécessairement une suite exacte $\operatorname{Hom}_A(M, N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N'') \to 0$.

Contre-exemple : $N = \mathbb{Z}$, $N'' = \mathbb{Z}/2\mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. Alors l'morphisme $\mathrm{id} \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ n'a pas d'antécédent dans $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$. En effet, si $\varphi \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$, on a $2\varphi(\bar{1}) = \varphi(2 \cdot \bar{1}) = \varphi(\bar{2}) = \varphi(\bar{0}) = 0$ donc $\varphi(\bar{1}) = 0$ et donc $\varphi = 0$.

Proposition D.30. Soit $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ une suite exacte de A-modules. Alors les conditions suivantes sont équivalentes :

(i) Il existe un morphisme $s : M'' \to M$ tel que $g \circ s = \mathrm{id}_{M''}$. On appelle s une **section** de g.

(ii) Il existe un morphisme $r : M \to M'$ tel que $r \circ f = \mathrm{id}_{M'}$. On appelle r une **rétraction** de f.

Si ces conditions sont satisfaites, alors nous avons des isomorphismes

$$M = \operatorname{Im} f \oplus \operatorname{Ker} r,\ M = \operatorname{Ker} g \oplus \operatorname{Im} s \text{ et } M \cong M' \oplus M''$$

et on dit que la suite exacte est **scindée**.

Démonstration. ✦ Supposons que **(i)** soit vraie, et démontrons que $M = \operatorname{Ker} g \oplus \operatorname{Im} s$. Soit $x \in M$. Alors $x = x - s(g(x)) + s(g(x))$. Or $s(g(x)) \in \operatorname{Im} s$, et $g(x - s(g(x))) = g(x) - g \circ s(g(x)) = g(x) - g(x) = 0$ donc $x - s(g(x)) \in \operatorname{Ker} g$. Donc $M = \operatorname{Ker} g + \operatorname{Im} s$.

Soit maintenant $x \in \operatorname{Ker} g \cap \operatorname{Im} s$. Alors il existe $x'' \in M''$ tel que $x = s(x'')$, et $0 = g(x) = g \circ s(x'') = x''$, donc $x = s(x'') = s(0) = 0$. Donc $\operatorname{Ker} g \cap \operatorname{Im} s = \{0\}$. Donc la somme est directe et $M = \operatorname{Ker} g \oplus \operatorname{Im} s$.

✦ De même, si on suppose que **(ii)** est vraie, on peut démontrer que $M = \operatorname{Im} f \oplus \operatorname{Ker} r$.

✦ Démontrons **(i)⇒(ii)**. Si on suppose que **(i)** est vraie, on a donc $M = \operatorname{Ker} g \oplus \operatorname{Im} s$. Construisons r. Soit $x \in M$, il s'écrit de manière unique $x = y + z$ avec $y \in \operatorname{Ker} g$ et $z \in \operatorname{Im} s$. Puisque $y \in \operatorname{Ker} g = \operatorname{Im} f$ et que f est injective, il existe un unique $y' \in M'$ tel que $y = f(y')$. On pose $r(x) = y'$.

Montrons que r est un morphisme : si $x = y + z \in M$ et $x_1 = y_1 + z_1 \in M$, soit $y' \in M'$ l'unique élément tel que $y = f(y')$ et soit $y'_1 \in M'$ l'unique élément tel que $y_1 = f(y'_1)$. On a donc $r(x) = y'$ et $r(x_1) = y'_1$. D'autre part, $x + x_1 = (y + y_1) + (z + z_1)$, et $y + y_1 = f(y') + f(y'_1) = f(y' + y'_1)$ donc $r(x + x_1) = y' + y'_1 = r(x) + r(x_1)$. De même, $r(ax) = ar(x)$ pour tout $a \in A$.

Enfin, vérifions que $r \circ f = \mathrm{id}_{M'}$. Soit $u \in M'$. Alors $f(u) \in \operatorname{Im} f$ donc la décomposition de $f(u)$ dans $\operatorname{Ker} g \oplus \operatorname{Im} s$ est $f(u) = f(u) + 0$. Par construction de r on a donc $r(f(u)) = u$ (l'unique antécédent de $f(u)$ par f).

✦ Démontrons **(ii)⇒(i)**. On sait que $M = \operatorname{Im} f \oplus \operatorname{Ker} r$ et on veut construire s. Soit donc $x'' \in M''$. Puisque g est surjectif, il existe $x \in M$ tel que $x'' = g(x)$. On peut écrire x de manière unique comme $x = y + z$ avec $y \in \operatorname{Im} f$ et $z \in \operatorname{Ker} r$. On veut poser $s(x'') = z$; montrons que c'est bien défini. Soit $x_1 \in M$ un autre antécédent de x'' par g. Alors on peut écrire $x_1 = y_1 + z_1$ avec $y_1 \in \operatorname{Im} f$ et $z_1 \in \operatorname{Ker} r$. On a alors $z - z_1 = (x - x_1) + (y_1 - y)$. Or $y \in \operatorname{Im} f$, $y_1 \in \operatorname{Im} f$, et $x - x_1 \in \operatorname{Ker} g = \operatorname{Im} f$, donc $z - z_1 \in \operatorname{Im} f \cap \operatorname{Ker} r = \{0\}$, donc $z = z_1$. Donc s est bien défini.

De plus, $g \circ s(x'') = g(z) = g(x) = x''$ puisque $y \in \operatorname{Im} f = \operatorname{Ker} g$, donc $g \circ s$.

Il reste à montrer que s est un morphisme. *(Exercice).*

✦ Finalement, démontrons que si la suite est scindée, on a $M \cong M' \oplus M''$. On sait que $M = \operatorname{Ker} g \oplus \operatorname{Im} s$. Or $\operatorname{Ker} g = \operatorname{Im} f$ et f est injectif, donc f définit un isomorphisme $M' \to \operatorname{Im} f = \operatorname{Ker} g$, donc $\operatorname{Ker} g \cong M'$. D'autre part, s est injectif puisque $g \circ s = \mathrm{id}_{M''}$, donc de même $\operatorname{Im} s \cong M''$. Finalement on a bien $M \cong M' \oplus M''$. D.30

Proposition D.31. Avec les notations du théorème **D.26**, soit $0 \to M' \xrightarrow{f} M \to M'' \xrightarrow{g} 0$ une suite exacte scindée de A-modules. Alors pour tout A-module N, la suite $0 \to \operatorname{Hom}_A(M'', N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N) \xrightarrow{\tilde{f}} \operatorname{Hom}_A(M', N) \to 0$ est une suite exacte.

Démonstration. On sait déjà que la suite $0 \to \operatorname{Hom}_A(M'', N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N) \xrightarrow{\tilde{f}} \operatorname{Hom}_A(M', N)$ est exacte, il reste à montrer que $\tilde{f}$ est surjectif. Soit $h \in \operatorname{Hom}_A(M', N)$. Puisque la suite est scindée, il existe $r \in \operatorname{Hom}_A(M, M')$ tel que $r \circ f = \mathrm{id}_{M'}$. Alors $h \circ r \in \operatorname{Hom}_A(M, N)$, et $\tilde{f}(h \circ r) = h \circ r \circ f = h \circ \mathrm{id}_{M'} = h$. D.31

Proposition D.32. Avec les notations du théorème **D.28**, soit $0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ une suite exacte scindée de A-modules. Alors pour tout A-module M, la suite $0 \to \operatorname{Hom}_A(M, N') \xrightarrow{\tilde{f}} \operatorname{Hom}_A(M, N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N'') \to 0$ est une suite exacte.

Démonstration. On sait déjà que la suite $0 \to \operatorname{Hom}_A(M, N') \xrightarrow{\tilde{f}} \operatorname{Hom}_A(M, N) \xrightarrow{\tilde{g}} \operatorname{Hom}_A(M, N'')$ est exacte, il reste à démontrer que $\tilde{g}$ est surjectif. Soit $h \in \operatorname{Hom}_A(M, N'')$. Puisque la suite est scindée, il existe $s \in \operatorname{Hom}_A(N'', N)$ tel que $g \circ s = \mathrm{id}_{N''}$. Alors $s \circ h \in \operatorname{Hom}_A(M, N)$, et $\tilde{g}(s \circ h) = g \circ s \circ h = \mathrm{id}_{N''} \circ h = h$. D.32

E Modules libres

Définition E.1. *Soit A un anneau. Un A-module **libre** est un A-module isomorphe à $A^{(I)}$ pour un ensemble non-vide I.*

Théorème E.2. Soit M un A-module. Alors il existe un A-module libre L et un morphisme surjectif $\varphi : L \to M$. En particulier, M est isomorphe à un quotient d'un A-module libre. De plus, si M est de type fini, on peut choisir L de type fini.

Démonstration. Soit S une partie génératrice de M (que l'on peut choisir finie si M est de type fini). Soit $L = A^{(S)}$. On définit φ en envoyant $(a_s)_{s\in S} \in A^{(S)}$ sur $\sum_{s\in S} a_s s \in M$ (notons que la somme est finie puisque tous les a_s sont nuls sauf un nombre fini d'entre eux, donc elle a bien un sens). C'est un morphisme, qui est surjectif puisque M est engendré par S.

On en déduit par le premier théorème d'isomorphisme un isomorphisme $A^{(S)} / \operatorname{Ker}\varphi \cong M$. E.2

E.1 Modules libres et bases

Définition E.3. *Soit M un A-module.*

(i) *On dit qu'une partie S de M est **libre** si pour toute partie finie T de S, la relation $\sum_{s\in T} a_s s = 0$ avec les $a_s \in A$ entraîne $a_s = 0$ pour tout $s \in T$.*

(ii) *On dit qu'une partie S de M est une **base** si c'est une partie libre et génératrice de M.*

Remarque E.4. **(i)** Soient M et N deux modules isomorphes. Il est facile de vérifier que M possède une base si et seulement si N possède une base.

(ii) Soit I un ensemble non vide. Le A-module libre $A^{(I)}$ admet pour base l'ensemble $\{\varepsilon_i; i \in I\}$ où, pour chaque $i \in I$, ε_j est l'élément $(x_i)_{i\in I}$ de $A^{(I)}$ défini par $x_i = 0$ si $i \neq j$ et $x_j = 1$. En particulier, A admet $\{1\}$ pour base.

(iii) Tout A-module ne possède pas de base. Contre-exemple : $\mathbb{Z}/6\mathbb{Z}$ en tant que $\mathbb{Z}$-module n'a pas de base : par l'absurde, si $\overline{x} \in \mathbb{Z}/6\mathbb{Z}$ est un élément d'une base, on a $6\overline{x} = \overline{0}$ alors que 6 n'est pas nul dans $\mathbb{Z}$; contradiction.

Proposition E.5. Un A-module M est libre si et seulement s'il possède une base.

Démonstration. D'après la remarque qui précède, un A-module libre possède une base.

Supposons maintenant que M soit un A-module qui possède une base, notée S. La démonstration du théorème **E.2** nous donne un morphisme surjectif $\varphi : A^{(S)} \to M$ défini par $\varphi(\sum_{s\in S} a_s\varepsilon_s) = \sum_{s\in S} a_s s$ avec les notations de la remarque ci-dessus. Il reste à démontrer que φ est injectif. Soit $x \in \operatorname{Ker}\varphi$. Alors $x = \sum_{s\in T} a_s\varepsilon_s$ où T est une partie finie de S, et $0 = \varphi(x) = \sum_{s\in T} a_s s$. Mais puisque S est une partie libre de M, on a $a_s = 0$ pour tout $s \in T$, et donc $x = 0$. Donc $\operatorname{Ker}\varphi = \{0\}$ et φ est un isomorphisme. Donc M est libre. E.5

Théorème E.6 (Propriété universelle)**.** Soit M un A-module et soit S une partie génératrice de M. Notons $\iota : S \to M$ l'inclusion. Alors le module M est libre de base S si et seulement si pour tout module N et toute application $\sigma : S \to N$ il existe un unique morphisme de A-modules $f : M \to N$ tel que $f \circ \iota = \sigma$.

Démonstration. ($\Rightarrow$) Supposons que M soit libre de base S. Si $x \in M$, il s'écrit de manière unique $x = \sum_{s\in T} a_s s$ où T est une partie finie de S et les a_s sont dans A.

Supposons un instant que f satisfaisant aux conditions de l'énoncé existe. Alors puisque f doit être A-linéaire et satisfaire à $f \circ \iota = \sigma$, on doit avoir

$$f(x) = \sum_{s\in T} a_s f(s) = \sum_{s\in T} a_s f(\iota(s)) = \sum_{s\in T} a_s \sigma(s).$$

On en déduit donc que si f existe, elle est unique.

Maintenant, posons $f(x) = \sum_{s\in T} a_s\sigma(s) \in N$. Alors f est bien définie car l'écriture de x est unique. On voit facilement que $f \circ \iota = \sigma$. Il reste à vérifier que f est un morphisme de A-modules (exercice).

($\Leftarrow$) Supposons que M vérifie la propriété universelle. Soit $N := A^{(S)}$. Alors il existe un morphisme de A-modules $f : M \to A^{(S)}$ vérifiant $f \circ \iota = \sigma$ où σ est l'injection naturelle $S \to A^{(S)}$ (donc $\sigma(s) = \varepsilon_s$ pour tout $s \in S$).

f est surjectif ; en effet, si $x \in A^{(S)}$, on peut écrire $x = \sum_{s\in T} a_s\varepsilon_s$ avec $T \subset S$ fini et $a_s \in A$ pour tout $s \in T$. Alors $x = \sum_{s\in T} a_s\sigma(s) = \sum_{s\in T} a_s f \circ \iota(s) = f(\sum_{s\in T} a_s\iota(s)) \in \operatorname{Im} f$.

Il reste à montrer que f est injectif. Soit donc $m \in \operatorname{Ker} f$. Puisque S est une partie génératrice de M, on peut écrire $m = \sum_{s\in T} a_s s = \sum_{s\in T} a_s\iota(s)$ où T est une partie finie de S. Alors $0 = f(m) = \sum_{s\in T} a_s f(\iota(s)) = \sum_{s\in T} a_s\sigma(s) = \sum_{s\in T} a_s\varepsilon_s$. Or $\{\varepsilon_s; s \in S\}$ est une base de $A^{(S)}$, donc $a_s = 0$ pour tout $s \in T$ et donc $m = 0$.

Donc f est un isomorphisme, et donc M est libre de base S. E.6

Remarque E.7. Attention ! Les A-modules n'ont pas les mêmes comportements que les espaces vectoriels !

- ✦ Nous avons déjà vu qu'un module n'était pas forcément libre.
- ✦ Un sous-module d'un module libre n'est pas forcément libre : Soit q un entier, et soit $A = \mathbb{Z}/q^2\mathbb{Z}$. L'idéal $\mathcal{I} = q\mathbb{Z}/q^2\mathbb{Z}$ de A est un sous-module de A, qui n'est pas libre. En effet, pour tout $x \in \mathcal{I}$, on a $qx = 0$ avec $q \neq 0$ dans A, donc aucune partie de $\mathcal{I}$ ne peut être libre et donc une base de $\mathcal{I}$.
- ✦ Un sous-module d'un module de type fini n'est pas forcément de type fini. Soit $A = \mathbb{R}^{\mathbb{N}}$. Alors *en tant que A-module, A* est (libre) de type fini (engendré par 1). Soit $\mathcal{I} = \mathbb{R}^{(\mathbb{N})}$: c'est un A-module puisque c'est un idéal, sous-module de A, mais il n'est pas de type fini. Par l'absurde : soient $x^1 = (x^1_n)_{n\in\mathbb{N}}, \dots, x^p$ des éléments de $\mathcal{I}$ qui engendrent $\mathcal{I}$ en tant que A-module. Pour chaque $j = 1, \dots, p$, notons $K_j = \left\{n \in \mathbb{N}; x^j_n \neq 0\right\}$. Chaque K_j est fini par définition de la somme directe. Posons $K = \cup_{j=1}^p K_j$.

  Soit $N \in \mathbb{N}$, avec $N \notin K$ (c'est possible puisque K est fini). Soit $x = (x_n)_{n\in\mathbb{N}}$ l'élément défini par $x_N = 1$ et $x_n = 0$ si $n \neq N$. Alors $x \in \mathcal{I}$, mais il est clair que $x \notin \langle x^1, \dots, x^p\rangle$ ce qui contredit le fait que $\left\{x^1, \dots, x^p\right\}$ engendre $\mathcal{I}$.

En revanche, nous allons voir que deux bases d'un A-module libre de type fini ont le même nombre d'éléments.

Théorème E.8. Soit M un A-module libre. Alors toutes les bases de M ont le même nombre d'éléments.

Démonstration. Soit $\{e_i, i \in I\}$ une base de M.

Soit $\mathfrak{m}$ un ideal maximal de A (Krull). On a déjà vu que $M/\mathfrak{m}M$ est un $A/\mathfrak{m}$-module (exercice C.2). De plus, puisque $\mathfrak{m}$ est un idéal maximal, $A/\mathfrak{m}$ est un corps, et donc $M/\mathfrak{m}M$ est un espace vectoriel sur $A/\mathfrak{m}$. On sait donc que toutes les bases de $M/\mathfrak{m}M$ en tant qu'espace vectoriel sur $A/\mathfrak{m}$ ont le même cardinal.

Or on voit facilement que $\{\overline{e}_i; i \in I\}$ est une base de $M/\mathfrak{m}M$ en tant qu'espace vectoriel sur $A/\mathfrak{m}$. En effet, il est clair que c'est une famille génératrice. De plus, supposons que l'on ait une relation de dépendance $\sum_{j\in J} \overline{a}_j\overline{e}_j = 0$ avec $J \subset I$ fini. Alors $x = \sum_{j\in J} a_j e_j \in \mathfrak{m}M$, donc on peut écrire $x = \sum_{p=1}^n b_p m_p$ avec $b_p \in \mathfrak{m}$ et $m_p \in M$ pour tout p. Mais puisque $\{e_i; i \in I\}$ est une base de M, on peut écrire $m_p = \sum_{k\in K} \lambda_{p,k}e_k$ où K est une partie finie de I et les $\lambda_{p,k}$ sont dans A. On a donc une deuxième écriture de x dans la base $\{e_i; i \in I\}$: $x = \sum_{k\in K}\sum_{p=1}^n b_k\lambda_{p,k}e_k$. Par unicité, on a $K = J$ et $a_j = b_j\sum_{p=1}^n \lambda_{p,j} \in \mathfrak{m}$ pour tout j. Donc $\overline{a}_j = 0$ pour tout j. La famille est donc libre.

Chaque base de M en tant que A-module fournit donc une base de $M/\mathfrak{m}M$ en tant qu'espace vectoriel sur $A/\mathfrak{m}$ de même cardinal, elles ont donc toutes le même cardinal. E.8

Définition E.9. *Soit M un A-module libre. Le nombre d'éléments d'une base est appelé le* ***rang*** *de M.*

Remarque E.10. Par convention, le module $\{0\}$ est libre de rang 0.

Exemple E.11. Soit A un anneau principal. Alors tout idéal non nul de A est libre de rang 1.

En effet, soit I un idéal non nul de A. Alors puisque A est principal il existe $a \in A$ tel que $I = (a)$. Il est facile de vérifier que a est une base de I (en utilisant le fait que A est intègre).

Proposition E.12. Soit M un A-module libre de base $\{e_i; i \in I\}$. Soit N un A-module et soit $f \in \mathrm{Hom}_A(M, N)$. Alors :

- **(i)** f est entièrement déterminé par $\{f(e_i); i \in I\}$. Plus précisément, étant donné $\{y_i; i \in I\} \subset N$, il existe un unique $f \in \mathrm{Hom}_A(M, N)$ tel que $f(e_i) = y_i$ pour tout $i \in I$.
- **(ii)** f est injectif si et seulement si $\{f(e_i); i \in I\}$ est libre, surjectif si et seulement si $\{f(e_i); i \in I\}$ engendre N et bijectif si et seulement si $\{f(e_i); i \in I\}$ est une base de N.

Démonstration. **(i)** On applique la propriété universelle des modules libres : si $\sigma : \{e_i; i \in I\} \to N$ est l'application qui à e_i associe y_i, alors on sait qu'il existe un unique morphisme de A-modules $f : M \to N$ tel que $f(e_i) = \sigma(e_i) = y_i$ pour tout $i \in I$.

(ii)
- ✧ Supposons f injectif. Soit J une partie finie de I et soient a_j, $j \in J$ des éléments de A tels que $\sum_{j\in J} a_j f(e_j) = 0$. Alors $f(\sum_{j\in J} a_j e_j) = 0$ et donc $\sum_{j\in J} a_j e_j = 0$. Puisque $\{e_i; i \in I\}$ est libre on en déduit que $a_j = 0$ pour tout $j \in J$. Donc $\{f(e_i); i \in I\}$ est libre.
  Supposons réciproquement que $\{f(e_i); i \in I\}$ est libre. Soit $x \in \mathrm{Ker}\, f$. On a $x \in M$, donc il existe $J \subset I$ fini et des éléments a_j, $j \in J$ de A tels que $x = \sum_{j\in J} a_j e_j$. On a donc $0 = f(x) = \sum_{j\in J} a_j f(e_j)$, donc $a_j = 0$ pour tout $j \in J$ et donc $x = 0$. Donc $\mathrm{Ker}\, f = \{0\}$.
- ✧ Supposons f surjectif. Soit $y \in N$. Alors il existe $x \in M$ tel que $y = f(x)$. Avec les notations ci-dessus, on a $y = \sum_{j\in J} a_j f(e_j) \in \langle\{f(e_i); i \in I\}\rangle$.
  Supposons que $\{f(e_i); i \in I\}$ engendre N. Soit $y \in N$. Alors il existe $J \subset I$ fini et des éléments a_j, $j \in J$ de A tels que $y = \sum_{j\in J} a_j f(e_j)$. Donc $y = f(\sum_{j\in J} a_j e_j) \in \mathrm{Im}\, f$. Donc $N = \mathrm{Im}\, f$.
- ✧ La fin est claire.

E.12

Proposition E.13. Deux modules libres de même rang sont isomorphes.

Démonstration. Soient M et N deux modules libres de même rang. Il existe donc un ensemble non vide I, une base $\{e_i; i \in I\}$ de M et une base $\{\varepsilon_i; i \in I\}$ de N (on peut supposer que les deux bases sont indexées par le même ensemble puisque les ensembles d'indices sont en bijection par hypothèse (même cardinal)). D'après la proposition précédente, on peut donc définir $f \in \mathrm{Hom}_A(M, N)$ en posant $f(e_i) = \varepsilon_i$ pour tout $i \in I$. Puisque l'image d'une base de M par f est une base de N, f est un isomorphisme. E.13

Proposition E.14. Soit M un A-module libre et soit N un A-module isomorphe à M. Alors N est libre de même rang que N.

Démonstration. En exercice. *cf.* remarque **E.4**. E.14

Proposition E.15. Soit $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ une suite exacte de A-modules.

- **(i)** On suppose que M'' est libre. Alors $M \cong M' \oplus M''$.
- **(ii)** On suppose que M'' et M' sont libres. Alors M est libre.
- **(iii)** On suppose que M'' et M' sont libres de rangs finis respectifs n' et n''. Alors M est libre de rang $n' + n''$.

Démonstration. **(i)** Nous allons démontrer que la suite est scindée, le résultat en découle.

Soit $\{e_i; i \in I\}$ une base de M''. Puisque g est surjectif, il existe $m_i \in M$ tel que $e_i = g(m_i)$ pour tout $i \in I$. On définit $s \in \mathrm{Hom}_A(M'', M)$ en posant $s(e_i) = m_i$ pour tout $i \in I$. Alors l'endomorphisme $g \circ s$ de M'' envoie e_i sur e_i pour tout $i \in I$, donc $g \circ s = \mathrm{id}_{M''}$. Donc la suite exacte est bien scindée.

(ii) Soit $\{e_i; i \in I\}$ une base de M'' et soit $\{\varepsilon_j; j \in J\}$ une base de M'. On pose $K = I \cup J$ et, pour tout $k \in K$, $x_k = \begin{cases} (0, e_k) & \text{si } k \in I \\ (\varepsilon_k, 0) & \text{si } k \in J. \end{cases}$ Alors $\{x_k; k \in K\}$ est une base de $M' \oplus M''$ *(exercice)*, qui est donc libre. Donc M, qui est isomorphe à $M' \oplus M''$, est libre.

(iii) Cela découle immédiatement de la démonstration du point précédent : le rang de M est $\mathrm{card}(K) = \mathrm{card}(I \cup J) = n'' + n'$. E.15

F Annulateurs et torsion

Définition-Proposition F.1. Soit A un anneau et soit M un A-module.

(1) Soit $x \in M$. L'ensemble $\mathrm{Ann}_A(x) := \{a \in A; ax = 0\}$ est un idéal de A, appelé **annulateur** de x.

(2) L'ensemble $\mathrm{Ann}_A(M) = \cap_{x \in M} \mathrm{Ann}_A(x)$ est un idéal de A appelé **annulateur** de M.

Démonstration. Exercice. F.1

Remarque F.2. On a vu que si I est un idéal de A et M est un A-module, alors M/IM est un A/I-module.

Donc pour tout idéal I de A contenu dans $\mathrm{Ann}_A(M)$, M est un A/I-module (puisque $IM = \{0\}$).

Exercice F.3. Soit M un A-module et soient N et P des A-modules. Alors

(1) $\mathrm{Ann}_A(N + P) = \mathrm{Ann}_A(N) \cap \mathrm{Ann}_A(P)$.

(2) L'ensemble $(N : P) := \{a \in A; aP \subset N\}$ est un idéal de A, égal à $\mathrm{Ann}_A\left((N + P)/N\right)$.

Définition F.4. *Soient A un anneau et M un A-module. On dit que $x \in M$ est **de torsion** si $\mathrm{Ann}_A(x) \neq \{0\}$.*

Définition-Proposition F.5. Soit A un anneau *intègre*, et soit M un A-module. Alors $T(M) := \{x \in M; x \text{ est de torsion}\}$ est un sous-module de M, appelé **sous-module de torsion** de M.

Démonstration.

- $0 \in T(M)$ donc $T(M) \neq \varnothing$.
- Soient x et y dans $T(M)$. Il existe donc $a \neq 0$ dans A tel que $ax = 0$ et $b \neq 0$ dans A tel que $by = 0$. Alors $ab \neq 0$ (puisque A est intègre) et $ab \in \mathrm{Ann}_A(x - y)$, car $ab(x - y) = b(ax) - a(bx) = 0$. Donc $x - y \in T(M)$. Donc $T(M)$ est un groupe abélien.
- Soit $a \in A$ et $x \in T(M)$. Alors il existe $b \neq 0$ dans A tel que $bx = 0$. On a donc $b(ax) = a(bx) = 0$, donc $b \in \mathrm{Ann}_A(ax)$, donc $ax \in T(M)$. F.5

Définition F.6. *Si $T(M) = \{0\}$, on dit que M est **sans torsion**. Si $M = T(M)$ on dit que M est **de torsion**.*

Proposition F.7. Soient A un anneau intègre et M un A-module. Alors $M/T(M)$ est un A-module sans torsion.

Démonstration. Soit $\overline{x} \in M/T(M)$ un élément de torsion. Alors il existe $a \in A$, $a \neq 0$, tel que $a\overline{x} = \overline{0}$, c'est-à-dire tel que $ax \in T(M)$. Il existe donc $b \in A$, $b \neq 0$, tel que $bax = 0$. Puisque A est intègre, $ba \neq 0$, donc $x \in T(M)$ et donc $\overline{x} = \overline{0}$. F.7

Proposition F.8. Soit A un anneau intègre, soient M et N deux A-modules, et soit $f \in \mathrm{Hom}_A(M, N)$. Alors $f(T(M)) \subset T(N)$.

Démonstration. Exercice. F.8

Proposition F.9. Soit A un anneau intègre et soit $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte de A-modules. Alors la suite $0 \to T(M') \xrightarrow{f_{|T(M')}} T(M) \xrightarrow{g_{|T(M)}} T(M'')$ est exacte.

Démonstration.
- ✦ Tout d'abord, la suite a bien un sens grâce à la proposition précédente, puisque $f(T(M')) \subset T(M)$ et $g(T(M)) \subset T(M'')$.
- ✦ $\mathrm{Ker}\left(f_{|T(M')}\right) = \mathrm{Ker}\, f \cap T(M') = \{0\}$ puisque f est injectif, donc $f_{|T(M')}$ est injectif.
- ✦ On a $g_{|T(M)} \circ f_{|T(M')} = (g \circ f)_{|T(M')} = 0$ car $\mathrm{Im}\, f \subset \mathrm{Ker}\, g$, donc $\mathrm{Im}\, f_{|T(M')} \subset \mathrm{Ker}\, g_{|T(M)}$.
- ✦ Montrons enfin que $\mathrm{Ker}\, g_{|T(M)} \subset \mathrm{Im}\, f_{|T(M')}$. Soit $x \in T(M)$ tel que $g(x) = 0$. Alors $x \in \mathrm{Ker}\, g = \mathrm{Im}\, f$ donc il existe $x' \in M'$ tel que $x = f(x')$. Il suffit de montrer que $x' \in T(M')$ pour avoir $x = f_{|T(M')}(x') \in \mathrm{Im}\, f_{|T(M')}$. Or x est de torsion, donc il existe $a \in A$, $a \neq 0$, tel que $ax = 0$. On a donc $f(ax') = af(x') = ax = 0$, donc $ax' = 0$ puisque f est injectif, et donc $x' \in T(M')$. F.9

Proposition F.10. Soit A un anneau intègre et soit M un A-module libre. Alors M est sans torsion.

Démonstration. Fixons une base $\{e_i; i \in I\}$ de M. Soit $x \in T(M)$; il existe donc $a \in A$, $a \neq 0$, tel que $ax = 0$. On peut écrire $x = \sum_{i \in I} \lambda_i e_i$ pour des $\lambda_i \in A$. On a donc $0 = ax = \sum_{i \in I} a\lambda_i e_i$. Comme la famille $\{e_i; i \in I\}$ est libre, on en déduit que pour tout $i \in I$ on a $a\lambda_i$. Mais $a \neq 0$ et A est intègre, donc $\lambda_i = 0$ pour tout $i \in I$ et finalement $x = 0$. F.10

G Restriction des scalaires

Proposition G.1. Soient A, B deux anneaux, $f : A \longrightarrow B$ un morphisme d'anneaux et M un B-module. L'application

$$\begin{array}{rccc} \mu & : & A \times M & \longrightarrow & M \\ & & (a, m) & \mapsto & f(a).m \end{array}$$

munit M d'une structure de A-module.

Démonstration. Exercice facile. G.1

Définition G.2. *Soient A, B deux anneaux, $f : A \longrightarrow B$ un morphisme d'anneaux et M un B-module. La structure de A-module induite par f sur M est appelée structure obtenue par **restriction des scalaires** via f.*

Exemple G.3. Le cas $A = \mathbb{R}$ et $B = \mathbb{C}$ permet de considérer tout $\mathbb{C}$-espace vectoriel comme un $\mathbb{R}$-espace vectoriel par restriction des scalaires.

Exemple G.4. Soient A un anneau et I un idéal de A. La projection canonique $\pi : A \longrightarrow A/I$ munit le A/I-module A/I d'une structure de A-module par restriction des scalaires. On vérifie facilement que cette structure n'est autre que celle définie par passage au quotient par I dans le A-module A.

Par exemple, le cas $A = \mathbb{Z}$ et $I = p\mathbb{Z}$ avec p premier est très utilisé en arithmétique.

H Algèbres

Soit k un anneau commutatif, unitaire. Dans cette section (seulement), A sera un anneau unitaire mais pas nécessairement commutatif.

Définition H.1. *Le **centre** de A est l'ensemble $Z(A) = \{a \in A; \forall x \in A,\ ax = xa\}$. C'est un sous-anneau (qui lui est commutatif) de A.*

Lorsque A est commutatif, $Z(A) = A$.

Définition H.2. *Une k-algèbre est un couple (A, f) où A est un anneau (unitaire mais pas nécessairement commutatif) et $f : k \to Z(A)$ est un morphisme d'anneaux. Par abus de langage, on parle alors de la k-algèbre A (en oubliant la mention explicite de f).*

*f est appelé **morphisme structural** de A.*

Si l'anneau A est commutatif on dit que l'algèbre A (ou (A, f)) est commutative.

Remarque H.3. Soit (A, f) une k-algèbre. Puisque A est un $Z(A)$-module **(exercice)** et $f : k \to Z(A)$ un morphisme d'anneaux, alors A est un k-module par restriction des scalaires (l'action de $\lambda \in k$ sur $a \in A$ est donnée par $\lambda \cdot a = f(\lambda)a$). Ainsi, une k-algèbre A est en particulier un anneau A muni d'une structure de k-module. Cependant, sur cette structure de k-module est imposée une condition de compatibilité avec le produit de A; en effet, pour $\lambda \in k$ et $x, y \in A$, on a $\lambda \cdot (xy) = f(\lambda)(xy) = (f(\lambda)x)y = (\lambda \cdot x)y$ et $\lambda \cdot (xy) = (f(\lambda)x)y = (xf(\lambda))y = x(f(\lambda)y) = x(\lambda \cdot y)$ (puisque $f(\lambda)$ est dans le centre de A).

Proposition H.4. Une k-algèbre est la donnée d'un anneau A et d'une application $\mu : k \times A \to A$ qui à (λ, a) associe $\lambda \cdot a$ et qui munit le groupe abélien A d'une structure de k-module, tels que pour $\lambda \in k$ et $x, y \in A$ on ait $\lambda \cdot (xy) = (\lambda \cdot x)y = x(\lambda \cdot y)$.

Démonstration. Exercice (on retrouve la définition en considérant $f : k \to Z(A)$, $\lambda \mapsto \lambda \cdot 1_A$). H.4

Définition H.5. *Soient (A, f) et (B, g) deux k-algèbres. Un **morphisme de k-algèbres** de A dans B est une application $h : A \to B$ qui est un morphisme d'anneaux et tel que $h \circ f = g$.*

On a les notions habituelles d'endomorphisme, isomorphisme et automorphisme de k-algèbres.

Lemme H.6. Soient (A, f) et (B, g) deux k-algèbres. Une application $h : A \to B$ est un morphisme de k-algèbres si et seulement si h est un morphisme d'anneaux et un morphisme de k-modules.

Démonstration. Exercice. H.6

Exemple H.7. **(a)** Soit A un anneau. L'application $\varphi_A : \mathbb{Z} \to Z(A)$ qui à s associe $s \cdot 1_A$ (somme de 1_A avec lui-même s fois) est un morphisme d'anneaux. Tout anneau est donc canoniquement muni d'une structure de $\mathbb{Z}$-algèbre.

(b) Si I est un idéal d'un anneau commutatif A, alors A/I est canoniquement muni d'une structure de A-algèbre (commutative) par la projection canonique.

(c) L'injection canonique d'un anneau commutatif A dans l'anneau de polynômes $A[X]$ munit $A[X]$ d'une structure de A-algèbre (commutative).

Remarque H.8. Soit (A, f) une k-algèbre. En général, f n'est pas injective. Cependant, si k est un corps et si A n'est pas nul, alors f est injective (puisque son noyau est un idéal de k distinct de k, donc nul).

Donc si k est un corps et si (A, f) est une k-algèbre, k s'identifie à un sous-anneau de A (via f et l'inclusion $Z(A) \hookrightarrow A$).

Définition H.9. *Soit A une k-algèbre commutative. Si $x_1, \dots, x_s$ sont des éléments de A, une **combinaison algébrique** en les $x_1, \dots, x_s$ est un élément de A de la forme*

$$\sum_{(i_1,\dots,i_s)\in\mathbb{N}^s} \lambda_{i_1,\dots,i_s} x_1^{i_1} \cdots x_s^{i_s}$$

les $\lambda_{i_1,\dots,i_s} \in k$ étant presque tous nuls (pour que cette somme ait un sens).

Définition H.10. *Soit k un anneau.*

- **(i)** *Une k-algèbre commutative A est de **type fini** (comme k-algèbre) s'il existe une famille finie $\{x_1, \dots, x_s\}$ d'éléments de A telle que tout élément de A soit une combinaison algébrique en les $x_1, \dots, x_s$. On dit que $\{x_1, \dots, x_s\}$ **engendre** A comme k-algèbre.*
- **(ii)** *Un anneau commutatif A est dit de **type fini** s'il est de type fini comme $\mathbb{Z}$-algèbre. [Les anneaux commutatifs sont les $\mathbb{Z}$-algèbres commutatives].*

Définition H.11. *Soient k un anneau et A une k-algèbre commutative. Une **sous-k-algèbre** (commutative) de A est un sous-anneau B de A tel que* $\operatorname{Im} f \subset B$.

Lemme H.12. Soient k un anneau et (A, f) une k-algèbre commutative. Une partie B de A est une sous-k-algèbre de A si et seulement si B est un sous-anneau de A qui est aussi un sous-k-module de A.

Démonstration. Exercice. H.12

IV Anneaux de polynômes

A Anneaux de polynômes

Dans toute cette section, A désigne un anneau.

Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{N}^n$ est muni d'une structure de monoïde commutatif (dont l'élément neutre est noté 0) par la loi de composition interne

$$\begin{array}{rccc} + & : & \mathbb{N}^n \times \mathbb{N}^n & \longrightarrow & \mathbb{N}^n \\ & & ((i_1,\dots,i_n),(j_1,\dots,j_n)) & \mapsto & (i_1+j_1,\dots,i_n+j_n) \end{array}$$

(c'est-à-dire que $\mathbb{N}^n$ est un ensemble muni d'une loi de composition interne qui est associative, qui admet un élément neutre et qui est commutative). Si $x \in \mathbb{N}^n$ et $p \in \mathbb{N}^*$, on note $p.x$ la somme $x + \cdots + x$ (p fois) et on pose $0.x = 0$. Pour $1 \leqslant i \leqslant n$, on pose $e_i = (0,\dots,0,1,0,\dots,0)$ (1 en i-ème position). Il est immédiat que tout élément de $\mathbb{N}^n$ s'écrit de façon unique $\sum_{i=1}^n u_i.e_i$ avec $u_i \in \mathbb{N}$.

On considère le A-module libre $A^{(\mathbb{N}^n)}$. Sur $A^{(\mathbb{N}^n)}$, on définit une loi de composition interne :

$$\begin{array}{rccc} \times & : & A^{(\mathbb{N}^n)} \times A^{(\mathbb{N}^n)} & \longrightarrow & A^{(\mathbb{N}^n)} \\ & & ((a_{\underline{i}})_{\underline{i}\in\mathbb{N}^n},(b_{\underline{i}})_{\underline{i}\in\mathbb{N}^n}) & \mapsto & (c_{\underline{i}})_{\underline{i}\in\mathbb{N}^n} \end{array},$$

où, pour $\underline{i} \in \mathbb{N}^n$, on pose $c_{\underline{i}} = \sum_{\underline{i}=\underline{j}+\underline{k}} a_{\underline{j}} b_{\underline{k}}$.

Théorème A.1. La loi de composition interne $+$ du A-module $A^{(\mathbb{N}^n)}$ et la loi de composition interne $\times$ définie ci-dessus munissent $A^{(\mathbb{N}^n)}$ d'une structure d'anneau. De plus, l'application $\varphi : A \longrightarrow A^{(\mathbb{N}^n)}$, qui à a dans A associe l'élément de $A^{(\mathbb{N}^n)}$ dont l'unique coefficient éventuellement non nul est celui d'indice 0 qui vaut a, est un morphisme injectif d'anneaux. Enfin, la structure de A-module de $A^{(\mathbb{N}^n)}$ induite par restriction des scalaires via φ coïncide avec la structure naturelle de A-module de (la somme directe de A-modules) $A^{(\mathbb{N}^n)}$.

Démonstration. Exercice. A.1

Remarque A.2.
- **(i)** Le théorème **A.1** montre que $A^{(\mathbb{N}^n)}$ est une A-algèbre de morphisme structural φ.
- **(ii)** Comme l'application φ est un morphisme injectif d'anneaux de A dans $A^{(\mathbb{N}^n)}$, on identifiera souvent les éléments de A et leur image par φ dans $A^{(\mathbb{N}^n)}$.
- **(iii)** Soient $a \in A$ et $x \in A^{(\mathbb{N}^n)}$. On peut calculer $a.x$ (si l'on utilise la structure de A-module de $A^{(\mathbb{N}^n)}$) et le produit $ax = \varphi(a)x$ (si l'on utilise la structure d'anneau de $A^{(\mathbb{N}^n)}$). Le théorème **A.1** montre qu'en fait $a.x = ax$.

Définition A.3. *Soit $1 \leqslant i \leqslant n$, on note X_i l'élément de $A^{(\mathbb{N}^n)}$ dont l'unique coefficient non nul est celui d'indice e_i qui vaut 1. Un élément de $A^{(\mathbb{N}^n)}$ de la forme $X_1^{i_1}\dots X_n^{i_n}$, avec $(i_1,\dots,i_n) \in \mathbb{N}^n$ s'appelle un* ***monôme*** *de $A^{(\mathbb{N}^n)}$ (en les $X_1,\dots,X_n$).*

Proposition A.4. L'ensemble des monômes de $A^{(\mathbb{N}^n)}$ en les $X_1,\dots,X_n$ est une base du A-module $A^{(\mathbb{N}^n)}$.

Démonstration. On note $\{\varepsilon_\sigma ; \sigma \in \mathbb{N}^n\}$ la base de $A^{(\mathbb{N}^n)}$ de la remarque **III.E.4**. On vérifie facilement que pour tout $(i_1,\dots,i_n) \in \mathbb{N}^n$, on a $X_1^{i_1}\dots X_n^{i_n} = \varepsilon_{(i_1,\dots,i_n)}$. Donc l'ensemble de tous les monômes de $A^{(\mathbb{N}^n)}$ est égal à la base $\{\varepsilon_\sigma ; \sigma \in \mathbb{N}^n\}$. A.4

Remarque A.5. La proposition **A.4** assure que tout élément de $A^{(\mathbb{N}^n)}$ s'écrit, de façon unique, sous la forme

$$\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)}.X_1^{i_1}\ldots X_n^{i_n},$$

où $a_{(i_1,\ldots,i_n)} \in A$, pour tout $(i_1,\ldots,i_n) \in \mathbb{N}^n$ (somme finie).

Définition A.6. *La A-algèbre $A^{(\mathbb{N}^n)}$ s'appelle l'**anneau des polynômes en n indéterminées $X_1,\ldots,X_n$, à coefficients dans** A. On la note souvent $A[X_1,\ldots,X_n]$.*

Exemple A.7. Lorsque le nombre d'indéterminées n'est pas trop élevé, on les note souvent $X, Y, Z, T, \ldots$ plutôt que $X_1, X_2, X_3, X_4, \ldots$.

Ainsi, l'anneau de polynômes en 2 indéterminées X, Y et à coefficients dans A sera noté $A[X,Y]$. Ses éléments s'écrivent de façon unique sous la forme $\sum_{(i,j)\in\mathbb{N}^2} a_{(i,j)}.X^iY^j$.

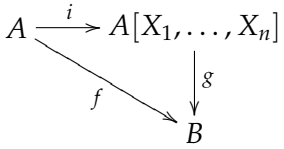
Théorème A.8 (Propriété universelle des anneaux de polynômes)**.** Soient B un anneau, $f : A \longrightarrow B$ un morphisme d'anneaux (B est donc muni d'une structure de A-algèbre commutative via f) et $b_1,\ldots,b_n \in B$. Il existe un morphisme de A-algèbres $g : A[X_1,\ldots,X_n] \longrightarrow B$ et un seul tel que, pour $1 \leqslant i \leqslant n$, $g(X_i) = b_i$.

Démonstration. On vérifie facilement que l'application $g : A[X_1,\ldots,X_n] \longrightarrow B$ définie par

$$g\left(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)}.X_1^{i_1}\ldots X_n^{i_n}\right) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\ldots,i_n)})b_1^{i_1}\ldots b_n^{i_n}$$

vérifie les propriétés requises. A.8

Remarque A.9. On reprend les notations du théorème **A.8**. Le fait que g soit un morphisme de A-algèbres, revient à dire que c'est un morphisme d'anneaux tel que le diagramme suivant soit commutatif :



(*cf.* Lemme **III.H.6**).

Exemple A.10. Soit A un anneau et soit I un idéal de A. Le morphisme d'anneaux $f : A \to (A/I)[X]$ obtenu par composition de la projection $\pi : A \to A/I$ et de l'inclusion $A/I \to (A/I)[X]$ induit donc grâce au théorème **A.8** un morphisme d'anneaux $\varphi_I : A[X] \to (A/I)[X]$ qui prolonge f et tel que $\varphi_I(X) = X$ (c'est-à-dire que $\varphi_I(\sum_{i=0}^n a_iX^i) = \sum_{i=0}^n \pi(a_i)X^i$). Il est clair que φ_I est surjectif.

Corollaire A.11. Soit $m \in \mathbb{N}^*$, $m \leqslant n$.

(i) Il existe un unique morphisme de A-algèbres $i_{m,n} : A[X_1,\ldots,X_m] \longrightarrow A[X_1,\ldots,X_n]$ tel que, pour $1 \leqslant i \leqslant m$, $i_{m,n}(X_i) = X_i$. De plus, $i_{m,n}$ est injectif et son image est la sous-A-algèbre de $A[X_1,\ldots,X_n]$ engendrée par $X_1,\ldots,X_m$.

(ii) Il existe un unique morphisme de A-algèbres $p_{n,m} : A[X_1,\ldots,X_n] \longrightarrow A[X_1,\ldots,X_m]$ tel que, pour $1 \leqslant i \leqslant n$, $p_{n,m}(X_i) = X_i$ si $i \leqslant m$ et $p_{n,m}(X_i) = 0$ sinon. De plus, $p_{n,m}$ est surjectif et son noyau est l'idéal $(X_{m+1},\ldots,X_n)$ de $A[X_1,\ldots,X_n]$ engendré par $X_{m+1},\ldots,X_n$.

(iii) On a $p_{n,m} \circ i_{m,n} = \mathrm{id}_{A[X_1,\ldots,X_m]}$.

Démonstration. **(i)** L'existence et l'unicité du morphisme $i_{m,n}$ se déduisent immédiatement de la propriété universelle des anneaux de polynômes. L'injectivité de $i_{m,n}$ est immédiate puisque cette application envoie la base canonique de $A[X_1, \dots, X_m]$ sur une famille libre de $A[X_1, \dots, X_n]$. Enfin, il est clair qu'un élément de $A[X_1, \dots, X_n]$ est dans l'image de $A[X_1, \dots, X_m]$ si et seulement s'il est combinaison algébrique des éléments $X_1, \dots, X_m$ de $A[X_1, \dots, X_n]$.

(ii) En exercice.

(iii) En exercice. A.11

Si B est une A-algèbre commutative de morphisme structural $f : A \longrightarrow B$, il est clair que l'anneau de polynômes $B[X]$ en une indéterminée X et à coefficients dans B est une A-algèbre commutative de morphisme structural $A \xrightarrow{f} B \xrightarrow{i_{1,B}} B[X]$.

Corollaire A.12. On suppose $n > 1$. On note B l'anneau de polynômes en $n-1$ indéterminées notées $Y_1, \dots, Y_{n-1}$ et à coefficients dans A : $B = A[Y_1, \dots, Y_{n-1}]$. Alors, pour $1 \leqslant i \leqslant n$, il existe un isomorphisme $\varphi_i : A[X_1, \dots, X_n] \longrightarrow B[Y]$ de A-algèbres et un seul tel que $\varphi_i(X_j) = Y_j$ si $j < i$, $\varphi_i(X_j) = Y_{j-1}$ si $j > i$ et $\varphi_i(X_i) = Y$. En particulier, les A-algèbres $A[X_1, \dots, X_n]$ et $B[Y]$ sont isomorphes.

Démonstration. La propriété universelle des anneaux de polynômes assure l'existence des morphismes φ_i de A-algèbres, pour $1 \leqslant i \leqslant n$. Le fait que ces morphismes soient des isomorphismes provient du fait qu'ils envoient une base en tant que A-module de $A[X_1, \dots, X_n]$ (les monômes en les $X_1, \dots, X_n$) sur une base en tant que A-module de $A[Y_1, \dots, Y_{n-1}][Y]$ (monômes en les $Y_1, \dots, Y_{n-1}$ et Y). A.12

Corollaire A.13. Soit A un anneau intègre et $n \in \mathbb{N}^*$. L'anneau de polynômes $A[X_1, \dots, X_n]$ en n indéterminées est intègre.

Démonstration. On procède par récurrence sur n. Le résultat est connu si $n = 1$ (il suffit de regarder les coefficients dominants des polynômes). Il suffit ensuite d'utiliser le corollaire **A.12** pour conclure. A.13

On rappelle que si B est un anneau, l'anneau de polynômes $B[Y]$ en une indéterminée à coefficients dans B est muni d'une application $\deg_Y : B[Y] \longrightarrow \{-\infty\} \cup \mathbb{N}$ qui à tout polynôme $P \in B[Y]$ associe son degré.

Définition A.14. *Soit $P \in A[X_1, \dots, X_n]$; on pose $\deg_{X_i} P = \deg_Y \varphi_i(P)$ où, pour $1 \leqslant i \leqslant n$, φ_i est le morphisme défini au corollaire **A.12**. La fonction $\deg_{X_i}$ est appelé le **degré partiel** en X_i.*

Outre les degrés partiels, on peut associer à tout polynôme un degré total. Si $i = (i_1, \dots, i_n)$ est dans $\mathbb{N}^n$, on appelle **longueur** de i l'élément de $\mathbb{N}$ défini par $|i| = \sum_{s=1}^{n} i_s$.

Définition A.15. *Soit $P = \sum_{(i_1,\dots,i_n) \in \mathbb{N}^n} a_{(i_1,\dots,i_n)} . X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n] \setminus \{0\}$, où $a_{(i_1,\dots,i_n)} \in A$, pour tout $(i_1, \dots, i_n) \in \mathbb{N}^n$. Le **degré total** de P, noté $\deg P$, est défini par*

$$\deg P = \sup \left\{ |i|,\ i = (i_1, \dots, i_n) \in \mathbb{N}^n \text{ tel que } a_{(i_1,\dots,i_n)} \neq 0 \right\}.$$

Le degré total du polynôme nul est $-\infty$, par convention.

B Fonctions polynomiales.

Dans toute cette section, A est un anneau.

Si $n \in \mathbb{N}^*$, on note $\mathcal{F}(A^n, A)$ l'ensemble des applications de A^n dans A. Il est bien connu que $\mathcal{F}(A^n, A)$ est un anneau. Pour tout élément $a \in A$, notons $f_a \in \mathcal{F}(A^n, A)$ l'application, dite constante, qui envoie tout élément de A^n sur a. L'application

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{F}(A^n, A) \\ a & \mapsto & f_a \end{array}$$

est un morphisme d'anneaux, comme on le vérifie facilement. On en déduit que $\mathcal{F}(A^n, A)$ est muni d'une structure de A-algèbre commutative. Si $m \in \mathbb{N}^*$, $m \leqslant n$, soit

$$\begin{array}{rccc} \pi_{n,m} \ : & A^n & \longrightarrow & A^m \\ & (\alpha_1, \ldots, \alpha_n) & \mapsto & (\alpha_1, \ldots, \alpha_m) \end{array} .$$

la surjection canonique. On en déduit une application

$$\begin{array}{rccc} \sigma_{m,n} \ : & \mathcal{F}(A^m, A) & \longrightarrow & \mathcal{F}(A^n, A) \\ & f & \mapsto & f \circ \pi_{n,m} \end{array} .$$

On vérifie facilement que $\sigma_{m,n}$ est un morphisme injectif de A-algèbres.

Soit $P = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} . X_1^{i_1} \ldots X_n^{i_n} \in A[X_1, \ldots, X_n]$, où $a_{(i_1,\ldots,i_n)} \in A$, pour tout $(i_1, \ldots, i_n) \in \mathbb{N}^n$. On associe à P la fonction $\widetilde{P} \in \mathcal{F}(A^n, A)$ définie par

$$\begin{array}{rccc} \widetilde{P} \ : & A^n & \longrightarrow & A \\ & (\alpha_1, \ldots, \alpha_n) & \mapsto & \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} \alpha_1^{i_1} \ldots \alpha_n^{i_n} \end{array} .$$

Cette fonction s'appelle la **fonction polynomiale** associée à P. Par abus de notation, pour $(\alpha_1, \ldots, \alpha_n) \in A^n$, on écrira souvent $P(\alpha_1, \ldots, \alpha_n)$ au lieu de $\widetilde{P}(\alpha_1, \ldots, \alpha_n)$.

Proposition B.1. Soit $n \in \mathbb{N}^*$. L'application $A[X_1, \ldots, X_n] \longrightarrow \mathcal{F}(A^n, A)$, $P \mapsto \widetilde{P}$ est un morphisme de A-algèbres. Son image est notée $\mathcal{F}_{\mathrm{pol}}(A^n, A)$ et est appelée la **A-algèbre des fonctions polynomiales** sur A^n.

Démonstration. C'est une simple vérification. B.1

Soit $n \in \mathbb{N}^*$. La proposition **B.1** montre que l'on dispose d'un morphisme surjectif de A-algèbres

$$\begin{array}{rccc} \varphi_n \ : & A[X_1, \ldots, X_n] & \longrightarrow & \mathcal{F}_{\mathrm{pol}}(A^n, A) \\ & P & \mapsto & \widetilde{P} \end{array} .$$

En outre, on vérifie facilement que, pour $m \in \mathbb{N}^*$, $m \leqslant n$, le diagramme suivant est commutatif :

$$\begin{array}{ccc} A[X_1, \ldots, X_m] & \xrightarrow{i_{m,n}} & A[X_1, \ldots, X_n] \\ \downarrow{\scriptstyle \varphi_m} & & \downarrow{\scriptstyle \varphi_n} \\ \mathcal{F}_{\mathrm{pol}}(A^m, A) & \xrightarrow[\sigma_{m,n}]{} & \mathcal{F}_{\mathrm{pol}}(A^n, A) \end{array} \tag{B.1}$$

Remarque B.2. **(1)** On sait que si K est un corps, le morphisme $\varphi_1 : K[X] \longrightarrow \mathcal{F}_{\mathrm{pol}}(K, K)$ est injectif si et seulement si K est infini.

(2) En fait, à l'aide du diagramme commutatif (**B.1**) appliqué avec $m = 1$ et $A = K$, il s'ensuit aussitôt que si K est fini et $n \in \mathbb{N}^*$, $\varphi_n : K[X_1, \ldots, X_n] \longrightarrow \mathcal{F}_{\mathrm{pol}}(K^n, K)$ n'est pas injectif.

Le théorème suivant montre l'injectivité de φ_n lorque K est infini.

Théorème B.3. Soit K un corps infini et $n \in \mathbb{N}^*$. Le morphisme φ_n de K-algèbres est un isomorphisme.

Démonstration. Il suffit de montrer que, pour tout $n \in \mathbb{N}^*$, φ_n est injectif (puisqu'il est surjectif par construction). On raisonne par récurrence sur n. Le cas $n = 1$ est connu. On suppose le résultat acquis jusqu'à l'ordre s, $s \in \mathbb{N}^*$. Soit $P \in K[X_1, \ldots, X_{s+1}]$; il existe une famille $\{P_i\}_{i\in\mathbb{N}}$ d'éléments de $K[X_1, \ldots, X_s]$ telle que $P = \sum_{i\in\mathbb{N}} P_i X_{s+1}^i$. Si l'on suppose P non nul, alors il existe $i_0 \in \mathbb{N}$ tel que $P_{i_0} \neq 0$. Par hypothèse de récurrence, on en déduit l'existence de $(a_1, \ldots, a_s) \in K^s$ tel que $\widetilde{P}_{i_0}(a_1, \ldots, a_s) \neq 0$. Soit enfin φ le morphisme de K-algèbres $\varphi : K[X_1, \ldots, X_{s+1}] \longrightarrow K[X_{s+1}]$ tel que, pour $1 \leqslant i \leqslant s$, $X_i \mapsto a_i$ et $X_{s+1} \mapsto X_{s+1}$. Alors, il est clair que $\varphi(P)$ est un polynôme non nul de $K[X_{s+1}]$. Il existe donc $a \in K$ tel que $\widetilde{\varphi(P)}(a) \neq 0$. On en déduit aussitôt que $\widetilde{P}$ ne s'annule pas sur $(a_1, \ldots, a_s, a)$, donc la fonction polynomiale associée à P est non nulle. B.3

C Arithmétique dans les anneaux de polynômes

C.1 Théorèmes de transfert.

Dans cette section, on étudie le transfert de la propriété d'être factoriel de l'anneau A à l'anneau $A[X]$.

On peut remarquer que, comme l'indique le corollaire **II.C.23**, la propriété d'un anneau d'être principal ne se transfère pas de l'anneau A à l'anneau $A[X]$. Il résulte aussi de **II.C.23** que la propriété d'un anneau d'être euclidien ne se transfère pas de l'anneau A à l'anneau $A[X]$.

On va montrer que, par contre, la propriété d'être factoriel se transfère de l'anneau A à l'anneau $A[X]$. Pour ce faire, il faut introduire la notion de contenu d'un polynôme.

Définition C.1. *On suppose A factoriel.*

(1) *Si $P \in A[X] \setminus \{0\}$, un élément de A est appelé un **contenu** de P si c'est un p.g.c.d. des coefficients de P.*

(2) *Un polynôme $P \in A[X] \setminus \{0\}$ est dit **primitif** si 1 est un p.g.c.d. de ses coefficients.*

Lemme C.2. Soit A un anneau factoriel. Soit $P \in A[X] \setminus \{0\}$. Alors $p \in A$ est un contenu de P si et seulement s'il existe $P_1 \in A[X]$ primitif tel que $P = pP_1$ et $\deg P_1 = \deg P$.

Démonstration. ($\Rightarrow$) Soit p un pgcd des coefficients de P (il existe puisque A est factoriel). Notons $P = \sum_{i=0}^n a_i X^i$. Alors pour tout i il existe $a_i' \in A$ tel que $a_i = pa_i'$. On a alors $P = pP_1$ avec $P_1 = \sum_{i=0}^n a_i' X^i \in A[X]$. Il est clair que $\deg P_1 = \deg P$. Il reste à montrer que P_1 est primitif.
Soit d un pgcd des coefficients de P_1. Alors pour tout i il existe $a_i'' \in A$ tel que $a_i' = da_i''$. Mais alors $a_i = dpa_i''$ pour tout i, donc dp divise tous les a_i, donc dp divise p qui est un pgcd des a_i. Donc d est inversible, et donc 1 est pgcd des coefficients de P_1.

($\Leftarrow$) Supposons que $P = pP_1$ avec P_1 primitif de même degré que P. Il est clair que p divise tous les coefficients de P, donc p divise le contenu de P. Posons $P_1 = \sum_{i=0}^n a_i' X^i$ et notons c un contenu de P. On a alors $c = pq$ avec $q \in A$ et $c \mid pa_i'$ pour tout i, donc on déduit que $q \mid a_i'$ pour tout i, et donc que q est inversible dans A puisque P_1 est primitif. Donc p est associé à c et donc p est un contenu de P. C.2

Lemme C.3 (Lemme de Gauss)**.** On suppose A factoriel. Soient P et Q des polynômes non nuls de $A[X]$.

(1) Si P et Q sont primitifs, alors PQ est primitif.

(2) Si p et q sont des contenus de P et Q respectivement, alors pq est un contenu de PQ.

Démonstration. **(1)** On raisonne par l'absurde. Supposons que 1 n'est pas p.g.c.d. des coefficients de PQ. Alors, puisque A est factoriel, il existe un pgcd des coefficients de PQ. Soit $\pi \in A$ un diviseur irréductible de ce pgcd ; il divise donc tous les coefficients de PQ. Soient d, e les degrés respectifs de P et Q ; comme P et Q sont primitifs, il existe au moins un coefficient de P et un coefficient de Q qui ne soit pas divisible par π. Posons $P = \sum_{i=0}^{d} a_i X^i$, $Q = \sum_{j=0}^{e} b_j X^j$, $i_0 = \inf\{i,\ 0 \leqslant i \leqslant d \text{ tq } \pi \nmid a_i\}$ et $j_0 = \inf\{j,\ 0 \leqslant j \leqslant e \text{ tq } \pi \nmid b_j\}$. Le coefficient d'indice $i_0 + j_0$ de PQ est

$$\sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j.$$

Mais alors, par définition de π, π divise le membre de gauche et le second terme du membre de droite dans l'équation ci-dessus, donc $\pi | a_{i_0} b_{j_0}$. Comme A est factoriel et π irréductible, il s'ensuit (condition d'Euclide) que π divise a_{i_0} ou b_{j_0}, ce qui constitue une contradiction. Ainsi 1 est p.g.c.d. des coefficients de PQ.

(2) On utilise le lemme **C.2**. Il existe des polynômes primitifs $P', Q' \in A[X]$ tels que $P = pP'$, $Q = qQ'$, $\deg P = \deg P'$ et $\deg Q = \deg Q'$. Alors $PQ = pqP'Q'$ avec $P'Q'$ primitif d'après **(1)** et $\deg(P'Q') = \deg(PQ)$. Alors pq est un contenu de PQ d'après le lemme **C.2**. C.3

Lemme C.4. Soient A un anneau factoriel et K son corps des fractions. Soit $P \in A[X]$. On suppose qu'il existe Q, R dans $K[X]$ tels que $P = QR$. Alors il existe Q', R' dans $A[X]$ et α, β dans $K \setminus \{0\}$ tels que $P = Q'R'$, $Q' = \alpha Q$, et $R' = \beta R$.

Remarque C.5. On rappelle que puisque A est factoriel, il est intègre, donc son corps des fractions existe. De plus, A peut être identifié à un sous-anneau de K.

Démonstration. En réduisant tous les coefficients de Q et R aux mêmes dénominateurs, on voit qu'il existe $q, r \in A$ et $Q_0, R_0 \in A[X]$ tels que $qQ = Q_0$ et $rR = R_0$. On a alors $\deg Q_0 = \deg Q$, $\deg R_0 = \deg R$ et $Q_0 R_0 = qrP$.

Soient c un contenu de Q_0 et d un contenu de R_0. On peut donc écrire $Q_0 = cQ_1$ et $R_0 = dR_1$ avec Q_1 et R_1 dans $A[X]$ primitifs et tels que $\deg Q_1 = \deg Q_0$ et $\deg R_1 = \deg R_0$ d'après le lemme **C.2**. On a donc $qrP = cdQ_1R_1$ avec Q_1R_1 primitif (lemme de Gauss), donc à l'aide du lemme **C.2** on en déduit que cd est un contenu de qrP et donc que qr divise cd : il existe $\lambda \in A$ tel que $cd = \lambda qr$ d'où $P = \lambda Q_1 R_1$. Finalement on pose $\alpha = \lambda c^{-1} q \in K$, $\beta = d^{-1} r \in K$, $Q' = \alpha Q$ et $R' = \beta R$. C.4

Remarque C.6. Soit A un anneau factoriel et K son corps des fractions. On a alors une injection $A \to K \to K[X]$ qui est un morphisme d'anneaux. On en déduit donc grâce à la propriété universelle des anneaux de polynômes un morphisme de A-algèbres $A[X] \to K[X]$ qui à X associe X. Il est facile de voir que ce morphisme est injectif, et donc que $A[X]$ peut être identifié à un sous-anneau de $K[X]$.

Théorème C.7. Soit A un anneau factoriel et soit K son corps des fractions.
Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes de $A[X]$ de degré supérieur ou égal à 1, primitifs et qui sont irréductibles dans $K[X]$.

Démonstration. On rappelle que $A[X]^\times = A^\times$ (A est intègre).

(1) Soit $a \in A$. Montrons que a est irréductible dans $A[X]$ si et seulement s'il est irréductible dans A.

- ✧ Si a est irréductible dans A, il est non nul et non inversible dans A et donc dans $A[X]$. De plus, si $a = PQ$, $P, Q \in A[X]$, alors $P, Q \in A$ et P ou Q est un élément inversible de A donc de $A[X]$.
- ✧ Réciproquement, si a est irréductible dans $A[X]$, il est non nul et non inversible dans $A[X]$ et donc dans A et si $a = bc$, $b, c \in A$, alors b ou c est inversible dans $A[X]$ et donc dans A.

(2) Soit P dans $A[X]$ de degré supérieur ou égal à 1. Alors P est non nul et non inversible dans $A[X]$.

✧ Supposons P primitif et irréductible dans $K[X]$. Si $P = QR$ avec $Q, R \in A[X]$, l'irréductibilité de P dans $K[X]$ assure que Q, par exemple, est un élément inversible de $K[X]$. Donc, $Q = a$ avec $a \in A \setminus \{0\}$. L'égalité $P = aR$ assure que si d est p.g.c.d. des coefficients de P, $a|d$. Mais P est primitif, donc $a \in A^\times$. Ainsi, P est irréductible dans $A[X]$.

✧ Réciproquement, supposons P irréductible dans $A[X]$. Si d est un contenu de P, alors $P = dP'$ avec $P' \in A[X]$ de degré $\geqslant 1$ donc non inversible, donc d est inversible dans A et donc P est primitif. Montrons que P est irréductible dans $K[X]$. Il n'est pas inversible dans $K[X]$ (de degré $\geqslant 1$). Si $P = QR$ dans $K[X]$, grâce au lemme **C.4** on peut supposer que Q et R sont dans $A[X]$. Or P est irréductible dans $K[X]$ donc par exemple Q est inversible dans $A[X]$ et donc Q est inversible dans $K[X]$. C.7

Théorème C.8. Si A est factoriel, alors $A[X]$ est factoriel.

Démonstration. ✦ On sait déjà que $A[X]$ est intègre puisque A est intègre.

✦ On commence par montrer que l'anneau $A[X]$ satisfait la condition (E). Soit $P \in A[X]$, non nul et non inversible dans $A[X]$.

Si P est de degré 0, il s'écrit comme produit d'irréductibles de A (et donc de $A[X]$ d'après le théorème **C.7**).

Si P est de degré $\geqslant 1$, P est non nul et non inversible dans $K[X]$ (où K est le corps des fractions de A). Comme $K[X]$ est principal (K est un corps) et donc factoriel, il existe $r \in \mathbb{N}^*$ et $P_1, \dots, P_r$ polynômes irréductibles de $K[X]$ tels que $P = P_1 \dots P_r$. Par réduction au même dénominateur, il existe $p \in A$ et $P'_1, \dots, P'_r \in A[X]$ tels que $pP = P'_1, \dots, P'_r$ et, pour $1 \leqslant i \leqslant r$, $\deg P_i = \deg P'_i$. Pour tout i, $1 \leqslant i \leqslant r$, soit d_i un contenu de P'_i. Alors pour chaque i on peut écrire $P'_i = d_i P''_i$ avec $P''_i \in A[X]$ primitif $\deg P''_i = \deg P_i$ d'après le lemme **C.2**, et $d := d_1 \dots d_r$ est un contenu de $P'_1 \dots P'_r = pP$. On en déduit donc que p divise d; écrivons $d = pq$ avec $q \in A$. Alors $P = qP''_1 \dots P''_r$. Chaque P''_i est irréductible dans $A[X]$ puisqu'il est primitif, de degré $\geqslant 1$ et irréductible dans $K[X]$ (il est associé à P_i dans $K[X]$). En décomposant q en un produit d'irréductibles de A (possible car A est factoriel) donc de $A[X]$, on obtient une décomposition en facteurs irréductibles de P dans $A[X]$.

✦ Pour montrer que $A[X]$ est factoriel, c'est-à-dire que la condition (U) est vérifiée, il suffit grâce au théorème **II.C.12)** de montrer que $A[X]$ satisfait la condition de primalité, c'est-à-dire de montrer qu'un élément irréductible de $A[X]$ engendre un idéal premier de $A[X]$. Soit P un polynôme irréductible de $A[X]$.

Si $P = a \in A$, alors a est un irréductible de A. On a un morphisme surjectif d'anneaux $A[X] \to (A/(a))[X]$ (*cf.* exemple **A.10**), et il est facile de voir qu'il induit un isomorphisme $A[X]/(aA[X]) \cong (A/(a))[X]$ par le premier théorème d'isomorphisme. Or A est factoriel et a irréductible dans A, donc $A/(a)$ est intègre, donc $A[X]/(aA[X]) \cong (A/(a))[X]$ est intègre, et donc $aA[X]$ est un idéal premier de $A[X]$.

Si maintenant $\deg P \geqslant 1$, alors P est primitif et irréductible dans $K[X]$ d'après **C.7**. Comme P est irréductible dans l'anneau factoriel $K[X]$, $PK[X]$ est premier dans $K[X]$. Il suffit donc de montrer que $PA[X] = PK[X] \cap A[X]$ pour conclure que $PA[X]$ est premier dans $A[X]$. Il est clair que $PA[X] \subset PK[X] \cap A[X]$. Montrons l'autre inclusion : soit $PQ \in PK[X] \cap A[X]$, avec $Q \in K[X]$ et $PQ \in A[X]$. Nous allons montrer que $Q \in A[X]$. En réduisant les coefficients de Q au même dénominateur, on peut écrire $dQ = Q'$ avec $d \in A$, $Q' \in A[X]$ et $\deg Q' = \deg Q$. De plus, quitte à diviser cette égalité par le contenu de Q', on peut supposer que Q' est primitif. Donc $dPQ = PQ'$ est primitif puisque P et Q' le sont. Or $PQ \in A[X]$, donc d est un contenu de dPQ (lemme **C.2**). On en déduit donc que d est inversible dans A, et donc que $Q = d^{-1}Q' \in A[X]$. C.8

Théorème C.9. Si A est factoriel et $n \in \mathbb{N}^*$, alors $A[X_1, \dots, X_n]$ est factoriel.

Démonstration. Par récurrence sur n à l'aide du théorème **C.8** et du corollaire **A.12**. C.9

Remarque C.10. On vérifie facilement que si A est un anneau tel que $A[X_1, \ldots, X_n]$ est factoriel, alors A est factoriel.

Cependant, en général, un sous-anneau ou un anneau quotient d'un anneau factoriel n'est pas factoriel. Par exemple, $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel mais c'est un sous-anneau de $\mathbb{C}$ qui est factoriel et c'est le quotient $\mathbb{Z}[X]/(X^2+3)$ de $\mathbb{Z}[X]$ qui est factoriel.

C.2 Tests d'irréductibilité.

Soit I un idéal de l'anneau A. On note $\varphi_I : A[X] \to (A/I)[X]$ le morphisme d'anneaux de l'exemple **A.10**.

Proposition C.11. Soient A un anneau factoriel et I un idéal premier de A. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $a_n \notin I$, $n \geqslant 1$; si $\varphi_I(P)$ est irréductible dans $(A/I)[X]$ ou dans $(\mathrm{Frac}(A/I))[X]$, alors P est irréductible dans $(\mathrm{Frac}\, A)[X]$.

Démonstration. Notons $K = \mathrm{Frac}\, A$. Supposons que $P = QR$ avec Q, R dans $K[X]$. Grâce au lemme **C.4**, on peut supposer que Q et R sont dans $A[X]$. Posons $Q = \sum_{i=0}^{q} b_i X^i$ et $R = \sum_{i=0}^{r} c_i X^i$ avec $b_q c_r \neq 0$. On a $\varphi_I(P) = \varphi_I(Q)\varphi_I(R)$. Mais $\deg \varphi_I(P) \geqslant 1$ (puisque $\overline{a}_n \neq 0$ dans A/I et $n \geqslant 1$), donc dans les deux cas de l'énoncé $\varphi_I(P)$ est irréductible dans $(\mathrm{Frac}(A/I))[X]$. Donc par exemple $\varphi_I(Q)$ est inversible dans $(\mathrm{Frac}(A/I))[X]$, et c'est donc un élément non nul de $\mathrm{Frac}(A/I)$. Donc $\deg \varphi_I(Q) = 0$. Mais $0 \neq \overline{a}_n = \overline{b}_q \overline{c}_r$, donc $\overline{b}_q \neq 0$, et donc $\deg \varphi_I(Q) = q$. Donc $\deg Q = q = 0$ et Q est une constante non nulle de K, donc inversible dans K et donc dans $K[X]$. Donc P est irréductible dans $K[X]$. C.11

Proposition C.12 (Critère d'Eisenstein)**.** Supposons A factoriel et considérons $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $n = \deg P \geqslant 1$. S'il existe un élément irréductible p de A tel que $p \nmid a_n$, $p | a_i$ pour $0 \leqslant i \leqslant n-1$ et $p^2 \nmid a_0$, alors P est irréductible dans $(\mathrm{Frac}\, A)[X]$.

Démonstration. Notons $K = \mathrm{Frac}\, A$. Puisque $\deg P \geqslant 1$, P n'est pas inversible dans $K[X]$. Supposons que P ne soit pas irréductible dans $K[X]$. Alors, il existe $Q, R \in K[X]$ tels que $P = QR$ et $0 < q = \deg Q < \deg P$ et $0 < r = \deg R < \deg P$. D'après le lemme **C.4**, on peut supposer que $Q, R \in A[X]$. Posons $Q = \sum_{j=0}^{q} b_j X^j$ et $R = \sum_{k=0}^{r} c_k X^k$. Comme p ne divise pas a_n, p ne divise ni b_q ni c_r. Comme p divise a_0 et p^2 ne divise pas a_0, l'égalité $a_0 = b_0 c_0$ assure que p divise b_0 ou c_0 (car A satisfait la condition d'Euclide) mais pas les deux. Quitte à échanger Q et R, on peut supposer que p divise c_0 et pas b_0. Soit donc $\ell = \inf\{1 \leqslant i \leqslant r \text{ tel que } p \nmid c_i\}$; comme $r < n$, l'égalité $a_\ell = b_0 c_\ell + \cdots + b_\ell c_0$ montre que $b_0 c_\ell$ est divisible par p et donc que c_ℓ est divisible par p. Ceci constitue une contradiction. C.12

V Anneaux et modules nœthériens

A Modules nœthériens

Nous avons vu qu'en général un sous-module d'un module de type fini n'est pas de type fini. Nous allons maintenant étudier une classe de modules pour lesquels cette propriété est vérifiée.

Définition-Proposition A.1. Soit M un A-module. Alors les propriétés suivantes sont équivalentes :

(I) Tout sous-module de M est de type fini.

(II) Toute suite croissante (pour l'inclusion) de sous-modules de M est stationnaire.

(III) Tout ensemble non vide de sous-modules de M contient un élément maximal.

Si ces conditions équivalentes sont vérifiées, on dit que M est **nœthérien**.

Démonstration. **(I)⇒(II)** Supposons que tout sous-module de M est de type fini. Soit $M_1 \subset M_2 \subset \ldots \subset M_n \subset \ldots$ une suite croissante de sous-modules de M.

Soit $N = \cup_{i \geqslant 1} M_i$. Alors N est un sous-module de M *(exercice : utilise le fait qu'on a une suite croissante de sous-modules).* N est donc un A-module de type fini par hypothèse. Soit $\{a_1, \ldots, a_r\}$ une partie génératrice de N. Pour chaque i, $1 \leqslant i \leqslant r$, il existe n_i tel que $a_i \in M_{n_i}$. Soit $s = \max\{n_i; i = 1, \ldots, r\}$. Alors $a_i \in M_s$ pour tout i, et donc $N \subset M_s \subset N$. Donc $N = M_s$, et donc $M_j = N = M_s$ pour tout $j \geqslant s$. La suite est stationnaire.

(II)⇒(III) Supposons que toute suite croissante de sous-modules de M est stationnaire. Soit $\mathcal{S}$ un ensemble non vide de sous-modules de M. Par l'absurde, on suppose que $\mathcal{S}$ ne contient pas d'élément maximal.

Soit $M_0 \in \mathcal{S}$. Puisque M_0 n'est pas maximal, il existe $M_1 \in \mathcal{S}$ tel que $M_0 \subsetneqq M_1$.

De même, M_1 n'est pas maximal, donc il existe $M_2 \in \mathcal{S}$ tel que $M_1 \subsetneqq M_2$.

Par récurrence, on construit une suite strictement croissante de sous-modules de M (dans $\mathcal{S}$). Cela contredit **(II)**.

(III)⇒(I) Supposons que tout ensemble non vide de sous-modules de M contient un élément maximal. Soit N un sous-module de M. On veut montrer que N est de type fini.

Soit $a_0 \in N$. Alors $\langle a_0 \rangle$ est un sous-module de N. Si $\langle a_0 \rangle = N$, c'est terminé.

Si $\langle a_0 \rangle \neq N$, alors il existe $a_1 \in N \backslash \langle a_0 \rangle$. Alors $\langle a_0, a_1 \rangle$ est un sous-module de N. Si $\langle a_0, a_1 \rangle = N$, c'est terminé.

Si $\langle a_0, a_1 \rangle \neq N$, alors il existe $a_2 \in N \backslash \langle a_0, a_1 \rangle$. Alors $\langle a_0, a_1, a_2 \rangle$ est un sous-module de N. etc.

Si l'on n'obtient pas N au bout d'un nombre fini d'étapes, on aura construit une suite $a_0, a_1, \ldots, a_n, \ldots$ d'éléments de N tels que pour tout n, $a_{n+1} \notin \langle a_0, \ldots, a_n \rangle$. Pour chaque p, posons $N_p = \langle a_0, \ldots, a_p \rangle$, et soit $\mathcal{S} = \{N_p; p \in \mathbb{N}\}$. D'après **(III)**, $\mathcal{S}$ a un élément maximal, N_{p_0}. Mais on a $N_{p_0+1} \in \mathcal{S}$ et $N_{p_0} \subsetneqq N_{p_0+1}$: contradiction avec le fait que N_{p_0} soit maximal.

Donc on doit obtenir N au bout d'un nombre fini d'étapes, et donc N est de type fini. A.1

Remarque A.2. Soit M un module nœthérien. Puisque M est un sous-module de M, il est de type fini.

Proposition A.3. Soit M un A-module nœtherien. Alors tout sous-module de M et tout module quotient de M est nœthérien.

Démonstration. Soit N un sous-module de M. Alors tout sous-module de N est un sous-module de M donc est de type fini. Donc N est nœthérien d'après **(I)**.

Soit $\overline{M} = M/N$ un quotient de M. Soit $\overline{M}_1, \ldots, \overline{M}_n, \ldots$ une suite croissante de sous-modules de $\overline{M}$. Notons $\pi : M \to \overline{M}$ la projection canonique, et pour tout n soit $M_n = \pi^{-1}(\overline{M}_n)$. Alors $M_1, \ldots, M_n, \ldots$ est une suite croissante de sous-modules de M, donc elle stationne, et donc puisque $\overline{M}_n = \pi\pi^{-1}(\overline{M}_n) = \pi(M_n)$ la suite $\overline{M}_1, \ldots, \overline{M}_n, \ldots$ stationne. Donc $\overline{M}$ est nœthérien d'après **(II)**. A.3

Proposition A.4. Soit M un A-module et soit N un sous-module de M. Si N et M/N sont nœthériens, alors M est nœthérien.

Démonstration. ✦ Etant donné un sous-module quelconque L de M, on peut lui associer le sous-module $L \cap N$ de N et le sous-module $(L+N)/N$ de M/N.

Montrons que si L' est un sous-module de L tel que $L' \cap N = L \cap N$ et $(L'+N)/N = (L+N)/N$, alors $L' = L$: il suffit de montrer que $L \subset L'$. Soit $x \in L$. Alors puisque $(L+N)/N = (L'+N)/N$, il existe $y \in L'$ et u et v dans N tels que $x + u = y + v$. Mais alors $x - y = v - u \in L \cap N$ (puisque $y \in L' \subset L$). Donc $x = y + v - u$ avec $y \in L'$ et $v - u \in L \cap N = L' \cap N \subset L'$, donc $x \in L'$. Donc $L' = L$.

✦ Maintenant montrons que M est nœthérien. Soit $M_1, \ldots, M_n, \ldots$ une suite croissante de sous-modules de M. Alors $(M_n \cap N)_n$ est une suite croissante de sous-modules de N qui est nœthérien, donc elle stationne, et $((M_n + N)/N)_n$ est une suite croissante de sous-modules de M/N qui est nœthérien, donc elle stationne. Il existe donc r tel que pour tout $n \geqslant r$ on ait $M_n \cap N = M_r \cap N$ et $(M_n + N)/N = (M_r + N)/N$. D'après la première partie de la démonstration on en déduit que $M_n = M_r$ pour tout $n \geqslant r$. Donc la suite $(M_n)_n$ stationne.

A.4

Corollaire A.5. Si $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ est une suite exacte de A-modules, alors M est nœthérien si et seulement si M' et M'' le sont.

Démonstration. $\operatorname{Im} f$ est un sous-module de M isomorphe à M', et M'' est isomorphe au quotient $M/\operatorname{Ker} g = M/\operatorname{Im} f$ de M. On conclut à l'aide des propositions **A.3** et **A.4**. A.5

Corollaire A.6. Soit M un A-module, et soient N et N' deux sous-modules nœthériens de M tels que $M = N + N'$. Alors M est nœthérien.

Démonstration. On a une suite exacte $0 \to N \to N + N' \to (N+N')/N \to 0$. Or N est nœthérien, et $(N+N')/N \cong N'/(N \cap N')$ est isomorphe à un quotient de N' qui est nœthérien, donc il est nœthérien. Donc d'après le corollaire **A.5**, $N + N'$ est nœthérien. A.6

Corollaire A.7. Soient M et N des A-modules. Alors $M \oplus N$ est nœthérien si et seulement si M et N sont nœthériens.

Démonstration. On utilise la suite exacte $0 \to M \to M \oplus N \to N \to 0$. A.7

B Anneaux nœthériens

Définition B.1. *Un anneau A est dit **nœthérien** s'il est nœthérien en tant que A-module sur lui-même. (Rappel : les sous-A-modules de A sont alors les idéaux de A).*

Exemple B.2. Tout anneau principal (et en particulier un corps) est nœthérien puisque tous ses idéaux sont principaux donc de type fini. Cela découle également du lemme **II.C.14**.

Proposition B.3. Soit A un anneau nœthérien. Soit M un A-module. Alors M est un A-module nœthérien si et seulement s'il est de type fini.

Démonstration. Si M est nœthérien, on a déjà dit qu'il est de type fini.

Supposons maintenant que M est de type fini. On sait que M est quotient d'un A-module libre, que l'on peut choisir de type fini puisque M est de type fini (*cf.* théorème **III.E.2**). Donc M est isomorphe à un quotient de A^n pour un $n \in \mathbb{N}^*$. Or A^n est somme directe de modules nœthériens (A), donc A^n est nœthérien. Donc M est nœthérien. B.3

Proposition B.4. Soit $\varphi : A \to B$ un homomorphisme d'anneaux surjectif. Si A est un anneau nœthérien, alors B est un anneau nœthérien.

Démonstration. Si J est un idéal de B, alors $\varphi^{-1}(J)$ est un idéal de A, donc de type fini, et donc $J = \varphi(\varphi^{-1}(J))$ est de type fini (engendré par les images par φ des générateurs de $\varphi^{-1}(J)$). B.4

Proposition B.5. Si A est noethérien, il satisfait la condition (E).

Démonstration. On raisonne par l'absurde. Supposons que l'ensemble $\mathcal{X}$ des éléments de A non nuls et non inversibles qui n'admettent pas de décomposition en produit d'irréductibles soit non vide. Alors, l'ensemble $\mathcal{F} := \{(x); x \in \mathcal{X}\}$ est aussi non vide et admet donc (par noethérianité) un élément maximal. Soit $a \in \mathcal{X}$ tel que (a) soit un élément maximal de $\mathcal{F}$. Comme a est dans $\mathcal{X}$, il est non nul, non inversible et non irréductible. Par suite, il existe b, c dans A, non nuls et non inversibles tels que $a = bc$. On a alors $(a) \subsetneqq (b)$ et $(a) \subsetneqq (c)$. On déduit alors de la maximalité de (a) dans $\mathcal{F}$ que (b) et (c) ne sont pas dans $\mathcal{F}$ et donc que b et c ne sont pas dans $\mathcal{X}$. Par suite, b et c admettent une décomposition en produit d'irréductibles. Mais, comme $a = bc$, il s'ensuit que a admet une décomposition en produit d'irréductibles, ce qui constitue une contradiction. B.5

Corollaire B.6. Un anneau nœthérien est factoriel si et seulement s'il est intègre et satisfait la condition (U).

Théorème B.7 (Théorème de la base de Hilbert)**.** Soit A un anneau nœthérien. Alors l'anneau $A[X]$ est nœthérien.

Démonstration. Supposons par l'absurde que $A[X]$ ne soit pas nœthérien. Il existe donc un idéal I de $A[X]$ qui n'est pas de type fini.

Soit $f_1 \in I$, $f_1 \neq 0$, de plus bas degré possible.

On sait que $I \neq (f_1)$, donc soit $f_2 \in I \setminus (f_1)$ de plus bas degré possible.

Par récurrence, pour tout $k \in \mathbb{N}^*$ on construit $f_{k+1} \in I \setminus (f_1, \dots, f_k)$ de plus bas degré possible.

Pour tout $k \in \mathbb{N}^*$, on note a_k le coefficient dominant de f_k et n_k le degré de f_k. On obtient une suite croissante d'idéaux de A :

$$(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, \dots, a_k) \subset \cdots$$

Puisque A est nœthérien, cette suite stationne, donc en particulier il existe $k \in \mathbb{N}^*$ tel que $(a_1, \dots, a_k) = (a_1, \dots, a_k, a_{k+1})$. On peut donc écrire $a_{k+1} = \sum_{i=1}^{k} \lambda_i a_i$ avec $\lambda_i \in A$.

Soit $g = f_{k+1} - \sum_{i=1}^{k} \lambda_i X^{n_{k+1}-n_i} f_i$. Il est clair que $g \in (f_1, \dots, f_{k+1}) \setminus (f_1, \dots, f_k)$ (sinon f_{k+1} serait dans $(f_1, \dots, f_k)$). De plus, f_{k+1} et tous les $X^{n_{k+1}-n_i} f_i$ sont de degré n_{k+1}, et le coefficient de $X^{n_{k+1}}$ dans g est $a_{k+1} - \sum_{i=1}^{k} \lambda_i a_i = 0$. On en déduit que $\deg g < n_{k+1}$, ce qui contredit la minimalité du degré de f_{k+1}. On a donc obtenu une contradiction.

Finalement, $A[X]$ est donc nœthérien. B.7

Autre démonstration. Soit I un idéal de $A[X]$. Montrons que I est de type fini.

Notons J l'ensemble des coefficients dominants d'éléments de I (avec 0). Montrons que J est un idéal de A.

✧ $J \neq \varnothing$ car $0 \in J$.

✧ Soient a, b dans J avec $a \neq b$. Il existe donc P, Q dans I tels que $P = aX^m + P'$ et $Q = bX^n + Q'$ avec $\deg P' < \deg P$ et $\deg Q' < \deg Q$. On a par exemple $m \geqslant n$, donc $a - b$ est le coefficient dominant de $P - X^{m-n}Q \in I$, donc $a - b \in J$.

✧ Si $\lambda \in A$ et $a \in J$ on a $P \in I$ tel que $P = aX^m + P'$ avec $\deg P' < \deg P$. Alors λa est le coefficient dominant de $\lambda P \in I$ donc $\lambda a \in J$.

Puisque A est nœthérien, J est un idéal de type fini : $J = (a_1, \ldots, a_r)$. Pour tout $i = 1, \ldots, r$, il existe $P_i \in I$ tel que $P_i = a_i X^{n_i} + P_i'$ avec $\deg P_i' < \deg P_i$. Posons $n = \max\{n_i; i = 1, \ldots, r\}$.

Soit K l'idéal de $A[X]$ engendré par $P_1, \ldots, P_r$. Alors K est contenu dans I. Soit M le A-module engendré par $1, X, \ldots, X^{n-1}$. Montrons que $I = I \cap M + K$.

Soit $P \in I$ quelconque. Si $\deg P < n$, alors $P \in I \cap M \subset I \cap M + K$. Supposons maintenant que $\deg P = d \geqslant n$. Alors $P = aX^d + P'$ avec $a \neq 0$ et $\deg P' < d$. On a donc $a \in J$ et donc $a = \sum_{i=1}^r u_i a_i$ avec $u_i \in A$. Alors $P - \sum_{i=1}^r u_i P_i X^{d-n_i}$ est dans I et de degré $< d$. On continue à soustraire des éléments de K jusqu'à obtenir $Q \in I$ avec $\deg Q < n$. On a alors $P = Q + R$ avec $R \in K$ et $Q \in I \cap M$. Donc $I = I \cap M + K$.

Puisque M est un A-module de type fini et A est nœthérien, M est nœthérien, donc son sous-module $I \cap M$ est de type fini. Notons $\{S_1, \ldots, S_t\}$ une partie génératrice du A-module $I \cap M$.

Alors $S_1, \ldots, S_t, P_1, \ldots, P_r$ engendrent l'idéal I de $A[X]$, qui est donc de type fini. B.7

Corollaire B.8. Si A est un anneau nœthérien, alors $A[X_1, \ldots, X_n]$ est un anneau nœthérien.

Démonstration. Par récurrence sur n en utilisant le corollaire **IV.A.12**. B.8

Corollaire B.9. Si A est un anneau nœthérien, alors $\mathcal{F}_{\text{pol}}(A^n, A)$ (anneau des fonctions polynomiales) est un anneau nœthérien.

Démonstration. Par définition, $\mathcal{F}_{\text{pol}}(A^n, A)$ est l'image de $A[X_1, \ldots, A_n]$ par un homomorphisme d'anneaux (**IV.B.1**). On conclut à l'aide du corollaire **B.8** et de la proposition **B.4**. B.9

VI Modules sur les anneaux principaux

Sauf mention explicite du contraire, on suppose dans ce chapitre que l'anneau A est principal. Donc A est intègre et tous ses idéaux sont principaux. Cependant, certaines démonstrations seront faites pour un anneau *euclidien*, et nous noterons $\nu : A \setminus \{0\} \to \mathbb{N}$ son stathme euclidien.

A Matrices équivalentes

Définition A.1. *Etant donnée une matrice $M \in \mathcal{M}_{s,n}(A)$, on considère les opérations suivantes (dites **opérations élémentaires sur les lignes** de M) :*

(L1) *On multiplie une ligne de M par un élément* inversible *de A.*

(L2) *On permute deux lignes de M.*

(L3) *On ajoute à une ligne donnée un multiple (quelconque) d'une autre ligne de M.*

Remarque A.2. On définit les matrices inversibles suivantes :

- ✦ Pour $1 \leqslant i \leqslant s$ et $\alpha \in A$ avec α *inversible*, on note $E_i(\alpha) \in \mathcal{M}_{s,s}(A)$ la matrice diagonale dont les coefficients sont égaux à 1 sauf le $i$me qui est égal à α.
- ✦ Pour $i \neq j$, on note $T_{ij} = (t_{k\ell})_{1\leqslant k,\ell\leqslant s}$ la matrice donnée par $\begin{cases} t_{kk} = 1 & \text{si } k \notin \{i,j\} \\ t_{ij} = 1 \\ t_{ji} = 1 \\ t_{k\ell} = 0 & \text{dans tous les autres cas.} \end{cases}$
- ✦ Pour $i \neq j$ et $\lambda \in A$, on note $F_{ij}(\lambda) \in \mathcal{M}_{s,s}(A)$ la matrice dont les coefficients diagonaux sont égaux à 1 et dont les autres coefficients sont nuls sauf celui de la $i$me ligne et $j$me colonne qui est égal à λ.

Alors **(L1)** revient à multiplier M à gauche par une matrice $E_i(\alpha)$, **(L2)** revient à multiplier M à gauche par une matrice T_{ij} et **(L3)** revient à multiplier M à gauche par une matrice $F_{ij}(\lambda)$.

Définition A.3. *On considère également les opérations suivantes (dites **opérations élémentaires sur les colonnes** de M) :*

(C1) *On multiplie une colonne de M par un élément* inversible *de A.*

(C2) *On permute deux colonnes de M.*

(C3) *On ajoute à une colonne donnée un multiple (quelconque) d'une autre colonne de M.*

Remarque A.4. Ces opérations reviennent à multiplier M à *droite* par les matrices $E_i(\alpha)$, T_{ij} et $F_{ij}(\lambda)$ de taille $n \times n$ définies comme ci-dessus.

Définition-Proposition A.5. Soient M et N dans $\mathcal{M}_{s,n}(A)$. On dit que N est **équivalente** à M si N peut être obtenue à partir de M en lui appliquant une succession d'opérations élémentaires sur les lignes et les colonnes. On note $M \sim N$. Ceci définit une relation d'équivalence sur $\mathcal{M}_{s,n}(A)$.

Remarque A.6. On peut démontrer que $M \sim N \iff \exists P \in \mathcal{GL}_s(A), Q \in \mathcal{GL}_n(A)$ tq $N = PMQ$.

Théorème A.7. Soit $R \in \mathcal{M}_{s,n}(A)$. Alors R est équivalente à une matrice de la forme $\mathrm{diag}(d_1, \ldots, d_t)$ avec $d_1 \mid d_2 \mid \ldots d_t$ dans A où $t = \min(s,n)$.

Démonstration. Nous allons démontrer ce résultat lorsque A est euclidien. Cette démonstration permettra alors d'obtenir un algorithme pour passer de R à la matrice des facteurs invariants.

Notons $R = (a_{ij})_{1\leqslant i\leqslant s, 1\leqslant j\leqslant n}$.

- ✦ Fixons i et j. Montrons que l'on peut remplacer tous les coefficients de la $i$me ligne et de la $j$me colonne (autres que a_{ij} lui-même) par les restes de leurs divisions euclidiennes par a_{ij}.
  Soit $k \neq j$. On a $a_{ik} = q_{ik}a_{ij} + r_{ik}$ avec $r_{ik} = 0$ ou $\nu(r_{ik}) < \nu(a_{ij})$. Si on soustrait q_{ik} fois la $j$me colonne à la $k$me colonne, et le coefficient de la $i$me ligne et de la $k$me colonne devient r_{ik}.
  On raisonne de même pour transformer la $j$me colonne.
- ✦ Notons $\mathcal{C}$ l'ensemble de tous les coefficients non nuls de toutes les matrices équivalentes à R. Soit $d_1 \in \mathcal{C}$ avec $\nu(d_1)$ minimal dans $\{\nu(x); x \in \mathcal{C}\}$, et supposons que d_1 soit l'un des coefficients de R (quitte à remplacer R par une matrice qui lui est équivalente). Quitte à permuter des lignes et/ou les colonnes de R, on peut supposer que d_1 est le coefficient de la première ligne et de la première colonne.
  On sait que l'on peut remplacer tous les coefficients de la première ligne et de la première colonne autres que d_1 par les restes de leurs divisions euclidiennes par d_1. Par minimalité de $\nu(d_1)$, tous ces restes sont nuls.
  On s'est donc ramenés à une matrice équivalente à R qui est de la forme $\begin{pmatrix} d_1 & 0 \\ 0 & R_1 \end{pmatrix}$ avec $R_1 \in \mathcal{M}_{s-1,n-1}(A)$.
  De plus, d_1 divise tous les coefficients de R_1. En effet, soit $2 \leqslant i \leqslant s$. Si on ajoute la première ligne de R à la $i$me, on a une matrice dont la $i$me ligne est $\begin{pmatrix} d_1 & a_{i2} & \cdots & a_{in} \end{pmatrix}$, et on sait d'après l'étape précédente que l'on peut remplacer tous les a_{ij} pour $j = 2, \ldots, n$ par le reste de la division euclidienne de a_{ij} par d_1. Par minimalité de $\nu(d_1)$ on en déduit que ces restes sont nuls, c'est-à-dire que $d_1 \mid a_{ij}$ pour tout $2 \leqslant j \leqslant n$.
- ✦ On applique les deux étapes précédentes à R_1. Cela ne changera pas la première ligne et la première colonne de R, et on en déduit que R est équivalente à une matrice de la forme $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & R_2 \end{pmatrix}$ avec $d_1 \mid d_2$ et d_2 divise tous les coefficients de R_2.
- ✦ Par récurrence, on obtient une matrice $\mathrm{diag}(d_1 \ldots, d_t)$ équivalente à R avec $d_1 \mid d_2 \mid \ldots \mid d_t$ et $t = \min(s, n)$. A.7

Remarque A.8. On obtient l'algorithme suivant :

Etape 1 Soit d_1 le coefficient non nul de R avec $\nu(d_1)$ minimal. Par permutation des lignes et des colonnes on place le coefficient non nul de R avec dont l'image par ν est minimale en position $(1, 1)$.

Etape 2 On ajoute des multiples de la première colonne (*resp.* ligne) aux autres colonnes (*resp.* lignes) afin d'obtenir des coefficients nuls ou dont l'image par ν est strictement inférieure à a_{11} sur la première ligne (*resp.* colonne).

Etape 3 On répète les étapes **1** et **2** jusqu'à obtenir une matrice de la forme $\begin{pmatrix} a_{11} & 0 \\ 0 & R_1 \end{pmatrix}$.

Etape 4 Si a_{11} divise tous les coefficients de R_1 on répète les étapes précédentes sur R_1.

Etape 5 Si a_{11} ne divise pas a_{ij} avec $i \geqslant 2$ et $j \geqslant 2$, on ajoute la $i$me ligne à la première et on reprend à l'étape **1**.

Exemple A.9. $A = \mathbb{Q}[X]$ et $R = \begin{pmatrix} X & 0 & 0 \\ 0 & 1-X & 0 \\ 0 & 0 & (1-X)(1+X) \end{pmatrix}$. L'anneau A est bien euclidien avec $\nu = \deg$.

Les opérations successives suivantes : $L_1 \to L_1 + L_2$; $C_2 \to C_2 + C_1$; $C_1 \leftrightarrow C_2$; $L_2 \to L_2 + (X-1)L_1$; $C_2 \to C_2 - XC_1$; $L_2 \to L_2 + L_3$; $C_3 \to C_3 + C_2$; $C_2 \leftrightarrow C_3$; $L_3 - (1+X)L_2$; $C_3 \to C_3 + XC_2$;

$C_2 \to -C_2$ et $C_3 \to -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X(X-1)(X+1) \end{pmatrix}$ donc les facteurs invariants sont 1, $X-1$ et $X(X-1)(X+1)$.

On sait que $D = PRQ$ où P est donnée par les opérations sur les lignes et Q est donnée par les opérations sur les colonnes. Pour les trouver, on applique les opérations que l'on a faites sur les lignes de R à I_3 (pour P) et les opérations que l'on a faites sur les colonnes de R à I_3 (pour Q). On obtient

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1-X & -X & -1 \\ (X-1)(X+1) & X(X+1) & X \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} 1 & 1-X & (1-X)(1+X) \\ 1 & -X & -X(1+X) \\ 0 & 1 & X \end{pmatrix}.$$

Exemple A.10. $A = \mathbb{Z}$ et $R = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$. L'anneau $\mathbb{Z}$ est bien euclidien avec $\nu = |\,|$.

La suite d'opérations sur les lignes et les colonnes $L_1 \leftrightarrow L_3$; $L_2 \to L_2 - 4L_1$; $L_3 \to L_3 - 7L_1$; $C_2 \to C_2 - 2C_1$; $C_3 \to C_3 - 3C_1$; $L_2 \to -L_2$; $L_3 \to L_3 + 2L_2$ et $C_3 \to C_3 - 2C_2$ donne $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. On sait que $D = PRQ$ avec P et Q obtenues comme dans l'exemple précédent. En pratique, nous voulons souvent Q^{-1} plutôt que Q, et celle-ci est obtenue en effectuant les opérations sur les colonnes inverses et dans l'ordre inverse. On obtient $P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 4 \\ 1 & -2 & 1 \end{pmatrix}$ et $Q^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

B Modules de type fini sur un anneau principal

Le but de cette partie est de démontrer le théorème de structure suivant :

Théorème B.1. Soit A un anneau principal et soit M un A-module de type fini. Alors

(i) Il existe $r \in \mathbb{N}$, $q \in \mathbb{N}$, et $a_1, \ldots, a_q$ dans A non nuls et non inversibles vérifiant $a_1 \mid \ldots \mid a_q$ tels que

$$M \cong A^r \oplus \bigoplus_{i=1}^{q} A/(a_i).$$

(ii) Les entiers r et q et les idéaux non nuls et distincts de A $(a_1), \ldots, (a_q)$ vérifiant $(a_1) \supset \cdots \supset (a_q)$ sont uniquement déterminés par le A-module M.

Les éléments a_i sont appelés les **facteurs invariants** de M.

Pour cela nous allons démontrer des résultats qui sont intéressants par eux-mêmes.

B.1 Sous-modules d'un module libre de type fini

Soit N un sous-module du A-module libre A^n. Puisque A est principal, il est nœthérien et donc A^n est un module nœthérien (somme directe de modules nœthériens). Donc le sous-module N de A^n est de type fini.

Nous voulons en fait montrer que N est libre (toujours dans le cas A principal), et que l'on peut choisir une base de N particulière.

Soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de A^n et soit $\mathcal{G} = \{x_1, \ldots, x_s\}$ un système générateur de N. Pour tout $1 \leqslant i \leqslant s$ on peut écrire $x_i = \sum_{j=1}^{n} a_{ij} e_j$ avec $a_{ij} \in A$ de manière unique.

Alors N est entièrement déterminé par le couple $(\mathcal{B}, R)$ où $\mathcal{B}$ est une base de A^n et R est la matrice $R = (a_{ij})_{1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n}$.

Voyons à quoi correspondent les opérations élémentaires sur la matrice R.

- ✦ Si on multiplie une colonne de R par un élément inversible α, cela revient à multiplier l'élément correspondant de $\mathcal{B}$ par α^{-1} et on obtient une nouvelle base de A^n.
- ✦ Si on échange deux colonnes de R, cela revient à échanger les éléments correspondants de $\mathcal{B}$, et on obtient une nouvelle base de A^n.
- ✦ Si on ajoute a fois la $i$me colonne à la $j$me ($a \in A$), cela revient à remplacer e_i par $e'_i = e_i - ae_j$. En effet, on a $x_i = \sum_{k=1}^{n} a_{ik}e_k = \sum_{1\leqslant k\leqslant n, k\neq i,j} a_{ik}e_k + a_{ii}e'_i + (aa_{ii} + a_{ij})e_j$ ce qui correspond bien à ajouter aa_{ii} à a_{ij} dans la colonne j pour tout i.
  On obtient alors une nouvelle base $\mathcal{B}'$ de A^n :
  - ✧ $\mathcal{B}'$ engendre A^n, puisque $e_i = e'_i + ae_j$.
  - ✧ $\mathcal{B}'$ est libre : si $\sum_{1\leqslant k\leqslant n, k\neq i} \lambda_k e_k + \lambda_i e'_i = 0$ avec $\lambda_p \in A$ pour tout p, alors $\sum_{1\leqslant k\leqslant n, k\neq j} \lambda_k e_k + (\lambda_j - a\lambda_i)e_j = 0$ donc $\lambda_k = 0$ pour tout $k \neq j$ et $\lambda_j - a\lambda_i = 0$ donc $\lambda_j = 0$.
- ✦ Si on multiplie une ligne de R par $\alpha \in A^\times$, cela revient à multiplier le générateur correspondant par α et on obtient un nouveau système générateur de N.
- ✦ Si on échange deux lignes de R, cela correspond à permuter les générateurs correspondants dans $\mathcal{G}$, et on obtient un système générateur de N.
- ✦ Si on ajoute a fois la $j$me ligne à la $i$me, cela revient à remplacer le générateur x_i par $x'_i = x_i + ax_j$, et on obtient un nouveau système générateur de N.

On en déduit que transformer la matrice R en matrice équivalente revient à changer de base de A^n et de système générateur pour N.

Théorème B.2 (de la base adaptée)**.** Soit M un A-module libre de rang n. Soit N un sous-module de M. Alors N est libre de rang au plus n. De plus, il existe un entier $0 \leqslant r \leqslant n$, une base $\mathcal{B} = \{e_1, \ldots, e_n\}$ de M et des éléments $d_1, \ldots, d_r$ non nuls de A tels que $d_1 \mid \ldots \mid d_r$ et $\{d_1e_1, \ldots, d_re_r\}$ soit une base de N.

Démonstration. Soit $\mathcal{C}$ une base de M et soit R la matrice $s \times n$ donnant les générateurs de N dans la base $\mathcal{C}$. On sait que R est équivalente à $R' = \mathrm{diag}(d_1, \ldots, d_t)$ avec $d_1 \mid \ldots \mid d_t$ dans A et $t = \min(s, n)$ d'après le théorème **A.7**. Les opérations sur les colonnes effectuées pour passer de R à R' donnent une nouvelle base $\mathcal{B} = \{e_1, \ldots, e_n\}$ de M. Soit r le nombre de d_i non nuls : $r \leqslant t \leqslant n$. Dans cette nouvelle base de M, les générateurs de N sont donnés par $g_i = d_ie_i$. Donc $N = \langle d_1e_1, \ldots, d_re_r\rangle$ (puisque les autres générateurs sont nuls). Enfin, on voit facilement que $\{d_1e_1, \ldots, d_re_r\}$ est une famille libre (A est intègre et les d_i sont non nuls pour $1 \leqslant i \leqslant r$) et donc une base de N, qui est donc libre de rang $r \leqslant n$. B.2

Remarque B.3. Le théorème ci-dessus se généralise au cas de modules qui ne sont pas de type fini. C'est une application du lemme de Zorn (*cf.* Lang, Algebra, Appendice 2, §2).

B.2 Structure des modules de type fini

Soit M un A-module. Alors M est de type fini si et seulement s'il existe $n \in \mathbb{N}$ tel que M soit un quotient de A^n. Notons $\varphi : A^n \twoheadrightarrow M$. On peut appliquer ce qui précède au sous-module $\mathrm{Ker}\,\varphi$ de A^n. Le quotient $M \cong A^n/\mathrm{Ker}\,\varphi$ est entièrement déterminé par le choix d'un couple $(\mathcal{B}, R)$ où $\mathcal{B}$ est une base de A^n et R est la matrice donnant les générateurs de $\mathrm{Ker}\,\varphi$ dans la base $\mathcal{B}$.

Définition B.4. *La matrice R est appelée* ***matrice des relations*** *de M relative à $\mathcal{B}$.*

Corollaire B.5. Soient A un anneau principal et M un A-module de type fini. Alors M est isomorphe comme A-module à $\bigoplus_{i=1}^{n} (A/(a_i))$ où les (a_i) sont des idéaux de A tels que $(a_i) \supset (a_{i+1})$.

Démonstration. Puisque M est de type fini, on sait que c'est un quotient d'un module libre de type fini A^n. On a donc un homomorphisme surjectif $\varphi : A^n \twoheadrightarrow M$.

Ker φ est un sous-module de A^n, donc d'après les théorèmes qui précèdent, il existe une base $\{e_1, \dots, e_n\}$ de A^n et une base $\{a_1 e_1, \dots, a_q e_q\}$ de Ker φ avec $a_1 \mid \dots \mid a_q$. On pose $a_i = 0$ pour $q \leqslant i \leqslant n$. Alors $M \cong A^n / \operatorname{Ker}\varphi \cong \bigoplus_{i=1}^n (Ae_i / Aa_i e_i) \cong \bigoplus_{i=1}^n (A/(a_i))$. *Pour le dernier isomorphisme, l'homomorphisme surjectif $A \to Ae_i \twoheadrightarrow Ae_i / Aa_i e_i$ qui à $\lambda \in A$ associe la classe de λe_i dans le quotient a pour noyau*

$$\begin{aligned}\{\lambda \in A; \lambda e_i = \mu a_i e_i \text{ avec } \mu \in A\} &= \{\lambda \in A; \exists \mu \in A \text{ tq } \lambda - \mu a_i \in \operatorname{Ann}_A(e_i)\} \\ &= \{\lambda \in A; \exists \mu \in A \text{ tq } \lambda - \mu a_i = 0\} = (a_i).\end{aligned}$$ B.5

Exemple B.6. Soit G le groupe abélien engendré par x_1, x_2 et x_3 soumis aux relations

$$\begin{aligned}-4x_1 - 6x_2 + 7x_3 &= 0 \\ 2x_1 + 2x_2 + 4x_3 &= 0 \\ 6x_1 + 6x_2 + 15x_3 &= 0.\end{aligned}$$

On veut écrire G comme une somme directe de groupes cycliques.

G est le quotient du groupe abélien libre $\mathbb{Z}^3$ de base $\{f_1, f_2, f_3\}$ par le sous-module K engendré par g_1, g_2 et g_3 avec $g_1 = -4f_1 - 6f_2 + 7f_3$, $g_2 = 2f_1 + 2f_2 + 4f_3$, $g_3 = 6f_1 + 6f_2 + 15f_3$. La matrice des relations de G est donc $R = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix}$. Grâce aux opérations élémentaires sur les lignes et les colonnes suivantes : $L_1 \leftrightarrow L_2$; $L_2 \to L_2 + 2L_1$; $L_3 \to L_3 - 3L_1$; $C_2 \to C_2 - C_1$; $C_3 \to C_3 - 2C_1$; $L_1 \to L_1 + L_3$; $C_3 \to C_3 - C_1$; $C_3 \leftrightarrow C_1$; $C_3 \to C_3 - 2C_1$; $L_2 \to L_2 - 15L_1$; $L_3 \to L_3 - 3L_1$; $L_2 \to -L_2$; $C_3 \to C_3 - 15C_2$; $L_3 \to -L_3$ (par exemple), on obtient $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$ et on en déduit que

$$G \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Pour avoir une présentation par générateurs et relations de G qui donne cet isomorphisme, nous avons besoin de Q^{-1}. Ici $P = \begin{pmatrix} 0 & -2 & 1 \\ -1 & -32 & 15 \\ 0 & -3 & 2 \end{pmatrix}$ et $Q^{-1} = \begin{pmatrix} 2 & 2 & 7 \\ 15 & 16 & 45 \\ 1 & 1 & 3 \end{pmatrix}$. La nouvelle base $\mathbf{f}^*$ de $\mathbb{Z}^3$ était obtenue grâce aux opérations sur les colonnes, soit $\mathbf{f} = Q\mathbf{f}^*$ et donc $\mathbf{f}^* = Q^{-1}\mathbf{f}$. Par conséquent les nouveaux générateurs pour G sont donnés par $\mathbf{x}^* = Q^{-1}\mathbf{x}$, soit

$$\begin{aligned}x_1^* &= 2x_1 + 2x_2 + 7x_3 \\ x_2^* &= 15x_1 + 16x_2 + 45x_3 \\ x_3^* &= x_1 + x_2 + 3x_3.\end{aligned}$$

Nous savons que les nouvelles relations sont $d_i x_i^* = 0$, donc

$$G = \langle x_1^*, x_2^*, x_3^* \mid x_1^* = 0, 2x_2^* = 0, 6x_3^* = 0 \rangle.$$

Corollaire B.7. Soit M un A-module de type fini. Alors il existe $r \in \mathbb{N}$, $q \in \mathbb{N}$ et $a_1, \dots, a_q$ dans A non nuls et non inversibles vérifiant $a_1 \mid \dots \mid a_q$ tels que $M \cong A^r \oplus A/(a_1) \oplus \dots \oplus A/(a_q)$.

Démonstration. On applique le Corollaire **B.5**. Soit r le nombre de a_i qui sont nuls, donc $(a_n) = \dots = (a_{n-r+1}) = \{0\}$ et donc pour $n - r < i \leqslant n$ on a $A/(a_i) = A$. De plus, si a_i est inversible, $(a_i) = A$ donc $A/(a_i) = \{0\}$ et on peut donc l'ignorer dans la décomposition. Quitte à renuméroter les a_i on suppose donc que a_1 (et donc tous les a_i non nuls, soit jusqu'à a_q) n'est pas inversible. Donc $M \cong \bigoplus_{i=1}^q A/(a_i) \oplus A^r$. B.7

Corollaire B.8. Avec les notations du théorème précédent, le sous module de torsion de M est $T(M) = A/(a_1) \oplus \cdots A/(a_q)$.

Démonstration. D'après le corollaire ci-dessus, on a $M \cong A^r \oplus A/(a_1) \oplus \cdots A/(a_q)$.

Il est clair que a_q annule tous les éléments de $A/(a_1) \oplus \cdots A/(a_q)$ donc $A/(a_1) \oplus \cdots A/(a_q) \subset T(M)$. Soit maintenant $x \in T(M)$. Puisque $x \in M$ on peut écrire $x = u + v$ avec $u \in A^r$ et $v \in A/(a_1) \oplus \cdots A/(a_q)$. Donc $a_q x = a_q u$. Puisque x est de torsion, il existe $\lambda \in \mathrm{Ann}_A(x)$, $\lambda \neq 0$. Alors $\lambda a_q u = 0$. Mais u est un élément du A-module libre A^r, donc $u = (\alpha_1, \ldots, \alpha_r)$ avec $\alpha_i \in A$, et donc $\lambda a_q \alpha_i = 0$ pour tout i; comme A est intègre et que λ et a_q sont non nuls, on a $\alpha_i = 0$ pour tout i et donc $u = 0$. Donc $x = v \in A/(a_1) \oplus \cdots A/(a_q)$ et donc $T(M) = A/(a_1) \oplus \cdots A/(a_q)$. B.8

Corollaire B.9. Soit M un A-module de type fini. Si M est sans torsion, alors M est libre.

Lemme B.10. Soit $M = \langle x \rangle$ un A-module monogène et soit $\mathrm{Ann}_A(x) = (d)$.

(i) M est isomorphe comme A-module à $A/(d)$.

(ii) Si $d = pq$ et p, q premiers entre eux dans A, alors $M = \langle y \rangle \oplus \langle z \rangle$ avec $y = qx$, $z = px$, $\mathrm{Ann}_A(y) = (p)$, $\mathrm{Ann}_A(z) = (q)$.

Démonstration. **(i)** On applique le premier théorème d'isomorphisme à l'homomorphisme de A-modules $\varphi : A \to M$ qui envoie 1 sur x.

(ii)
- ✦ Il est clair que $p \in \mathrm{Ann}_A(y)$ puisque $py = pqx = dx = 0$ donc $(p) \subset \mathrm{Ann}_A(y)$. Soit maintenant $c \in \mathrm{Ann}_A(y)$. On a donc $0 = cy = cqx$ donc $cq \in \mathrm{Ann}_A(x) = (pq)$ donc $cq = pqr$ avec $r \in A$. Donc $c = pr \in (p)$ et donc $\mathrm{Ann}_A(y) = (p)$.
- ✦ Puisque A est principal on sait qu'il existe $u, v \in A$ tels que $1 = up + vq$. Donc $x = upx + vqx = uz + vy \in \langle x \rangle + \langle y \rangle$. Donc $\langle x \rangle = \langle y \rangle + \langle z \rangle$.
- ✦ Soit maintenant $t \in \langle y \rangle \cap \langle z \rangle$. Alors $pt = 0$ puisque $t \in \langle y \rangle$ et $p \in \mathrm{Ann}_A(y)$, et $qt = 0$ de même. Donc $t = upt + vqt = 0$. Donc $\langle y \rangle \cap \langle z \rangle = \{0\}$ et donc $M = \langle y \rangle \oplus \langle z \rangle$. B.10

Corollaire B.11. Soit M un A-module de type fini. Alors $M \cong \bigoplus A/(p^{n_r})$ où p parcourt les éléments irréductibles de A et où les n_r sont des entiers positifs presque tous nuls.
Les p^{n_r} sont appelés les **diviseurs élémentaires** de M.

Démonstration. On sait que $M \cong \bigoplus_{i=1}^{n} A/(a_i)$. On factorise chaque $a_i = u \prod p^{n_{p,i}}$ avec u inversible et p irréductible. On décompose ensuite à l'aide du lemme **B.10**. B.11

Remarque B.12. Si $A = \mathbb{Z}$, on retrouve la classification des groupes abéliens de type fini.

Théorème B.13 (Unicité des facteurs invariants)**.** Soient $r, s \in \mathbb{N}^*$. On considère deux suites $(a_1) \supset \cdots \supset (a_r)$ et $(b_1) \supset \cdots \supset (b_s)$ d'idéaux de A distincts de A. Si les A-modules $\bigoplus_{i=1}^{r} A/(a_i)$ et $\bigoplus_{j=1}^{s} A/(b_j)$ sont isomorphes, alors $r = s$ et, pour $1 \leqslant i \leqslant r$, $(a_i) = (b_i)$.

Pour démontrer ce théorème, nous aurons besoin du lemme suivant.

Lemme B.14. - Soit p un élément irréductible de A et d un élément de A. On pose $M = A/(d)$. Pour $n \in \mathbb{N}$, le A-module $p^n M/p^{n+1}M$ est isomorphe au A-module $A/(p)$ si p^{n+1} divise d et est nul sinon.

Démonstration. Soit $n \in \mathbb{N}$. On un morphisme surjectif de A-modules $A \longrightarrow M \longrightarrow p^n M \subset M$ qui envoie $a \in A$ sur $p^n(a + (d))$. On en déduit un morphisme surjectif $\varphi_n : A \longrightarrow M \longrightarrow p^n M/p^{n+1}M$ par composition avec la projection canonique. On vérifie aisément que $a \in A$ est dans le noyau de φ_n si et seulement s'il existe $b, c \in A$ tels que $p^n a = p^{n+1}b + cd$ c'est-à-dire si et seulement si $p^n a \in (p^{n+1}, d)$. Si p^{n+1} divise d, alors $(p^{n+1}) = (p^{n+1}, d)$ et on obtient facilement que $\mathrm{Ker}\, \varphi_n = (p)$. Sinon, p étant irréductible, le p.g.c.d. de p^{n+1} et d est de la forme p^r avec $r \in \mathbb{N}$, $r \leqslant n$, de sorte que $ap^n \in (p^r) = (p^{n+1}, d)$ pour tout $a \in A$. B.14

Démonstration du théorème. On peut toujours supposer que $r \leqslant s$. Mais alors, quitte à rajouter à la fin de la liste $(a_1) \supset \cdots \supset (a_r)$ des idéaux égaux à $\{0\}$, on peut supposer que $r = s$.

Pour $1 \leqslant i \leqslant r$, on pose $M_i = A/(a_i)$. En outre, posons $M = \oplus_{i=1}^{r} M_i$. Il est facile de montrer que, si p est un élément de A, on a un isomorphisme de A-modules :

$$p^n M/p^{n+1}M \cong \bigoplus_{i=1}^{r} p^n M_i/p^{n+1}M_i.$$

Supposons maintenant p irréductible. D'après le lemme **B.14**, le A-module $p^n M/p^{n+1}M$ est isomorphe au A-module $(A/(p))^t$ où t est le cardinal de l'ensemble $\{i \in \{1,\dots,r\}; p^{n+1}|a_i\}$. De plus, comme A est principal, l'anneau $A/(p)$ est un corps et les A-modules $p^n M/p^{n+1}M$ et $(A/(p))^t$ (isomorphes en tant que A-modules) sont des $A/(p)$-espaces vectoriels, isomorphes en tant que $A/(p)$-espaces vectoriels.

Soit à présent i entier tel que $1 \leqslant i \leqslant r$. Puisque $a_1 \mid \dots \mid a_i \mid \dots \mid a_r$, ce qui précède montre donc que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|a_i \iff \dim_{A/(p)} p^n M/p^{n+1}M \geqslant r+1-i.$$

Bien sûr, on a de même que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|b_i \iff \dim_{A/(p)} p^n M/p^{n+1}M \geqslant r+1-i.$$

Finalement, on a montré que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|a_i \iff p^{n+1}|b_i.$$

En écrivant les décompositions de a_i et b_i en produit de facteurs irréductibles, on en déduit que $(a_i) = (b_i)$. B.13

C Application à la réduction d'un endomorphisme d'un espace vectoriel

Soit $\mathbb{K}$ un corps commutatif, soit E un espace vectoriel de dimension finie n sur $\mathbb{K}$ et soit $\varphi \in \mathrm{End}_{\mathbb{K}}(E)$ (endomorphisme $\mathbb{K}$-linéaire).

Posons $A = \mathbb{K}[X]$, alors A est un anneau euclidien. L'application $A \times E \to E$ qui à $(P(X), v)$ associe $P(\varphi)(v)$ définit une structure de A-module sur E (cette structure de A-module dépend de φ).

Puisque E est de dimension finie sur $\mathbb{K}$, c'est un A-module de type fini (en effet, toute base de E comme $\mathbb{K}$-espace vectoriel est une famille génératrice du A-module E). De plus, il est de torsion car sinon il contiendrait $A = \mathbb{K}[X]$ (*cf.* corollaire **B.7**) qui est de dimension infinie sur $\mathbb{K}$. On pourra donc appliquer ce qui précède à E.

C.1 Facteurs invariants

Définition C.1. *Le **polynôme caractéristique** de φ est le polynôme $\chi_\varphi(X) = \det(\varphi - X\,\mathrm{id}_E)$.*

*Le **polynôme minimal** $m_\varphi(X)$ de φ est le générateur unitaire de $\mathrm{Ann}_A(E)$ (qui est un idéal principal). C'est le polynôme unitaire de plus petit degré qui annule φ.*

On peut décomposer E à l'aide du corollaire **B.5** :

$$E = \bigoplus_{i=1}^{r} E_i \text{ où } E_i = Ae_i^* \text{ est monogène avec } \mathrm{Ann}_A(e_i^*) = (q_i) \text{ et } q_i \mid q_{i+1} \text{ pour tout } i = 1,\dots,r-1.$$

On a $E_i \cong \mathbb{K}[X]/(q_i)$.

On peut supposer que les q_i sont unitaires et non constants. Ce sont les facteurs invariants du A-module E. On les appelle aussi les **facteurs invariants** de φ. On verra plus loin comment appliquer ce qui précède pour calculer ces facteurs invariants.

Il est facile de voir que $\mathrm{Ann}_A(E) = (q_r)$, donc :

Proposition C.2. Le polynôme minimal de φ est le facteur invariant unitaire du A-module E de plus haut degré. De plus, tous les facteurs invariants de E divisent m_φ.

Nous allons maintenant caractériser les facteurs invariants de φ, puis retrouver le théorème de Cayley-Hamilton.

Remarque C.3. Chaque E_i est stable par φ car E_i est un sous-A-module de E (et appliquer φ revient à faire agir $X \in A$). On peut donc considérer $\varphi_{|E_i} \in \mathrm{End}_{\mathbb{K}}(E_i)$.

Proposition C.4. Fixons i avec $1 \leqslant i \leqslant r$. Posons $q_i(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$. Alors $\left\{e_i^*, \varphi(e_i^*), \ldots, \varphi^{m-1}(e_i^*)\right\}$ est une base de E_i, et dans cette base, la matrice de $\varphi_{|E_i}$ s'écrit

$$\mathcal{C}_{q_i} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ & & & & -a_1 \\ & I_{m-1} & & & \vdots \\ & & & & -a_{m-1} \end{pmatrix}.$$

Cette matrice est appelée **matrice compagnon** de q_i.

Démonstration. ✦ On sait que $E_i = Ae_i^* = \{P(X)e_i^*\}$ donc E_i est engendré comme $\mathbb{K}$-espace vectoriel par $\{X^s e_i^*; s \in \mathbb{N}\}$. De plus, pour $s \geqslant m$, la division euclidienne donne $X^s = Q(X)q_i(X) + R(X)$ avec $\deg R < m$, donc $X^s e_i^* = Q(X)q_i(X)e_i^* + R(X)e_i^* = R(X)e_i^*$ puisque $q_i \in \mathrm{Ann}_A(e_i^*)$. Donc $\{X^s e_i^*; 0 \leqslant s < m\}$ est une partie génératrice du $\mathbb{K}$-espace vectoriel E_i.

✦ $\{X^s e_i^*; 0 \leqslant s < m\}$ est une famille libre du $\mathbb{K}$-espace vectoriel E_i. En effet, si $\sum_{s=0}^{m-1} \lambda_s X^s e_i^* = 0$ avec $\lambda_s \in \mathbb{K}$, alors le polynôme $\sum_{s=0}^{m-1} \lambda_s X^s$ est dans $\mathrm{Ann}_A(e_i^*) = (q_i)$ donc q_i le divise. Mais $\deg \sum_{s=0}^{m-1} \lambda_s X^s < m$, donc $\sum_{s=0}^{m-1} \lambda_s X^s = 0$ dans $\mathbb{K}[X]$. Donc $\lambda_s = 0$ pour tout s.
Donc $\{X^s e_i^*; 0 \leqslant s < m\}$ est bien une base du $\mathbb{K}$-espace vectoriel E_i. De plus $X^s e_i^* = \varphi^s(e_i^*)$ donc on a bien la base de l'énoncé.

✦ Pour tout s avec $0 \leqslant s \leqslant m-2$ on a $\varphi(X^s e_i^*) = X \cdot X^s e_i^* = X^{s+1} e_i^* = \varphi^{s+1}(e_i^*)$. Enfin, $\varphi(X^{m-1} e_i^*) = X^m e_i^* = (q_i(X) - \sum_{s=0}^{m-1} a_s X^s) e_i^* = -\sum_{s=0}^{m-1} a_s X^s e_i^*$. Donc la matrice de $\varphi_{|E_i}$ dans cette base est bien celle de l'énoncé. C.4

Corollaire C.5. Il existe une base de E dans laquelle la matrice de φ est

$$\mathcal{C}(q_1, \ldots, q_r) := \begin{pmatrix} \mathcal{C}_{q_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}_{q_r} \end{pmatrix}.$$

Démonstration. On applique ce résultat à chacun des modules cycliques de la décomposition de E. La réunion des bases de la proposition **C.4** donne une base de E dans laquelle la matrice de φ est $\mathcal{C}(q_1, \ldots, q_r)$. C.5

Proposition C.6. Soit φ un endomorphisme de E. On suppose qu'il existe une base de E dans laquelle la matrice de φ est de la forme $\mathcal{C}(q_1, \ldots, q_r)$ avec $q_i \in \mathbb{K}[X]$ unitaires et $q_1 \mid \ldots \mid q_r$. Alors les q_i sont les facteurs invariants de φ (c'est-à-dire du A-module E défini par φ).

Démonstration. Par hypothèse, E est une somme directe de sous-espaces vectoriels stables par φ; notons-les $E_1, \ldots, E_r$. On a donc une base $\mathcal{B}_i$ de E_i dans laquelle la matrice de $\varphi_{|E_i}$ est la matrice

compagnon $\mathcal{C}_{q_i}$ par hypothèse. Soit e_i^* le premier vecteur de $\mathcal{B}_i$. Alors $Ae_i^* \subset E_i$ puisque E_i est stable par φ, c'est donc un A-module. De plus, il est clair en regardant la matrice que

$$\mathcal{B}_i = \left\{e_i^*, \varphi(e_i^*), \dots, \varphi^{m-1}(e_i^*)\right\} = \left\{e_i^*, Xe_i^*, \dots, X^{m-1}e_i^*\right\}$$

où m est la dimension sur $\mathbb{K}$ de E_i, donc $E_i = Ae_i^*$ est le module cyclique engendré par e_i^*. Toujours en regardant la matrice, on voit facilement que $q_i(X) = X^m + \sum_{s=0}^{m-1} a_s X^s$ est dans $\mathrm{Ann}_A(e_i^*)$. Notons $(p) = \mathrm{Ann}_A(e_i^*)$. Alors $p \mid q_i$ et $\deg p = \deg q_i$ (sinon on aurait une $\mathbb{K}$-combinaison linéaire nulle des éléments de $\mathcal{B}_i$) donc $\mathrm{Ann}_A(e_i^*) = (p) = (q_i)$. Donc $E_i \cong A/(p) = A/(q_i)$ et donc $E \cong \oplus_{i=1}^r A/(q_i)$. Par unicité des facteurs invariants du A-module E, on en déduit que les q_i sont les facteurs invariants de φ. C.6

Proposition C.7. Soit $\varphi \in \mathrm{End}_{\mathbb{K}}(E)$.

(i) Le polynôme caractéristique de la matrice compagnon $\mathcal{C}_q$ est $(-1)^{\deg q} q$.

(ii) $\chi_\varphi = (-1)^n q_1 \dots q_r$.

(iii) m_φ divise χ_φ. Autrement dit, $\chi_\varphi(\varphi) = 0$ (théorème de Cayley-Hamilton).

(iv) χ_φ divise m_φ^n.

Démonstration. **(i)** Exercice.

(ii) Clair d'après le corollaire **C.5**.

(iii) $m_\varphi = q_r$ divise $(-1)^n q_1 \dots q_r = \chi_\varphi$.

(iv) Pour tout $i = 1, \dots, r$, on sait que q_i divise $q_r = m_\varphi$. Donc $\chi_\varphi = (-1)^n q_1 \dots q_r$ divise m_φ^r qui divise m_φ^n (puisque $r \leqslant n$). C.7

Corollaire C.8. Le polynôme caractéristique de φ a les mêmes facteurs irréductibles que le polynôme minimal de φ.

C.2 Calcul des facteurs invariants

On a vu dans le corollaire **B.5** et le théorème **B.2** comment trouver les facteurs invariants d'un module de type fini.

Proposition C.9. Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de E comme $\mathbb{K}$-espace vectoriel et soit M la matrice de φ dans la base $\mathcal{B}$. Alors E est un quotient d'un A-module libre de base $\{\varepsilon_1, \dots, \varepsilon_n\}$ telle que la classe ε_i dans le quotient soit e_i, et la matrice des relations du A-module E relative à $\{\varepsilon_1, \dots, \varepsilon_n\}$ est ${}^tM - XI_n$.
Donc pour trouver les facteurs invariants de φ (ou de E), on applique le théorème **A.7** à ${}^tM - XI_n$.

Démonstration. Ici, le A-module E est de type fini. On l'écrit comme le quotient d'un A-module libre : $\mathcal{B}$ engendre E comme A-module, donc E est un quotient de A^n. Notons $\{\varepsilon_1, \dots, \varepsilon_n\}$ une base du A-module libre A^n. Soit $\theta : A^n \twoheadrightarrow E$ l'homomorphisme de A-modules défini par $\theta(\varepsilon_i) = e_i$ pour tout i. Alors $E \cong A^n / \operatorname{Ker}\theta$.

Posons $M = (a_{ij})_{1 \leqslant i,j \leqslant n}$. Alors $\varphi(e_i) = \sum_i a_{ji} e_j$ pour tout i, c'est-à-dire que $\sum_i a_{ji} e_j - Xe_i = 0$, donc pour tout i l'élément $x_i = \sum_i a_{ji}\varepsilon_j - X\varepsilon_i$ est dans le noyau de θ. Les coordonnées de x_i dans la base $\{\varepsilon_1, \dots, \varepsilon_n\}$ forment la $i$me ligne de ${}^tM - XI_n$. Donc pour conclure, il nous faut montrer que les x_i engendrent $\operatorname{Ker}\theta$. On a déjà l'inclusion $\sum_{i=1}^n Ax_i \subset \operatorname{Ker}\theta$.

On vient de voir que pour tout i, $X\varepsilon_i$ est dans $(\oplus_{j=1}^n \mathbb{K}\varepsilon_j) + \sum_{i=1}^n Ax_i$, donc par récurrence, on peut dire de même pour tout $X^m\varepsilon_i$ et donc pour tout $P(X)\varepsilon_i$ avec $P(X) \in A$. Soit maintenant $z \in \operatorname{Ker}\theta$. Puisque $\{\varepsilon_1, \dots, \varepsilon_n\}$ est une base du A-module A^n, on peut écrire $z = \sum_i P_i(X)\varepsilon_i$ avec $P_i \in A$. D'après ce qui précède, on peut donc écrire $z = \sum_{i=1}^n \lambda_i \varepsilon_i + y$ avec $y \in Ax_1 + \dots + Ax_n$ et $\lambda_i \in \mathbb{K}$. On sait déjà que $y \in \operatorname{Ker}\theta$ par l'inclusion que l'on a déjà montrée, donc on a aussi $\sum_{i=1}^n \lambda_i \varepsilon_i = z - y \in \operatorname{Ker}\theta$.

Donc en appliquant θ on a $\sum_{i=1}^n \lambda_i e_i = 0$. Or $\{e_1, \dots, e_n\}$ est une $\mathbb{K}$-base de E, donc tous les λ_i sont nuls et donc $z = y \in Ax_1 + \cdots + Ax_n$.

Finalement on a bien $\operatorname{Ker}\theta = Ax_1 + \cdots + Ax_n$. C.9

Exemple C.10. Soit $\varphi \in \mathcal{M}_3(\mathbb{K})$ dont la matrice dans la base canonique $\{e_1, e_2, e_3\}$ est $T = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$.

On veut trouver les facteurs invariants de φ.

On considère donc la matrice ${}^tT - XI_3 = \begin{pmatrix} 1-X & 1 & 1 \\ -1 & -1-X & -1 \\ 1 & 0 & -X \end{pmatrix}$. Les opérations suivantes : $C_2 \leftrightarrow C_1$; $L_2 \to L_2 + (X+1)L_1$; $C_2 \to C_2 - (1-X)C_1$; $C_3 \to C_3 - C_1$; $L_2 \leftrightarrow L_3$; $C_3 \to C_3 + XC_2$; $L_3 \to L_3 + X^2 L_2$; $C_3 \to -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3 - X \end{pmatrix}$.

On en déduit que les facteurs invariants de φ sont $X^3 - X$ et que $\mathbb{K}^3 \cong \mathbb{K}[X]/(X^3 - X)$ comme $\mathbb{K}[X]$-module.

La matrice compagnon de $X^3 - X$ est $\mathcal{C}_{X^3-X} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Soit $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ la base canonique de $\mathbb{K}[X]^3$ (l'image de ε_i dans le quotient $\mathbb{K}^3$ est e_i). On obtient la nouvelle base de $\mathbb{K}[X]^3$, donnant les générateurs des modules cycliques dans la décomposition de $\mathbb{K}^3$, en lui appliquant Q^{-1}. Ici $Q^{-1} = \begin{pmatrix} 1-X & 1 & 1 \\ 1 & 0 & -X \\ 0 & 0 & -1 \end{pmatrix}$, donc la nouvelle base est donnée par $\varepsilon_1^* = (1-X)\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\varepsilon_2^* = \varepsilon_1 - X\varepsilon_3$ et $\varepsilon_3^* = -\varepsilon_3$. Seul e_3^*, la classe de ε_3^* dans le quotient de $\mathbb{K}[X]^3$, engendre un module cyclique non trivial (puisque les autres correspondent à des facteurs invariants égaux à 1 ; on peut aussi vérifier que la classe de ε_1^* qui est $(I_3 - T)(e_1) + e_2 + e_3$ et la classe de ε_2^* qui est $e_1 - T(e_3)$ sont nulles), et une $\mathbb{K}$-base de ce module cyclique est $e_3^* = -e_3$, $Te_3^* = -e_1$, $T^2 e_3^* = -e_1 - e_2 - e_3$ puisque $X^3 - X$ est de degré 3. Dans cette base la matrice de la transformation T est $\mathcal{C}_{X^3-X}$.

C.3 Forme de Jordan

Nous avons également vu une autre décomposition d'un module de type fini sur un anneau principal, faisant intervenir des irréductibles de A, dans le corollaire **B.11**.

Nous allons supposer dans cette partie que le corps $\mathbb{K}$ est algébriquement clos. Les polynômes irréductibles de $\mathbb{K}[X]$ sont donc les polynômes de la forme $X - \lambda$ avec $\lambda \in \mathbb{K}$.

On a une décomposition $E \cong \bigoplus_{i=1}^r Ae_i^*$ avec $\operatorname{Ann}_A(e_i^*) = (q_i)$, q_i unitaires et $q_1 \mid \dots \mid q_r$. On décompose chaque q_i en produit de facteurs irréductibles : $q_i = \prod_j (X - \lambda_{ij})^{n_{ij}}$ avec $\lambda_{ij} \in \mathbb{K}$ et $n_{ij} \in \mathbb{N}$. On sait par le lemme **B.10** (ou corollaire **B.11**) que

$$E \cong \bigoplus_{i,j} \mathbb{K}[X]/((X - \lambda_{ij})^{n_{ij}}).$$

Plus précisément, $\mathbb{K}[X]/((X - \lambda_{ij})^{n_{ij}})$ est isomorphe au sous-module cyclique de E engendré par $\prod_{k \neq j}(X - \lambda_{ik})^{n_{ik}} e_i^*$.

Chacun des facteurs $\mathbb{K}[X]/((X - \lambda_{ij})^{n_{ij}})$ est stable par φ puisque c'est un sous-$\mathbb{K}[X]$-module de E. Nous allons écrire la matrice de la restriction de φ à l'un d'eux dans une certaine base.

Soit donc $\mathbb{K}[X]/((X - \lambda)^s)$ l'un de ces facteurs, et notons w un générateur de ce module cyclique. Il a pour base $\{w, (X-\lambda)w, \dots, (X-\lambda)^{s-1}w\}$ *[comme dans la démonstration de la proposition* ***C.4*** *on a* $\dim_{\mathbb{K}} \mathbb{K}[X]/((X-\lambda)^s) = s$ *et la famille est libre sur* $\mathbb{K}$ *et contient* s *éléments donc c'est une base].* La matrice de φ dans cette base est celle de l'action de X. On a :

$$X \cdot w = (X - \lambda)w + \lambda w$$
$$X \cdot (X - \lambda)w = (X - \lambda)^2 w + \lambda(X - \lambda)w$$

$\cdots$

$X \cdot (X-\lambda)^p w = (X-\lambda)^{p+1} w + \lambda (X-\lambda)^p w$

$\cdots$

$X \cdot (X-\lambda)^{s-1} w = (X-\lambda)^s w + \lambda (X-\lambda)^{s-1} w = \lambda (X-\lambda)^{s-1} w.$

Donc la matrice est

$$J_s(\lambda) = \begin{pmatrix} \lambda & 0 & & & & \\ 1 & \lambda & \ddots & & \mathbf{0} & \\ 0 & 1 & \ddots & \ddots & & \\ \vdots & 0 & \ddots & \ddots & \ddots & \\ \vdots & \vdots & \ddots & \ddots & \lambda & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}$$

C'est bien un bloc de Jordan. Son polynôme caractéristique est $(\lambda - X)^s$, qui est égal au signe près au diviseur élémentaire correspondant au facteur $\mathbb{K}[X]/(X-\lambda)^s$.

Corollaire C.11. Si $\mathbb{K}$ est un corps algebriquement clos, toute matrice carrée est triangularisable.

Remarque C.12. A partir de la réduite de Jordan, on peut retrouver les invariants.

On construit un tableau de la façon suivante :

- ✦ A chaque valeur propre λ_{ij} on associe une ligne : on remplit les lignes avec les $(X-\lambda_{ij})^{n_{ij}}$ avec les n_{ij} en ordre décroissant, et on complète avec des 1 pour avoir des lignes de même longueur.
- ✦ Pour obtenir les facteurs invariants, on fait le produit colonne par colonne.

Exemple C.13. Les diviseurs élémentaires (polynômes unitaires égaux au signe près aux polynômes caractéristiques des blocs de Jordan) de

$$\begin{pmatrix} \boxed{2} & 0 & 0 & 0 & 0 \\ 0 & \boxed{\begin{matrix} 3 & 0 & 0 \\ 1 & 3 & 0 \\ 0 & 1 & 3 \end{matrix}} & 0 & 0 & 0 \\ 0 & 0 & \boxed{2} & 0 & 0 \\ 0 & 0 & 0 & \boxed{\begin{matrix} 3 & 0 \\ 1 & 3 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & \boxed{\begin{matrix} 3 & 0 & 0 \\ 1 & 3 & 0 \\ 0 & 1 & 3 \end{matrix}} \end{pmatrix}$$

sont $X-2$, $(X-3)^3$, $X-2$, $(X-3)^2$ et $(X-3)^3$.

$\lambda = 2$	$X-2$	$X-2$	1
$\lambda = 3$	$(X-3)^3$	$(X-3)^3$	$(X-3)^2$
Résultat	$(X-2)(X-3)^3$	$(X-2)(X-3)^3$	$(X-3)^2$
	(q_3)	(q_2)	(q_1)

Exemple C.14. On reprend l'exemple **C.10** avec $\mathbb{K} = \mathbb{C}$. On veut trouver la forme de Jordan de φ. On sait que $\mathbb{C}^3 \cong \mathbb{C}[X]e_3^* \cong \mathbb{C}[X]/(X^3 - X)$ avec $e_3^* = -e_3$ (e_3 est le troisième vecteur de la base canonique de $\mathbb{C}^3$). On a $X^3 - X = X(X-1)(X+1)$ qui est la décomposition en facteurs irréductibles. Donc $E \cong \langle (X-1)(X+1)e_3^* \rangle \oplus \langle X(X+1)e_3^* \rangle \oplus \langle X(X-1)e_3^* \rangle$, les modules cycliques ayant pour annulateurs dans l'ordre (X), $(X-1)$ et $(X+1)$. Ces modules cycliques sont tous de dimension 1, donc les blocs de Jordan sont de taille 1×1 et ne contiennent que la valeur propre. Donc dans la base $\{(X-1)(X+1)e_3^*; X(X+1)e_3^*; X(X-1)e_3^*\}$ la matrice de φ est

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

On peut reécrire la base :

$$(X-1)(X+1)e_3^* = (T-I_3)(T+I_3)(-e_3) = -e_1 - e_2$$
$$X(X+1)e_3^* = T(T+I_3)(-e_3) = -2e_1 - e_2 - e_3$$
$$X(X-1)e_3^* = T(T-I_3)(-e_3) = -e_2 - e_3.$$

VII Localisation

C'est un outil d'algèbre commutative, utile en géométrie algébrique (on étudie les ensembles de solutions d'équations polynomiales).

A est un anneau commutatif unitaire.

A Anneaux de fractions

Définition A.1. *Soit A un anneau. Une **partie multiplicative** S de A est une partie de A qui contient* 1 *et qui est stable par multiplication.*

Soit A un anneau et soit S une partie multiplicative de A.

Idée : On veut considérer un ensemble de quotients de la forme $\frac{a}{s}$ avec $a \in A$ et $s \in S$, et le munir d'une structure d'anneau.

On définit une relation d'équivalence sur $A \times S$ par

$$(a,s) \sim (a',s') \iff \exists t \in S \text{ tel que } t(as' - a's) = 0.$$

(L'insertion du t est nécessaire car on ne suppose pas que A est intègre.)

C'est bien une relation d'équivalence :

- $(a,s) \sim (a,s)$ car $as - sa = 0$.
- Si $(a,s) \sim (a',s')$, il existe $t \in S$ tel que $t(as' - a's) = 0$, donc $t(a's - as') = 0$ et donc $(a',s') \sim (a,s)$.
- Si $(a,s) \sim (a',s')$ et $(a',s') \sim (a'',s'')$, il existe $t \in S$ et $t' \in S$ tels que $t(as' - a's) = 0$ et $t'(a's'' - a''s') = 0$. Donc $tt'(as's'' - a'ss'' + a's''s - a''s's) = 0$ et donc $tt's'(as'' - a''s) = 0$ avec $tt's' \in S$. Donc $(a,s) \sim (a'',s'')$.

On forme le quotient $A \times S/\sim$, dont les éléments sont notés $\frac{a}{s}$. On note ce quotient $S^{-1}A$.

On remarque que si $0 \in S$, alors $S^{-1}A = \{0\}$ (en prenant $t = 0$, on voit que tout (a,s) est équivalent à $(0,1)$). On va donc supposer dans la suite que $0 \notin S$. En particulier, pour tous $s, s' \in S$, on a $ss' \in S$ donc $ss' \neq 0$.

Définition-Proposition A.2. $S^{-1}A$ est un anneau commutatif unitaire, dit **anneau de fractions**, pour les opérations suivantes :

- $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$
- $\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$.

L'unité est $\frac{1}{1}$ et l'élément nul est $\frac{0}{1}$.

Démonstration. L'addition est bien définie : si $\frac{a}{s} = \frac{a_1}{s_1}$ et $\frac{a'}{s'} = \frac{a'_1}{s'_1}$, on doit vérifier que $\frac{a_1 s'_1 + a'_1 s_1}{s_1 s'_1} = \frac{as' + a's}{ss'}$. Or il existe $t \in S$ et $t' \in S$ tels que $t(a_1 s - a s_1) = 0$ et $t'(a'_1 s' - a' s'_1) = 0$. Donc $tt'\,(ss'(s'_1 a_1 + s_1 a'_1) - s_1 s'_1(as' + sa')) = 0$, d'où le résultat.

De même, la multiplication est bien définie.

Il reste à vérifier que A est bien un anneau, commutatif et unitaire. A.2

Remarque A.3. L'application $\varphi : A \to S^{-1}A$ définie par $\varphi(a) = \dfrac{a}{1}$ est un morphisme d'anneaux.

Proposition A.4 (Propriété universelle)**.** Soit A un anneau, soit S une partie multiplicative de A ($0 \notin S$) et soit $\varphi : A \to S^{-1}A$ le morphisme d'anneaux ci-dessus. Pour tout anneau B et pour tout morphisme d'anneaux $f : A \to B$ tel que pour tout $s \in S$, $f(s)$ est inversible dans B, il existe un unique morphisme d'anneaux $g : S^{-1}A \to B$ tel que $g \circ \varphi = f$.

Démonstration. Posons $g(\dfrac{a}{s}) = (f(s))^{-1} f(a)$. Alors

- ✦ g est bien défini : si $\dfrac{a}{s} = \dfrac{a'}{s'}$, alors il existe $t \in S$ tel que $t(as' - a's) = 0$, d'où $f(t)(f(a')f(s) - f(a)f(s')) = 0$. En multipliant par $f(t)^{-1}f(s)^{-1}f(s')^{-1}$, on obtient $f(s)^{-1}f(a) = f(s')^{-1}f(a')$.
- ✦ g est un morphisme (exercice).
- ✦ $g \circ \varphi = f : g \circ \varphi(a) = g(\dfrac{a}{1}) = f(1)^{-1}f(a) = f(a)$.
- ✦ g est unique : on doit avoir $f(a) = g(\varphi(a)) = g(\dfrac{a}{1}) = g(\dfrac{a}{s}\dfrac{s}{1}) = g(\dfrac{a}{s})g(\dfrac{s}{1}) = g(\dfrac{a}{s})g(\varphi(s)) = g(\dfrac{a}{s})f(s)$, d'où l'unicité pour $g(\dfrac{a}{s})$. A.4

Exemple A.5. **(1)** Soit A un anneau. On peut prendre $S = A^\times$, l'ensemble des éléments inversibles de A. Dans ce cas φ est un isomorphisme $A \cong S^{-1}A$ (puisque $\dfrac{a}{s} = \dfrac{as^{-1}}{1} = \varphi(as^{-1})$, φ est surjective et si $\varphi(a) = 0$, il existe t inversible tel que $ta = 0$ d'où $a = 0$ donc φ est injective).

(2) Soit A un anneau *intègre* et soit $S = A \setminus \{0\}$. Alors $S^{-1}A$ est un corps, le **corps des fractions de** A.
Par exemple, si $A = \mathbb{Z}$ et $S = \mathbb{Z} \setminus \{0\}$ on obtient $S^{-1}A = \mathbb{Q}$.

(3) Soit A un anneau et soit P un idéal premier de A. Alors $S = A \setminus P$ est une partie multiplicative. On note $A_P := S^{-1}A$ l'anneau des fractions de A.

Remarque A.6. Si A est intègre et si $0 \notin S$, alors le morphisme d'anneaux $\varphi : A \to S^{-1}A$ est injectif.
En effet, si $\varphi(a) = 0 = \dfrac{0}{1}$, il existe $t \in S$ tel que $ta = 0$. Comme A est intègre et $t \neq 0$, on a $a = 0$.
De plus, $S^{-1}A$ est alors intégre.
En effet, si $\frac{a}{s}\frac{b}{t} = \frac{0}{1}$ avec $a \in A$, $b \in A$, $s \in S$ et $t \in S$, alors il existe $u \in S$ tel que $uab = 0$. On a $u \in S$ et $0 \notin S$ donc $u \neq 0$, donc comme A est intègre on a $ab = 0$, donc $a = 0$ ou $b = 0$ et donc $\frac{a}{s} = \frac{0}{1}$ ou $\frac{b}{s} = \frac{0}{1}$.

B Modules de fractions

Soient A un anneau, M un A-module et S une partie multiplicative de A.
On définit une relation d'équivalence sur $M \times S$ par

$$(m, s) \sim (m', s') \iff \exists t \in S \text{ tel que } t(s'm - sm') = 0.$$

(Exercice).

Définition-Proposition B.1. $S^{-1}M := M \times S / \sim$ est un $S^{-1}A$-module dont les éléments sont notés $\dfrac{m}{s}$ pour $m \in M$ et $s \in S$, pour les opérations suivantes :

- ✦ $\dfrac{m}{s} + \dfrac{m'}{t} = \dfrac{tm + sm'}{st}$ pour $m, m' \in M$ et $s, t \in S$.
- ✦ $\dfrac{a}{s}\dfrac{m}{t} = \dfrac{am}{st}$ pour $m \in M$, $a \in A$ et $s, t \in S$.

Démonstration. Exercice. B.1

Proposition B.2. Soit $f : M \to N$ un morphisme de A-modules. Alors l'application $S^{-1}f : S^{-1}M \to S^{-1}N$ définie par $(S^{-1}f)(\frac{m}{s}) = \frac{f(m)}{s}$ est un morphisme de $S^{-1}A$-modules. De plus, si $g : N \to P$ est un autre morphisme de A-modules, on a $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$. Enfin, $S^{-1}\,\mathrm{id}_M = \mathrm{id}_{S^{-1}M}$.

Démonstration. Exercice. Il faut vérifier que $S^{-1}f$ est bien définie. B.2

Proposition B.3. Soient A un anneau et S une partie multiplicative de A. Soit $M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte de A-modules. Alors $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ est une suite exacte de $S^{-1}A$-modules.

Démonstration.
- ✦ On a $g \circ f = 0$ donc $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$. Donc $\mathrm{Im}\, S^{-1}f \subset \mathrm{Ker}\, S^{-1}g$.
- ✦ Soit $\frac{m}{s} \in \mathrm{Ker}\, S^{-1}g$. Alors $\frac{g(m)}{s} = \frac{0}{1}$ dans $S^{-1}M''$, et donc il existe $t \in S$ tel que $tg(m) = 0$. Donc $g(tm) = 0$ et donc $tm \in \mathrm{Ker}\, g = \mathrm{Im}\, f$. Donc il existe $m' \in M'$ tel que $tm = f(m')$. On en déduit que $\frac{m}{s} = \frac{f(m')}{st} = S^{-1}f(\frac{m'}{st}) \in \mathrm{Im}\, S^{-1}f$. B.3

Proposition B.4. Il existe des isomorphismes de $S^{-1}A$-modules :

(i) $S^{-1}(M + N) = S^{-1}M + S^{-1}N$ (où M et N sont deux A-modules).

(ii) $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$ (où M et N sont deux sous-modules d'un module donné).

(iii) $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$ (où N est un sous-modules de M).

Démonstration. **(i)** Exercice facile.

(ii) Il est clair que $S^{-1}(M \cap N) \subset S^{-1}M \cap S^{-1}N$.
Soit $\frac{y}{s} = \frac{z}{t}$ avec $y \in M$, $z \in N$, $s, t \in S$. Alors il existe $u \in S$ tel que $u(ty - sz) = 0$. On a $w := uty = usz \in M \cap N$. Donc $\frac{y}{s} = \frac{w}{uts} \in S^{-1}(M \cap N)$.

(iii) On a une suite exacte $0 \to N \to M \to M/N \to 0$. En applicant S^{-1} on obtient une suite exacte $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$. On a donc $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$. B.4

Notation. Soit A un anneau et soit P un idéal premier. On a déjà dit que $S = A \setminus P$ est une partie multiplicative et que l'on note $A_P = S^{-1}A$ dans ce cas.

Si M est un A-module, on note aussi $M_P = S^{-1}M$. Enfin, si $f \in \mathrm{Hom}_A(M, N)$ on note $f_P : M_P \to N_P$ le morphisme $S^{-1}f$ de $S^{-1}A$ modules.

Proposition B.5. Soit M un A-module. Alors les propriétés suivantes sont équivalentes :

(i) $M = \{0\}$.

(ii) Pour tout idéal premier P de A, on a $M_P = \{0\}$.

(iii) Pour tout idéal maximal $\mathfrak{m}$ de A, on a $M_\mathfrak{m} = \{0\}$.

Démonstration. Il est clair que **(i)**⇒**(ii)**⇒**(iii)**. Il reste à montrer que **(iii)**⇒**(i)**.

On suppose que $M_\mathfrak{m} = \{0\}$ pour tout idéal maximal $\mathfrak{m}$ et que $M \neq \{0\}$. Soit $x \in M \setminus \{0\}$. Soit $\mathcal{A}$ l'annulateur de x. Alors $\mathcal{A}$ est un idéal de A, qui n'est pas égal à A (car $1 \notin \mathcal{A}$). Donc $\mathcal{A}$ est contenu dans un idéal maximal $\mathfrak{m}$.

Dans $M_\mathfrak{m}$ on a $\frac{x}{1} = 0$ par hypothèse, donc il existe $t \in S = A \setminus \mathfrak{m}$ tel que $tx = 0$. Or $t \notin \mathcal{A}$ (car $t \notin \mathfrak{m}$) : contradiction.

Donc $M = \{0\}$. B.5

Proposition B.6. Soit $\varphi : M \to N$ un morphisme de A-modules. Si P est un idéal premier de A, on note $\varphi_P : M_P \to N_P$ le morphisme de A_P-modules $S^{-1}\varphi$ pour $S = A \setminus P$. Alors les propriétés suivantes sont équivalentes :

(i) φ est injectif.

(ii) φ_P est injectif pour tout idéal premier P de A.

(iii) $\varphi_{\mathfrak{m}}$ est injectif pour tout idéal maximal $\mathfrak{m}$ de A.

Démonstration. **(i)⇒(ii)**. Puisque φ est injectif on a une suite exacte $0 \to M \xrightarrow{\varphi} N$. On applique S^{-1} avec $S = A \setminus P$, d'où une suite exacte $0 \to M_P \xrightarrow{\varphi_P} N_P$. Donc φ_P est injectif.

(ii)⇒(iii). Evident.

(iii)⇒(i). Soit M' le noyau de φ. On a une suite exacte $0 \to M' \to M \xrightarrow{\varphi} N$. Soit $\mathfrak{m}$ un idéal maximal de A; on obtient une suite exacte $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}}$. Or $\varphi_{\mathfrak{m}}$ est injectif, donc $M'_{\mathfrak{m}} = \{0\}$. C'est vrai pour tout idéal maximal $\mathfrak{m}$, donc $M = \{0\}$ d'après la proposition précédente. B.6

Proposition B.7. Soit $\varphi : M \to N$ un morphisme de A-modules. Alors les propriétés suivantes sont équivalentes :

(i) φ est surjectif.

(ii) φ_P est surjectif pour tout idéal premier P de A.

(iii) $\varphi_{\mathfrak{m}}$ est surjectif pour tout idéal maximal $\mathfrak{m}$ de A.

Démonstration. Exercice. B.7

Proposition B.8. Soit A un anneau intègre, soit M un A-module et soit S une partie multiplicative de A. Alors $T(S^{-1}M) = S^{-1}(T(M))$ où $T(M)$ désigne le sous-module de torsion de M.

Démonstration. On rappelle que $S^{-1}A$ est intègre donc on peut considérer le sous-module de torsion de $S^{-1}M$. (On suppose toujours que $0 \notin S$.) On note $\varphi : A \to S^{-1}A$ le morphisme d'anneaux défini par $\varphi(a) = \frac{a}{1}$, qui est ici injectif.

- ✦ Soit $\frac{m}{s} \in S^{-1}(T(M))$ avec $m \in T(M)$ et $s \in S$. Alors il existe $a \in A$, $a \neq 0$ tel que $am = 0$. Donc $\frac{a}{1}\frac{m}{s} = 0$ avec $\frac{a}{1} = \varphi(a) \neq 0$ (puisque A est intègre φ est injective) et donc $\frac{m}{s} \in T(S^{-1}M)$.
- ✦ Soit $\frac{m}{s} \in T(S^{-1}M)$. Alors il existe $\frac{a}{t} \in S^{-1}A$, $\frac{a}{t} \neq 0$, tel que $\frac{a}{t}\frac{m}{s} = 0$. On a donc $u \in S$ tel que $uam = 0$. Or A est intègre, u et a ne sont pas nuls, donc $ua \neq 0$ et donc $m \in T(M)$. Donc $\frac{m}{s} \in S^{-1}(T(M))$. B.8

Proposition B.9. Soit A un anneau intègre et soit M un A-module. Alors les assertions suivantes sont équivalentes :

(i) M est sans torsion.

(ii) M_P est sans torsion pour tout idéal premier P de A.

(iii) $M_{\mathfrak{m}}$ est sans torsion pour tout idéal maximal $\mathfrak{m}$ de A.

Démonstration. Pour **(i)⇒(ii)** (l'équivalence **(i)⇒(iii)**) se fait de même) :

M est sans torsion si et seulement si $T(M) = \{0\}$ (par définition), si et seulement si pour tout idéal premier P on a $T(M)_P = \{0\}$ d'après la proposition **B.5**, si et seulement si pour tout idéal premier P on a $T(M_P) = \{0\}$ d'après la proposition **B.8**, si et seulement si pour tout idéal premier P, M_P est sans torsion. B.9

Proposition B.10. Soit A un anneau et S une partie multiplicative de A. Alors, si A est un anneau noethérien, $S^{-1}A$ est un anneau noethérien.

Démonstration. Soit I un idéal de $S^{-1}A$. Notons $\varphi : A \to S^{-1}A$ le morphisme d'anneaux défini par $\varphi(a) = \frac{a}{1}$. Alors $\varphi^{-1}(I)$ est un idéal de A qui est nœthérien, donc il est de type fini : $\varphi^{-1}(I) = (a_1, \ldots, a_n)$, $a_i \in A$. Vérifions que $\{\varphi(a_1), \ldots, \varphi(a_n)\}$ engendre I.

Il est clair que $\varphi(a_i) \in I$ puisque $a_i \in \varphi^{-1}(I)$. Réciproquement, soit $x \in I$. Alors $x = \dfrac{a}{s}$ avec $a \in A$ et $s \in S$. Or $\varphi(a) = \dfrac{a}{1} = \dfrac{s}{1}x \in I$, donc $a \in \varphi^{-1}(I)$, donc il existe $\lambda_1, \ldots, \lambda_n$ dans A tels que $a = \sum_{i=1}^{n} \lambda_i a_i$. On a alors $x = \sum_{i=1}^{n} \dfrac{\lambda_i}{s}\varphi(a_i)$.

Donc $I = (\varphi(a_1), \ldots, \varphi(a_n))$ est bien de type fini. Donc $S^{-1}A$ est nœthérien. B.10

Références

- Dummit & Foote
- Jean Fresnel, Anneaux (BU)
- Ruaud-Warusfel
- Sharp
- Cameron
- Zariski-Samuel
- Jacobson, Basic Algebra I (BM)
- A. Jebli, Algebre commutative (BU)
- Douady vol. 1 (BU)
- Bigonnet-Reversat-Zhang (BU 512 REV)
- Francinou-Gianella
- Atiyah-MacDonald
- MacLane-Birkhoff (BU)