Table des matières

Module I.6

Algèbre commutative

Un peu d'histoire

Les principales sources de l'algèbre commutative sont, dans l'ordre chronologique : la théorie algébrique des nombres, la théorie des invariants et la géométrie algébrique.

Au XIX^{ème} siècle, Kummer, puis Dedekind, ont généralisé la théorie classique de la divisibilité (qui remontait pour l'essentiel à Euclide) sous la forme de théorie des *idéaux des anneaux d'entiers algébriques*.

Au tournant du XX^{ème} siècle, Hilbert a formalisé la théorie des invariants (dont l'essentiel des résultats jusque là reposait sur les calculs compliqués de l'école anglaise), en particulier les problèmes de finitude, à l'aide de la théorie des *idéaux des anneaux de polynômes*.

Les mêmes structures ont été retrouvées par les géomètres algébristes du premier quart de XX^{ème} siècle (Emil Artin, Emmy Noether et leur école) et ont donné naissance à la théorie des *anneaux noetheriens*. Le lecteur notera que tous les mathématiciens cités (mis à part Euclide) sont allemands.

Comme les groupes, les anneaux se sont répandus dans toutes les mathématiques, y compris en analyse, avec les anneaux de fonctions. Il y a en effet un lien profond entre les espaces de la géométrie différentielle ou analytique et les anneaux : de même qu'en géométrie affine ou euclidienne les espaces vectoriels de formes linéaires, qui généralisent les coordonnées, servent à repérer les points, de même les anneaux de fonctions servent à repérer et distinguer les points d'espaces plus généraux. Les anneaux de fonctions numériques continues ont été axiomatisés par Gelfand sous le nom d'*anneaux normés*. Un anneau muni d'une telle structure peut être considéré comme anneau des fonctions continues sur un espace topologique défini *a posteriori*. Grothendieck a généralisé ce point de vue en montrant que *tout anneau commutatif* peut être vu comme l'anneau des fonctions « régulières » sur un espace analogue à une « variété algébrique ». Enfin, Connes, inspiré par la mécanique quantique (où les fonctions sont remplacées par des opérateurs dont le produit n'est pas commutatif) a montré que l'on pouvait faire de la géométrie avec tout anneau, même non commutatif.

Selon un usage maintenant bien établi, ce chapitre [1] devrait donc former un tout avec les deux suivants (géométrie algébrique et arithmétique), ces derniers étant conçus comme des applications de techniques générales exposées ici (en ce qui concerne l'arithmétique, on reléguerait donc ailleurs la *théorie analytique des nombres*). En fait, nous aborderons largement la géométrie algébrique et l'arithmétique à travers des outils variés et des méthodes *ad hoc*, laissant leur exposé systématique à un cours de maitrise.
En principe, l'algèbre commutative est la théorie des anneaux commutatifs et de leurs idéaux. Sous cette forme, nous l'avons déjà rencontrée dans le module « Compléments d'algèbre » du cours de L2. En fait, une évolution marquante essentiellement due à l'école algébrique allemande a été la *linéarisation* des méthodes. De même que l'étude des corps (et des groupes) fait largement appel aux espaces vectoriels, de même l'étude des idéaux se plonge dans celle des *modules*. Le chapitre commence donc par l'exposé du langage des modules, qui généralise l'algèbre linéaire de L1. Nous abordons ensuite les *rudiments* de la riche théorie des anneaux et des modules noetheriens. (Nous appliquerons cette théorie dans le module I.7.) Pour conclure, nous développons le cas des anneaux principaux : la théorie est alors complète (on sait décrire avec précision tous les modules de type fini) et, dans le cas euclidien, effective (on dispose de bons algorithmes). Elle offre de plus des applications étonnantes aux groupes abéliens, dont nous aurons l'usage dans le module I.8, et à la réduction des endomorphismes, que nous avons rencontrée en L2.

1 MODULES SUR UN ANNEAU COMMUTATIF

1.1 Le langage des modules

On fixe une fois pour toutes un anneau commutatif A, avec les notations usuelles pour les opérations et les éléments neutres.

Définition 1. On dit qu'un groupe abélien $(E,+)$ est muni d'une structure de *module* sur l'anneau commutatif A, ou encore de *A-module* si l'on a une loi de composition (ou multiplication) externe $(a,x)\mapsto a.x$ de $A\times E$ dans E vérifiant les axiomes suivants :

$$\forall a,b\in A\ ,\ \forall x\in E\ ,\ (a+b).x = a.x+b.x, \tag{1}$$
$$\forall a\in A\ ,\ \forall x,y\in E\ ,\ a.(x+y) = a.x+a.y, \tag{2}$$
$$\forall a,b\in A\ ,\ \forall x\in E\ ,\ a.(b.x) = (ab).x, \tag{3}$$
$$\forall x\in E\ ,\ 1.x = x. \tag{4}$$

Le point de la notation $a.x$ est en général omis dans l'écriture : $a.x=ax$.

[1] Nous éviterons d'appeler « module » un chapitre qui traite essentiellement des *modules sur un anneau commutatif* !

Pour tout $a \in A$, l'application $\lambda_a : x \mapsto a.x$ de E dans lui-même est un endomorphisme de groupe. De plus, l'application $a \mapsto \lambda_a$ est un morphisme de l'anneau commutatif A dans l'anneau $\mathrm{End}(E,+)$ des endomorphismes du groupe E. (Ce dernier anneau n'est en général pas commutatif ; sa multiplication est la composition des endomorphismes.) Réciproquement, tout morphisme φ de l'anneau A dans l'anneau $\mathrm{End}(E,+)$ des endomorphismes d'un groupe abélien E permet de munir ce dernier d'une structure de A-module : il suffit de poser $a.x := \varphi(a)(x)$.

Comme dans le cas des espaces vectoriels, on a quelques conséquences immédiates : la commutativité de l'addition peut être déduite des autres axiomes en calculant de deux manières $(1+1)(x+y)$; si l'on note (temporairement) 0_E l'élément neutre de E, on a : $\forall a \in A\ ,\ a.0_E = 0_E$ et $\forall x \in E\ ,\ 0.x = 0_E$; de même, $(-1).x = -x$. Sauf exception, nous écrirons simplement 0 pour 0_E.

Exemples.

1. Si A est un corps, on retrouve la notion d'espace vectoriel.
2. Si $A = \mathbb{Z}$, reprenant les notations introduites pour les groupes abéliens ($2x = x+x$, etc), on voit que $m.x = mx$ (si $m \in \mathbb{N}$) ou $-m'x$ (si $m = -m', m' \in \mathbb{N}$). Ainsi, *tout groupe abélien peut être considéré d'une manière unique comme un $\mathbb{Z}$-module*. La théorie des groupes abéliens est donc un cas particulier de la théorie des modules.
3. Le groupe A^n est muni d'une structure de A-module par la loi : $a.(a_1,\dots,a_n); = (aa_1,\dots,aa_n)$. Pour $n = 0$, par convention, on obtient le *module trivial* $\{0\}$ que l'on note parfois 0.
4. De même, en posant $a.(a_i) := (aa_i)$, on fait des groupes A^I et $A^{(I)}$ des A-modules.
5. Soient $V_1(x,y)$ et $V_2(x,y)$ deux champs de vecteurs continus sur un ouvert Ω de $\mathbb{R}^2$. L'application $(x,y) \mapsto V_1(x,y) + V_2(x,y)$ est un champ de vecteurs continu sur Ω. De même, si $V(x,y)$ est un champ de vecteurs continu sur Ω et si f est une fonction continue de Ω dans $\mathbb{R}$, l'application $(x,y) \mapsto f(x,y)V(x,y)$ est un champ de vecteurs continu sur Ω. On définit ainsi un module sur l'anneau $\mathcal{C}(\Omega,\mathbb{R})$.
6. Soit $f : A \to B$ un morphisme d'anneaux. En posant $a.b := f(a)b$, on fait de B un A-module. Il n'est d'ailleurs pas nécessaire de supposer B commutatif. Si l'on suppose de plus que $\mathrm{Im}\, f$ est *central* dans B, autrement dit, que pour $a \in A$ et $x \in B$, on a $f(a)x = xf(a)$, alors il y a compatibilité entre les multiplications externe et interne dans B : $\forall a \in A\ ,\ \forall x,y \in B\ ,\ (a.x)y = x(a.y) = a.(xy)$. On dit alors que B est une *A-algèbre*, ce qui généralise la terminologie du cours de L2.

Pour toute famille $(x_i) \in E^I$ d'éléments du A-module E, on appelle *combinaison linéaire des x_i* toute expression de la forme $\sum_{i\in I} a_i x_i$, où $(a_i) \in A^{(I)}$ est une famille *à support fini* d'éléments de A (autrement dit, presque tous les a_i sont nuls). Les règles de calcul sur les combinaisons linéaires sont essentiellement les mêmes que celles données dans le cours de L1 dans le cadre des espaces vectoriels. La principale différence concerne les familles libres et liées, nous y reviendrons plus loin.

1.1.1 Sous-modules

Définition 2. Un *sous-module* (ou *sous-A-module*) du A-module E est un sous-groupe additif E' qui est de plus stable pour la loi externe :

$$\forall a \in A \ , \ \forall x \in E' \ , \ ax \in E'.$$

Le sous-groupe E' est alors automatiquement muni d'une structure de A-module par la restriction des deux lois de E. Bien entendu, $\{0\}$ est un sous-module de E (appelé *sous-module trivial*) et E est lui-même un sous-module.

Exemples.

1. Dans le cas d'un corps, un sous module est un sous–espace vectoriel.
2. Dans le cas de l'anneau $\mathbb{Z}$, un sous-module est un sous-groupe.
3. On définit des sous-modules de A^n en considérant les ensembles de solutions de systèmes d'équations linéaires : $a_1x_1 + \cdots + a_nx_n = 0$, $b_1x_1 + \cdots + b_nx_n = 0$, etc. (Tout sous-module ne s'obtient pas ainsi, voir l'exercice I.6.4 de la page 60.)
4. Le module A^I admet le sous-module $A^{(I)}$ ainsi que le *sous-module diagonal* formé des familles (a_i) telles que $\forall i, j \ , \ a_i = a_j$.
5. Soit $d \in A$. Alors $dE := \{dx \mid x \in E\}$ est un sous-module de E. Cette construction peut se généraliser : si $\mathfrak{A}$ est un idéal de A, on pose $\mathfrak{A}E := \{\sum a_i x_i \mid \forall i \ , \ a_i \in \mathfrak{A}, x_i \in E\}$. C'est un sous-module de E. (On retrouve dE en prenant $\mathfrak{A} := dA$.)

Exercice 1.
Quels sont les sous-modules du A-module A ?

Solution. Ce sont les idéaux de A.

Pour toute famille $(x_i) \in E^I$, l'ensemble des combinaisons linéaires $\sum a_i x_i$ est un sous-module de E, appelé *sous-module engendré par les* x_i :

$$\sum_{i \in I} Ax_i := \left\{ \sum_{i \in I} a_i x_i \ \middle| \ (a_i) \in A^{(I)} \right\}.$$

Par exemple, le sous-module engendré par $x \in E$ est $Ax := \{ax \mid a \in A\}$, le sous-module engendré par $x, y \in E$ est $Ax + Ay := \{ax + by \mid a, b \in A\}$, etc. Pour toute famille $(E_j)_{j \in J}$ de sous-modules de E, l'intersection $\bigcap_{j \in J} E_j$ est un sous-module de E.

L'intersection de tous les sous-modules contenant les x_i (donc également le plus petit sous-module contenant les x_i) n'est autre que le sous-module $\sum_{i\in I} Ax_i$ engendré par les x_i.

On dit que $(x_i) \in E^I$ est une *famille génératrice* (ou un *système générateur*) de E si E est engendré par les x_i. Il revient au même de dire que tout élément de E est combinaison linéaire des x_i :

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

On dit que E est un module *de type fini* s'il admet un système générateur fini : $E = Ax_1 + \cdots + Ax_n$.

Sommes de sous-modules.

Si les E_j sont des sous-modules de E, le sous-module engendré par $\bigcup_{j\in J} E_j$ est la *somme des* E_j, qui se calcule comme suit :

$$\sum_{j\in J} E_j = \left\{ \sum_{j\in J} x_j \;\middle|\; \forall j \in J\ ,\ x_j \in E_j \right\},$$

où l'on se restreint évidemment aux familles $(x_j)_{j\in J}$ à support fini. On dit que la somme des sous-modules E_j est *directe* si l'on a l'implication :

$$\sum_{j\in J} x_j = 0 \Longrightarrow \forall j\ ,\ x_j = 0.$$

On dit également que les E_j *sont en somme directe*. Dans ce cas, on écrit :

$$\sum_{j\in J} E_j = \bigoplus_{j\in J} E_j.$$

Cela revient à dire que toute élément de $\sum_{j\in J} E_j$ s'exprime de manière *unique* sous la forme $\sum_{j\in J} x_j$. Le critère suivant, démontré en L2 pour les sous–espaces vectoriels s'adapte sans problème : pour que les sous-modules $E_1, \ldots, E_n$ soient en somme directe, il faut, et il suffit, que $E_i \cap (E_1 + \cdots + E_{i-1}) = \{0\}$ pour $1 \leqslant i \leqslant n$. (Bien entendu, l'ordre choisi pour les indices est arbitraire.) Dans le cas particulier où $E = E_1 \oplus E_2$, on dit que les sous-modules E_1 et E_2 sont *supplémentaires* l'un de l'autre. On dit alors que E_1 et E_2 sont *facteurs directs* de E.

Matrices et combinaisons linéaires.

Soit $\mathcal{X} := (x_1, \dots, x_n)$ une famille finie d'éléments de E. On définit une famille finie $\mathcal{Y} := (y_1, \dots, y_p)$ de combinaisons linéaires des x_i par les formules : $y_j = \sum_{i=1}^{n} a_{i,j}x_i$ $(1 \leqslant j \leqslant p)$. Ces formules peuvent être abrégées en :

$$\mathcal{Y} = \mathcal{X}M,$$

où $M := (a_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}}$ est une matrice de $M_{n,p}(A)$. Cette écriture suit les règles du calcul matriciel (à cela près que l'on devrait alors écrire $y_j = \sum_{i=1}^{n} x_i a_{i,j}$, contrairement à l'usage d'écrire les scalaires à gauche).

Exercice 2.
Exprimer matriciellement le sous-module F engendré par la famille $\mathcal{X} := (x_1, \dots, x_n)$.

Solution. C'est l'ensemble des combinaisons linéaires des x_i :

$$F = \{a_1x_1 + \cdots + a_nx_n \mid (a_1, \dots, a_n) \in A^n\} = \{\mathcal{X}M \mid M \in M_{n,1}(A)\} = \mathcal{X}A^n,$$

à condition d'identifier, comme il est d'usage, A^n avec $M_{n,1}(A)$ (écriture en vecteurs colonnes).

Ce calcul est cohérent. Par exemple, si l'on introduit une famille $\mathcal{Z} := (z_1, \dots, z_q)$ par les formules : $z_j = \sum_{j=1}^{p} b_{j,k}y_j$ $(1 \leqslant k \leqslant q)$, on peut écrire $\mathcal{Z} = \mathcal{Y}N$, où $N := (b_{j,k})_{\substack{1\leqslant j\leqslant p\\ 1\leqslant k\leqslant q}} \in M_{p,q}(A)$, et l'on vérifie sans peine que $\mathcal{Z} = \mathcal{X}P$, où $P := MN \in M_{n,q}(A)$.

Proposition 1. Soit $\mathcal{X} := (x_1, \dots, x_n)$ une famille finie d'éléments de E. Soit $\mathcal{Y} := (y_1, \dots, y_n)$ la famille définie par les formules : $y_j = \sum_{i=1}^{n} a_{i,j}x_i$ $(1 \leqslant j \leqslant n)$, où $M := (a_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}} \in M_n(A)$. Le sous-module F engendré par les x_i et le sous-module G engendré par les y_j vérifient les relations :

$$(\det M)F \subset G \subset F.$$

Démonstration. La relation $G \subset F$ est évidente. Pour l'autre relation, on écrit $\mathcal{Y} = \mathcal{X}M$, que l'on multiplie à droite par $N := {}^t\tilde{M}$ (transposée de la comatrice). Or, la démonstration donnée dans le cours de L1 que $M{}^t\tilde{M} = {}^t\tilde{M}M = (\det M)I_n$ est valable sur un anneau commutatif arbitraire. On en déduit que $(\det M)\mathcal{X} = \mathcal{Y}N$, et la conclusion s'ensuit. ■

1.1.2 Annulateurs, torsion

Voici la première différence importante entre modules et espaces vectoriels : l'implication $a.x = 0 \Rightarrow a = 0 \quad$ ou $\quad x = 0_E$ est *fausse* en général. Prenons par exemple $A := \mathbb{Z}$ et $E := \mathbb{Z}/6\mathbb{Z}$ (deuxième exemple ci-dessus). Alors, dans $\mathbb{Z}/6\mathbb{Z}$, on a l'égalité : $2.\overline{3} = \overline{0}$, bien que $2 \neq 0$ et $\overline{3} \neq \overline{0}$. (Ici, on a pris $a := 2$ et $x := \overline{3}$.)

On appelle *annulateur d'un élément* $x \in E$ l'idéal $\mathrm{Ann}_A(x) := \{a \in A \mid ax = 0_E\}$, également noté $\mathrm{Ann}(x)$. (Le lecteur consciencieux vérifiera que c'est bien un idéal). On appelle *annulateur du module* E l'idéal $\mathrm{Ann}_A(E) := \bigcap_{x \in E} \mathrm{Ann}_A(x) = \{a \in A \mid \forall x \in E\ ,\ ax = 0_E\}$, également noté $\mathrm{Ann}(E)$. Le module E est dit *fidèle* si $\mathrm{Ann}_A(E) = \{0\}$.

Si E est un module sur l'anneau $B := A/\mathfrak{A}$, on peut le voir comme un A-module en posant $a.x := \overline{a}x$ (où $\overline{a}$ désigne la classe de $a \in A$ dans $A/\mathfrak{A}$). Il est clair que ce A-module (que l'on dénote encore abusivement E) est tel que $\mathfrak{A} \subset \mathrm{Ann}_A(E)$. Réciproquement, si E est un A-module tel que $\mathfrak{A} \subset \mathrm{Ann}_A(E)$, on en fait un module sur $A/\mathfrak{A}$ en posant : $\overline{a}.x := ax$; le lecteur vérifiera que le membre de droite de cette égalité ne dépend pas du représentant particulier $a \in A$ de $\overline{a} \in B$. La condition $\mathfrak{A} \subset \mathrm{Ann}_A(E)$ peut également s'écrire $\mathfrak{A}E = \{0\}$. Par exemple, les modules sur $\mathbb{Z}/n\mathbb{Z}$ sont exactement les groupes abéliens G tels que $nG = \{0\}$. Ainsi, nous *identifierons* les modules sur $A/\mathfrak{A}$ aux A-modules tels que $\mathfrak{A}E = \{0\}$. Nous constaterons que toutes les constructions qui suivent (sous-modules, applications linéaires ...) sont les mêmes pour les deux objets. En particulier, tout A-module E est canoniquement un $A/\mathrm{Ann}_A(E)$-module fidèle.

On dit que $x \in E$ est *de torsion* si $\mathrm{Ann}_A(x) \neq \{0\}$. L'ensemble des éléments de torsion de E est noté $\mathrm{Tor}_A(E)$, ou $\mathrm{Tor}(E)$. Pour tout $a \in A$, nous noterons :

$$E(a) := \{x \in E \mid ax = 0\}. \tag{5}$$

C'est bien entendu un sous-module de E, et $\mathrm{Tor}_A(E) = \bigcup_{a \neq 0} E(a)$. Le module E est dit *de torsion* (resp. *sans torsion*) si $\mathrm{Tor}_A(E) = E$ (resp. si $\mathrm{Tor}_A(E) = \{0\}$).

Si A est intègre, $\mathrm{Tor}_A(E)$ est un sous-module de E, le *sous-module de torsion*). En effet, soient $x, y \in \mathrm{Tor}_A(E)$, donc $ax = by = 0$ avec $a, b \neq 0$. Alors $ab(x + y) = 0$ et $ab \neq 0$ (c'est ici qu'intervient l'hypothèse d'intégrité de A). En fait, on a toujours : $E(a) + E(b) \subset E(ab)$. La stabilité par multiplication externe est laisée au lecteur (elle ne requiert pas l'intégrité).

Exercice 3.
Qu'en est-il si $E := A := \mathbb{Z}/6\mathbb{Z}$?

Solution. Pour tout anneau A, $\mathrm{Tor}_A(A)$ est l'ensemble des diviseurs de 0 dans A. Par exemple, pour $A := \mathbb{Z}/6\mathbb{Z}$, c'est $\{\overline{0}, \overline{2}, \overline{3}, \overline{4}\}$: ce n'est pas un sous-groupe (ni un sous-module, ni un idéal).

Exercice 4.
Calculer les annulateurs des éléments du $\mathbb{Z}$-module $E := \mathbb{Q}/\mathbb{Z}$. Qu'en déduire pour $\mathrm{Ann}_{\mathbb{Z}}(E)$, pour $\mathrm{Tor}_{\mathbb{Z}}(E)$?

Solution. Soit $x := \overline{r} \in \mathbb{Q}/\mathbb{Z}$, où $r := \dfrac{a}{b} \in \mathbb{Q}$ (fraction irréductible). Alors $nx = 0 \Leftrightarrow b|na$, et $\mathrm{Ann}_A(x) = b\mathbb{Z}$. Tous les éléments sont donc de torsion et $\mathrm{Tor}_{\mathbb{Z}}(E) = E$; mais ils n'ont pas d'annulateur commun et $\mathrm{Ann}_{\mathbb{Z}}(E)$ est trivial.

> ***Remarque***. Si E est de torsion et de type fini et si A est intègre, alors $\mathrm{Ann}_A(E)$ n'est pas trivial. En effet, on écrit $E = Ax_1 + \cdots + Ax_n$ et il existe $a_1, \ldots, a_n$ non nuls tels que $a_i x_i = 0$ $(1 \leqslant i \leqslant n)$. On a alors $a_1 \cdots a_n \in \mathrm{Ann}_A(E)$. L'exercice précédent montre donc que $\mathbb{Q}/\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module de type fini. (Voir également l' exercice I.6.6 de la page 60.)

1.2 Applications linéaires

Définition 3. Une *application linéaire* (ou encore *A-linéaire*) du A-module E dans le A-module F est un morphisme f du groupe additif $(E, +)$ dans le groupe additif $(F, +)$ tel que de plus :

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

On dit aussi que f est un *morphisme de A-modules*. L'ensemble des morphismes du A-module E dans le A-module F est noté $\mathrm{Hom}_A(E, F)$. Les éléments de $\mathrm{Hom}_A(E, E)$, ensemble que l'on note $\mathrm{End}_A(E)$, sont appelés *endomorphismes* du A-module E.

Il revient au même d'exiger que f préserve les combinaisons linéaires $f(ax+by) = af(x)+bf(y)$. Plus généralement, on a alors : $f\left(\sum a_i x_i\right) = \sum a_i f(x_i)$.

Exemples.

1. Si A est un corps, on retrouve la notion d'application linéaire entre espaces vectoriels.
2. Si $A = \mathbb{Z}$, les applications linéaires sont simplement les morphismes de groupes (abéliens par hypothèse).

3. Pour tout module E, l'identité Id_E est un morphisme. Le composé des morphismes $f : E \to F$ et $g : F \to G$ est un morphisme $g \circ f : E \to G$. Si $f : E \to F$ est un morphisme bijectif, son inverse f^{-1} est un morphisme : on dit que c'est un *isomorphisme* (un *automorphisme* si $E = F$).
4. L'application constante $x \mapsto 0$ est un morphisme, appelé *morphisme trivial*. Si E ou F est le module trivial $\{0\}$, c'est le seul morphisme de E dans F.
5. Pour tout module E, les applications de la forme $x \mapsto ax$, où $a \in A$ est fixé, sont des endomorphismes de E.
6. Supposons que l'on ait une somme directe : $E = E_1 \oplus \cdots \oplus E_n$. Comme dans le cas des espaces vectoriels, on lui associe des projections p_i, qui sont des endomorphismes idempotents de E tels que $\mathrm{Im}\, p_i = E_i$, $p_i p_j = 0$ si $i \neq j$ et $p_1 + \cdots + p_n = \mathrm{Id}_E$. Réciproquement, si des endomorphismes idempotents vérifient ces deux dernières équations, les $E_i := \mathrm{Im}\, p_i$ ont pour somme directe E.

Proposition 2. Soit $f : E \to F$ un morphisme de A-modules. Soient $E' \subset E$ et $F' \subset F$ des sous-modules. Alors $f(E')$ est un sous-module de F et $f^{-1}(F')$ est un sous-module de E. En particulier, l'image $\mathrm{Im}\, f$ est un sous-module de F et le noyau $\mathrm{Ker}\, f$ est un sous-module de E.

Démonstration. C'est la même que dans le cas des espaces vectoriels. ■

Il est immédiat que $\mathrm{Hom}_A(E, F)$ est un sous-groupe du groupe de tous les morphismes de $(E, +)$ dans $(F, +)$. Si l'on définit af comme l'application linéaire $x \mapsto af(x)$, on fait de $\mathrm{Hom}_A(E, F)$ un A-module. L'application $(f, g) \mapsto g \circ f$ de $\mathrm{Hom}_A(E, F) \times \mathrm{Hom}_A(F, G)$ dans $\mathrm{Hom}_A(E, G)$ est A-bilinéaire (c'est-à-dire linéaire séparément en chaque argument) et vérifie les propriétés habituelles (associativité, neutralité de Id_E et Id_F, etc). En particulier, $\mathrm{End}_A(E)$ est un anneau (en général non commutatif). Le groupe de ses unités (éléments inversibles) est le groupe $\mathrm{Aut}_A(E)$ des *automorphismes* du A-module E (isomorphismes de E dans lui-même). Comme les homothéties $\lambda_a : x \mapsto ax$ sont centrales dans $\mathrm{End}_A(E)$ (c'est la définition même de la linéarité), le morphisme $a \mapsto \lambda_a$ fait de $\mathrm{End}_A(E)$ une A-algèbre (ce terme a été défini page 5).

Matrices et applications linéaires.

Les applications linéaires de A dans F sont les applications de la forme $a \mapsto ax$, où $x \in F$ est fixé. Plus généralement, les applications linéaires de A^n dans F sont les applications de la forme $f(a_1, \ldots, a_n) = a_1 y_1 + \cdots + a_n y_n$, où $y_1, \ldots, y_n \in F$. En fait, y_i est l'image de $e_i := (0, \ldots, 1, \ldots, 0) = (\delta_{i,j})_{1 \leqslant j \leqslant n} \in A^n$.
Pour décrire les applications linéaires de A^n dans A^p, il est d'usage d'écrire les éléments

sous forme de colonnes, *i.e.* d'identifier A^n à $M_{n,1}(A)$ et A^p à $M_{p,1}(A)$. Les applications linéaires ont alors la forme $X \mapsto MX$, où $M \in M_{p,n}(A)$. L'essentiel du calcul matriciel de cours de L1 s'applique tel quel. Par exemple, les modules $\mathrm{Hom}_A(A^n, F)$ et F^n sont isomorphes. De même, les modules $\mathrm{Hom}_A(A^n, A^p)$ et $M_{p,n}(A)$ sont isomorphes, et les modules $\mathrm{End}_A(A^n)$ et $M_n(A)$ sont isomorphes.

Le cas des isomorphismes et des automorphismes mérite un peu d'attention. Soient $M \in M_{p,n}(A)$ et $N \in M_{n,p}(A)$ deux matrices telles que $MN = I_p$ et $NM = I_n$. Soit $\mathfrak{M}$ un idéal maximal arbitraire de A. Si l'on note $k := A/\mathfrak{M}$ le corps résiduel, en appliquant le morphisme $A \to k$, on obtient des égalités $\overline{M}\ \overline{N} = I_p$ et $\overline{N}\ \overline{M} = I_n$ entre matrices sur le corps k. On sait alors que l'on a nécessairement $n = p$.
Soit maintenant $M \in M_n(A)$ une matrice *carrée* admettant un inverse à droite : $MN = I_n$. La multiplicativité du déterminant (valable sur tout anneau) entraine que $\det M \in A^*$, groupe des unités (éléments inversibles) de A. Réciproquement, si $\det M \in A^*$, alors $(\det M)^{-1}{}^t\tilde{M}$ est l'inverse à droite et à gauche de M, et c'est donc son unique inverse.

Applications linéaires et familles

À toute famille $\underline{x} := (x_i)_{i\in I} \in E^I$, on associe un morphisme :

$$\begin{cases} \varphi_{\underline{x}} : A^{(I)} \to E, \\ (a_i)_{i\in I} \mapsto \sum\limits_{i\in I} a_i x_i. \end{cases} \tag{6}$$

On obtient ainsi un isomorphisme $\underline{x} \mapsto \varphi_{\underline{x}}$ de E^I sur $\mathrm{Hom}_A\left(A^{(I)}, E\right)$. Les propriétés du morphisme $\varphi_{\underline{x}}$ traduisent des propriétés de la famille $(x_i)_{i\in I}$. On étend ainsi la terminologie des espaces vectoriels.

Par exemple, pour que le morphisme $\varphi_{\underline{x}}$ soit surjectif, il faut, et il suffit, que $(x_i)_{i\in I}$ soit une famille génératrice. On définit alors le *module des relations* entre les générateurs x_i comme le noyau de $\varphi_{\underline{x}}$:

$$R := \mathrm{Ker}\,\varphi_{\underline{x}} = \{(a_i)_{i\in I} \in A^{(I)} \mid \sum_{i\in I} a_i x_i = 0\}. \tag{7}$$

Pour que le morphisme $\varphi_{\underline{x}}$ soit injectif, il faut, et il suffit, qu'il n'existe aucune relation linéaire non triviale entre les x_i :

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

On dit alors que la famille $(x_i)_{i\in I}$ est *libre*, ou que les x_i sont *linéairement indépendants*. Une famille $(x_i)_{i\in I}$ qui n'est pas libre est dite *liée*, et les x_i sont dits *liés* ou *linéairement dépendants*. Voici quelques exemples de difficultés dans l'usage de ces notions pour les modules (en contraste avec les espaces vectoriels).

Exercice 5.
À quelle condition la famille (x) est-elle liée ?

Solution. Si x est de torsion (même non nul).

Attention. Si les x_i sont liés, on ne peut en déduire que l'un est combinaison linéaire des autres. Par exemple, deux éléments du A-module A sont toujours liés : s'ils sont tous deux nuls, c'est évident, sinon on a la relation $a.b + (-b).a = 0$; mais l'un n'est pas toujours multiple de l'autre.
Une famille libre maximale n'est pas nécessairement génératrice. Par exemple, la famille (x) du A-module A est libre maximale si, et seulement si, x ne divise pas 0, mais elle n'est génératrice que si x est inversible.
Une famille génératrice minimale n'est pas nécessairement libre. Par exemple, la famille $(2, 3)$ du $\mathbb{Z}$-module $\mathbb{Z}$ est génératrice minimale (aucune de ses sous-familles strictes n'est génératrice) mais elle n'est pas libre.

On peut traduire en termes matriciels les notions de famille génératrice, de famille libre, dans le cas de familles finies. On utilise pour cela les notations introduites page 8.
Dire que $\mathcal{X} := (x_1, \ldots, x_n)$ est génératrice, c'est dire que tout $x \in E$ s'écrit $\mathcal{X}U$, avec $U \in M_{n,1}(A)$. Modulo l'identification de A^n avec $M_{n,1}(A)$ (écriture en colonnes), on peut donc écrire symboliquement : $E = \mathcal{X}A^n$.
Dire que $\mathcal{X} := (x_1, \ldots, x_n)$ est libre, c'est dire que, pour tout $M \in M_{n,1}(A)$, on a : $\mathcal{X}M = 0 \Rightarrow M = 0$. Cela reste d'ailleurs vrai pour des matrices $M \in M_{n,p}(A)$, puisque les composants de $\mathcal{X}M$ sont alors les $\mathcal{X}U$, où U est une colonne de M. Par exemple, $\mathcal{X}M = \mathcal{X}$ est équivalent à $M = I_n$.

Exercice 6.
Montrer que si $\mathcal{X} := (x_1, \ldots, x_n)$ et $\mathcal{Y} := (y_1, \ldots, y_p)$ sont libres et engendrent le même module, alors $n = p$.

Solution. D'après ce qui précède, il y a des matrices $M \in M_{n,p}(A)$ et $N \in M_{p,n}(A)$ telles que $\mathcal{Y} = \mathcal{X}M$ et $\mathcal{X} = \mathcal{Y}N$. On a alors $MN = I_n$ et $NM = I_p$. Mais on a vu page 12 que ce n'est possible que si $n = p$.

1.2.1 Produits, sommes directes

Soit $(E_i)_{i\in I}$ une famille de A-modules. On sait munir le produit cartésien $\prod_{i\in I} E_i$ d'une structure de groupe. En posant :

$$a.(x_i)_{i\in I} := (a.x_i)_{i\in I},$$

on en fait un A-module, appelé *module produit*. Chaque projection $p_j : (x_i)_{i\in I} \mapsto x_j$ est un morphisme surjectif de $\prod_{i\in I} E_i$ sur le facteur E_j. On définit de même une injection de E_j dans le module produit en envoyant x sur l'élément $(x_i)_{i\in I}$ dont la composante d'indice j vaut x et les autres sont nulles. Cette injection permet d'identifier E_j à un sous-module de $\prod_{i\in I} E_i$, ce que nous ferons donc. La somme des sous-modules $E_j \subset \prod_{i\in I} E_i$ est formée des éléments $(x_i)_{i\in I}$ dont presque toutes les composantes (c'est-à-dire toutes sauf un nombre fini) sont nulles. Ce sous-module est appelé *somme directe extérieure* des E_i et noté $\coprod_{i\in I} E_i$. Par exemple, si $\forall i \in I\ ,\ E_i = A$, alors $\prod_{i\in I} E_i = A^I$ et $\coprod_{i\in I} E_i = A^{(I)}$. Naturellement, si I est fini, $\coprod_{i\in I} E_i = \prod_{i\in I} E_i$.

Si les E_i sont des sous-modules d'un module E, on peut définir un morphisme $(x_i)_{i\in I} \mapsto \sum_{i\in I} x_i$ de $\coprod_{i\in I} E_i$ dans E. L'image de ce morphisme est la somme $\sum_{i\in I} E_i \subset E$. Pour que les sous-modules E_i soient en somme directe, il faut, et il suffit, que le morphisme ci-dessus soit injectif. Dans ce cas, on a un isomorphisme : $\coprod_{i\in I} E_i \simeq \bigoplus_{i\in I} E_i$. Pour cette raison, il est fréquent de ne pas distinguer les deux notions et de noter indifféremment $\bigoplus_{i\in I} E_i$ la somme directe extérieure des modules E_i (laquelle est *toujours* définie) et la somme directe des sous-modules $E_i \subset E$ (c'est-à-dire leur somme, sous réserve que ces sous-modules soient bien en somme directe). Plus généralement, si l'on a des morphismes $f_i : E_i \to F$, on peut définir un morphisme $\sum f_i : \coprod E_i \to F$ par $x \mapsto \sum f_i(x)$. En général, ce morphisme de s'étend pas à $\prod E_i$.

Attention. En première approximation, il revient au même d'écrire $E \simeq E_1 \times E_2$ ou $E = E_1 \oplus E_2$. La seconde relation implique évidemment la première, mais elle est plus précise : elle signifie que l'on a fait un choix particulier de deux sous-modules supplémentaires l'un de l'autre $E_1, E_2 \subset E$. Nous verrons par exemple à la section 3.2 qu'un même groupe admet les deux décompositions : $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (facteurs invariants) et $G = G_2 \oplus G_3$, avec $G_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $G_3 \simeq \mathbb{Z}/3\mathbb{Z}$ (décomposition primaire), mais la deuxième relation concerne des sous-groupes bien identifiés de G, alors que la première ne donne que des informations sur la structure (*i.e.* à isomorphisme près).

1.2.2 Quotients

Proposition et définition 3. Soit $E' \subset E$ un sous-module. Il existe alors sur le groupe quotient E/E' une unique structure de A-module telle que la projection canonique $p : E \to E/E'$ soit A-linéaire. On dit alors que le module E/E' est le *(module) quotient* de E par E'.

Démonstration. La démonstration est en tous points similaire à celle donnée pour les espaces vectoriels. On pose bien entendu :

$$a.\overline{x} := \overline{a.x}.$$

■

Sur un corps, on retrouve la notion d'espace vectoriel quotient, sur $\mathbb{Z}$ celle de groupe (abélien) quotient. Si $\mathfrak{A}$ est un idéal, le module quotient $A/\mathfrak{A}$ est le même que celui obtenu en considérant $A/\mathfrak{A}$ comme une A-algèbre (page 5) ou comme un A-module annulé par $\mathfrak{A}$ (page 9). Si $E = E_1 \oplus E_2$, la restriction à E_2 de la projection $E \to E/E_1$ est un isomorphisme. Si un sous-modules de E admet des supplémentaires, ceux-ci sont donc tous isomorphes entre eux.

La propriété caractéristique du quotient est la suivante : pour qu'un morphisme $f : E \to F$ se factorise en $\overline{f} \circ p : E \to E/E' \to F$, il faut, et il suffit, que $f(E') = \{0\} \subset F$. On dit que f *passe au quotient* en $\overline{f} : E/E' \to F$. Plus généralement, si $F' \subset F$ est un sous-module tel que $f(E') \subset F'$, alors f passe au quotient en $\overline{f} : E/E' \to F/F'$.

Théorème 4 (Premier théorème d'isomorphisme pour les modules). Soit $f : E \to F$ un morphisme. L'isomorphisme de groupes $E/\operatorname{Ker} f \simeq \operatorname{Im} f$ est alors un isomorphisme de A-modules.

Démonstration. La démonstration est en tous points similaire à celle donnée pour les espaces vectoriels. ■

Corollaire 5 (Deuxième théorème d'isomorphisme pour les modules). Soient $E'' \subset E' \subset E$ des sous-modules. Alors E'/E'' s'identifie à un sous-module de E/E'' et le quotient est :

$$\frac{E/E''}{E'/E''} \simeq \frac{E}{E'}.$$

Notons que l'on a ainsi une correspondance bijective entre les sous-modules E' de E contenant E'' et les sous-modules E'/E'' de E/E''.

Corollaire 6 (Troisième théorème d'isomorphisme pour les modules). Soient $E_1, E_2 \subset E$ deux sous-modules de E. On a un isomorphisme naturel :

$$E_1/(E_1 \cap E_2) \simeq (E_1 + E_2)/E_2.$$

Démonstration. À titre d'illustration de la méthode, qui est tout à fait générale, prouvons ce théorème. Le morphisme composé $E_1 \to E_1 + E_2 \to (E_1 + E_2)/E_2$ est surjectif, parce que (avec des notations évidentes) $(e_1 + e_2) \pmod{E_2}$ est l'image de $e_1 \in E_1$. Son noyau est $E_1 \cap E_2$. le théorème 4 de la page précédente s'applique donc. ■

Exemples.

1. Si (x_i) est une famille génératrice de E, le morphisme surjectif $\varphi_{\underline{x}}$ de la page 12 admet pour noyau le module des relations R, d'où un isomorphisme $A^{(I)}/R \simeq E$. Par cet isomorphisme, les applications linéaires $E \to F$ s'identifient aux applications linéaires de $A^{(I)}$ dans F qui passent au quotient par R, c'est-à-dire qui s'annulent sur R.
2. Un module de type fini est isomorphe à un module de la forme A^n/R.
3. Un module *monogène*, c'est-à-dire engendré par un seul élément x, est l'image de A par l'application linéaire $a \mapsto ax$, dont le noyau est $\mathrm{Ann}_A(x)$. On a donc un isomorphisme $E \simeq A/\mathrm{Ann}_A(x)$. Les modules monogènes sont donc exactement les modules qui sont, à isomorphisme près, de la forme $A/\mathfrak{A}$. Un tel module est de torsion si, et seulement si, $\mathfrak{A} \neq \{0\}$. Un module de torsion monogène est dit *cyclique*.

Exercice 7.
On dit qu'un module est *simple* s'il est non trivial et n'admet pour sous-modules que lui-même et $\{0\}$. À quoi ressemble un tel module ?

Solution. Il est nécessairement monogène, donc de la forme $A/\mathfrak{A}$ Ses sous-modules sont en bijection avec les idéaux de A contenant $\mathfrak{A}$: ce dernier idéal doit donc être maximal.

1.2.3 Modules sur $K[X]$

Nous allons illustrer le vocabulaire des modules sur un exemple important, celui de l'anneau $A := K[X]$ des polynômes sur un corps K. L'étude sera considérablement enrichie

à la section 3.3 en tenant compte de la principalité de A.

Soit E un $K[X]$-module. C'est, en particulier, un K-espace vectoriel, que l'on notera V pour distinguer les deux structures. (Dans la terminologie du paragraphe 1.3.2, on dira que V a été obtenu par *restriction de l'anneau des scalaires de A à K*, et l'on notera $V = E_{[K]}$.) Les éléments de V et de E sont donc les mêmes. L'application $x \mapsto X.x$ est K-linéaire, c'est donc un endomorphisme $\varphi \in \mathcal{L}_K(V)$. De plus, pour tout polynôme $P \in K[X]$, et tout $x \in V$ (ou $x \in E$, cela revient au même), on a $P(\varphi)(x) = P(X).x = P.x$: au membre droit, c'est la loi externe du $K[X]$-module qui intervient ; elle est donc entièrement déterminée par φ.

Réciproquement, soient V un K-espace vectoriel et $\varphi \in \mathcal{L}_K(V)$ un endomorphisme de V. On peut *poser* :

$$\forall P \in K[X]\ ,\ \forall x \in V\ ,\ P.x := P(\varphi)(x). \tag{8}$$

Le lecteur consciencieux vérifiera soigneusement que l'on définit ainsi un $K[X]$-module, que nous noterons V_φ. Nous allons détailler le « dictionnaire » entre la théorie des espaces vectoriels munis d'un endomorphisme φ et la théorie des $K[X]$-modules.

Un sous-module de V_φ est un sous–espace vectoriel qui est stable par multiplication par X (il est clair que cela entraine la stabilité par multiplication par tout $P \in K[X]$). C'est donc un sous–espace vectoriel stable par φ.

Si $\varphi \in \mathcal{L}_K(V)$ et $\psi \in \mathcal{L}_K(W)$, un morphisme de $K[X]$-modules de V_φ dans W_ψ est une application linéaire $f : V \to W$ telle que de plus $f(X.x) = X.f(x)$ (il est clair que cela entraine que $f(P.x) = P.f(x)$ pour tout $P \in K[X]$). Or, par définition, $f(X.x) = f\big(\varphi(x)\big)$ et $X.f(x) = \psi\big(f(x)\big)$. Un $K[X]$-morphisme est donc une application linéaire qui *entrelace* φ et ψ :

$$f \circ \varphi = \psi \circ f. \tag{9}$$

En particulier, un endomorphisme du $K[X]$-module V_φ est un endomorphisme du K-espace vectoriel V qui commute avec φ. On en tire la conséquence suivante :

Proposition et définition 7. Soient $\varphi \in \mathcal{L}_K(V)$ et $\psi \in \mathcal{L}_K(W)$. Pour que les $K[X]$-modules V_φ et W_ψ soient isomorphes, il faut, et il suffit, qu'il existe un isomorphisme $f : V \to W$ tel que $\psi = f \circ \varphi \circ f^{-1}$. On dit alors que φ et ψ sont *semblables*.

Lorsque $V = W$, on retrouve, bien entendu, la définition usuelle.

Exercice 8.
Traduire cette notion matriciellement.

Solution. Soient $\mathcal{B}$ (resp. $\mathcal{C}$) une base du K-espace vectoriel V (resp. W) et M (resp. N) la matrice de φ (resp. ψ) dans cette base. Soit P la matrice de f relativement aux bases $\mathcal{B}$ et $\mathcal{C}$. La condition $\psi = f \circ \varphi \circ f^{-1}$ équivaut alors à l'égalité : $N = PMP^{-1}$ (formules de changement de base). Ainsi, φ et ψ sont semblables si, et seulement si, leurs matrices dans des bases arbitraires le sont.

Théorème 8. Soit $\varphi \in \mathcal{L}_K(V)$. Le K-espace vectoriel V est de dimension finie si, et seulement si, le $K[X]$-module V_φ est de torsion de type fini.

Démonstration. Supposons que V est de dimension finie. Alors toute base de V est *a fortiori* un système générateur de V_φ, qui est donc de type fini. (Argument : tout élément est combinaison linéaire des éléments de la base avec des coefficients dans K donc dans $K[X]$). Par ailleurs, il existe un polynôme annulateur P de φ. (Rappelons la raison : l'application linéaire $P \mapsto P(\varphi)$ de $K[X]$ dans $\mathcal{L}_K(V)$ ne peut être injective à cause des dimensions.) On a donc : $\forall x \in V\ ,\ P.x = P(\varphi)(x) = 0$, *i.e.* $P \in \mathrm{Ann}_{K[X]}(V_\varphi)$.
Supposons réciproquement que V_φ est de torsion de type fini. Soient $x_1, \ldots, x_n$ des générateurs et $P_1, \ldots, P_n$ non nuls tels que $P_1.x_1 = \cdots = P_n.x_n = 0$. Alors le morphisme surjectif $K[X]^n \to V_\varphi$ passe au quotient en un morphisme surjectif :

$$K[X]/<P_1> \times \cdots \times K[X]/<P_n> \to V_\varphi.$$

Ce morphisme de $K[X]$-modules est en même temps une application linéaire surjective de K-espaces vectoriels, dont la source est un espace vectoriel de dimension finie $\sum \deg P_i$ et dont le but est le K-espace vectoriel V, qui est donc de dimension finie. ■

Comme application, voici une preuve élémentaire du théorème de Cayley-Hamilton. Soit $\varphi \in \mathcal{L}_K(V)$, où V est de dimension finie. Soit $M = (a_{i,j}) \in M_n(K)$ la matrice de φ dans la base $\mathcal{B} := (e_1, \ldots, e_n)$ du K-espace vectoriel V. On note $M' := M - XI_n = (a'_{i,j}) \in M_n(K[X])$. Des égalités :

$$X.e_j = \varphi(e_j) = \sum_{i=1}^{n} a_{i,j} e_i,$$

on tire les égalités $\sum_{i=1}^{n} a'_{i,j} e_i = 0$ dans V_φ, ce que l'on peut écrire : $\mathcal{B}M' = (0, \ldots, 0) \in V_\varphi^n$.
D'après la proposition 1 de la page 8, on en déduit que $(\det M')V_\varphi = 0$. Notant $\chi_M := \det M' \in K[X]$ le polynôme caractéristique de M et φ, cela signifie que $\chi_M(\varphi)$ est l'endomorphisme nul de V. Les formules de Cramer constituent l'unique ingrédient non trivial de cette preuve.

Modules cycliques. Sur un anneau quelconque A, les modules cycliques sont (à isomorphisme près) les modules de la forme $A/\mathfrak{A}$, où $\mathfrak{A}$ est un idéal propre non nul. Sur

$A := K[X]$, ce sont donc les modules de la forme $K[X]/<P>$, où $P := X^n + a_1 X^{n-1} + \cdots a_n \in K[X]$ avec $n \geqslant 1$.

Notons $x := X \pmod P$ et munissons le K-espace vectoriel $V := K[X]/<P>$ de la base des $e_i := x^i$ $(0 \leqslant i \leqslant n-1)$. On a donc $X.e_i = x^{i+1} = e_{i+1}$ pour $0 \leqslant i \leqslant n-2$ et $X.e_{n-1} = x^n = -a_1 x^{n-1} - \cdots - a_n = -a_n e_0 - \cdots - a_1 e_{n-1}$. L'endomorphisme φ qui définit le module $V_\varphi := K[X]/<P>$ est donc cyclique (les $\varphi^i(e_0)$ pour $i \in [\![0, n-1]\!]$ forment une base) et la matrice de φ dans la base $(e_0, \ldots, e_{n-1})$ est la matrice compagnon :

$$C_P := \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 0 & \ldots & 1 & -a_0 \end{pmatrix}$$

L'annulateur de V_φ est l'idéal $<P>$, et P est donc le polynôme minimal de C_P (exercice I.6.19 de la page 61). Comme deux modules isomorphes ont même annulateur, on voit que C_P et C_Q sont semblables si, et seulement si, $P = Q$.

1.3 Rudiments de fonctorialité

1.3.1 Suites exactes

Le langage des suites exactes est extrêmement commode pour parler de sous-modules et de modules quotients.

Définition 4. On dit que le diagramme de morphismes de A-modules :

$$E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} E_{n-1} \xrightarrow{f_n} E_n \tag{10}$$

est une *suite exacte* si elle est « exacte en chaque E_i » $(1 \leqslant i \leqslant n-1)$, *i.e.* $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$. Autrement dit, $f_{i+1} \circ f_i = 0$ et $f_{i+1}(x) = 0 \Rightarrow x \in \operatorname{Im} f_i$.

Dans ce qui suit, nous noterons abusivement 0 le module trivial $\{0\}$. La suite $0 \to E' \xrightarrow{f} E$ est exacte si, et seulement si, $\operatorname{Ker} f = 0$, c'est-à-dire si, et seulement si, f est injective. De même, la suite $E \xrightarrow{g} E'' \to 0$ est exacte si, et seulement si, $\operatorname{Im} g = E''$, c'est-à-dire si, et seulement si, g est surjective.

Soit $E_1 \subset E$, et notons $E_2 := E/E_1$. On a alors une suite exacte :

$$0 \to E_1 \hookrightarrow E \longrightarrow E_2 \to 0. \tag{11}$$

On appelle *suite exacte courte* une suite exacte de la forme :

$$0 \to E' \xrightarrow{f} E \xrightarrow{g} E'' \to 0. \tag{12}$$

On n'a pas besoin de préciser les morphismes extrêmes, car ils sont nécessairement triviaux. L'exactitude en E' dit que f est injectif. On peut donc identifier E' à son image $\operatorname{Im} f \subset E$. L'exactitude en E'' dit que g est surjectif. On peut donc identifier E'' à $E/\operatorname{Ker} g$. Comme $\operatorname{Ker} g = \operatorname{Im} f$, on obtient finalement un isomorphisme de E/E' sur E''. La suite exacte (12) s'identifie donc à la suite exacte (11).

On peut exprimer plus rigoureusement ces identifications comme suit. Notons $E_1 := \operatorname{Im} f = \operatorname{Ker} g$ et $E_2 := E/E_1$. Notons u l'isomorphisme de E' sur E_1 (corestriction de f) et v l'isomorphisme de E'' sur E_2 (inverse de l'isomorphisme de $E/\operatorname{Ker} g$ sur $\operatorname{Im} g$ déduit du théorème 4 de la page 15). On a alors un *isomorphisme de suites exactes*, c'est-à-dire un diagramme commutatif dans lequel les flèches verticales sont des isomorphismes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E' & \xrightarrow{f} & E & \xrightarrow{g} & E'' & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \mathrm{Id}_E} & & \downarrow{\scriptstyle v} & & \downarrow \\
0 & \longrightarrow & E_1 & \xrightarrow{i} & E & \xrightarrow{p} & E_2 & \longrightarrow & 0
\end{array}$$

En un certain sens, toute suite exacte (10) est fabriquée à partir de suites exactes courtes. posons en effet $F_i := \operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$ (pour $1 \leqslant i \leqslant n-1$). On a alors des suites exactes courtes :

$$0 \to F_i \hookrightarrow E_i \xrightarrow{f_{i+1}} F_{i+1} \to 0$$

C'est encore vrai pour $i := 0$ si l'on pose $F_0 := \operatorname{Ker} f_1$. Réciproquement, si l'on a des suites exactes $0 \to F_i \to E_i \to F_{i+1} \to 0$, les morphismes composés $E_i \to F_{i+1} \to E_{i+1}$ s'assemblent en une suite exacte (10).

Exemple. Si $(x_i)_{i\in I}$ est une famille génératrice de E, de module des relations R (défini page 12), on a une suite exacte courte : $0 \to R \hookrightarrow A^{(I)} \to E \to 0$. Soit $(r_j)_{j\in J}$ une famille génératrice de R. Le morphisme surjectif $A^{(J)} \to R$ se traduit par une suite exacte : $A^{(J)} \to R \to 0$. En composant $A^{(J)} \to R \to A^{(I)}$, on obtient finalement une suite exacte :

$$A^{(J)} \longrightarrow A^{(I)} \longrightarrow E \to 0. \tag{13}$$

Cette suite s'appelle une *présentation de* E. On dit aussi que l'on a décrit E par *générateurs et relations*.

Suites exactes scindées. Reprenant l'exemple 6 de la page 11, on voit que le sous-module $E' \subset E$ est facteur direct de E si, et seulement si, il est l'image d'un *projecteur* (*i.e.* d'un endomorphisme idempotent) : un endomorphisme p de E d'image E' et tel que $p_{E'} = \mathrm{Id}_{E'}$. Plus généralement, un morphisme injectif $f : E' \to E$ identifie E' à un facteur direct E_1 de E si, et seulement si, il admet une *rétraction*, c'est-à-dire un morphisme $r : E \to E'$ tel que $r \circ f = \mathrm{Id}_{E'}$. Dualement, un morphisme surjectif $g : E \to E''$ se restreint en un isomorphisme d'un facteur direct E_2 de E sur E'' si, et seulement si, il admet une *section*, c'est-à-dire un morphisme $s : E'' \to E$ tel que $g \circ s = \mathrm{Id}_{E''}$.
Nous dirons qu'une suite exacte courte (12) est *scindée* si l'une des propriétés équivalentes suivantes est vérifiée : (i) $\mathrm{Im}\, f$ est facteur direct de E ; (ii) le morphisme f admet une rétraction ; (iii) Le morphisme g admet une section. Il revient au même de dire que la suite (12) est isomorphe à une suite exacte de la forme :

$$0 \to E_1 \longrightarrow E_1 \oplus E_2 \longrightarrow E_2 \to 0. \tag{14}$$

Exercice 9.
Étudier le cas de : $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \to 0$, où $n \in \mathbb{N}^*$.

Solution. Comme le morphisme $x \mapsto nx$ est injectif d'image $n\mathbb{Z}$, qui est le noyau du morphisme surjectif $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, il s'agit d'une suite exacte courte. Elle n'est pas scindée car $\mathbb{Z}$ ne contient aucun sous-groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

1.3.2 Changement de l'anneau des scalaires

Une opération importante de l'algèbre commutative est le *changement d'anneau de base*.

Restriction de l'anneau des scalaires. Si $A \subset B$ est un sous-anneau, alors tout A-module peut être vu comme un A-module par simple restriction de la loi externe. Plus généralement, soit $f : A \to B$ un morphisme d'anneaux commutatifs. Pour tout B-module E, on peut définir une loi externe $A \times E \to E$ en posant $a.x := f(a).x$ (cette dernière expression étant déjà définie). On fait ainsi de E un A module. Pour distinguer les deux structures sur E, on note parfois $E_{[A]}$ le A-module obtenu par *restriction de l'anneau des scalaires*. Ainsi, B lui-même peut être vu comme A-module (page 5). Le cas où $B := A/\mathfrak{A}$ a été décrit page 9. L'exemple de $K \to K[X]$ a été vu au paragraphe 1.2.3.

L'opération la plus importante est l'*extension de l'anneau des scalaires*. Pour tout morphisme d'anneaux commutatifs $f : A \to B$, elle permet d'associer à tout A-module E un B-module, noté $B \otimes_A E$ ou $E_{(B)}$. Nous ne décrirons cette opération que dans des cas simples.

Attention. L'extension et la restriction des scalaires ne sont pas réciproques l'une de l'autre (exercice I.6.23 de la page 61).

Extension des scalaires de A à $A/\mathfrak{A}$. Soit $\mathfrak{A}$ un idéal de A et notons $B := A/\mathfrak{A}$. Pour tout A-module E, le A-module $E/\mathfrak{A}E$ est annulé par $\mathfrak{A}$, donc on peut le considérer comme un B-module (page 9) : ce B-module est normalement noté $E_{(B)}$. Notons le temporairement $\overline{E}$.
Pour toute application linéaire $f : E \to F$, il est clair que $f(\mathfrak{A}E) \subset \mathfrak{A}F$. On a donc, par passage au quotient, un morphisme de B-modules : $\overline{f} : \overline{E} \to \overline{F}$. Les propriétés suivantes se vérifient aisément : $\overline{\mathrm{Id}_E} = \mathrm{Id}_{\overline{E}}$; et $\overline{g \circ f} = \overline{g} \circ \overline{f}$. On dit que l'*extension des scalaires de A à $A/\mathfrak{A}$ est un foncteur covariant*. Cela implique logiquement que, si $E \simeq F$, alors $\overline{E} \simeq \overline{F}$.

Exercice 10.
Démontrer que, si $A^n \simeq A^p$, alors $n = p$.

Solution. On étend les scalaires de A à $K := A/\mathfrak{M}$, où $\mathfrak{M}$ est un idéal maximal de A. On en déduit que $K^n \simeq K^p$, et l'on applique la théorie de la dimension des espaces vectoriels. (Voir également les exercices I.6.24 de la page 61 et I.6.25 de la page 62.)

Extension des scalaires de A à $S^{-1}A$. Soit S une partie multiplicative de A et soit $B := S^{-1}A$. Pour tout A-module E, on peut définir une relation d'équivalence sur $E \times S$ en posant :

$$(x, s) \sim (x', s') \Longleftrightarrow \exists t \in S \ : \ t(sx' - s'x) = 0.$$

L'ensemble quotient est noté $S^{-1}E$ et la classe de (x, s) dans $S^{-1}E$ est notée x/s. Exactement comme dans lors de la construction de l'anneau des fractions $S^{-1}A$, on munit $S^{-1}E$ d'une structure de groupe en posant : $(x/s) + (y/t) := (tx + sy)/(st)$. On en fait de plus un $S^{-1}A$-module en posant : $(a/s).(x/t) := (ax)/(st)$. C'est le module $E_{(B)}$ dans le cas où $B := S^{-1}A$. Notons le temporairement $\tilde{E}$.
Pour toute application linéaire $f : E \to F$, l'application $x/s \mapsto f(x)/s$ est bien définie, et c'est un morphisme de $S^{-1}E$ dans $S^{-1}F$. Notons le temporairement $\tilde{f}$. On a les propriétés : $\widetilde{\mathrm{Id}_E} = \mathrm{Id}_{\tilde{E}}$; et $\widetilde{g \circ f} = \tilde{g} \circ \tilde{f}$. On dit que l'*extension des scalaires de A à $S^{-1}A$ est un foncteur covariant*. Cela implique logiquement que, si $E \simeq F$, alors $\tilde{E} \simeq \tilde{F}$.

Exercice 11.
À quelle condition a-t-on $S^{-1}E = 0$?

Solution. La condition nécessaire et suffisante est que l'annulateur de tout $x \in E$ rencontre S.

La construction précédente est particulièrement utile lorsque A est un anneau intègre et que $S := A\setminus\{0\}$. Dans ce cas, $K := S^{-1}A$ est le corps des fractions de A et le A-module E donne lieu à un K-espace vectoriel $E_{(K)}$.

Proposition et définition 9. Le cardinal d'une famille libre maximale de E est égal à la dimension du K-espace vectoriel $E_{(K)}$. On l'appelle *rang* du A-module E et on le note $\operatorname{rg} E$. Par convention, s'il existe des familles libres infinies, le rang est ∞.

Démonstration. On établit d'abord que la famille $(x_1, \dots, x_n)$ de E est libre si, et seulement si, la famille $(x_1/1, \dots, x_n/1)$ de $E_{(K)}$ l'est (facile et laissé au lecteur). On remarque ensuite que toute famille libre finie de $E_{(K)}$ est, à un facteur $1/s$ près, de cette forme. ■

Corollaire 10. Si $E' \subset E$, alors $\operatorname{rg} E' \leqslant \operatorname{rg} E$. L'égalité a lieu si, et seulement si, $\operatorname{rg}(E/E') = 0$, c'est-à-dire si E/E' est de torsion.

Démonstration. On vérifie sans peine que dans ce cas, $E'_{(K)} \to E_{(K)}$ est injective, d'où l'inégalité. La condition nécessaire et suffisante d'égalité repose sur les considérations qui suivent. ■

La propriété essentielle du foncteur d'extension des scalaires de A à $S^{-1}A$ est qu'il est *exact* (exercice I.6.26 de la page 62). Autrement dit, dans notre cas, si $0 \to E' \to E \to E'' \to 0$ est une suite exacte courte de A-modules, on obtient par extension des scalaires une suite exacte : $0 \to E'_{(K)} \to E_{(K)} \to E''_{(K)} \to 0$. On en déduit que $\operatorname{rg}(E) = \operatorname{rg}(E') + \operatorname{rg}(E'')$, ce qui renforce le corollaire précédent.

On peut voir $E_{(K)}$ comme un A-module (restriction des scalaires !) et l'application $x \mapsto x/1$ de E dans $E_{(K)}$ est A-linéaire. Son noyau est formé des x tels que $tx = 0$ pour un $t \neq 0$, d'où l'égalité :

$$\operatorname{Tor}_A(E) = \operatorname{Ker}(E \to E_{(K)}).$$

D'après l'exercice 11 de la page ci-contre, E est de torsion si, et seulement si, $E_{(K)} = 0$. Ainsi, la suite exacte courte $0 \to \operatorname{Tor}_A(E) \to E \to E/\operatorname{Tor}_A(E) \to 0$ devient-elle, après extension des scalaires, la suite exacte : $0 \to 0 \to E_{(K)} \to \big(E/\operatorname{Tor}_A(E)\big)_{(K)} \to 0$, autrement dit, l'isomorphisme $E_{(K)} \simeq \big(E/\operatorname{Tor}_A(E)\big)_{(K)}$.

1.3.3 Modules d'homomorphismes

Fixons le module source E. Pour tout morphisme $u : F_1 \to F_2$, l'application $f \mapsto u \circ f$ est un morphisme de $\mathrm{Hom}_A(E, F_1)$ dans $\mathrm{Hom}_A(E, F_2)$. Notons temporairement $\mathrm{Hom}_A(E, u)$ ce morphisme. On a les règles suivantes : si u est l'identité de F, alors $\mathrm{Hom}_A(E, u)$ est l'identité de $\mathrm{Hom}_A(E, F)$; si l'on se donne $u : F_1 \to F_2$ et $v : F_2 \to F_3$, alors $\mathrm{Hom}_A(E, v \circ u) = \mathrm{Hom}_A(E, v) \circ \mathrm{Hom}_A(E, u)$. Ces propriétés se résument en disant que $\mathrm{Hom}_A(E, -)$ est un *foncteur* qui transforme modules en modules et applications linéaires en applications linéaires. On en déduit facilement (par pure logique) que, si u est un isomorphisme, alors $\mathrm{Hom}_A(E, u)$ est un isomorphisme. On voit également que, si u est injectif, alors $\mathrm{Hom}_A(E, u)$ est injectif (*i.e.* $u \circ f \Rightarrow f = 0$). Mais il est faux que la surjectivité soit préservée (exercice I.6.9 de la page 60).

Fixons maintenant le module cible F. Pour tout morphisme $u : E_1 \to E_2$, l'application $f \mapsto f \circ u$ est un morphisme de $\mathrm{Hom}_A(E_2, F)$ dans $\mathrm{Hom}_A(E_1, F)$. Notons temporairement $\mathrm{Hom}_A(u, F)$ ce morphisme. On a les règles suivantes : si u est l'identité de E, alors $\mathrm{Hom}_A(u, F)$ est l'identité de $\mathrm{Hom}_A(E, F)$; si l'on se donne $u : E_1 \to E_2$ et $v : E_2 \to E_3$, alors $\mathrm{Hom}_A(v \circ u, F) = \mathrm{Hom}_A(u, F) \circ \mathrm{Hom}_A(v, F)$. Ces propriétés se résument en disant que $\mathrm{Hom}_A(-, F)$ est un *foncteur contravariant* qui transforme modules en modules et applications linéaires en applications linéaires. Si u est un isomorphisme, alors $\mathrm{Hom}_A(u, F)$ est un isomorphisme. On voit également que, si u est surjectif, alors $\mathrm{Hom}_A(E, u)$ est injectif (*i.e.* $f \circ u = 0 \Rightarrow f = 0$). Mais il est faux que l'injectivité soit transformée en surjectivité (exercice I.6.9 de la page 60).

Morphismes et relations linéaires. Soit $(x_i)_{i \in I}$ une famille génératrice de E. Dans ce cas, un morphisme $f : E \to F$ est uniquement déterminé par les $f(x_i) \in F$: si l'on connait les images $y_i := f(x_i)$, on peut calculer, pour tout $x := \sum_{i \in I} a_i x_i$ son image $f(x) := \sum_{i \in I} a_i y_i$. Noter cependant que, les y_i étant donnés, l'*existence* d'un morphisme f tel que $\forall i \in I\ ,\ f(x_i) = y_i$ n'est pas garantie ; seule l'unicité est garantie. Cela peut se traduire en disant que le morphisme suivant est injectif :

$$\begin{cases} \mathrm{Hom}_A(E, F) \to F^I, \\ f \mapsto \big(f(x_i)\big), \end{cases}$$

Quelle condition doit-on imposer aux y_i pour qu'il existe un tel morphisme f ? Soit R le module des relations entre les x_i (défini page 12). Il est clair que pour toute relation $\sum_{i \in I} a_i x_i = 0$ entre les x_i, c'est-à-dire pour tout $(a_i)_{i \in I} \in R$, il est *nécessaire* que l'on ait

$\sum_{i\in I} a_i y_i = 0$. Autrement dit, la famille $(y_i)_{i\in I} \in F^I$ doit appartenir au sous-module :

$$F' := \{(y_i)_{i\in I} \in F^I \mid \forall (a_i)_{i\in I} \in R\ ,\ \sum_{i\in I} a_i y_i = 0\}.$$

Pour tout $\underline{y} := (y_i)_{i\in I} \in F^I$, notons $\psi_{\underline{y}}$ le morphisme $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i y_i$ de R dans F. On reconnait dans F' le noyau du morphisme :

$$\begin{cases} F^I \to \mathrm{Hom}_A(R, F), \\ (y_i)_{i\in I} \mapsto \psi_{\underline{y}}. \end{cases}$$

Ainsi, l'image du morphisme injectif $\mathrm{Hom}_A(E, F) \to F^I$ est incluse dans le noyau F' du morphisme ci-dessus. Grâce au paragraphe 1.2.2, nous pouvons vérifier qu'il y a même égalité. En effet, dire que $(y_i)_{i\in I}$ est élément du noyau F', c'est dire que le morphisme $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i y_i$ de $A^{(I)}$ dans F s'annule sur le sous-module $R \subset A^{(I)}$, donc qu'il *passe au quotient* en un morphisme de $A^{(I)}/R$ dans F. Mais $A^{(I)}/R$ s'identifie précisément à E. Dans le langage du paragraphe 1.3.1, on peut interpréter cette construction comme suit. On a une suite exacte : $0 \to R \to A^{(I)} \to E \to 0$. On lui applique le foncteur contravariant $\mathrm{Hom}_A(-, F)$ et l'on obtient des morphismes : $\mathrm{Hom}_A(E, F) \to \mathrm{Hom}_A(A^{(I)}, F) \to \mathrm{Hom}(R, F)$. Modulo l'identification de $\mathrm{Hom}_A(A^{(I)}, F)$ avec F^I, nous venons de construire la suite exacte :

$$0 \to \mathrm{Hom}_A(E, F) \to F^I \to \mathrm{Hom}(R, F).$$

2 CONDITIONS DE FINITUDE

2.1 Modules de présentation finie

2.1.1 Modules libres de rang fini

Pour que le morphisme $\varphi_{\underline{x}}$ introduit page 12 soit bijectif, il faut, et il suffit, que la famille $(x_i)_{i\in I}$ soit libre et génératrice ; ou, de manière équivalente, que tout élément de E soit de manière unique combinaison linéaire des x_i :

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

Définition 5. Une famille libre et génératrice est appelée une *base*. On dit que le A-module E est *libre* (resp. *libre de rang fini*) s'il admet une base (resp. une base finie).

Exemples. Les modules libres (resp. libres de rang fini) sont donc les modules isomorphes à un module de la forme $A^{(I)}$ (resp. A^n). Par exemple, tout K-espace vectoriel (resp. de dimension finie) est un module libre (resp. de rang fini). Un idéal de A est un module libre si, et seulement s'il est principal et engendré par un élément sans torsion, *i.e.* non diviseur de 0. Le module $A/\mathfrak{A}$ est libre si, et seulement si, $\mathfrak{A} = A$ ou $\mathfrak{A} = 0$.

À toute base $\mathcal{B} := (x_i)_{i\in I}$ du A-module libre E, on associe des *formes linéaires coordonnées* π_i, caractérisées par l'égalité :

$$\forall x \in E\ ,\ x = \sum_{i\in I} \pi_i(x)x_i.$$

On peut également définir les projecteurs $p_i : x \mapsto \pi_i(x)x_i$, qui correspondent à la décomposition en somme directes : $E = \bigoplus_{i\in I} Ax_i$. Réciproquement, si l'on a une telle décomposition *et si les x_i sont sans torsion*, alors $(x_i)_{i\in I}$ est une base de E.

Théorème et définition 11. (i) Un module libre E est de rang fini si, et seulement s'il admet un système générateur fini.
(ii) Toutes les bases d'un module libre de rang fini E ont même nombre d'éléments. Ce nombre est appelé *rang de E* et noté $\operatorname{rg} E$.

Démonstration. (i) On peut supposer que $E := A^{(I)}$. Si E admet un système générateur fini, on a un morphisme surjectif : $A^n \to A^{(I)}$. Soient $\mathfrak{M}$ un idéal maximal de A et $K := A/\mathfrak{M}$ le corps résiduel. Par extension des scalaires $A \to K$, on a une application linéaire surjective $K^n \to K^{(I)}$ entre K-espaces vectoriels. On en déduit que $\operatorname{card} I \leqslant n$.
(ii) L'inégalité ci-dessus, appliquée dans les deux sens, implique que toutes les bases ont même nombre d'éléments. ■

Corollaire 12. Tout système générateur d'un module libre de rang n a au moins n éléments.

Proposition 13. Toute famille libre d'un module libre de rang n a au plus n éléments.

Démonstration. Lorsque A est intègre de corps des fractions K, l'isomorphisme $E \simeq A^n$ (avec $n := \operatorname{rg} E$) entraine $E_{(K)} \simeq K^n$ et l'on reconnait la définition du rang donnée précédemment (proposition 9 de la page 23). Pour un anneau commutatif quelconque, la démonstration est plus compliquée et reportée à l'exercice I.6.30 de la page 62. ■

Soit $\mathcal{B} := (e_1, \ldots, e_n)$ une base du A-module E (qui est donc libre de rang n). Tout élément de E s'écrit de manière unique $\mathcal{B}U$, où $U \in M_{n,1}(A)$ est le vecteur-colonne de ses coordonnées. Plus généralement, toute famille $\mathcal{X} := (x_1, \ldots, x_p) \in E^p$ s'écrit de manière unique $\mathcal{X} = \mathcal{B}M$, où $M \in M_{n,p}(A)$.

Pour que la famille $\mathcal{X}$ soit génératrice, il faut, et il suffit, que les e_i soient combinaisons linéaires des x_j, autrement dit, que l'on puisse écrire $\mathcal{B} = \mathcal{X}N$, avec $N \in M_{p,n}(A)$. Mais :

$$\mathcal{B} = \mathcal{X}N \Longleftrightarrow \mathcal{B} = \mathcal{B}MN \Longleftrightarrow MN = I_n,$$

et l'on voit que $\mathcal{X} := \mathcal{B}M$ est génératrice si, et seulement si, la matrice M est inversible à droite. Les relations $\mathcal{X} = \mathcal{B}M$ et $\mathcal{B} = \mathcal{X}N$ entrainent également $\mathcal{X} = \mathcal{X}NM$. Si la famille $\mathcal{X}$ est une base, elle est libre, et l'on a $NM = I_p$. Les égalités $MN = I_n$ et $NM = I_p$ impliquent $p = q$ et $M, N \in GL_n(A)$, $N = M^{-1}$. Réciproquement, si $\mathcal{X} = \mathcal{B}M$, où $M \in GL_n(A)$, alors $\mathcal{X}$ est génératrice (vu plus haut) ; et l'on voit qu'elle est libre, car, si $U \in M_{n,1}(A)$:

$$\mathcal{X}U = 0 \Rightarrow \mathcal{B}MU = 0 \Rightarrow MU = 0 \Rightarrow U = 0.$$

Ainsi, pour une base $\mathcal{B}$ donnée, l'application $M \mapsto \mathcal{B}M$ est une bijection de $GL_n(A)$ sur l'ensemble des bases de E. Comme dans le cas des espaces vectoriels, on en déduit :

Proposition 14. Si L est libre de rang fini, l'action de $\mathcal{GL}(L)$ sur les bases de L est simplement transitive.

On a vu que $\mathrm{Hom}_A(A^n, A^p)$ était isomorphe à $M_{p,n}(A)$. Plus généralement, soient E un module libre de base $\mathcal{B} := (e_1, \ldots, e_n)$ et F un module libre de base $\mathcal{C} := (f_1, \ldots, f_p)$. À tout morphisme $\varphi : E \to F$, on associe la *matrice du morphisme φ relativement aux bases $\mathcal{B}$ et $\mathcal{C}$* ; c'est la matrice $M := (a_{i,j}) \in M_{p,n}(A)$ définie par les relations :

$$\forall j \in [\![1, p]\!] \ , \ \varphi(e_j) = \sum_{i=1}^{p} a_{i,j} f_i.$$

Autrement dit, c'est la matrice M telle que $\varphi(\mathcal{B}) = \mathcal{C}M$. Bien entendu, lorsque $\varphi \in \mathrm{End}_A(E)$, il est d'usage de prendre $\mathcal{C} := \mathcal{B}$ et de parler de la la *matrice de l'endomorphisme φ relativement à la base $\mathcal{B}$*. Toutes les formules données dans le cours de L1 concernant les changements de base s'adaptent ici telles quelles, avec des démonstrations identiques (on a vu que les matrices de changement de base sont inversibles), ce qui justifie les définitions suivantes :

Définition 6. Deux matrices $M, M' \in M_{p,n}(A)$ sont dites *équivalentes* s'il existe $P \in GL_p(A)$ et $Q \in GL_n(A)$ telles que $M' = PMQ^{-1}$. Deux matrices $M, M' \in M_n(A)$ sont dites *semblables* s'il existe $P \in GL_n(A)$ telle que $M' = PMP^{-1}$.

Ces relations d'équivalence correspondent respectivement à une action du groupe $GL_p(A) \times GL_n(A)$ sur $M_{p,n}(A)$, et à une action du groupe $GL_n(A)$ sur $M_n(A)$. La relation de similitude est peu étudiée dans le cas des matrices sur un anneau.

2.1.2 Modules de présentation finie

Soit E un module de type fini. Pour tout système générateur $(x_1, \ldots, x_n)$ de E, le module des relations entre les x_i est le noyau R du morphisme $\varphi_{\underline{x}} : A^n \to E$ (page 12). Si le module R est lui-même de type fini, il y a une morphisme surjectif $A^p \to R$, et, comme à la page 20, on a une suite exacte :

$$A^p \xrightarrow{M} A^n \longrightarrow E \to 0 \quad \text{avec} \quad M \in M_{n,p}(A). \tag{15}$$

Définition 7. On dit que le module E est *de présentation finie* s'il admet un système générateur fini dont le module des relations est de type fini.

On prouve à l'exercice I.6.33 de la page 63 que, dans ce cas, le module des relations de *tout* système générateur fini est de type fini. Tout espace vectoriel de dimension finie est un module de présentation finie. Le module de type fini (car monogène) $A/\mathfrak{A}$ est de présentation finie si, et seulement si, l'idéal $\mathfrak{A}$ est de type fini. Nous verrons à la section 2.2 que, sur un anneau noetherien (c'est-à-dire tel que tout idéal est de type fini), tout module de type fini est de présentation finie. C'est donc en particulier vrai sur un anneau principal.

Il revient au même de dire que E est de présentation finie, que l'on peut l'insérer dans une suite exacte du type (15). En termes plus intrinsèques, E s'insère dans une suite exacte du type suivant :

$$L_2 \xrightarrow{\varphi} L_1 \longrightarrow E \to 0 \quad \text{avec} \quad \varphi \in \mathrm{Hom}_A(L_2, L_1), \tag{16}$$

où L_1 et L_2 sont libres de rang fini (ici, n et p). Réciproquement,d' une présentation (16), on déduit une présentation (15) par choix de bases de L_1 et L_2 ; la matrice M est donc déterminée à partir de φ *à équivalence près*. De ces présentations, on déduit les isomorphismes :

$$E \simeq A^n/MA^p \simeq L_1/\varphi(L_2).$$

Le sous-module $MA^p \subset A^n$ image de $M : A^p \to A^n$. est le sous-module engendré par les colonnes de M.

Exemple. Soit $M \in M_{n,p}(A)$. Supposons que M est équivalente à une matrice :

$$D := \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_k & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{pmatrix} = \sum_{i=1}^{k} d_i E_{i,i} \tag{17}$$

pour un certain $k \in [\![0, \min(n,p)]\!]$ et des éléments $d_1, \dots, d_k$ de $A \setminus \{0\}$. Le module E de présentation $A^p \xrightarrow{M} A^n \to E \to 0$ est donc isomorphe au module A^n/DA^p. Si l'on note $(e_1, \dots, e_n)$ la base canonique de A^n, les colonnes de D sont $d_1e_1, \dots, d_ke_k$ et $(p-k)$ colonnes nulles, et l'on a :

$$E \simeq \frac{Ae_1 \oplus \dots \oplus Ae_n}{Ad_1e_1 \oplus \dots \oplus Ad_ke_k} \simeq \frac{A}{Ad_1} \times \dots \times \frac{A}{Ad_k} \times A^{n-k}.$$

Exercice 12.
Dans cet exemple, quel est le rang de E ? On suppose de plus que $d_1|d_2|\cdots|d_k$ (d'après le module « Compléments d'algèbre » du L2, cette situation se réalise à coup sûr si A est euclidien). Quel est l'annulateur de E ? Qu'est ce qui est indépendant du choix de la présentation ?

Solution. Le rang de E est $n-k$ et l'annulateur de E est Ad_k. L'entier $n-k$ ne dépend donc que de la classe d'isomorphie de E, et il en est de même de d_k, à facteur inversible près. On verra à la section 3 que tous les d_i sont déterminés par E à facteur inversible près.

Attention. Dans cet exemple (qui sera très important pour la section 3), le rang de la matrice de présentation M est k, alors que le rang du module E est $n-k$.

Exemple. Soient $A := K[X,Y]$, et $E := <X^2, XY, Y^2>$ (idéal de A). Le morphisme surjectif $A^3 \to E$ correspondant à ce système de générateurs est $(P,Q,R) \mapsto X^2P + XYQ + Y^2R$. Son noyau est le sous-module de A^3 engendré par $(Y,-X,0)$ et $(0,Y,-X)$ (exercice 13 de la page suivante). On a donc une présentation : $A^2 \xrightarrow{M} A^3 \to E \to 0$ avec $M := \begin{pmatrix} Y & 0 \\ -X & Y \\ 0 & -X \end{pmatrix}$.
Dans cet exemple, $n = 3$ (nombre de générateurs), $p = 2$ (nombre de relations génératrices de R), le rang de la matrice de présentation M est 2, celui du module E est 1 (idéal non trivial de A).

Exercice 13.
Prouver que le noyau de $A^3 \to E$ est bien engendré par $(Y,-X,0)$ et $(0,Y,-X)$.

Solution. Il est évident que ces deux éléments sont bien dans le noyau. Si $X^2P+XYQ+Y^2R=0$, alors Y divise X^2P, donc P, et $P=YF$, d'où : $(P,Q,R)=F(Y,-X,0)+(0,Q_1,R_1)$, où $(0,Q_1,R_1)$ est dans le noyau. On a donc : $XYQ_1+Y^2R_1=0$, d'où $XQ_1+YR_1=0$, et Y divise XQ_1, donc Q_1, donc $Q_1=GY$ et $R_1=-GX$, d'où $(0,Q_1,R_1)=G(0,Y,-X)$, et finalement : $(P,Q,R)=F(Y,-X,0)+G(0,Y,-X)$.

2.1.3 Idéaux de Fitting d'un module de présentation finie

Soit $M \in M_{n,p}(A)$. Pour tout $k \in \mathbb{N}$, notons $\mathfrak{D}_k(M)$ l'idéal engendré par les mineurs d'ordre k de M ; pour $k > \min(n,p)$, on a $\mathfrak{D}_k(M) := 0$. Les $\mathfrak{D}_k(M)$ sont appelés les *idéaux déterminantiels* de la matrice M.

Exercice 14.
Que valent les $\mathfrak{D}_m(D)$ pour la matrice D de la forme (17), page 29 ?

Solution. On voit d'abord que $\mathfrak{D}_m(D)$ est nul si $m > k$ et engendré par les $d_{i_1}\cdots d_{i_m}$ avec $i_1 < \cdots < i_m$ sinon. Vues les conditions de divisibilité, on a donc $\mathfrak{D}_m(D) = Ad_1\cdots d_m$.

Proposition 15. (i) Soient $M' \in M_{m,n}(A)$, $M \in M_{n,p}(A)$ et $M'' \in M_{p,q}(A)$. Alors $\mathfrak{D}_k(M'M)$ et $\mathfrak{D}_k(MM'')$ sont inclus dans $\mathfrak{D}_k(M)$.
(ii) Si M et N sont équivalentes, alors $\mathfrak{D}_k(M) = \mathfrak{D}_k(N)$.

Démonstration. Soient $i_1 < \cdots < i_k$ des indices distincts de lignes de M' (donc aussi de lignes de $M'M$) et $j_1 < \cdots < j_k$ des indices distincts de colonnes de M (donc aussi de colonnes de $M'M$). Notons $\Delta_{\underline{i},\underline{j}}$ le mineur de $M'M$ correspondant à ces indices de lignes et de colonnes ; $\underline{i},\underline{j}$ désignent donc les multiindices $(i_1,\ldots,i_k),(j_1,\ldots,j_k)$.
Le nombre n de colonnes de M' est également le nombre de lignes de M. Pour chacune des lignes L_ℓ de M (avec $1 \leqslant \ell \leqslant n$), notons $L_{\ell,\underline{j}}$ la ligne obtenue en ne gardant que les coefficients dont le deuxième indice est $j_1,\ldots,j_k$.
La sous-matrice de $M'M$ dont $\Delta_{\underline{i},\underline{j}}$ est le déterminant a pour lignes : $\begin{cases} p_{i_1,1}L_{1,\underline{j}} + \cdots + p_{i_1,r}L_{n,\underline{j}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ p_{i_k,1}L_{1,\underline{j}} + \cdots + p_{i_k,r}L_{n,\underline{j}} \end{cases}$.
Le déterminant $\Delta_{\underline{i},\underline{j}}$ est donc (par multilinéarité) une combinaison linéaire à coefficients dans A de déterminants de la forme : $\det(L_{i'_1,\underline{j}},\ldots,L_{i'_k,\underline{j}})$. En particulier, c'est un élément

de l'idéal $\mathfrak{D}_k(M)$. Il en découle que $\mathfrak{D}_k(M'M) \subset \mathfrak{D}_k(M)$. L'inclusion $\mathfrak{D}_k(MM'') \subset \mathfrak{D}_k(M)$ se démontre de manière similaire.
(ii) Si M et M' sont équivalentes, il découle de la question (i) utilisée dans les deux sens que $\mathfrak{D}_k(M) = \mathfrak{D}_k(M')$. ■

Théorème et définition 16. Soit E un A-module de présentation finie. Choisissons une présentation de la forme (15), page 28. Alors, pour tout $k \leqslant n$, l'idéal $\mathfrak{D}_{n-k}(M)$ ne dépend que de E, et non de la présentation choisie particulière. On le note $\mathfrak{F}_k(E)$. On pose $\mathfrak{F}_k(E) := A$ pour $k > n$. Les $\mathfrak{F}_k(E)$ sont appelés *idéaux de Fitting* du A-module E.

Démonstration. Pour une présentation de la forme (16), page 28, les différents choix de bases pour L_1 et L_2 conduisent à des matrices équivalentes, donc aux mêmes idéaux déterminantiels $\mathfrak{D}_k$, donc, n étant fixé, aux mêmes idéaux de Fitting $\mathfrak{F}_k$.
Nous allons d'abord considérer un système générateur de E fixé (donc n est fixé) et montrer que les idéaux $\mathfrak{D}_k$ ne dépendent pas du système générateur $(r_1, \dots, r_p)$ choisi pour le module des relations $R \subset A^n$. L'ordre des r_i n'influe pas, car il ne change que le signe de certains déterminants mineurs, donc pas l'idéal que ces derniers engendrent.
Étant donnés deux systèmes générateurs $\mathcal{R}$, $\mathcal{R}'$ de R, le système générateur $\mathcal{R}''$ obtenu par juxtaposition des deux peut être obtenu à partir de l'un quelconque des deux par des ajouts successifs d'éléments. Il suffit donc de vérifier que l'ajout d'un générateur à $\mathcal{R} := (r_1, \dots, r_p)$ ne change rien, car alors $\mathcal{R}$ sera « équivalent » à $\mathcal{R}''$ lequel sera « équivalent » à $\mathcal{R}'$, autrement dit, le choix d'un système générateur particulier de R ne changera rien.
Or, l'ajout de r_{p+1} à $(r_1, \dots, r_p)$ revient à l'ajout à droite de M d'une colonne qui est combinaison linéaire des précédentes. tous les nouveaux mineurs d'ordre k qui apparaissent sont alors de déterminant nul.
De manière similaire, on est ramené à étudier l'effet de l'ajout d'un générateur $x_{n+1} := a_1x_1 + \cdots + a_nx_n$. Le nouveau module des relations $R' \subset A^{n+1}$ est engendré par $R \times \{0\}$ (relations entre $x_1, \dots, x_n$) et la relation $(a_1, \dots, a_n, -1)$. La matrice M est donc remplacée par la matrice $M' \in M_{n+1,p+1}(A)$ obtenue en ajoutant une ligne nulle et la colonne ${}^t(a_1, \dots, a_n, -1)$ à M. Il est facile de vérifier que $\mathfrak{D}_{k+1}(M') = \mathfrak{D}_k(M)$, d'où l'égalité de $\mathfrak{D}_{(n+1)-\ell}(M')$ et de $\mathfrak{D}_{n-\ell}(M)$, qui est exactement l'invariance voulue. ■

Exemple. Si M est équivalente à la matrice D de la forme (17), page 29, les idéaux de Fitting du module E de présentation $A^p \xrightarrow{M} A^n \to E \to 0$ sont : $\mathfrak{F}_0(E) = Ad_1 \cdots d_k$, $\mathfrak{F}_1(E) = Ad_1 \cdots d_{k-1}$, …, $\mathfrak{F}_k(E) = \mathfrak{F}_{k+1}(E) = \cdots = A$.

2.2 Modules sur les anneaux noetheriens

La théorie des *anneaux* noetheriens est le coeur de l'algèbre commutative, mais c'est la théorie des *modules* noetheriens qui mène le plus simplement aux premiers résultats.

2.2.1 Modules et anneaux noetheriens

Rappelons (module « Fondements » du cours de L1) qu'un ensemble ordonné X est dit noetherien si toute suite croissante dans X est stationnaire ; ou, de manière équivalente, si toute partie (ou famille) finie non vide dans X admet un élément maximal (*i.e.* non strictement majoré).

Théorème et définition 17. Un A-module E est dit *noetherien* s'il vérifie l'une des conditions équivalentes suivantes :
(i) Tout sous-module de E est de type fini.
(ii) Toute suite croissante de sous-modules de E est stationnaire.
(ii') Toute famille non vide de sous-modules de E admet un élément maximal.

Démonstration. L'équivalence de (ii) et de (ii') résulte du rappel ci-dessus, appliqué à l'ensemble des sous-modules de E ordonné par l'inclusion.
Supposons vérifiée la condition (i). Soit (E'_i) une suite croissante de sous-modules de E. Alors $E' := \bigcup E'_i$ est un sous-module de E : la stabilité par la loi externe est évidente, et, si $x, y \in E'$, on a $x \in E'_j$, $y \in E'_k$ donc $x, y \in E'_{\max(j,k)}$, d'où $x + y \in E'_{\max(j,k)} \subset E'$.
Par l'hypothèse (i), le sous-module E' est de type fini. Soient $x_1, \dots, x_n$ des générateurs. Chaque x_i est élément d'un E'_{j_i}, donc tous sont éléments de E'_j, où $j := \max(j_1, \dots, j_n)$. Alors $E'_j = E'$ et la suite (E'_i) stationne en $i := j$.
Supposons vérifiée la condition (ii). Soit E' un sous-module de E et supposons qu'il n'est pas de type fini (preuve par l'absurde). Soit $x_0 \in E'$ (par exemple 0). Supposons $x_0, \dots, x_n$ choisis dans E'. Alors $E'_n := Ax_0 + \cdots + Ax_n$ est strictement inclus dans E' (puisque ce dernier n'est pas de type fini) et l'on choisit $x_{n+1} \in E' \setminus E'_n$. La suite des sous-modules E'_i est alors strictement croissante, contredisant l'hypothèse (ii). ■

Ainsi, tout K-espace vectoriel de dimension finie est un module noetherien : ce point est non trivial (théorie de la dimension dans le cours de L1).

Théorème 18. Soient E' un sous-module de E et $E'' := E/E'$ le quotient. Alors E est noetherien si, et seulement si, E' et E'' le sont.

Démonstration. Supposons E noetherien. Les sous-modules de E' sont en particulier des sous-modules de E, donc de type fini. Les sous-modules de E'' sont des images par la

projection canonique $p : E \to E''$ de sous-modules de E, donc de type fini. D'après le critère (i) du théorème 17 de la page précédente, E' et E'' sont donc noetheriens.
Supposons E' et E'' noetheriens. Nous allons appliquer à E le critère (ii) du théorème 17 de la page ci-contre. Soit (E_i) une suite croissante de sous-modules de E. La suite croissante des sous-modules $E_i \cap E' \subset E'$ stationne en un entier j. La suite croissante des sous-modules $p(E_i) \subset E''$ stationne en un entier k. Si $n := \max(j, k)$, il découle du lemme suivant que la suite (E_i) stationne en l'entier n. ■

Lemme 19. Soient $E_1 \subset E_2$ deux sous-modules de E tels que $E_1 \cap E' = E_2 \cap E'$ et $p(E_1) = p(E_2)$. Alors $E_1 = E_2$.

Démonstration. Soit $x \in E_2$. Alors $p(x) \in p(E_2) = p(E_1)$, et il existe $y \in E_1$ tel que $p(x) = p(y)$. On a alors $x - y \in \operatorname{Ker} p = E'$ et $x - y \in E_2$ (car $x, y \in E_2$) donc $x - y \in E_2 \cap E' = E_1 \cap E'$. Puisque $y \in E_1$ et $x - y \in E_1$, on conclut enfin que $x \in E_1$. ■

Corollaire 20. Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte courte (paragraphe 1.3.1). Alors E est noetherien si, et seulement si, E' et E'' le sont.

Remarque. Si $E' \subset E$ et $E'' := E/E'$ sont de type fini, alors E est de type fini, et si E est de type fini, alors E'' est de type fini (exercice I.6.31 de la page 63). Mais, si E est de type fini, on ne peut conclure que E' est de type fini (prendre $E := A$ et $E' :=$ un idéal qui n'est pas de type fini). C'est la mise en défaut de cette implication qui justifie l'introduction des modules noetheriens, dont la définition est obtenue en « stabilisant » une propriété qui n'est pas stable par passage aux sous-modules.

Corollaire 21. (i) Tout produit fini de modules noetheriens est un module noetherien.
(ii) Toute somme finie de sous-modules noetherien d'un module arbitraire est un module noetherien.

Démonstration. (i) Si E_1 et E_2 sont noetheriens, et si $E := E_1 \times E_2$, alors on peut appliquer le théorème à $E' := E_1$, avec $E'' \simeq E_2$. On achève la preuve par récurrence.
(ii) L'application $(x_1, \ldots, x_n) \mapsto x_1 + \cdots + x_n$ est surjective de $F := E_1 \times \cdots \times E_n$ sur $G := E_1 + \cdots + E_n$ et permet d'identifier G à un quotient de F, qui est noetherien d'après (i). ■

Définition 8. Un *anneau noetherien* est un anneau A qui est noetherien en tant que A-module.

De manière équivalente, l'anneau A est noetherien s'il vérifie l'une des conditions équivalentes suivantes :
(i) Tout idéal de A est de type fini.
(ii) Toute suite croissante d'idéaux de A est stationnaire.
(ii') Toute famille non vide d'idéaux de A admet un élément maximal.

Ainsi, tout corps et tout anneau principal sont des anneaux noetheriens. Si A est noetherien, $A/\mathfrak{A}$ est noetherien pour tout idéal $\mathfrak{A}$. On a prouvé dans la section « Anneaux principaux » du module « Compléments d'algèbre » de L2 que, si A est principal, alors $A[X]$ est noetherien. Cela sera généralisé au paragraphe 2.2.2.

Exercice 15.
Si S est une partie multiplicative de l'anneau noetherien A, démontrer à l'aide du critère (i) que l'anneau $S^{-1}A$ est noetherien.

Solution. Soit $f : a \mapsto a/1$ le morphisme canonique de A dans $S^{-1}A$. Pour tout idéal $\mathfrak{A}$ de $S^{-1}A$ et pour tout système générateur (a_i) de l'idéal $f^{-1}(\mathfrak{A})$ de A, on vérifie facilement que les $f(x_i)$ engendrent $\mathfrak{A}$.

Un exemple d'anneau non noetherien est l'anneau des polynômes en une infinité dénombrable d'indéterminées $K[(X_n)_{n\geqslant 1}]$: l'idéal engendré par tous les X_n n'est pas de type fini. La suite des idéaux $<X_1, \ldots, X_n>$ est strictement croissante. Pour un autre exemple, voir l'exercice I.6.40 de la page 64.

Théorème 22. (i) Tout module de type fini sur un anneau noetherien est un module noetherien.
(ii) Tout module de type fini sur un anneau noetherien est un module de présentation finie.

Démonstration. Si A est un anneau noetherien, le module A^n est noetherien (corollaire 21 de la page précédente). Le module de type fini E s'écrit A^n/R (comme tout module de type fini). Comme il est quotient du module noetherien A^n, il est noetherien (théorème 18 de la page 32). Comme R est de type fini, comme sous-module de A^n qui est noetherien, E est de présentation finie. ■

Remarque. Un anneau est dit *artinien* si l'ensemble de ses idéaux, ordonné par inclusion, est artinien (module « fondements » du cours de L1). On démontre que tout anneau artinien est noetherien, mais c'est assez difficile. La réciproque est fausse, comme le montre l'exemple de la suite strictement décroissante des idéaux $2^n\mathbb{Z}$ de l'anneau noetherien $\mathbb{Z}$. De plus, tout module artinien n'est pas noetherien (exercice I.6.58 de la page 65).

2.2.2 Anneaux de polynômes

Théorème 23. Soit A un anneau noetherien. Alors l'anneau des polynômes $A[X]$ est noetherien.

Démonstration. La preuve ressemble à celle donnée dans le cas où A est principal (section « Anneaux principaux » du module « Compléments d'algèbre » de L2). Soit $\mathfrak{A}$ un idéal de $A[X]$. Notons :

$$\mathfrak{A}_n := \{a \in A \mid \exists\ aX^n + \cdots \in \mathfrak{A}\}.$$

Comme dans *loc. cit.*, on voit que les $\mathfrak{A}_n$ forment une suite croissante d'idéaux de A, qui stationne donc en un entier p. Pour $k \in [\![0, p]\!]$, on choisit des générateurs :

$$\mathfrak{A}_k = <a_{k,1}, \ldots, a_{k,n_k}>.$$

Pour chaque $k \in [\![0, p]\!]$ et chaque $\ell \in [\![1, n_k]\!]$, on choisit $P_{k,\ell} = a_{k,l}X^k + \cdots \in \mathfrak{A}$ (c'est possible par définition). On va montrer que l'ensemble de ces $P_{k,\ell}$ engendre l'idéal $\mathfrak{A}$. Soit donc $P \in \mathfrak{A}$, de degré d, que l'on écrit $P = aX^d + \cdots$, avec $a \in \mathfrak{A}_d$.

Si $d > p$, on a $\mathfrak{A}_d = \mathfrak{A}_p$, donc $a \in \mathfrak{A}_p$ s'écrit $a = \sum_{i=1}^{n_p} \alpha_i a_{p,i}$. Le poynôme $Q := P - X^{d-p} \sum_{i=1}^{n_p} \alpha_i P_{p,i}$ est élément de $\mathfrak{A}$ et $\deg Q < \deg P$. En réitérant cette opération, on se ramène au second cas.

Si $d \leqslant p$, le coefficient $a \in \mathfrak{A}_p$ s'écrit $a = \sum_{i=1}^{n_d} \alpha_i a_{d,i}$. Le poynôme $Q := P - \sum_{i=1}^{n_d} \alpha_i P_{d,i}$ est élément de $\mathfrak{A}$ et $\deg Q < \deg P$. En réitérant cette opération, on se ramène à 0. ■

Un théorème analogue existe pour les séries formelles (exercice I.6.47 de la page 64).

Corollaire 24 (Théorème de la base de Hilbert). Pour tout corps K, l'anneau $K[X_1, \ldots, X_n]$ est noetherien.

La démonstration ci-dessus est de nature algorithmique : elle s'apparente à une division euclidienne, mais par rapport à une famille de polynômes. La théorie des *bases de Gröbner* donne une assise efficace à ce genre de méthodes. Nous l'aborderons dans le module I.7. Dans ce même module, nous rencontrerons des *K-algèbres de type fini* : ce sont les algèbres de la forme $K[X_1, \ldots, X_n]/\mathfrak{A}$ (le nom est justifié à l'exercice I.6.48 de la page 64).

Corollaire 25. Une algèbre de type fini sur un corps est un anneau noetherien.

3 MODULES SUR LES ANNEAUX PRINCIPAUX

Nous allons élucider la structure des modules de type fini sur un anneau principal. Le cas de l'anneau $\mathbb{Z}$ nous fournira alors la structure des groupes abéliens de type fini, en particulier celle des groupes abéliens finis. Le cas de l'anneau $K[X]$ nous permettra de retrouver l'essentiel de la théorie de la réduction des endomorphismes sur un corps.

3.1 Modules libres de rang fini sur un anneau principal

On fixe l'anneau principal A. Tout A-module de type fini E admet une desription de la forme $E \simeq L/R$, où L est libre de rang fini, et où R est un sous-module de L. Il est donc naturel d'étudier les sous-modules d'un module libre de rang fini. Comme pour l'algèbre linéaire en L1, il y a une approche « géométrique » (manipulations de bases, projections) et une approche « algorithmique » (opérations sur des matrices).

3.1.1 Approche géométrique

Soit R un sous-module du module libre de rang fini L. Pour toute forme linéaire $\pi : L \to A$, l'image $\pi(R)$ de R est un sous-module de A, c'est-à-dire un idéal de A. On peut donc écrire $\pi(R) = Ad_\pi$, où $d_\pi \in A$ est unique à un facteur inversible près. Puisque A est noetherien, il existe même une forme linéaire φ (non nécessairement unique) telle que l'idéal $\varphi(R)$ est maximal parmi les idéaux $\pi(R)$.

Lemme 26. On suppose R non trivial, et φ choisie comme ci-dessus.
(i) Soient $d \in A$ tel que $\varphi(R) = Ad$ et $r \in R$ tel que $\varphi(r) = d$. Alors $r \in dL$, et, si $e \in L$ est l'unique élément tel que $r = de$, on a $\varphi(e) = 1$.
(ii) Avec ces choix, en notant $L' := \operatorname{Ker}\varphi$, on a de plus les décompositions :

$$\begin{aligned} L &= Ae \oplus L', \\ R &= Ar \oplus (L' \cap R). \end{aligned}$$

Démonstration. (i) L'existence de d et de r est évidente par définition. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base arbitraire de L et notons $\pi_1, \ldots, \pi_n$ les formes linéaires coordonnées associées à $\mathcal{B}$. Les $\pi_i(R)$ ne sont pas tous nuls (sinon R serait trivial), ce qui montre au passage que $d \neq 0$. Nous allons prouver que d divise les $d_i := \pi_i(r)$, ce qui entrainera que $r = \sum_{i=1}^{n} \pi_i(r)e_i \in dL$. Puisque $d \neq 0$, les assertions sur e en découleront.
Pour $i \in [\![1, n]\!]$, soit $\delta = ad + bd_i$ le pgcd de d et d_i (relation de Bézout dans l'anneau principal A). Posons $\psi := a\pi + b\varphi$ Alors $\psi(r) = ad + bd_i = \delta$ et $Ad \subset A\delta \subset \psi(R)$. Par maximalité de $Ad = \varphi(R)$, on a $Ad = A\delta$, donc d divise bien d_i.

(ii) Puisque $\varphi(e) = 1$, les applications linéaires $p : x \mapsto \varphi(x)e$ et $q : x \mapsto x - \varphi(x)e$ sont deux projecteurs qui donnent lieu à la décomposition $L = Ae \oplus \operatorname{Ker}\varphi$. Puisque $\varphi(R) = Ad$, on a $p(R) = Ade = Ar \subset R$, et ces projecteurs induisent par restriction à R la décomposition $R = Ar \oplus \operatorname{Ker}(\varphi_{|_R}) = Ar \oplus (\operatorname{Ker}\varphi \cap R)$. ■

Théorème 27. Tout sous-module d'un module libre de rang fini est libre de rang fini.

Démonstration. Soit R un sous-module du module libre de rang fini L. On sait déjà que $\operatorname{rg} R \leqslant \operatorname{rg} L$ (corollaire 10 de la page 23). On raisonne par récurrence sur le rang du module R (c'est-à-dire le cardinal d'une famille libre maximale). Si ce rang est 0, alors $R = \{0\}$ (car L est sans torsion, donc tout élément non nul constitue une famille libre) et le théorème est trivial. Sinon, on applique le lemme, et l'on a : $R = Ar \oplus R'$, avec $r \neq 0$. Comme $\operatorname{rg} R = 1 + \operatorname{rg} R'$, l'hypothèse de récurrence entraine que R' est libre, donc R également. ■

Notons que ce théorème ne peut être vérifié que pour un anneau principal : en l'appliquant au module $L := A$, qui est libre de rang 1, on en déduirait que tout idéal est libre de rang 0 (donc nul) ou 1 (donc principal engendré par un élément non diviseur de 0).

Théorème 28 (de la base adaptée). Soit R un sous-module du module libre L de rang n. Il existe alors une base $\mathcal{B} := (e_1, \ldots, e_n)$ de L et des éléments $d_1, \ldots, d_k$ $(0 \leqslant k \leqslant n)$ non nuls de A vérifiant les relations de divisibilité :

$$d_1 | d_2 | \cdots | d_k, \tag{18}$$

tels que la famille $\mathcal{B}' := (d_1 e_1, \ldots, d_k e_k)$ soit une base de R.

Démonstration. Si $R = \{0\}$, le théorème est trivial (avec n'importe quelle base de L et $k := 0$). Supposons $R \neq \{0\}$. On reprend les conclusions du lemme 26 de la page précédente, en notant $e_1 := e$ et $d_1 := d$. On a donc :

$$\begin{aligned} L &= Ae_1 \oplus L', \\ R &= Ad_1 e_1 \oplus (L' \cap R). \end{aligned}$$

D'après le théorème 27, L' est libre de rang $n - 1$. Si $L' \cap R = \{0\}$, la conclusion est immédiate (on adjoint à e_1 une base quelconque de L'). Dans le cas général, on raisonne par récurrence sur le rang de L. On peut donc supposer la conclusion vérifiée par le sous-module $R \cap L' \subset L'$ et écrire :

$$\begin{aligned} L' &= Ae_2 \oplus \cdots \oplus Ae_n, \\ L' \cap R &= Ad_2 e_2 \oplus \cdots \oplus Ad_k e_k, \end{aligned}$$

avec $d_2|\cdots|d_k$. Il reste seulement à vérifier que $d_1|d_2$. Notant $\pi_1,\ldots,\pi_n$ les formes linéaires coordonnées associées à la base $(e_1,\ldots,e_n)$, posons $\psi := \pi_1+\pi_2$. On voit facilement que $\psi(R) = Ad_1 + Ad_2$, qui contient Ad_1. Par maximalité, on en déduit que $Ad_1 + Ad_2 = Ad_1$, autrement dit que $d_1|d_2$ comme souhaité. ■

Exemple. Soient $L := \mathbb{Z}^2$ et $R := \mathbb{Z}(a,b)$ où $(a,b) \in \mathbb{Z}^2$. Nous allons déterminer une base adaptée de L, en commençant par appliquer le lemme 26 de la page 36.
Si $a = b = 0$, n'importe quelle base convient.
Sinon, pour toute forme linéaire $\varphi(x,y) = ux+vy$ sur L, on a $\varphi(R) = \mathbb{Z}(au+bv) \subset \mathbb{Z}a+\mathbb{Z}b = \mathbb{Z}\delta$, où δ est le pgcd de a,b. Notons $a = \delta a'$, $b = \delta b'$ avec $a' \wedge b' = 1$.
L'idéal $\varphi(R)$ est donc maximal (parmi les idéaux de cette forme) lorsque $au + bv = \delta$ (relation de Bézout). On aura donc (avec les notations du lemme) $r = (a,b)$, $d = \delta$ et $e = (a',b')$. Pour compléter e en une base adaptée, on peut choisir simplement (c,d) tels que $a'd - b'c = 1$, par exemple $(-v,u)$. On peut également utiliser le second projecteur du lemme : $(x,y) \mapsto (x,y) - (ux+vy)(a',b')$. l'image de la base canonique est formée des vecteurs $(1,0) - u(a',b') = (vb',-ub')$ et $(0,1) - v(a',b') = (-va',ua')$, c'est donc $\mathbb{Z}(-v,u)$ et l'on trouve le même supplémentaire !

Corollaire 29. Pour que R soit facteur direct de L, il faut, et il suffit, que le module L/R soit sans torsion.

Démonstration. Si R est facteur direct de L, alors L/R est isomorphe à l'un quelconque des supplémentaires de R, donc à un sous-module de L, et il est sans torsion.
Réciproquement, il faut remarquer que l'on a :

$$L/R \simeq A/Ad_1 \oplus \cdots \oplus A/Ad_k \oplus A \oplus \cdots \oplus A.$$

Pour que ce module soit sans torsion, il faut que tous les A/Ad_i soit nuls, c'est-à-dire les d_i inversibles. Dans ce cas, on a $L = R \oplus Ae_{k+1} \oplus \cdots \oplus Ae_n$. ■

Naturellement, l'entier k est le rang de R, il est donc uniquement déterminé. L'exercice suivant montre qu'il en est de même de Ad_k.

Exercice 16.
Calculer le module $\mathrm{Tor}_A(L/R)$ et son annulateur.

Solution. D'après le calcul du corollaire, $\mathrm{Tor}_A(L/R) = A/Ad_1 \oplus \cdots \oplus A/Ad_k$. L'annulateur de ce module est l'intersection des annulateurs des facteurs, c'est-à-dire l'intersection des Ad_i, c'est-à-dire Ad_k en vertu des relations de divisibilité.

On verra à la section 3.2 que ce sont en fait tous les Ad_i qui sont uniquement déterminés.

3.1.2 Approche algorithmique

Voici maintenant une preuve matricielle du théorème de la base adaptée. Pour cela, nous devons admettre *a priori* que le sous-module R du module libre de rang fini L est lui-même de type fini : cela découle de la théorie des modules noetheriens (théorème 22 de la page 34). Soient donc $\mathcal{X} := (x_1, \dots, x_n)$ une base de L et $\mathcal{Y} := (y_1, \dots, y_p)$ un système générateur de R, que l'on écrit dans la base : $\mathcal{Y} = \mathcal{X}M$, avec $M \in M_{n,p}(A)$.

Théorème 30 (Algorithme du pivot sur un anneau principal). La matrice M est équivalente à une matrice D de la forme (17), page 29 telle que $d_1 | \cdots | d_k$.

Démonstration. Dans le cas où A est un anneau euclidien, la preuve a été donnée dans la section « Anneaux euclidiens » du module « Compléments d'algèbre » de L2 (algorithme du pivot sur un anneau euclidien). Dans le cas plus général où A est seulement supposé principal, la preuve est plus compliquée (exercice I.6.51 de la page 65). ■

On a donc $M = PDQ^{-1}$, avec $P \in GL_n(A)$ et $Q \in GL_p(A)$. L'égalité $\mathcal{Y} = \mathcal{X}M$ entraine $\mathcal{Y}Q = \mathcal{X}PD$. La famille $\mathcal{B} := \mathcal{X}P$ est une base $(e_1, \dots, e_n)$ de L. La famille $\mathcal{Y}' := \mathcal{Y}Q$ est une famille génératrice de R (exercice I.6.7 de la page 60), et l'on a :

$$\mathcal{Y}' = \mathcal{B}D = (d_1 e_1, \dots, d_k e_k, 0, \dots, 0).$$

Naturellement, la famille $\mathcal{B}' := (d_1 e_1, \dots, d_k e_k)$ engendre le même module que $\mathcal{Y}'$ et, les d_i étant non nuls, elle est libre. C'est donc une base (adaptée) de R. L'algorithme du pivot sur un anneau principal fournit donc une nouvelle preuve du théorème de la base adaptée.

Exercice 17.
Appliquer la méthode au sous module R de $L := \mathbb{Z}^2$ engendré par $y_1 := (-10, -8)$ et $y_2 := (14, 10)$.

Solution. La famille $\mathcal{Y} := (y_1, y_2)$ peut être décrite en vecteurs colonnes par la matrice $M := \begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}$, *i.e.*, en identifiant $\mathbb{Z}^2$ à $M_{2,1}(\mathbb{Z})$, on a $R = M\mathbb{Z}^2$. Avec les notations qui précèdent, cela revient à dire que l'on a choisi pour base $\mathcal{X} := (x_1, x_2)$ de L la base canonique formée des vecteurs $x_1 := (1, 0)$ et $x_2 := (0, 1)$ (ou de leurs écritures en colonnes).

Selon un exemple de *loc. cit.*, la matrice M est mise sous forme canonique $D := \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$ par les opérations élémentaires $L_1 \leftrightarrow L_2$, $C_2 \leftarrow C_2 + C_1$, $L_2 \leftarrow L_2 - L_1$, $C_1 \leftrightarrow C_2$, $C_2 \leftarrow C_2 + 4C_1$ et $L_2 \leftarrow L_2 - L_1$. Traduisant ces opérations en multiplications par des matrices de transvection et de permutation, on obtient l'égalité : $M = PDQ^{-1}$,

avec $P := \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$ et $Q := \begin{pmatrix} 1 & 5 \\ 1 & 4 \end{pmatrix}$. La matrice P a pour colonnes une nouvelle base $\mathcal{B} := (e_1, e_2)$ de $L = \mathbb{Z}^2$; on a donc $e_1 = (2, 1)$ et $e_2 = (1, 0)$. La matrice $MQ = PD$ a pour colonne un nouveau système générateur (y'_1, y'_2) de R. On trouve $y'_1 = 2e_1$ et $y'_2 = 6e_2$, d'où la base adaptée $\mathcal{B}' := (2e_1, 6e_2)$ de R.

Puisque la matrice $\mathrm{Diag}(u_1, \ldots, u_k, 1, \ldots, 1)$ est inversible, chaque d_i peut être remplacé par $u_i d_i$ avec $u_i \in A^*$ arbitraire. Pour énoncer une assertion d'unicité concernant des d_i, remarquons qu'il revient au même de se donner l'élément $d \neq 0$ à facteur inversible près ou de se donner l'idéal non trivial Ad. La première partie du théorème ci-dessous est la généralisation aux anneaux principaux du théorème qui dit que deux matrices de même format sur un corps sont équivalentes si, et seulement si, elles ont le même rang.

Théorème et définition 31. (i) Soit $M \in M_{p,n}(A)$. Soit D une matrice équivalente à M et de la forme (17), page 29 avec $d_1 | \cdots | d_k$. La suite des idéaux Ad_i est uniquement déterminée par la classe d'équivalence de M. On les appelle *facteurs invariants de* M.
(ii) Soit R un sous-module du module libre L de rang n. Soient $\mathcal{B} := (e_1, \ldots, e_n)$ une base de L et $\mathcal{B}' := (d_1 e_1, \ldots, d_k e_k)$ une base adaptée de R (théorème 28 de la page 37). La suite des idéaux Ad_i est uniquement déterminée par R et L. On les appelle *facteurs invariants de* R *dans* L.

Démonstration. (i) D'après la proposition 15 de la page 30, les idéaux déterminantiels $\mathfrak{D}_i(M)$ sont égaux aux $\mathfrak{D}_i(D)$ et ne dépendent que de la classe d'équivalence. D'après l'exercice 14 de la page 30, ce sont les idéaux $Ad_1 \cdots d_i$. La donnée de ces derniers est équivalente à celle des Ad_i. (On ne prend en compte ici que les $\mathfrak{D}_i(M)$ non nuls).
(ii) Pour des bases arbitraires $\mathcal{C}$ et $\mathcal{C}'$ de L et R, la matrice M telle que $\mathcal{C}' = \mathcal{C}M$ est déterminée à équivalence près. Les facteurs invariants de R dans L sont les facteurs invariants des matrices de cette classe. ■

Dans le cas des anneaux $\mathbb{Z}$ et $K[X]$, chaque idéal non trivial a un générateur privilégié (respectivement positif ou unitaire) et il est d'usage de prendre pour facteurs invariants ces éléments de l'anneau (et non les idéaux qu'ils engendrent).

Exemple. Soit $M := \begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}$ et $D := \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$. On voit que $\mathfrak{D}_1(M) = \mathfrak{D}_1(D) = 2\mathbb{Z}$ et $\mathfrak{D}_2(M) = \mathfrak{D}_2(D) = 12\mathbb{Z}$. Les facteurs invariants sont donc 2 et $\dfrac{12}{2} = 6$. Ce sont également les facteurs invariants de $R := \mathbb{Z}(-10, -8) + \mathbb{Z}(14, 10)$ dans $\mathbb{Z}^2$.

Exercice 18.
Quels sont les facteurs invariants de $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$?

Solution. Si $M = 0$, la suite des facteurs invariants est une liste vide. Si $M \neq 0$, le premier facteur invariant est le pgcd δ de a, b, c, d (défini à facteur inversible près). Si $\det M = 0$, c'est le seul. Si $\det M \neq 0$, le deuxième (et dernier) facteur invariant est $\dfrac{\det M}{\delta}$ (défini à facteur inversible près).

3.1.3 Vecteurs primitifs

Il découle de la preuve du théorème de la base adaptée que Ad_1 est le plus grand des idéaux $\varphi(R)$, où $\varphi : L \to A$ est une forme linéaire. Appliquons cette remarque à un sous-module monogène $R := Ax$.

Proposition et définition 32. Soit $x \in L \setminus \{0\}$. Les conditions suivantes sont équivalentes :
(i) Le sous-module $R := Ax$ est un facteur direct de L.
(ii) Il existe une forme linéaire $\varphi : L \to A$ telle que $\varphi(x) = 1$.
(iii) L'élément x peut être complété en une base de L.
(iv) L'élément x est *indivisible*, autrement dit, une égalité $x = dy$ dans L n'est possible que si $d \in A^*$.
(v) Le module L/Ax est sans torsion.
On dit alors que x est un élément (ou un vecteur) *primitif*.

Démonstration. Outre le théorème 28 de la page 37, on applique le lemme 26 de la page 36 et le corollaire 29 de la page 38. ■

Exercice 19.
Appliquer l'équivalence de (iii) et de (iv) lorsque $L := A^n$.

Solution. Prenant $x := (a_1, \ldots, a_n)$, on trouve que, si $a_1, \ldots, a_n \in A$ sont premiers entre eux dans leur ensemble, alors il existe une matrice inversible sur A dont ils forment la première ligne (ou colonne). (La réciproque est beaucoup plus facile.) Pour $n := 2$, c'est essentiellement le théorème de Bézout.

Méthode de complétion de la matrice. Soit $a := (a_1, \ldots, a_n)$ un vecteur primitif de A^n. Il existe donc une forme linéaire $\varphi(x_1, \ldots, x_n) := u_1x_1 + \cdots + u_nx_n$ telle que $\varphi(a) = u_1a_1 + \cdots + u_na_n = 1$. On peut calculer les u_i en appliquant le théorème de

Bézout à a_1 et a_2, puis à $a_1 \wedge a_2$ et a_3, etc.
On sait que $A^n = Aa \oplus \operatorname{Ker}\varphi$ et que ces deux facteurs directs sont les images respectives des projecteurs $p : x \mapsto \varphi(x)a$ et $q : x \mapsto x - \varphi(x)a$. Le noyau $\operatorname{Ker}\varphi$ est donc engendré par les images $q(\varepsilon_1), \ldots, q(\varepsilon_n)$ des vecteurs de la base canonique $(\varepsilon_1, \ldots, \varepsilon_n)$. La matrice de cette famille est la matrice de q dans la base canonique :

$$q(\varepsilon_j) = \varepsilon_j - u_j a \Longrightarrow M = I_n - (a_i u_j).$$

Les facteurs invariants de $\operatorname{Ker}\varphi$ dans L sont les $(n-1)$ idéaux $A, \ldots, A$ (exercice I.6.55 de la page 65). L'algorithme du pivot doit nous donner une égalité : $M = P\operatorname{Diag}(1, \ldots, 1, 0)Q^{-1}$. Les $(n-1)$ premières colonnes de P forment une base de $\operatorname{Ker}\varphi$. En mettant en tête la colonne a, on obtient la matrice inversible annoncée par l'exercice.

Exercice 20.
Compléter $a := (6, 15, 10) \in \mathbb{Z}^3$ en une matrice inversible.

Solution. On a $(-2)\times 6 + (1)\times 15 = 3 = 6 \wedge 15$ et $(-3)\times 3 + (1)\times 10 = 1 = 3 \wedge 10 = 6 \wedge 15 \wedge 10$, d'où $(6) \times 6 + (-3) \times 15 + (1) \times 10 = 1$. On prendra donc :

$$\varphi(x, y, z) = 6x - 3y + z \Longrightarrow M = \begin{pmatrix} -35 & 18 & -6 \\ -90 & 46 & -15 \\ -60 & 30 & -9 \end{pmatrix}.$$

Comme $a \in \operatorname{Ker} M$ et $\operatorname{Tr} M = 2$ (projecteur de rang 2 dans $\mathbb{Z}^3$ donc dans $\mathbb{Q}^3$), le calcul a des chances d'être correct ... L'algorithme du pivot donne nécessairement $D := \operatorname{Diag}(1, 1, 0)$ et :

$$MQ = PD = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 3 & 0 \end{pmatrix} \quad \text{avec} \quad Q := \begin{pmatrix} 1 & 0 & 6 \\ 2 & 1 & 15 \\ 0 & 3 & 10 \end{pmatrix} \quad \text{et} \quad P := \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 6 & -3 & 1 \end{pmatrix}^{-1}.$$

Les deux premières colonnes de MQ, augmentées du vecteur de départ en première colonne, donnent la matrice $\begin{pmatrix} 6 & 1 & 0 \\ 15 & 2 & 1 \\ 10 & 0 & 3 \end{pmatrix}$, dont le déterminant vaut 1.

3.2 Modules de type fini sur un anneau principal

3.2.1 Facteurs invariants d'un module de type fini

Théorème et définition 33. Tout module de type fini E sur un anneau principal A est isomorphe à un produit fini de modules monogènes :

$$E \simeq A/\mathfrak{A}_1 \times \cdots \times \mathfrak{A}/\mathfrak{A}_n, \tag{19}$$

où les $\mathfrak{A}_i$ sont des idéaux tels que $\mathfrak{A}_1 \subset \cdots \subset \mathfrak{A}_n \neq A$. Ces idéaux (dont certains, nécessairement les premiers, peuvent être nuls) sont déterminés de manière unique. On les appelle *facteurs invariants* du module E. Le nombre des facteurs invariants nuls est le rang de E.

Démonstration. On écrit $E \simeq L/R$, où L est libre de rang fini. Avec les notations du théorème de la base adaptée (théorème 28 de la page 37), on a : $L/R \simeq A/Ad_1 \times \cdots \times A/Ad_n$, où l'on a posé $d_{k+1}, \ldots, d_n := 0$. Les idéaux $\mathfrak{A}_i$ sont donnés par les formules : $\mathfrak{A}_1 := Ad_n, \ldots, \mathfrak{A}_n := Ad_1$. Le nombre de $\mathfrak{A}_i$ nuls est donc $r := n - k = \operatorname{rg} E$: on a $\mathfrak{A}_1 = \cdots = \mathfrak{A}_r = 0$. D'après l'exemple de la page 31, les $\mathfrak{A}_i$ non nuls vérifient les relations : $\mathfrak{A}_{r+1} \cdots \mathfrak{A}_i = \mathfrak{F}_{i-r-1}(E)$. D'après le théorème 16 de la page 31, ils sont donc déterminés par (la classe d'isomorphie de) E. ■

Concrètement, les facteurs invariants du module $A/Ad_1 \times \cdots \times A/Ad_k \times A^r$ sont $0, \ldots, 0$ (r fois), $Ad_k, \ldots, Ad_1$.

Attention. On ne confondra pas les expressions « facteurs invariants de la matrice M », « facteurs invariants du sous-module R dans le module libre de rang fini L » et « facteurs invariants du module de type fini E ».

Il découlait du corollaire 29 de la page 38 que $\operatorname{Tor}(E)$ est facteur direct de E. Dans l'écriture (19) ci-dessus, le module $A/Ad_1 \times \cdots \times A/Ad_k$ correspond à un sous-module bien déterminé de E, le sous-module $\operatorname{Tor}(E)$. Les facteurs $A/Ad_1, \ldots, A/Ad_k$ sont cycliques (la définition a été donnée page 16). *A contrario*, le module $A/Ad_{k+1} \times \cdots \times A/Ad_n = A^r$ (avec $r := n - k = \operatorname{rg} E$) correspond à n'importe quel supplémentaire de $\operatorname{Tor}(E)$ dans E.

Corollaire 34. Tout module de type fini E est somme directe de $\operatorname{Tor}(E)$ et d'un module libre de rang fini. Le sous-module $\operatorname{Tor}(E)$ est somme directe de modules cycliques.

Corollaire 35. Tout module sans torsion de type fini sur un anneau principal est libre.

Corollaire 36. Tout module de torsion de type fini sur un anneau principal est somme directe de modules cycliques.

Point Méthode

Pour calculer pratiquement les facteurs invariants de E, on choisit d'abord une présentation $A^p \xrightarrow{M} A^n \to E \to 0$ avec $M \in M_{n,p}(A)$. On peut alors calculer les idéaux déterminantiels $\mathfrak{D}_i(M)$. On ordonne ceux de ces idéaux qui sont non nuls et propres : $0 \neq A\delta_k \subset \cdots \subset A\delta_1 \neq A$. On pose ensuite $d_1 := \delta_1$ et, pour $2 \leqslant i \leqslant k$, $d_i := \dfrac{\delta_i}{\delta_{i-1}}$.
Une autre méthode, clairement praticable si A est euclidien, est d'appliquer l'algorithme du pivot pour trouver une matrice D de la forme (17), page 29.
Le rang de E est alors égal à $r := n - k$. Les facteurs invariants sont $\mathfrak{A}_1, \ldots, \mathfrak{A}_r := 0$ et $\mathfrak{A}_{r+1} := Ad_k$, …, $\mathfrak{A}_n := Ad_1$.

Notons que, dans le cas d'un corps, la première méthode de calcul des Ad_i revient au calcul du rang par détermination du plus grand mineur de déterminant non nul, alors que la deuxième méthode revient au calcul du rang par la méthode du pivot de Gauß : et nous savons bien que cette dernière est *beaucoup* moins chère.

Exercice 21.
Calculer les facteurs invariants de $\mathbb{Z}/a\mathbb{Z}$ en utilisant d'abord le seul générateur $\overline{1}$, puis en utilisant la famille génératrice $(\overline{1}, \overline{b})$ ($b \in \mathbb{Z}$).

Solution. Dans le premier cas, on a la présentation $\mathbb{Z} \xrightarrow{M} \mathbb{Z} \to 0$, où $M := (a)$ et $n = p = 1$. Les seuls idéaux déterminantiels non nuls sont $\mathfrak{D}_0(M) = \mathbb{Z}$ et $\mathfrak{D}_1(M) = a\mathbb{Z}$. Les idéaux de Fitting $\mathfrak{F}_\ell(E) = \mathfrak{D}_{n-\ell}(M)$ sont donc : $\mathfrak{F}_0 = a\mathbb{Z}$ et $\mathfrak{F}_1(E) = \mathbb{Z}$. L'unique facteur invariant est $\mathfrak{A}_1 = a\mathbb{Z}$.
Dans le second cas, le module des relations entre les générateurs est $R := \{(x, y) \in \mathbb{Z}^2 \mid x+by \equiv 0 \pmod{a}\}$. Il est engendré par $(b, -1)$ et $(a, 0)$. On a donc la présentation $\mathbb{Z}^2 \xrightarrow{M} \mathbb{Z}^2 \to 0$, où $M := \begin{pmatrix} b & a \\ -1 & 0 \end{pmatrix}$, $n = 2$ et $p = 2$. Les seuls idéaux déterminantiels non nuls sont $\mathfrak{D}_0(M) = \mathbb{Z}$, $\mathfrak{D}_1(M) = \mathbb{Z}$ et $\mathfrak{D}_2(M) = a\mathbb{Z}$. Les idéaux de Fitting sont donc : $\mathfrak{F}_0 = a\mathbb{Z}$, $\mathfrak{F}_1(E) = \mathbb{Z}$ et $\mathfrak{F}_2(E) = \mathbb{Z}$. L'unique facteur invariant est encore $\mathfrak{A}_1 = a\mathbb{Z}$.

3.2.2 Diviseurs élémentaires d'un module de torsion de type fini

Dans tout ce paragraphe, nous fixons un ensemble de représentants P de l'ensemble des irréductibles de A pour la relation "être associé" (voir la section sur les anneaux factoriels du module « Compléments d'algèbre » de L2). Dans le cas de $\mathbb{Z}$, nous prenons bien entendu

les nombres premiers de $\mathbb{N}^*$, et, dans le cas de $K[X]$, les polynômes irréductibles unitaires. Soit $d \neq 0$, que l'on décompose en $d = u \prod_{p\in P} p^{v_p(d)}$ (dans ce produit, presque tous les facteurs valent 1), avec $u \in A^*$. Le lemme chinois fournit un isomorphisme d'anneaux :

$$\frac{A}{Ad} \simeq \prod_{p\in P} \frac{A}{Ap^{v_p(d)}}.$$

C'est en fait clairement un isomorphisme de A-modules. (Dans le produit, presque tous les facteurs sont des modules triviaux.) Soit maintenant E un A-module de torsion de type fini. On a donc un isomorphisme $E \simeq \frac{A}{Ad_1} \times \cdots \times \frac{A}{Ad_k}$, qui, combiné avec le précédent, donne :

$$E \simeq \prod_{p\in P} E_p, \quad \text{avec} \quad E_p \simeq \prod_{i=1}^{k} \frac{A}{Ap^{v_p(d_i)}}.$$

Nous allons voir que la décomposition en les facteurs E_p est intrinsèque : on a $E = \bigoplus_{p\in P} E_p$ pour des sous-modules parfaitement déterminés de p.

Exercice 22.
Calculer les sous-modules $E(\alpha)$ de $E := A/Ad$. (Notation introduite page 9.)

Solution. Les éléments de $E(\alpha)$ sont les $\overline{a}$ tels que $d|a\alpha$. Si l'on note $\delta := d \wedge \alpha$ et $d' := \frac{d}{\delta}$, $\alpha' := \frac{\alpha}{\delta}$, on a les équivalences : $d|a\alpha \Leftrightarrow d'|a\alpha' \Leftrightarrow d'|a$, d'où :

$$E(\alpha) = Ad'/Ad \simeq A/A\delta.$$

On distinguera soigneusement l'*égalité* $E(\alpha) = Ad'/Ad$ de l'*isomorphisme* $E(\alpha) \simeq A/A\delta$.

Lemme 37 (Lemme des noyaux). Pour tout $d \in A$ non nul, notons $q_1, \ldots, q_s$ les *facteurs primaires* $p^{v_p(d)}$ non triviaux de d, et posons $q_i' := \frac{d}{q_i}$. Il existe $u_1, \ldots, u_s$ tels que $u_1q_1' + \cdots + u_sq_s' = 1$. Les endomorphismes $x \mapsto \pi_i(x) = u_iq_i'x$ sont des projections de $E(d)$ sur les $E(q_i)$, et l'on a une décomposition :

$$E(d) = \bigoplus_{i=1}^{s} E(q_i) = \bigoplus_{p\in P} E\left(p^{v_p(d)}\right).$$

Démonstration. Les q_i' sont premiers entre eux dans leur ensemble, d'où l'existence des u_i. Comme $q_iq_i' = d$, on a $\operatorname{Im}\pi_i \subset E(q_i)$. D'autre part, si $i \neq j$, on a $d|q_i'q_j'$, d'où l'on déduit que chaque π_i est l'identité sur $E(q_i)$ et nul sur les autres $E(q_j)$. ∎

Application aux équations différentielles linéaires à coefficients constants.. Le lemme des noyaux permet d'éclairer certains calculs du module « Équations différentielles » du cours de L2. Si l'on munit le $\mathbb{C}$-espace vectoriel $\mathcal{C}^\infty(\mathbb{R},\mathbb{C})$ de l'endomorphisme $D : f \mapsto f'$, on en fait un $K[X]$-module (paragraphe 1.2.3). Résoudre l'équation différentielle linéaire homogène $P(D)(f) = 0$ revient à déterminer le module $E(d)$, où $d := P(X)$. Le lemme des noyaux suggère de rechercher la décomposition primaire $d = \prod q_i$, et de résoudre les équations simplifiées $q_i x_i = 0$. Dans notre cas, on décompose $P = \prod (X - \lambda_i)^{r_i}$, et l'on est ramené aux équations différentielles $(D - \lambda_i)^{r_i}(f_i) = 0$, qui sont en effet beaucoup plus simples.
Le « calcul symbolique » des solutions d'équations avec second membre (*loc. cit.*) se prête à un traitement analogue. Pour résoudre dans un A-module l'équation $dx = y$, reprenons les notations du lemme des noyaux. On résout séparément les équations $q_i x_i = y$. On voit alors que $x := \sum u_i x_i$ convient :

$$dx = \sum du_i x_i = \sum u_i q_i' q_i x_i = y,$$

puisque $q_i x_i = y$ et que $\sum u_i q_i' = 1$. Le lecteur est invité à traduire ce calcul avec $d := P(X)$, $x := f$ et $y := b$ (notations de *loc. cit.*). Le lien avec la décomposition en éléments simples se fait ainsi :

$$\frac{1}{d} = \sum \frac{u_i q_i'}{q_i q_i'} = \sum \frac{u_i}{q_i}.$$

Il faut toutefois remarquer que ce raisonnement algébrique présuppose que le second membre b est dans $\mathcal{C}^\infty(\mathbb{R},\mathbb{C})$. Il est donc moins général que le calcul un peu pénible de l'an dernier !

À l'opposé, si l'on fixe $p \in P$, on constate que les $E(p^n)$ forment une suite croissante de sous-modules de E, dont la réunion est donc un sous-module. Ce module est appelé *sous-module (ou composante) de p-torsion de E* et noté :

$$E_p := \bigcup_{n \geqslant 0} E(p^n).$$

Exercice 23.
Calculer les sous-modules de p-torsion de $E := A/Ad$.

Solution. D'après l'exercice précédent, si p ne divise pas d, $E(p^n) = 0$ pour tout n, donc $E_p = 0$. Si p est un facteur premier de d, il suffit de calculer $E(p^n)$ pour n assez grand, mais il faut le calculer exactement (et non à isomorphisme près) pour pouvoir passer à la réunion. Si l'on écrit $d = p^{v_p(d)} d_p'$ (donc p ne divise pas d_p'), on a : $E(p^n) = Ad_p'/Ad$ dès que $n \geqslant v_p(d)$. On en déduit : $E_p = Ad_p'/Ad \simeq A/Ap^{v_p(d)}$.

Théorème et définition 38. Soit E un A-module de torsion (pas nécessairement de type fini). Alors E est la somme directe de ses sous-modules de p-torsion :

$$E = \bigoplus_{p\in P} E_p. \tag{20}$$

Cette décomposition est appelée *décomposition primaire de* E.

Démonstration. Soit $x \in E$. Puisque E est de torsion, il existe d non nul, tel que $x \in E(d)$. En appliquant le lemme 37 de la page 45 (ii), on voit que $x \in \sum E\left(p^{v_p(d)}\right)$, et *a fortiori* que $x \in \sum_{p\in P} E_p$.
Pour prouver l'unicité de la décomposition de x, on se ramène par l'argument habituel à l'unicité de la décomposition de 0. Suposons donc $0 = \sum_{p\in P} x_p$, où les $x_p \in E_p$ sont presque tous nuls. Pour chacun des x_p non nuls, on a $x_p \in E(p^{n_p})$ pour un certain entier n_p. Posant $d := \prod p^{n_p}$, on voit que l'on est ramené à l'assertion d'unicité du lemme 37 de la page 45. ■

Exemple. Soit $E := K/A$. Le même genre de calculs que dans l'exercice 4 de la page 10 donne :

$$\begin{aligned} \forall a \neq 0\ ,\ E(a) &= Aa^{-1}/A \simeq A/Aa, \\ \forall p \in P\ ,\ \forall n \geqslant 0\ ,\ E(p^n) &= Ap^{-n}/A \simeq A/Ap^n, \\ E_p &= A[p^{-1}]/A, \end{aligned}$$

où l'on note $A[p^{-1}] := \bigcup Ap^{-n}$ la sous A-algèbre de K engendrée par p^{-1}.

Dans le cas où E est de torsion de type fini, il existe d tel que $E = E(d)$ et la décomposition primaire s'identifie à celle obtenue au lemme 37 de la page 45.

Exercice 24.
Appliquer le théorème à $E := A/Ad$ sans invoquer le lemme chinois.

Solution. Avec les notations de l'exercice précédent, on a :

$$E = \bigoplus_{p\in P} Ad'_p/Ad \simeq \prod_{p\in P} A/Ap^{v_p(d)}.$$

Théorème et définition 39. Soit E un module de torsion de type fini. Il existe alors une unique décomposition :

$$E \simeq \prod_{p\in P}\prod_{i\geqslant 1} \frac{A}{Ap^{r_i(p)}}, \tag{21}$$

où, pour chaque $p \in P$, la suite des entiers $r_i(p)$ est décroissante et stationne en 0, et où, pour presque tout $p \in P$, cette suite est identiquement nulle.
Les idéaux $Ap^{r_i(p)}$ tels que $r_i(p) \geqslant 1$ (ou, de manière moins intrinsèque, les éléments $p^{r_i(p)}$ eux-mêmes) sont appelés *diviseurs élémentaires* du A-module E.

Démonstration. L'existence peut se prouver de deux manières différentes. On peut d'abord décomposer chaque facteur cyclique obtenu par le corollaire 36 de la page 44 à l'aide de l'exercice ci-dessus. Pour chaque $p \in P$, on range alors en ordre décroissant les exposants non nuls qui apparaissent (ils sont en nombre fini) et l'on complète la suite de ces exposants par des 0.
On peut également remarquer que le corollaire 36, appliqué à chaque composante E_p, donne une décomposition de la forme $\prod_{i\geqslant 1} \frac{A}{Ap^{r_i(p)}}$. On range les entiers $r_i(p)$ en une suite décroissante. (Si la composante E_p est triviale, on prend tous les $r_i(p)$ nuls.)
L'unicité se déduit sans peine des théorèmes invoqués (voir aussi l'exercice I.6.60 de la page 66), mais il est plus intéressant de montrer comment reconstruire les facteurs invariants à partir des diviseurs élémentaires. Avec les notations du théorème 33 de la page 43, on a ici $r = 0$ et, pour tous les indices i tels que l'un des $r_i(p)$ est non nul :

$$\mathfrak{A}_i = \prod_{p\in P} Ap^{r_i(p)}$$

■

Corollaire 40. Tout module de torsion de type fini est isomorphe à un produit du type :

$$A/Aq_1 \times \cdots \times A/Aq_s,$$

les q_i étant primaires non triviaux (c'est-à-dire puissances d'éléments de P d'exposants non nuls). La suite $(q_1, \ldots, q_s)$ est unique à l'ordre près.

Exercice 25.
(i) Soient p, q, r des éléments premiers deux à deux distincts. Quels sont les diviseurs élémentaires du module dont les facteurs invariants sont pq, p^2qr et $p^3q^2r^2$?

(ii) Quels sont les facteurs invariants du module dont les diviseurs élémentaires sont p, p^2, p^3, p^4, q^2, q^3, q^4, r^3, r^4 ?

Solution. (i) En décomposant chaque facteur invariant en la liste de ses facteurs primaires (*i.e.* puissances de nombres premiers distincts), on trouve la liste : p, p^2, p^3, q, q^2, r, r^2.
(ii) On range sur des lignes successives les puissances décroissantes des éléments premiers, en complétant par des 1 pour avoir des lignes de longueur égale, puis on effectue le produit colonne par colonne : $\begin{matrix} p^4 & p^3 & p^2 & p \\ q^4 & q^3 & q^2 & 1 \\ r^4 & r^3 & 1 & 1 \\ p^4q^4r^4 & p^3q^3r^3 & p^2q^2 & p \end{matrix}$. Les facteurs invariants sont donc : $\mathfrak{A}_1 := Ap^4q^4r^4$, $\mathfrak{A}_2 := Ap^3q^3r^3$, $\mathfrak{A}_3 := Ap^2q^2$ et $\mathfrak{A}_4 := Ap$.

3.2.3 Application aux groupes abéliens

Théorème 41. Les $\mathbb{Z}$-modules de torsion de type fini sont les groupes abéliens finis.

Démonstration. Il est évident qu'un groupe abélien fini est de type fini (il est engendré par ses éléments) et de torsion (cela découle du théorème de Lagrange). Soit G un $\mathbb{Z}$-module de torsion de type fini. Il y a alors un isomorphisme $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \simeq G$, avec $d_1, \ldots, d_k \neq 0$, ce qui implique la finitude de G. ■

Tous les résultats qui suivaet sont de simples traductions de ceux qui précèdent.

Théorème et définition 42. Tout groupe abélien de type fini G est isomorphe à un produit du type :

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z},$$

où les d_i sont des entiers naturels différents de 1 tels que $d_1|d_2|\cdots|d_n$ (certains peuvent être nuls). les d_i sont uniquement déterminés par ces conditions. Ce sont les *facteurs invariants* de G.

Théorème 43. (i) Tout groupe abélien de type fini G est somme directe de son sous-groupe $\mathrm{Tor}(G)$, qui est fini, et d'un groupe abélien libre de rang fini (*i.e.* isomorphe à $\mathbb{Z}^r$, où r est le rang de G).
(ii) Tout groupe abélien sans torsion de type fini est libre.
(iii) Tout groupe abélien fini est somme directe de groupes cycliques.

Exercice 26.
En déduire le résultat suivant, dû à Gauß : dans un groupe abélien fini G, il existe un élément dont l'ordre est le ppcm des ordres de tous les éléments. (Voir aussi les exercices I.6.62 de la page 66 et I.6.63 de la page 66.)

Solution. On écrit $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$ avec $1 \neq d_1|d_2|\cdots|d_n \neq 0$. Les ordres des éléments de G divisent tous d_n et l'élément qui correspond à $(0, \ldots, 0, 1)$ est d'ordre d_n.

Exercice 27.
Démontrer que tous les groupes abéliens d'ordre quadratfrei (c'est-à-dire non divisible par un carré non trivial) sont cycliques.

Solution. Les facteurs invariants ne peuvent être que 1 et l'ordre n donné. (Voir aussi l'exercice I.6.64 de la page 66.)

Théorème 44. Tout groupe abélien fini est isomorphe à un produit du type :

$$\mathbb{Z}/\mathbb{Z}q_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}q_s,$$

les q_i étant primaires non triviaux (c'est-à-dire puissances de nombres premiers d'exposants non nuls). La suite $(q_1, \ldots, q_s)$ est unique à l'ordre près.

Exercice 28.
Combien y a-t-il de groupes abéliens d'ordre 12 ?

Solution. Les suites $(q_1, \ldots, q_s)$ de primaires non triviaux telles que $q_1 \cdots q_s = 12$ sont, à l'ordre près : $(2, 2, 3)$ et $(4, 3)$. Il n'y a donc que deux groupes : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, qui est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$; et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, qui est isomorphe à $\mathbb{Z}/12\mathbb{Z}$. Les deux isomorphismes sont dus au lemme chinois. (Voir aussi l'exercice I.6.65 de la page 66.)

Exercice 29.
Déterminer tous les groupes d'ordre p^2. (On a montré dans le module « Actions de groupes » de L2 que ces groupes sont abéliens.)

Solution. Les seules listes de diviseurs élémentaires possibles sont (p, p) et (p^2), donnant le groupe $(\mathbb{Z}/p\mathbb{Z})^2$ (qui est le groupe additif du corps fini $\mathbb{F}_{p^2}$) et le groupe cyclique $\mathbb{Z}/p^2\mathbb{Z}$.

3.3 Applications à la réduction des endomorphismes

Soient K un corps commutatif (au paragraphe 3.3.2, on le supposera algébriquement clos, puis égal à $\mathbb{C}$) et $A := K[X]$. Nous allons exploiter la principalité de A pour compléter les résultats du paragraphe 1.2.3.

3.3.1 Invariants de similitude d'un endomorphisme

Soient V un K-espace vectoriel de dimension finie n et φ un endomorphisme de V. Le A-module V_φ introduit au paragraphe 1.2.3 est de torsion et de type fini. De plus, la classe de similitude de l'endomorphisme φ détermine la classe d'isomorphie du A-module V_φ et réciproquement. Par ailleurs, si $M \in M_n(K)$ est la matrice de φ dans une base quelconque de V, la classe de similitude de l'endomorphisme φ détermine la classe de similitude de la matrice M et réciproquement.

Définition 9. On appelle *invariants de similitude de l'endomorphisme* $\varphi \in \mathcal{L}_K(V)$ les facteurs invariants du module V_φ (définition 33 de la page 43). On appelle *invariants de similitude de la matrice* $M \in M_n(K)$ les invariants de similitude de l'endomorphisme représenté par M dans une base arbitraire.

D'après les remarques qui précèdent la définition, celle-ci a bien un sens. De plus, les invariants de similitude d'une matrice ou d'un endomorphisme déterminent sa classe de similitude et réciproquement.

Puisque le module de type fini V_φ est de torsion, ses facteurs invariants sont des idéaux principaux engendrés par des polynômes non constants $P_1|\cdots|P_k$, que l'on peut choisir unitaires. Ils sont alors totalement déterminés par les facteurs invariants idéaux, et réciproquement. il est donc d'usage d'appeler invariants de similitude d'une matrice ou d'un endomorphisme les polynômes $P_1, \ldots, P_k$ ainsi définis.

Théorème 45. Toute matrice $M \in M_n(K)$ est semblable à une unique matrice diagonale par blocs dont les blocs sont des matrices compagnons de polynômes unitaires $P_1, \ldots, P_k$ tels que $P_1|\cdots|P_k$:

$$M \sim \begin{pmatrix} C_{P_1} & & 0 \\ & \ddots & \\ 0 & & C_{P_k} \end{pmatrix} \tag{22}$$

Démonstration. On invoque la décomposition de V_φ en modules cycliques, et l'étude des $K[X]$-modules cycliques page 18. ■

Corollaire 46. Le polynôme annulateur de M est P_k. Son polynôme caractéristique est $P_1 \cdots P_k$.

Démonstration. La première assertion découle de la décomposition $V_\varphi \simeq K[X]/<P_1> \times \cdots \times K[X]/<P_k>$. La deuxième a été prouvée en L2. ■

Corollaire 47. Soit L un corps commutatif contenant K. Si deux matrices $M, M' \in M_n(K)$ sont semblables dans $M_n(L)$, elles sont semblables dans $M_n(K)$.

Démonstration. La « forme canonique » du théorème est dans $M_n(K)$, celle obtenue dans le corps L est nécessairement la même. ■

Exercice 30.
Calculer la dimension du commutant de φ. (Utiliser l'exercice I.6.61 de la page 66.)

Solution. On trouve $\sum_{i=1}^{k} (2k - 2i + 1) \deg P_i$.

Le calcul pratique des invariants de similitude repose sur le résultat suivant.

Proposition 48. Soient $\varphi \in \mathcal{L}_K(V)$ et M la matrice de φ dans une base $\mathcal{B} := (e_1, \ldots, e_n)$ de V. On a alors une présentation :

$$K[X]^n \xrightarrow{M - XI_n} K[X]^n \longrightarrow V_\varphi \longrightarrow 0. \tag{23}$$

Démonstration. Le noyau R du morphisme $K[X]^n \to V_\varphi$ correspondant au système générateur $\mathcal{B}$ est formé des n-uplets $(P_1, \ldots, P_n) \in K[X]^n$ tels que $P_1(\varphi)(e_1) + \cdots + P_n(\varphi)(e_n) = 0$. Notons $M := (a_{i,j})$ et $M' := M - XI_n = (a'_{i,j})$, où $a'_{i,j} := a_{i,j} - X\delta_{i,j}$. On a $\varphi(e_j) = \sum a_{i,j} e_i$, donc $\sum a'_{i,j} e_i = 0$, et les colonnes de P' sont dans le noyau R, donc $\operatorname{Im} P' \subset R$.
Pour tout polynôme P, l'égalité $P(Y) - P(X) = (Y - X)Q(X, Y)$ avec $Q \in K[X, Y]$ entraine : $P(M) - P(XI_n) = M'N' = N'M'$, où $N' := Q(M, XI_n)$. Ainsi, les colonnes de $P(M) - P(XI_n)$ sont éléments de R. Autrement dit, pour tout $j \in [\![1, n]\!]$, le vecteur colonne de coefficients $(0, \ldots, P(X), \ldots, 0)$ ($j^{ème}$ position) est congru modulo $\operatorname{Im} M'$ à la j-^{ème} colonne de $P(M)$. On en déduit : $K[X]^n = \operatorname{Im} M' + K^n$. Comme la restriction de $K[X]^n \to V_\varphi$ à K^n est injective (la famille $\mathcal{B}$ est libre sur K), on voit que $R = \operatorname{Im} M'$. ■

Corollaire 49. Les invariants de similitude de φ et de M sont les facteurs invariants de $M - XI_n \in M_n(K[X])$.

Exemple. Pour calculer les invariants de similitude de $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$, on calcule les facteurs invariants de $\begin{pmatrix} a-X & b \\ c & d-X \end{pmatrix} \in M_2(K[X])$, donc ses idéaux de Fitting :
$\mathfrak{F}_1 = <a - X, b, c, d - X>$, de générateur 1 sauf si M est scalaire ; dans ce cas, il vaut $X - a$.
$\mathfrak{F}_2 = <(a - X)(d - X) - bc>$, de générateur le polynôme caractéristique.

Exercice 31.

Calculer les invariants de similitude de $M := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix}$.

Solution. On trouve $\mathfrak{F}_1 = \mathfrak{F}_2 = K[X]$ et $\mathfrak{F}_3 = <\chi_M>$, d'où un unique invariant de similitude χ_M.

La démonstration de la proposition 48 est liée à l'extension des scalaires de A à $A[X]$ (paragraphe 1.3.2). Décrivons ce foncteur pour un anneau A quelconque. Pour tout A-module E, on définit un $A[X]$-module $E[X]$ (c'est notre $E_{(B)}$ lorsque $B := A[X]$) de la manière suivante : c'est le A-module $E^{(\mathbb{N})}$, où l'on écrit $\sum e_i X^i$ la famille à support fini $(e_i)_{i\in\mathbb{N}} \in E^{(\mathbb{N})}$ (exactement comme on l'avait fait pour construire les polynômes sur A à partir de $A^{(\mathbb{N})}$). Ainsi, la multiplication externe peut être décrite par la formule :

$$\left(\sum_{i\in\mathbb{N}} a_i X^i\right)\left(\sum_{j\in\mathbb{N}} e_j X^j\right) := \sum_{k\in\mathbb{N}} \left(\sum_{i+j=k} a_i e_j\right) X^k.$$

Tout morphisme de A-modules $f : E \to F$ s'étend en un morphisme $\overline{f} : E[X] \to F[X]$, en posant $\overline{f}\left(\sum e_i X^i\right) := \sum f(e_i) X^i$.
Par ailleurs, tout endomorphisme φ d'un A-module E permet de définir un $A[X]$-module E_φ (exactement comme on l'a fait au paragraphe 1.2.3 lorsque A est un corps). On a alors une suite exacte de $A[X]$-modules :

$$0 \to E[X] \to E[X] \to E_\varphi \to 0,$$

où la première flèche non triviale est $X\,\mathrm{Id} - \overline{\varphi}$, et oùla seconde flèche non triviale est donnée par la formule : $\sum e_i X^i \mapsto \sum \varphi^i(e_i)$. (Voir aussi l'exercice I.6.77 de la page 67.)

3.3.2 Applications de la décomposition primaire

Pour appliquer les résultats du paragraphe 3.2.2, nous supposerons le corps K algébriquement clos. Dans ce cas, les facteurs premiers distingués (ceux de P) peuvent être choisis de la forme $(X-\lambda)$ et les facteurs primaires de la forme $(X-\lambda)^m$.

La décomposition de V_φ en somme directe de composantes primaires s'exprime sous la forme d'une décomposition de V en somme directe de sous–espaces vectoriels :

$$V = \bigoplus_{\lambda\in\Sigma} V_\lambda.$$

D'après *loc. cit.*, les $X-\lambda$ qui indexent une composante primaire non triviale sont les diviseurs du polynôme annulateur, autrement dit, les valeurs propres de φ. L'ensemble fini Σ des $\lambda\in\mathbb{C}$ tels que la composante V_λ (associée au facteur premier $X-\lambda$) est non triviale est donc le spectre de φ.

Le fait que V_λ est le sous–espace vectoriel sous-jacent à un sous-module signiafie que c'est un sous-espace stable par φ. De plus, on a l'égalité des ensembles sous-jacents :

$$V_\lambda = \bigcup_{m\geqslant 0} V_\varphi\big((X-\lambda)^m\big) = \bigcup_{m\geqslant 0} \operatorname{Ker}(\varphi-\lambda\operatorname{Id}_V)^m,$$

autrement dit, V_λ est le sous-espace caractéristique associé à la valeur propre λ.

Si l'on applique maintenant le théorème de structure à cette composante primaire, on trouve une décomposition en sous-modules : $K[X]/<(X-\lambda)^{m_1}>\times\cdots\times K[X]/<(X-\lambda)^{m_r}>$, à laquelle correspond une décomposition en sous-espaces stables : $V_\lambda = V_{\lambda,m_1}\oplus\cdots\oplus V_{\lambda,m_1}$.

Pour décrire matriciellement un $K[X]$-module V_ψ de la forme $K[X]/<(X-\lambda)^m>$, le plus simple est de choisir la base des $e_i := (X-\lambda)^i \pmod{(X-\lambda)^m}$ pour $0\leqslant i\leqslant m-1$. Les égalités $(X-\lambda)e_i = e_{i+1}$ $(0\leqslant i<m-1)$ et $(X-\lambda)e_{m-1}=0$ se traduisent par $\psi(e_i)=e_{i+1}+\lambda e_i$ $(0\leqslant i<m-1)$ et $\psi(e_{m-1})=\lambda e_{m-1}$. La matrice de ψ dans cette base est donc : $\begin{pmatrix} \lambda & 1 & \dots & 0 & 0\\ 0 & \lambda & \dots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & \lambda & 1\\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$.

La décomposition primaire suivie de la décomposition en modules cycliques, avec choix adéquat d'une base, redonne donc la décomposition de Jordan. Les polynômes caractéristiques $(X-\lambda)^{m_i}$ des blocs de Jordan sont les diviseurs élémentaires de V_φ.

3.3.3 Initiation au calcul fonctionnel

Notons, dans tout ce qui suit, Σ le spectre de l'endomorphisme φ du K-espace vectoriel de dimension finie V ; le corps K est supposé algébriquement clos. Ainsi, l'ensemble des premiers privilégiés de $K[X]$ est $P := \{X - \lambda \mid \lambda \in K\}$ et la décomposition primaire $E = \bigoplus E_p$ de $E := V_\varphi$ se ramène ici à la décomposition en espaces caractéristiques $V = \bigoplus_{\lambda\in\Sigma} V_\lambda$.

Si l'on étend les scalaires de $A := K[X]$ à $S^{-1}A$, on est conduit à la remarque suivante : le morphisme naturel de E_p dans $S^{-1}E_p$ est trivial si $S \cap A \neq \varnothing$; il est bijectif sinon. Puisque $S^{-1}\bigoplus E_p = \bigoplus S^{-1}E_p$, cela signifie que l'espace vectoriel sous-jacent à $S^{-1}E$ est la somme directe des V_λ tels que $S \cap <X - \lambda> = \varnothing$. Réciproquement, cela entraine que, si S ne contient que des polynômes qui ne s'annulent pas sur Σ, alors $S^{-1}A$ opère sur V par la loi externe du $S^{-1}A$-module $S^{-1}V_\varphi$.

Proposition 50. Le morphisme d'algèbres $P \mapsto P(\varphi)$ de $K[X]$ dans $\mathcal{L}_K(V)$ s'étend en un morphisme de $K(X)_\Sigma$ dans $\mathcal{L}_K(V)$, où l'on note $K(X)_\Sigma$ la K-algèbre des fractions rationnelles définies en tout point de Σ.

Concrètement, cela se traduit ainsi : si $R = S/T \in K(X)_\Sigma$, avec $S, T \in K[X]$ et T ne s'annulant pas sur Σ, alors T est premier avec le polynôme minimal P de φ. On écrit : $UT + VP = 1$, d'où $\big(T(\varphi)\big)^{-1} = U(\varphi)$ et l'on pose : $R(\varphi) := S(\varphi)U(\varphi)$. Ainsi, *on a réussi à définir $R(\varphi)$ pour toute fraction rationnelle R qui est définie sur le spectre de φ.*

Précisons ce calcul lorsque le corps K est de caractéristique nulle. La restriction ψ de φ au sous–espace vectoriel V_λ (qui est stable) s'écrit $\psi = \lambda\,\mathrm{Id} + \nu$, où ν est un endomorphisme nilpotent de V_λ. Pour calculer la restriction $R(\psi)$ de $R(\varphi)$ à ce sous-espace, on invoque la formule de Taylor pour $R(\lambda + X)$: le développement limité à l'ordre $d := \dim V_\lambda$ donne (puisque $\nu^d = 0$) :

$$R(\psi) = \sum_{i=0}^{d-1} \frac{1}{i!} R^{(i)}(\lambda)\nu^i.$$

Pour recoller ces restrictions aux sous-espaces caractéristiques, prenons un point de vue matriciel. La matrice $M \in M_n(K)$ étant mise sous forme de Jordan $M = P\,\mathrm{Diag}(D_1, \ldots, D_k)P^{-1}$, on a $R(M) = P\,\mathrm{Diag}\big(R(D_1), \ldots, R(D_k)\big)P^{-1}$ et, si $D_i = \lambda_i I_{d_i} + N_i$, comme $N_i^{d_i} = 0$:

$$R(D_i) = \sum_{j=0}^{d_i-1} \frac{1}{j!} R^{(j)}(\lambda) N_i^j.$$

Lorsque le corps de base est $K := \mathbb{C}$, on peut définir $R(\varphi)$ pour des fonctions R encore plus générales, grâce à l'analyse : penser au cas de l'exponentielle et du logarithme ! Nous remplaçons l'indéterminée X par la variable $z \in \mathbb{C}$ et commençons par le cas d'une série entière $f(z) := \sum a_n z^n$ de rayon de convergence $\rho > 0$. Alors, pour que $\sum a_n \varphi^n$ soit défini, il suffit que tous les modules des valeurs propres soient strictement plus petits que ρ, *i.e.* que le disque ouvert de convergence contienne Σ. Il est par ailleurs nécessaire que tous les modules des valeurs propres soient inférieurs ou égaux à ρ, *i.e.* que le disque fermé de convergence contienne Σ. Ces deux implications ne sont pas exactement réciproques l'une de l'autre, mais nous n'examinerons pas plus précisément ce qui se passe dans les cas limites. Par passage à la limite à partir des polynômes, on vérifie sans peine que, pour deux telles fonctions f et g, on a alors les formules naturelles :

$$(\lambda f + \mu g)(\varphi) = \lambda f(\varphi) + \mu g(\varphi) \quad \text{et} \quad (fg)(\varphi) = f(\varphi) \circ g(\varphi) = g(\varphi) \circ f(\varphi).$$

Autrement dit, la proposition 50 de la page précédente s'étend à la $\mathbb{C}$-algèbre des fonctions holomorphes sur le disque ouvert $\overset{\circ}{D}(0, \rho)$, pourvu que celui-ci contienne Σ.

De même, on peut calculer $f(\varphi)$ en se restreignant à un sous-espace caractéristique V_λ sur lequel φ se restreint en $\psi = \lambda \operatorname{Id} + \nu$, où ν est un endomorphisme nilpotent de V_λ. On retrouve la formule de Taylor tronquée :

$$f(\psi) = \sum_{i=0}^{d-1} \frac{1}{i!} f^{(i)}(\lambda) \nu^i.$$

Matriciellement, si l'on a la réduction de Jordan $M = P \operatorname{Diag}(D_1, \ldots, D_k) P^{-1}$, avec $D_i = \lambda_i I_{d_i} + N_i$ et $N_i^{d_i} = 0$:

$$f(M) = P \operatorname{Diag}\big(f(D_1), \ldots, f(D_k)\big) P^{-1} \quad \text{et} \quad f(D_i) = \sum_{j=0}^{d_i - 1} \frac{1}{j!} f^{(j)}(\lambda) N_i^j.$$

Si l'on a une fonction f holomorphe au voisinage d'un point z_0 non nécessairement nul, voisinage contenant $\overset{\circ}{D}(z_0, \rho)$, et ce dernier disque contenant Σ, il suffit de considérer la fontion $f(z_0 + z)$ pour pouvoir appliquer ce qui précède. Cependant, l'usage des séries entières présente deux inconvénients :

1. Si f est holomorphe sur un ouvert contenant Σ, il n'y a pas nécessairement un disque ouvert contenant Σ et contenu dans cet ouvert. Par exemple, cette méthode ne permet pas d'étendre la détermination principale du logarithme définie sur $\mathbb{C} \setminus \mathbb{R}_-$ pour l'appliquer à un endomorphisme ou une matrice dont i et $-\mathrm{i}$ seraient valeurs propres.
2. Si l'on calcule les développements en série entière de f en divers points, il ne va pas de soi que les différents calculs de $f(\varphi)$ soient compatibles, même si f est donnée globalement.

L'outil magique pour résoudre ces problèmes est l'intégrale de Cauchy. Nous présenterons les calculs sous forme matricielle, mais ils s'appliquent aussi bien aux endomorphismes et même dans un cadre beaucoup plus général (celui des « anneaux normés » de Gelfand, par exemple).

Définition 10. Soit Σ le spectre de $M \in M_n(\mathbb{C})$. L'application :

$$\lambda \mapsto \mathrm{R}(M,\lambda) := (\lambda I_n - M)^{-1} \tag{24}$$

de $\mathbb{C} \setminus \Sigma$ dans $\mathbb{C}$ est appelée *(fonction) résolvante de* M.

Ne pas confondre ce terme avec celui utilisé dans la théorie des équations différentielles (cours de L2). La résolvante est une fonction analytique de $\mathbb{C}\setminus\Sigma$ dans $\mathbb{C}$. En fait, appliquant les relations de Cramer à la matrice $\lambda I_n - M$, on voit que ses coefficients sont rationnels avec pour dénominateur commun le polynôme caractéristique. Si $\lambda_0 \in \mathbb{C} \setminus \Sigma$, il est facile d'obtenir un développement en série entière au voisinage de λ_0 :

$$\mathrm{R}(M,\lambda_0+z) = (\lambda_0 I_n - M + zI_n)^{-1} = \sum_{k\geqslant 0} (-1)^k (\lambda_0 I_n - M)^{-k-1} z^k = \sum_{k\geqslant 0} (-1)^k \mathrm{R}(M,\lambda_0)^{k+1} z^k.$$

> ***Remarque***. Si Σ était vide, on aurait une fonction entière sur $\mathbb{C}$. Il est facile de démontrer qu'elle est nulle à l'infini (par exemple, avec le développement en série au voisinage de ∞, voir l'exercice I.6.79 de la page 68). D'après le théorème de Liouville, elle serait identiquement nulle, ce qui contredit sa définition comme inverse. Le spectre n'est donc jamais vide, ce qui constitue une nouvelle démonstration du théorème de d'Alembert-Gauß.

Soit f une fonction holomorphe sur un ouvert Ω de $\mathbb{C}$. Pour tout lacet de classe $\mathcal{C}^1$ dans $\Omega' := \Omega \setminus \Sigma$, on notera :

$$f_\gamma(M) := \frac{1}{2\mathrm{i}\pi} \int_\gamma f(\lambda) R(M,\lambda)\, d\lambda. \tag{25}$$

De la théorie de Cauchy découle que $f_\gamma(M)$ ne dépend en fait que de la classe d'homotopie du lacet γ dans Ω'. Avec les notations précédentes, il est clair que l'on a :

$$f_\gamma(M) = P\,\mathrm{Diag}\big(f_\gamma(D_1),\dots,f_\gamma(D_k)\big)P^{-1}.$$

On est donc ramené au calcul de $f_\gamma(D)$, où $D = \lambda I_d + N$, avec $N^d = 0$. La formule de Cauchy donne :

$$f_\gamma(D) = \mathrm{Ind}_\lambda(\gamma) \sum_{i=0}^{d} \frac{1}{i!} f^{(i)}(\lambda) D^i.$$

Théorème et définition 51. On suppose que Ω est un ouvert connexe contenant Σ Pour tout lacet γ dans Ω' tournant une fois positivement autour de Σ, la valeur de $f_\gamma(M)$ est la même. Sur tout disque ouvert de Ω où f est développable en une série entière, l'application de cette série à M a pour somme $f_\gamma(M)$. La matrice obtenue est notée $f(M)$.

On a ainsi étendu la proposition 50 de la page 55 à la $\mathbb{C}$-algèbre des fonctions holomorphes sur Ω.

EXERCICE TYPE CORRIGÉ

Dualité. Si l'on tente d'adapter la théorie de la dualité des espaces vectoriels aux modules en posant $E^* := \mathrm{Hom}_A(E, A)$, on rencontre des difficultés. Par exemple, il est facile de voir que, pour un module de torsion E sur un anneau intègre, toute forme linéaire s'annule (argument : $ax = 0 \Rightarrow af(x) = 0 \Rightarrow f(x) = 0$), donc $E^* = \{0\}$. On peut définir un morphisme canonique de M dans M^{**}, mais il n'est en général ni injectif ni surjectif. Même pour un module libre de rang fini E, l'orthogonalité (module « Algèbre bilinéaire » de L2) n'induit pas une bijection entre sous-modules de E et seux de E^* (exercice I.6.4 de la page 60). Une approche valable pour les modules de torsion de type fini est proposée à l'exercice I.6.0.

I.6.0 Soit A un anneau principal de corps des fractions A. Pour tout A-module de torsion de type fini E, on définit son *dual* en posant : $\hat{E} := \mathrm{Hom}_A(E, K/A)$. Le but de l'exercice est de montrer qu'il y a bien « dualité ».

(i) Vérifier que le module K/A est de torsion et *divisible*, c'est-à-dire que l'endomorphisme $x \mapsto dx$ est surjectif pour $d \neq 0$.

(ii) Pour un module cyclique $E := Ax$ d'annulateur Ad, montrer que $\hat{E}$ s'identifie à $(K/A)(d) = Ad^{-1}/A \simeq A/Ad$.

(iii) Expliciter un isomorphisme de $\widehat{E_1 \times E_2}$ sur $\hat{E}_1 \times \hat{E}_2$.

(iv) En déduire que, pour tout module de torsion de type fini E, on a $\hat{E} \simeq E$.

(v) Définir, par analogie avec la bidualité des espaces vectoriels un morphisme $E \to \hat{\hat{E}}$.

(vi) Soit $x \in E := A/Ad$ non nul. Montrer qu'il existe $\varphi \in \hat{E}$ tel que $\varphi(x) \neq 0$. En déduire que le morphisme $E \to \hat{\hat{E}}$ est injectif.

(vii) Dans le cas où $A := \mathbb{Z}$ ou $A := K[X]$, montrer que ce morphisme est bijectif. (Voir aussi les exercices I.6.73 de la page 67 et I.6.74 de la page 67.)

Solution. (i) Soit $x := \dfrac{a}{b} \pmod A \in K/A$. Alors $ax = 0$ (donc K/A est de torsion) et $x = dy$, où $y := \dfrac{a}{db} \pmod A \in K/A$ (donc K/A est divisible).

(ii) Pour tout module F, choisir $\varphi : Ax \to F$ revient à choisir $y := \varphi(x) \in F$ tel que $dy = 0$, et $\mathrm{Hom}(Ax, F)$ s'identifie à $F(d)$. (C'est un cas particulier de la discussion de la page 24.) L'élément $x := r \pmod A \in K/A$ vérifie $dx = 0$ si, et seulement si, $dr \in A$, d'où $(K/A)(d) = Ad^{-1}/A$, qui est isomorphe à A/Ad par passage au quotient de l'isomorphisme $a \mapsto ad$ de A sur Ad.

(iii) Soit $\varphi : \widehat{E_1 \times E_2} \to K/A$. Alors $\varphi_1 : x \mapsto \varphi(x, 0)$ et $\varphi_2 : y \mapsto \varphi(0, y)$ donnent $(\varphi_1, \varphi_2) \in \hat{E}_1 \times \hat{E}_2$. (C'est un cas particulier de l'exercice I.6.10 de la page suivante.)

(iv) L'isomorphisme $\hat{E} \simeq E$ est vrai pour tout module cyclique (question (ii)) et passe au produit (question (iii)). D'après le corollaire 36 de la page 44, il est vrai pour tout module de torsion de type fini. *Mais cet isomorphisme n'est pas canonique.* Il dépend en effet du choix d'une décomposition en facteurs cycliques. De plus, même si E est cyclique, l'isomorphisme dépend du choix d'un générateur.

(v) À tout $x \in E$, on associe le morphisme $ev_x : \varphi \mapsto \varphi(x)$ de $\hat{E}$ dans K/A. Il est clair que $x \mapsto ev_x$ est un morphisme $E \to \hat{\hat{E}}$.

(vi) Identifions E à un produit de modules cycliques. Si $x \in E$ est non nul, son image y par l'une des projections sur ces modules est non nulle. Il suffit donc de vérifier que si $y \in A/Ad$ est non nul, il existe $\psi : A/Ad \to K/A$ tel que $\psi(y) \neq 0$. Mais il suffit de considérer un isomorphisme de A/Ad sur $Ad^{-1}/A \subset K/A$.

Soit maintenant x un élément du noyau de $E \to \hat{\hat{E}}$. Cela signifie que, pour tout $\varphi \in \hat{E}$, on a $\varphi(x) = 0$. D'après ce que l'on vient de voir, cela n'est possible que si $x = 0$.

(vii) Dans le cas où $A := \mathbb{Z}$, on a une application injective entre deux groupes finis de même cardinal : elle est donc bijective. Dans le cas où $A := K[X]$, on a une application linéaire injective entre deux espaces vectoriels de même dimension : elle est donc bijective. (Pour le cas général, voir l'exercice I.6.73 de la page 67.)

POUR ALLER PLUS LOIN

Exercices sur la section 1

I.6.1 Quel est le noyau du morphisme de groupes de A dans $\mathrm{End}_A(E)$ qui, à $a \in A$, associe l'homothétie $x \mapsto ax$? Que signifie alors la notion de module fidèle ?

I.6.2 $*$ Soient A un anneau local d'idéal maximal $\mathfrak{M}$ (voir les exercices du module « Compléments d'algèbre » du cours de L2) et E un A-module de type fini. Montrer que, si $E = \mathfrak{M}E$, alors $E = \{0\}$. En déduire plus généralement que, si F est un sous-module de E tel que $E = F + \mathfrak{M}E$, alors $E = F$ (*lemme de Nakayama*).

I.6.3 Soient F, G, H des sous-modules de E. A-t-on $F \cap (G + H) = (F \cap G) + H$?

I.6.4 Soit A un anneau intègre. On dit que le sous-module $F \subset E$ est *saturé* si :

$$\forall a \in A \setminus \{0\}\ ,\ \forall x \in E\ ,\ ax \in F \Longrightarrow x \in F.$$

Montrer que F est un sous-module saturé si, et seulement si, E/F est sans torsion. Montrer que $\mathrm{Tor}_A(E)$ est un sous-module saturé. Montrer que tout sous-module de A^n défini par un système d'équations linéaires : $a_1x_1 + \cdots + a_nx_n = 0$, $b_1x_1 + \cdots + b_nx_n = 0 \ldots$ est saturé. En déduire un exemple de sous-module de A^n qui ne peut être défini par un système d'équations linéaires. Ce sous-module est-il une intersection de noyaux de formes linéaires ?

I.6.5 Soit A un anneau intègre et soit E un module de torsion de type fini. Montrer qu'alors $\mathrm{Ann}_A(E) \neq \{0\}$.

I.6.6 Soient A un anneau intègre et K son corps des fractions. Reprendre l'exercice 4 de la page 10 pour le A-module K/A. Ce module est-il de type fini ?

I.6.7 Soit $\mathcal{Y} := (y_1, \ldots, y_p)$ une famille d'éléments de E qui engendre le sous-module $F \subset E$ et soit $Q \in M_{p,n}(A)$. Montrer que la famille $\mathcal{Y}' := \mathcal{Y}Q$ engendre un module $F' \subset F$. Si $Q \in GL_p(A)$, montrer que $F' = F$.

I.6.8 Montrer que le sous-module diagonal de A^I (exemples de la page 6) est isomorphe à A. (On suppose I non vide.)

I.6.9 (i) Vérifier que, si $u : F_1 \to F_2$ est injectif, $f \mapsto u \circ f$ de $\mathrm{Hom}_A(E, F_1)$ dans $\mathrm{Hom}_A(E, F_2)$ l'est aussi. Examiner le cas où $A := \mathbb{Z}$, $E := \mathbb{Z}/2\mathbb{Z}$, $F_1 := \mathbb{Z}$ et $F_2 := \mathbb{Z}/2\mathbb{Z}$.
(ii) Vérifier que, si $u : E_1 \to E_2$ est surjectif, $f \mapsto f \circ u$ de $\mathrm{Hom}_A(E_2, f)$ dans $\mathrm{Hom}_A(E_1, F)$ l'est aussi. Examiner le cas où $A := \mathbb{Z}$, $F := \mathbb{Z}$, $E_1 := 2\mathbb{Z}$ et $E_2 := \mathbb{Z}$.

I.6.10 (i) Définir un isomorphisme naturel entre $\mathrm{Hom}_A(E, \prod F_i)$ et $\prod \mathrm{Hom}_A(E, F_i)$.
(ii) Définir un isomorphisme naturel entre $\mathrm{Hom}_A(\coprod E_i, F)$ et $\prod \mathrm{Hom}_A(E_i, F)$. Qu'obtient-on en prenant $E_i := A$ pour tout i ?

I.6.11 Soient $E_i' \subset E_i$ des sous-modules. Calculer $\coprod E_i \cap \prod E_i'$.

I.6.12 Identifier $\mathrm{Hom}_A(A/\mathfrak{A}, F)$ à un sous-module de F. Calculer $\mathrm{End}_A(A/\mathfrak{A})$. À quelle condition (nécessaire et suffisante) a-t-on $A/\mathfrak{A} \simeq A/\mathfrak{A}'$? Établir une bijection entre les idéaux de A et les classes d'isomorphie de modules cycliques.

I.6.13 Tout morphisme entre deux modules simples est soit trivial soit un isomorphisme.

I.6.14 La famille (x_i) est libre si, et seulement si, les x_i ne sont pas de torsion et les Ax_i sont en somme directe.

I.6.15 $*$ Soit $x \in E$. Pour qu'il existe une forme linéaire $\pi : E \to A$ telle que $\pi(x) = 1$, il faut, et il suffit, que x ne soit pas de torsion (*i.e.* $\mathrm{Ann}_A(x) = 0$) et que Ax soit facteur direct de E.

I.6.16 $*$ Montrer que l'idéal I est facteur direct de A si, et seulement s'il est engendré par un idempotent.

I.6.17 Soit $f : E \to F$ un morphisme et soient $E' \subset E$ et $F' \subset f(E')$. Définir un isomorphisme $E'/f^{-1}(F') \simeq f(E')/F'$.

I.6.18 Soient E_1, E_2 des sous-modules de E. Définir un isomorphisme de $\dfrac{E_1 \times E_2}{E_1 \cap E_2}$ sur $E_1 + E_2$.

I.6.19 Soit $\varphi \in \mathcal{L}_K(V)$, où V est de dimension finie, donc V_φ de torsion de type fini. Que représente alors l'annulateur de V_φ ?

I.6.20 (i) Soit $A := K[X]/<P>$. Qu'est-ce qu'un A-module ?
(ii) Soit $A := K[X_1, \ldots, X_n]$. Qu'est-ce qu'un A-module ?

I.6.21 Quels sont les sous $K[X]$-modules de $\prod K[X]/(X - a_i)$?

I.6.22 Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Soit $(b_i)_{i\in I}$ un système générateur du A-module B et $(x_j)_{(j\in J}$ un système générateur du B-module E. Montrer que $(b_i x_j)_{(i,j)\in I\times J}$ est un système générateur du A-module $E_{[B]}$.

I.6.23 Vérifier que les opérations d'extension et de restriction des scalaires ne sont pas réciproques l'une de l'autre dans les cas $B := A/\mathfrak{A}$ et $B := S^{-1}A$.

I.6.24 $*$ (i) Montrer que, si $E \to F$ est surjectif, alors $E/\mathfrak{A}E \to F/\mathfrak{A}F$ l'est aussi.
(ii) En déduire que, si $A^n \to A^p$ est surjectif, alors $n \geqslant p$. Interpréter en termes de familles génératrices de A^p.
(iii) Donner un exemple où $E \to F$ est injectif, mais pas $E/\mathfrak{A}E \to F/\mathfrak{A}F$.

I.6.25 $**$ (i) On note $B := A/\mathfrak{A}$. Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte courte de A-modules. Montrer que, par extension des scalaires, on obtient une suite exacte : $E'_{(B)} \to E_{(B)} \to E''_{(B)} \to 0$. On dit que ce foncteur est *exact à droite*.
(ii) Montrer que, si la suite de départ est scindée, la suite obtenue peut être complétée à gauche et qu'elle est scindée.

I.6.26 $**$ On note $B := S^{-1}A$. Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte courte de A-modules. Montrer que, par extension des scalaires, on obtient une suite exacte : $0 \to E'_{(B)} \to E_{(B)} \to E''_{(B)} \to 0$. On dit que ce foncteur est *exact*.

I.6.27 $*$ (i) Montrer que si l'on applique le foncteur covariant $\mathrm{Hom}_A(E, -)$ à une suite exacte courte $0 \to F' \to F \to F'' \to 0$, on obtient une suite exacte : $0 \to \mathrm{Hom}_A(E, F') \to \mathrm{Hom}_A(E, F) \to \mathrm{Hom}_A(E,$
On dit que ce foncteur est *exact à gauche.*
(ii) Montrer que si l'on applique le foncteur contravariant $\mathrm{Hom}_A(-, F)$ à une suite exacte courte $0 \to E' \to E \to E'' \to 0$, on obtient une suite exacte : $0 \to \mathrm{Hom}_A(E'', F) \to \mathrm{Hom}_A(E, F) \to \mathrm{Hom}_A(E', F)$.
On dit que ce foncteur est *exact à gauche.*
(iii) Montrer dans chaque cas que, si l'on part d'une suite exacte scindée, la suite exacte obtenue peut être prolongée à droite en une suite exacte courte.

I.6.28 $**$ Soit E un module qui vérifie la propriété suivante : toute surjection $F \to E \to 0$ est scindée (*i.e.* admet une section). Montrer que E est facteur direct d'un module de la forme $A^{(I)}$. Montrer la réciproque. On dit que E est *projectif*. Montrer qu'alors le foncteur covariant $\mathrm{Hom}_A(E, -)$ est exact (il transforme suites exactes courtes en suites exactes courtes).

Exercices sur la section 2

I.6.29 $*$ Soit E un module libre de rang n. Montrer que tout système générateur de n éléments est une base de E.

I.6.30 $**$ (i) Soient A un anneau commutatif et $M \in M_{n,n+1}(A)$. On suppose que M contient un mineur $n \times n$ de déterminant non nul. Montrer que les colonnes de M sont liées.
(ii) Soit $r \leqslant n$ maximum tel qu'il existe un mineur $r \times r$ de déterminant non nul. Soit $M' \in M_{n,r+1}(A)$ la matrice obtenue en conservant les r colonnes qui interviennent dans ce mineur et une autre colonne. Montrer que les colonnes de M' sont liées.
(iii) En déduire que toute famille libre d'un module libre de rang n a au plus n éléments. Que peut-on dire des familles libres de n éléments ?

I.6.31 $*$ (i) Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte courte. On suppose E de type fini. Montrer que E'' est de type fini.
(ii) On suppose E' et E'' de type fini. Montrer que E est de type fini.

I.6.32 (i) On se donne deux morphismes $f : L \to E$ et $g : F \to E$. On suppose L libre et g surjectif. Définir un morphisme $u : L \to F$ tel que $f = g \circ u$.
(ii) On se donne deux morphismes $f : L \to M$ et $g : F \to E$. On suppose L libre et g surjectif. Pour tout $v : M \to E$, définir un morphisme $u : L \to M$ tel que $v \circ f = g \circ u$. Vérifier que $u\big(\operatorname{Ker} f\big) \subset \operatorname{Ker} g$.

I.6.33 $**$ (i) On se donne deux suites exactes : $L_2 \xrightarrow{f_2} L_1 \xrightarrow{f_1} E \to 0$ et $E_2 \xrightarrow{g_2} E_1 \xrightarrow{g_1} E \to 0$. On suppose L_1 et L_2 libres de rang fini. Construire successivement $u_1 : L_1 \to E_1$ et $u_2 : L_2 \to E_2$ tels que le diagramme suivant est commutatif :

$$\begin{array}{ccccccc} L_2 & \xrightarrow{f_2} & L_1 & \xrightarrow{f_1} & E & \longrightarrow & 0 \\ \downarrow{\scriptstyle u_2} & & \downarrow{\scriptstyle u1} & & \downarrow{\scriptstyle \mathrm{Id}_E} & & \downarrow \\ E_2 & \xrightarrow{g_2} & E_1 & \xrightarrow{g_1} & E & \longrightarrow & 0 \end{array}$$

(ii) Montrer que $E_1 = \operatorname{Im} u_1 + \operatorname{Im} g_2$, et en déduire un morphisme surjectif $\operatorname{Im} g_2 \to E_1/\operatorname{Im} u_1$, dont le noyau est $\operatorname{Im} g_2 \cap \operatorname{Im} u_1$.
(iii) Calculer le noyau du morphisme composé $E_2 \to E_1/\operatorname{Im} u_1$.
(iv) On suppose g_2 injectif. Démontrer que E_2 est de type fini.
(v) Déduire de ce qui précède que, si E est de présentation finie, le module des relations de tout système générateur fini est de type fini.

I.6.34 Soient $M, N \in M_{p,n}(A)$ deux matrices équivalentes. Expliciter un isomorphisme de A^n/MA^p sur A^n/NA^p.

I.6.35 Démontrer que la suite des idéaux déterminantiels $\mathfrak{D}_k(M)$ est décroissante et que la suite des idéaux de Fitting $\mathfrak{F}_k(E)$ est croissante.

I.6.36 (i) Donner une présentation du $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ avec une matrice dans $M_1(\mathbb{Z})$.
(ii) Si $n = pq$ avec $p \wedge q = 1$, utiliser le lemme chinois pour donner une présentation avec une matrice dans $M_2(\mathbb{Z})$.
(iii) Calculer les idéaux de Fitting par les deux présentations.

I.6.37 $*$ Donner une présentation de l'idéal $<X, Y>^n$ de $K[X, Y]$. Calculer les idéaux de Fitting.

I.6.38 Démontrer le théorème 18 de la page 32 en utilisant le critère (ii) pour la première implication et le critère (i) pour l'implication réciproque.

I.6.39 Dans un anneau noetherien intègre, tout élément non nul et non inversible est produit d'irréductibles.

I.6.40 Montrer que l'anneau $\mathcal{C}(\mathbb{R},\mathbb{R})$ n'est pas noetherien.

I.6.41 Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte. Démontrer que E est artinien si, et seulement si, E' et E'' le sont.

I.6.42 Soit φ un endomorphisme injectif d'un module artinien E. Montrer que φ est bijectif. En déduire que tout morphisme injectif entre des modules artiniens isomorphes est bijectif.

I.6.43 $**$ (i) On appelle *longueur* $\ell(E)$ *d'un module* E la borne supérieure des entiers n tels qu'il existe une suite *strictement* croissante $E_0 \subset \cdots \subset E_n$ de sous-modules de E. Quels sont les modules de longueur 0 ? de longueur 1 ?
(ii) Montrer que E est de longueur finie si, et seulement s'il est artinien et noetherien.
(iii) Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte. Montrer que $\ell(E) = \ell(E') + \ell(E'')$.

I.6.44 $**$ Soit E un module de longueur finie. On dit qu'une suite strictement croissante $E_0 \subset \cdots \subset E_n$ est *maximale* si l'on ne peut y insérer (à l'intérieur, à gauche ou à droite) un nouveau sous-module. Montrer que, pour une telle suite, $E_0 = 0$, $E_n = E$, les E_{i+1}/E_i sont simples et $n = \ell(E)$. Réciproque ?

I.6.45 Démontrer que toute algèbre de dimension finie sur un corps est un anneau noetherien et artinien.

I.6.46 $*$ Démontrer que tout anneau artinien intègre est un corps.

I.6.47 $**$ Soit A un anneau noetherien. Démontrer que $A[[X]]$ est noetherien.

I.6.48 Soit A une K-algèbre. On dit qu'elle est de type fini s'il existe $x_1, \ldots, x_n \in A$ tels que A est la plus petite K-algèbre contenant les x_i. Montrer que cela équivaut à la condition suivante : l'unique morphisme de $K[X_1, \ldots, X_n]$ dans A tel que $X_i \mapsto x_i$ (modules sur les polynômes de L2) est surjectif.

Exercices sur la section 3

Dans tous les exercices qui suivent, l'anneau A est principal.

I.6.49 Déduire directement (c'est-à-dire sans invoquer les résultats du paragraphe 2.2.1) du théorème 27 de la page 37 que tout sous-module d'un module de type fini sur un anneau principal est lui-même de type fini.

I.6.50 (i) Appliquer le théorème 28 de la page 37 à $L := \mathbb{Z}^n$ et à $R := \mathbb{Z}(a_1, \dots, a_n)$.
(ii) Appliquer le théorème 28 de la page 37 à $L := \mathbb{Z}^2$ et à $R := \mathrm{Ker}\big((x,y) \mapsto (y - ax) \pmod p\big)$.

I.6.51 $**$ Définir un algorithme de pivot pour un anneau principal quelconque. Outre les permutations, on s'autorise les transformations de la forme $\begin{cases} L_i \leftarrow aL_i + bL_j, \\ L_j \leftarrow cL_i + dL_j, \end{cases}$ où $ad - bc \in A^*$. En déduire le théorème 30 de la page 39.

I.6.52 Quels sont les facteurs invariants de $A(a,b) + A(c,d) \subset A^2$?

I.6.53 Avec les notations du théorème 28 de la page 37, montrer que le sous-module $Ae_1 \oplus Ae_k$ de L ne dépend que de R. Est-il vrai que la famille $(e_1, \dots, e_k)$ ne dépend que de R ?

I.6.54 Soit L un module libre de rang fini. Montrer que le *contenu* de $x \in L$, c'est-à-dire le pgcd de ses coordonnées dans une base, est indépendant du choix de la base.

I.6.55 Si R est un supplémentaire de Aa dans le module libre L de rang n, les facteurs invariants de R dans L sont les $(n-1)$ idéaux $A, \dots, A$.

I.6.56 Quel est le lien entre le lemme 37 de la page 45 et le lemme des noyaux du module « Réduction des matrices » de L2 ?

I.6.57 Montrer que le module K/A admet un sous-module exactement dans chaque classe d'isomorphie de module cyclique.

I.6.58 $*$ (i) Montrer que le module $(K/A)_p$ admet pour sous-modules propres les Ap^{-n}/A et eux seuls. en déduire qu'il est artinien et non noetherien.
(ii) Le module K/A est artinien (resp. noetherien) si, et seulement si, A n'a qu'un nombre fini d'idéaux premiers (resp. est un corps).

I.6.59 $**$ Étudier les foncteurs qui à E associent $E(a)$, E_p, $\mathrm{Tor}_A(E)$. Sont-ils exacts ?

I.6.60 $**$ (i) Soit E un module de torsion de type fini. Pour tout premier p, et pour tout entier n, montrer que $\dfrac{p^n E}{p^{n+1}E}$ s'identifie à un espace vectoriel de dimension finie sur le corps A/Ap.
(ii) Calculer cette dimension lorsque E est de la forme (21), page 48.
(iii) En déduire une nouvelle preuve de l'unicité des diviseurs élémentaires, puis une preuve de l'unicité des facteurs invariants qui ne passe pas par les idéaux de Fitting.

I.6.61 $*$ Montrer que le module des endomorphismes d'un module de torsion de type fini de facteurs invariants $Ad_1, \ldots, Ad_k$ tels que $d_1 | \cdots | d_k$ est isomorphe à $\prod (A/Ad_i)^{2k-2i+1}$.

I.6.62 Montrer que le résultat de l'exercice 26 de la page 50 peut être en défaut pour un groupe fini non abélien.

I.6.63 $*$ Déduire de l'exercice 26 de la page 50 que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

I.6.64 Reprendre l'exercice 27 de la page 50 en utilisant les diviseurs élémentaires.

I.6.65 Reprendre l'exercice 28 de la page 50 en utilisant les facteurs invariants.

I.6.66 Déterminer tous les groupes abéliens d'ordre $n \leqslant 15$.

I.6.67 $*$ Déterminer la décomposition primaire du groupe $\mathbb{Q}/\mathbb{Z}$ et du groupe $\mathrm{Tor}(\mathbb{C}^*)$.

I.6.68 $**$ (i) Soit G un groupe abélien de torsion égal à sa composante de p-torsion G_p. On suppose que, pour tout $n \geqslant 0$, le groupe G contient un seul sous-groupe d'ordre p^n. Démontrer que G_p est isomorphe à la composante de p-torsion de $\mathbb{Q}/\mathbb{Z}$.
(ii) Soit K un corps algébriquement clos de caractéristique nulle. Démontrer que le groupe $\mathrm{Tor}(K^*) = \mu_\infty(K)$ des racines de l'unité dans K est isomorphe à $\mathbb{Q}/\mathbb{Z}$.
(iii) Que dire si K est de caractéristique $p > 0$?

I.6.69 $**$ Soit I un A-module de torsion divisible (voir l'exercice I.6.0 de la page 58). Soient $E' \subset E$ des A-modules. Montrer que tout morphisme $E' \to I$ se prolonge en un morphisme $E \to I$. (On dit que I est un *module injectif*.)

I.6.70 $**$ (i) Pour $a \in A \setminus \{0\}$, montrer que A/Aa n'a qu'un nombre fini de sous-modules.
(ii) À l'aide de l'exercice I.6.43 de la page 64, en déduire que les A-modules artiniens et noetheriens sur A sont exactement les A-modules de torsion et de type fini.

I.6.71 Montrer que le $K[X]$-module $\big(K[X]/(X-a)\big)^2$ est artinien et noetherien, mais qu'il admet une infinité de sous-modules si K est infini.

I.6.72 $*$ Calculer la longueur de A/Ap^n, de A/Aa, d'un module de torsion de type fini.

I.6.73 $**$ Montrer que tout endomorphisme injectif d'un module de torsion de type fini est bijectif. En déduire que le morphisme $E \to \hat{\hat{E}}$ de l'exercice I.6.0 de la page 58 est un isomorphisme quelque soit l'anneau principal A.

I.6.74 $**$ Montrer qu'en associant à un module de torsion de type fini E son dual $\hat{E}$, on définit un foncteur contravariant exact (*i.e.* qui transforme une suite exacte en une suite exacte).

I.6.75 $*$ Soit G un groupe abélien fini. On appelle *caractère* de G un morphisme de groupes de G dans $\mathbb{C}^*$. Montrer que les caractères forment (pour la multiplication) un groupe abélien isomorphe au $\mathbb{Z}$-module $\hat{G} := \mathrm{Hom}_A(G, \mathbb{Q}/\mathbb{Z})$. Traduire dans ce cadre les résultats des exercices I.6.73, I.6.0 de la page 58 et I.6.74.

I.6.76 Calculer les invariants de similitude de $M := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

I.6.77 $**$ Montrer que l'image de l'endomorphisme $X^d \,\mathrm{Id} - \overline{\varphi}^d$ de $E[X]$ admet comme supplémentaire *en tant que A-module* le sous A-module : $E_{d-1}[X] := \sum_{i=0}^{d-1} EX^i$. Pour tout $j \in \mu_d$ (racines $d^{\,èmes}$ de l'unité), soit $P_j(T,X) := \dfrac{X^d - T^d}{X - jT}\cdot$ Vérifier que $V \mapsto \sum_{j\in\mu_d} d(j\varphi)^{d-1} P_j(\varphi, X) V(j\varphi)$ est un projecteur sur ce supplémentaire.

I.6.78 Soit f une application quelconque de $X \subset K$ dans K. Soit $M = P\,\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)P^{-1}$. On suppose que $\{\lambda_1, \ldots, \lambda_n\} \subset X$. Montrer que, si l'on pose $f(M) := P\,\mathrm{Diag}\big(f(\lambda_1), \ldots, f(\lambda_n)\big)P^{-1}$, le résultat ne dépend en effet que de M et non de la diagonalisation choisie.

I.6.79 (i) Démontrer les relations suivantes concernant la résolvante :

$$\mathrm{R}(\varphi,\lambda)-\mathrm{R}(\varphi,\mu)=(\mu-\lambda)\mathrm{R}(\varphi,\lambda)\mathrm{R}(\varphi,\mu)=(\mu-\lambda)\mathrm{R}(\varphi,\mu)\mathrm{R}(\varphi,\lambda).$$

(ii) Donner le développement en série de $\mathrm{R}(\varphi,\lambda)$ au vosinage de ∞.

I.6.80 $*$ Comment calculer $f_\gamma(M)$ à partir de $f(M)$?

INDICATIONS

I.6.1 C'est $\mathrm{Ann}_A(M)$.

I.6.2 Appliquer la proposition 1 de la page 8.

I.6.3 Oui si, et seulement si, $H \subset F$.

I.6.5 Si $x_1, \ldots, x_n$ sont des générateurs, $\mathrm{Ann}_A(E) = \bigcap \mathrm{Ann}_A(x_i)$.

I.6.6 Si A n'est pas un corps, pour voir que l'annulateur est trivial, remarquer que $dK \subset A$ avec $d \neq 0$ entraine $d \in A^*$.

I.6.7 On a $F' = \mathcal{Y}'A^p = \mathcal{Y}QA^p \subset \mathcal{Y}A^p = F$. Si Q est inversible, $QA^p = A^p$.

I.6.19 C'est l'idéal engendré par le polynôme minimal de φ.

I.6.30 (i) Si l'on note C_j la $j^{\text{ème}}$ colonne de M et D_j le déterminant de M privé de cette colonne, on déduit des formules de Cramer que $\sum(-1)^j d_j C_j = 0$.

I.6.31 (i) L'image d'une famille génératrice de E est génératrice.
(ii) En juxtaposant une famille génératrice de E' au relèvement d'une famille génératrice de E'', on obtient une famille génératrice de E.

I.6.32 Si (e_i) est une base de L, il suffit de prescrire les $u(e_i)$.

I.6.33 (i) Appliquer deux fois l'exercice I.6.32 de la page 63.
(ii) Si $x \in E_1$, écrire $g_1(x)$ sous la forme $f_1(y)$ et en déduire que $x - u_1(y) \in \mathrm{Ker}\, g_1 = \mathrm{Im}\, g_2$.
(iii) Par une démarche analogue (« diagram chasing », ou « chasse au lion ») on trouve $\mathrm{Ker}\, g_2 + \mathrm{Im}\, u_2$.
(iv) Lui appliquer l'exercice I.6.31 de la page 63.

I.6.36 Les matrices sont (n) (idéaux déterminantiels : $n\mathbb{Z}$) et $\mathrm{Diag}(p, q)$ (idéaux déterminantiels : $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ et $pq\mathbb{Z} = n\mathbb{Z}$). Idéaux de Fitting : $n\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Z}$ ...

I.6.37 Générateurs : $(X^{n-i}Y^i)_{0 \leqslant i \leqslant n}$.
Relations : les $(0, \ldots, Y, -X, \ldots, 0)$.
Idéaux déterminantiels : $\mathfrak{D}_k(M) = <X, Y>^k$.

I.6.39 Sinon, il existerait un contre-exemple a tel que Aa est maximal.

I.6.40 Considérer la suite des idéaux $<|x|^{1/n}>$.

I.6.41 Même méthode que pour les anneaux noetheriens.

I.6.42 Considérer la suite des $\mathrm{Im}\, \varphi^n$.

I.6.43 (ii) Si E est artinien et noetherien, pour montrer qu'il est de longueur finie, considérer $F \subset E$ le plus petit possible qui ne l'est pas et $G \subset F$ le plus grand possible tel que F/G ne l'est pas, puis trouver une contradiction.
(iii) Pour montrer que $\ell(E) \leqslant \ell(E') + \ell(E'')$, invoquer le lemme 19 de la page 33.

I.6.46 Considérer la suite des idéaux $<x^n>$.

I.6.47 Introduire $\mathfrak{A}_n := \{a \in A \mid \exists a X^n + \cdots \in \mathfrak{A}\}$, mais où les $\cdots$ désignent des termes de degrés supérieurs.

I.6.51 L'invariant de boucle est le minimum des *tailles* des coefficients non nuls, la taille d'un élément de A étant le nombre total de facteurs premiers dans sa décomposition.

I.6.53 Le relier à $\mathrm{Tor}_A(L/R)$.

I.6.54 S'inspirer de la proposition 32 de la page 41.

I.6.60 La dimension demandée est égale au nombre d'indices i tels que $r_i(p) > n$.

I.6.61 Le module des morphismes de A/Ad dans $\prod A/Ad'$ est isomorphe à $A/A\delta$, où $\delta := d \wedge d'$.

I.6.63 Il y a dans K^* au plus d éléments d'ordre divisant d.

I.6.67 Le groupe $\mathrm{Tor}(\mathbb{C}^*)$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$.

I.6.68 Construire une suite d'éléments $x_n \in G$ tels que $x_0 = 1$, $x_n^p = x_{n-1}$ et en déduire des isomorphismes *compatibles* $p^{-n} \pmod{Z} \mapsto x_n$ de $p^{-n}\mathbb{Z}/\mathbb{Z}$ sur $G(p^n)$.

I.6.69 Commencer par le cas où $E = E' + Ax$, en s'inspirant de l'exercice I.6.0 de la page 58 (vi). Achever avec le lemme de Zorn.

I.6.73 Utiliser les exercices I.6.70 de la page 67 et I.6.42 de la page 64.

I.6.74 Utiliser l'exercice I.6.69 de la page 66.

I.6.75 L'image de G dans $\mathbb{C}^*$ est contenue dans le groupe $\mathrm{Tor}(\mathbb{C})$ qui est isomorphe à $\mathbb{Q}/\mathbb{Z}$ via l'exponentielle.

I.6.76 On trouve (X, X^2).