ELEMENTS D'ALGEBRE COMMUTATIVE

Maîtrise de Mathématiques
Université d'Angers
2003/04

D. Schaub

Chapitre 2

Modules sur un anneau

2.1 Modules et homomorphismes

2.1.1 Définition :

Soit A un anneau unitaire. Un ensemble M muni d'une structure de groupe abélien est un A-module à (gauche) ou module (à gauche) sur A si M est muni d'une application $\cdot : A \times M \to M$ telle que :

$$\begin{cases} (a+b)\cdot x &= a\cdot x + b\cdot x \\ (ab)\cdot x &= a\cdot(b\cdot x) \\ a\cdot(x+y) &= a\cdot x + a\cdot y \\ 1\cdot x &= x \end{cases}$$

pour tous $a, b \in A, x, y \in M$.

On définit de manière analogue un A-module à droite. Si A commutatif, les deux notions se confondent. Chaque fois qu'on ne précisera pas, l'anneau considéré sera commutatif.

Exemples : • un anneau A est un A-module à gauche (et à droite) sur lui-même ;

• un idéal $\mathcal{I}$ (à gauche, etc ...) d'un anneau A est un A-module à gauche, etc ...) ;

• tout groupe abélien G est un $\mathbb{Z}$-module ;

• un espace vectoriel V sur un corps k est un k-module, mais aussi un $\mathrm{End}_k(V)$-module à gauche ; et $V^* = \mathrm{Hom}_k(V, k)$ est un $\mathrm{End}_k(V)$-module à droite ;

Exercice : Montrer que si V est un k-espace vectoriel et $u \in \mathrm{End}_k(V)$, on peut définir sur V une structure de $k[X]$-module.

2.1.2 Homomorphismes

Définition 2.1.1 *Une application $f : M \to N$ entre deux A-modules est un homomorphisme de A-modules ou application A-linéaire si, pour tous $\lambda, \mu \in A$ et $x, y \in M$, on a : $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$).*

L'ensemble des applications A-linéaires de M dans N se note $\mathrm{Hom}_A(M, N)$. Il est naturellement muni d'une structure de groupe abélien par : $\forall x \in M, (f+g)(x) = f(x) + g(x)$.

Si de plus A est **commutatif** alors, il est muni d'une opération externe définie par : $\forall x \in M, (\lambda \cdot f)(x) = \lambda \cdot f(x)$ qui alors a les propriétés requises pour que $\mathrm{Hom}_A(M, N)$ soit un A-module (si A n'est pas commutatif, alors, en général, $(\lambda f)(ax) \neq a(\lambda f)(x)$).

Définition 2.1.2 *Un sous-ensemble N de M est un sous-A-module de M s'il est un sous-groupe de $(M,+)$ et s'il est stable par la multiplication externe.*

On vérifie immédiatement que : N est un sous-module d'un A-module M ssi $\forall a,b \in A$, $\forall x,y \in N$, $ax+by \in N$.

Exemples : Si f est un homomorphisme de A-modules de M vers N, $\ker(f)$ et $\mathrm{Im}(f)$ sont des sous-modules de M et N respectivement.

2.1.3 Opérations sur les sous-modules

Soit M un A-module et N et N' des sous-modules de M.
* La *somme* de N et N', $N+N' = \{x+y \mid x \in N, y \in N'\}$, est clairement un sous- module de M

* L'intersection de N et N' est un sous-module de M. Plus généralement, une intersection quelconque de sous-modules de M est un sous-module de M.

* L' ensemble des sommes finies d'éléments de la forme ax où $a \in \mathcal{I}$ et $x \in M$ est aussi un sous-module de M, noté $\mathcal{I}M$.

Définition 2.1.3 *Si S est un sous-ensemble d'un A-module M, l'intersection de tous les sous-modules contenant S est appelé le sous-module engendré par S. (souvent noté $< S >$).*

Les éléments de S sont appelés *générateurs* du sous-module $< S >$.
Si un module est engendré par un sous-ensemble fini $\{x_1, \ldots, x_n\}$ d'éléments, on dira que M est un A-module *de type fini.*

Définition 2.1.4 *Soit M un A-module et S un sous-ensemble de M. On appelle combinaison linéaire d'éléments de S toute somme finie d'éléments $ax, a \in A, x \in S$.*

L'ensemble $N(S)$ des combinaisons linéaires d'éléments de S est un sous-module de M.

Lemme 2.1.1 *$N(S) =< S >$ est le plus petit sous-module de M contenant S.*

Preuve : Il est clair que $N(S)$ est un sous-module et qu'il contient S, par conséquent, $N(S)$ contient $< S >$.

D'autre part, toute combinaison linéaire d'éléments de S appartient à tout sous-module contenant S, donc à l'intersection de tous ces sous-modules, d'où $< S > \subset N(S)$.

Ce sous-module est bien le plus petit sous-module contenant S puisque tout sous-module contenant S contient l'intersection de tous les sous-modules contenant S.

Définition 2.1.5 *Les éléments de S sont dits linéairement indépendants ou formant un système libre (ou linéairement indépendant) si la nullité de toute combinaison linéaire d'éléments de S implique la nullité de tous les coefficients, autrement dit si pour toute partie finie T de S, et tout ensemble $a_t, t \in T$ d'éléments de A, $\sum_t a_t t = 0 \Rightarrow a_t = 0, \forall t$. Sinon, on dit qu'il est lié (ou linéairement dépendant).*

S est une base de M si $S \neq \emptyset$, S engendre M et S est libre.

Un A-module M est dit libre si M admet une base ou si $M = 0$. Le rang d'un A-module libre est le cardinal d'une base (voir exercice ci-dessous).

Exemples : A, A^n sont des A-modules libres (en particulier, $\mathbb{Z}$, $\mathbb{Z}^n$ sont des $\mathbb{Z}$-modules libres) mais pas $A/aA,\ a \in A$. Tout espace vectoriel sur un corps k est un k-module libre.

Remarque : L'exemple A/aA montre que tout A-module n'admet pas nécessairement une base. En effet, pour tout élément y de A/aA, on a $ay = 0$, par conséquent tout ensemble à un élément est lié (et a fortiori donc, tout système non vide).

Exercice : Montrer que si M est libre, toutes ses bases ont même cardinal et si M et N sont deux modules libres admettant des bases de même cardinal, alors ils sont isomorphes (indication : on pourra montrer que si un A-module M peut-être engendré par n éléments, alors tout système de $n+1$ éléments est lié).

2.1.4 Modules quotients

Soit M un A-module et N un sous-module de M. Considérons sur M la relation d'équivalence R définie par : $xRy \Leftrightarrow x - y \in N$. L'ensemble quotient M/R, qu'on notera plutôt M/N, est muni d'une structure naturelle de A-module par les opérations : $\forall x, y \in M, a \in A$,

$$(x+N)(y+N) = x+y+N; \quad a(x+N) = ax+N.$$

Il faut bien entendu vérifier que ces opérations sont ainsi bien définies (à savoir, vérifier que si $x'Rx$ et $y'Ry$, alors $(x'+y')R(x+y)$ et $ax'Rax$), puis qu'elles confèrent effectivement à M/N une structure de A-module. On dira que M/N est muni de la structure de A-module quotient.

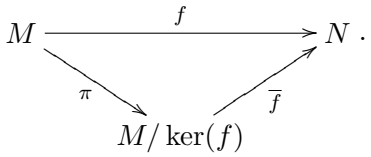
La surjection canonique $\pi : M \to M/N$ est alors un homomorphisme de A-modules.

Cas particulier Si I est un idéal de A, alors IM est un sous-module de M et M/IM est un A-module quotient de M. Mais M/IM a également une structure naturelle de A/I-module, puisqu'on peut définir la multiplication externe par : $(a+I)(x+IM) = ax+IM$.

Exercice : Vérifier que la structure naturelle de M/IM coïncide avec la structure induite par l'épimorphisme naturel $\pi : A \to A/I$.

Rappelons encore le théorème de factorisation (pour une démonstration dans le cas des groupes voir, par exemple, cours de licence, et il suffit alors de remarquer que les différentes applications sont A-linéaires)

Théorème 2.1.1 *Si $f : M \to N$ est une application A-linéaire alors f se factorise à travers $M/\ker(f)$ ie. il existe $\overline{f}$, A-linéaire, telle que le diagramme suivant est commutatif*



2.1.5 Propriétés

Proposition 2.1.1 *(i) Soient N et N' des sous-modules d'un A-module M. On a un isomorphisme naturel :*

$$\frac{N}{N \cap N'} \cong \frac{N+N'}{N'}.$$

(ii) Soient $M" \subseteq M' \subseteq M$ trois A-modules, on a un isomorphisme naturel :

$$\frac{M/M"}{M'/M"} \cong \frac{M}{M'}.$$

(iii) Soit $f : M \to M'$ une application A-linéaire et N' un sous-module de M'. Alors $f^{-1}(N')$ est un sous-module de M et l'application composée $f' = \pi' \circ f : M \to M'/N'$ se factorise à travers une injection (A-linéaire) :

$$\overline{f} : \frac{M}{f^{-1}(N')} \to \frac{M'}{N'}.$$

Preuve : (i) Il suffit de voir que l'application $N \to \dfrac{N+N'}{N'}$ définie à partir de l'inclusion de N dans $N+N'$ est surjective et son noyau est exactement $N \cap N'$.
(ii) Comme $M" \subseteq M'$, on a une surjection naturelle $\dfrac{M}{M"} \to \dfrac{M}{M'}$ et son noyau est clairement $\dfrac{M'}{M"}$.
(iii) On vérifie facilement que $f^{-1}(N')$ est un sous-module de M. On pose alors $\overline{f}(\overline{x}) = \pi' \circ f(x)$ où x est un représentant de $\overline{x}$ et on vérifie que $\overline{f}$ est ainsi bien définie. L'injectivité est immédiate par définition.

2.1.6 Produit de modules

Définition 2.1.6 *Etant donnés deux A-modules M et N, on définit le A-module produit de M et N par : $M \times N$ est l'ensemble produit de M et N et on munit cet ensemble des lois : $\forall x, x' \in M, \forall y, y' \in N, (x,y) + (x',y') = (x+x', y+y')$ et $\forall a \in A, a \cdot (x,y) = (ax, ay)$.*

On vérifie immédiatement que $M \times N$ muni de ces deux lois a une structure de A-module.

Remarque-Exercice : Soient N et N' des sous-modules d'un A-module M tels que $N \cap N' = \{0\}$. Alors $N + N'$ (noté $N \oplus N'$ et nommé *somme directe*) est un A-module isomorphe à $N \times N'$.

Identifiant alors N à $N \times \{0\}$ et N' à $\{0\} \times N'$, on peut identifier $N \oplus N'$ à $N \times N'$.

Exercice : Définir le produit direct et la somme directe d'une famille quelconque de A-modules. En développer les propriétés fonctorielles.

2.1.7 Compléments

Lemme 2.1.2 ***Lemme de Nakayama*** *Soit M un A-module de type fini. Soit $\mathcal{I}$ un idéal de A contenu dans le radical de Jacobson (intersection de tous les idéaux maximaux) de A. Alors, si $\mathcal{I}M = M$, on a :$M = 0$.*

Preuve : Supposons $M \neq 0$ et soit $\{x_1, .., x_n\}$ un système minimal de générateurs de M. Alors : $\mathcal{I}M = M \Leftrightarrow x_n = a_1x_1 + .. + a_nx_n$ avec $a_i \in \mathcal{I}$. D'où : $(1-a_n)x_n = a_1x_1 + .. + a_{n-1}x_{n-1}$. Mais $\mathcal{I} \subseteq R(A)$, et, par conséquent, $1 - a_n$ est inversible (tout élément non inversible appartient à au moins un idéal maximal, donc si $1-a_n$ n'était pas inversible, on en déduirait que 1 appartient à un idéal maximal !), d'où l'on déduit que : $x_n \in < x_1, .., x_{n-1} >$, ce qui contredit la minimalité.

Corollaire 2.1.1 *Soit M un A-module, N, N' des sous-modules de M et $\mathcal{I}$ un idéal de A. Supposons que $M = N + \mathcal{I}N'$ et que : soit $\mathcal{I}$ est nilpotent, soit $\mathcal{I} \subseteq R(A)$ et N' est de type fini, alors $M = N$.*

Preuve : Il faut remarquer que $M/N = \mathcal{I}(M/N)$: en effet, $M = N + \mathcal{I}N'$ implique que, a fortiori, $M = N + N'$.

D'où : $\dfrac{M}{N} = \dfrac{N+N'}{N} = \dfrac{N'}{N \cap N'}$.

Mais, par ailleurs, $M = N + \mathcal{I}N' \Leftrightarrow \dfrac{M}{N} = \dfrac{\mathcal{I}N'}{\mathcal{I}N' \cap N} = \mathcal{I}\dfrac{N'}{N' \cap N}$.

Conclusion : $\dfrac{M}{N} = \mathcal{I}(\dfrac{M}{N})$, d'où :

$-$ $>$ dans la première hypothèse,

$$\mathcal{I}^n = 0 \Leftrightarrow \frac{M}{N} = \mathcal{I}(\frac{M}{N}) = \mathcal{I}^2(\frac{M}{N}) = \ldots = \mathcal{I}^n(\frac{M}{N}) = 0;$$

$-$ $>$ dans la deuxième hypothèse, on applique Nakayama à $\dfrac{M}{N} = \dfrac{N'}{N \cap N'}$, ce dernier étant de type fini par hypothèse.

2.1.8 Exemple des espaces vectoriels sur un corps

Un espace vectoriel sur un corps k est un k-module.

Proposition 2.1.2 *Pour un espace vectoriel, un système de vecteurs vérifie les équivalences suivantes : base $\Leftrightarrow$ système libre maximal $\Leftrightarrow$ système générateur minimal.*

Idée de preuve : Prendre un système libre maximal et rajouter un élément ....

Attention c'est précisément cela qui n'est plus vrai pour un module !

Remarque : Tout système libre maximal d'un **module** n'est pas nécessairement générateur comme le montre l'exemple suivant : dans le $\mathbb{Z}$-module $\mathbb{Z}$ (qui est d'ailleurs libre car $\{1\}$ est une base), le système $\{2\}$ est libre maximal, mais pas générateur.

Théorème 2.1.2 ***de la base incomplète*** *Soit E un espace vectoriel sur k et $S \subseteq E$ un système de vecteurs linéairement indépendants, alors, il existe une base B contenant S.*

Preuve : Rappelons le lemme de Zorn : *Tout système ordonné inductif (càd. tel que tout sous-ensemble totalement ordonné est majoré) admet un élément maximal.* Soit $\Sigma = \{S' \subseteq E$, libres, $S' \supseteq S\}$. On montre que Σ est ordonné inductivement i.e. que tout sous-ensemble totalement ordonné T de Σ est majoré. D'où, Σ admet un élément maximal qui est précisément une base cherchée.

Remarques : 1. Ce théorème a pour conséquences importantes l'existence d'un *supplémentaire*. Contre-exemple pour un module : le sous-$\mathbb{Z}$-module $2\mathbb{Z}$ de $\mathbb{Z}$ n'a pas de supplémentaire.

2. De tout cela, on tire la notion de *dimension* pour un espace vectoriel, notion qui n'a pas d'équivalent pour un A-module quelconque.

2.2 Modules de fractions

Définition 2.2.1 *Soit M un A-module et $S \subset A$ une partie multiplicative. On définit $S^{-1}M$ comme le quotient de $M \times S = \{(x,s) | x \in M,\ s \in S\}$ par la relation d'équivalence $(x,s) \sim (y,t) \Leftrightarrow \exists u \in S,\ u(xt - ys) = 0$. On notera la classe de (x,s) par $\dfrac{x}{s}$.*

On peut munir $S^{-1}M$ d'une structure de $S^{-1}A$-module de la manière suivante :

$$\frac{x}{s} + \frac{x'}{s'} = \frac{xs' + x's}{ss'} \quad \text{et} \quad \frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}.$$

Remarque : A travers l'homomorphisme d'anneaux $\phi : A \to S^{-1}A$, $S^{-1}M$ est naturellement muni d'une structure de A-module. En particulier, $S^{-1}A$ a une structure naturelle de A-module.

Proposition 2.2.1 *S^{-1} commute aux sommes finies, intersections finies, et quotients.*

La preuve est laissée en exercice.

Remarque : Si $f : M' \to M$ est un homomorphisme de A-modules, on définit $S^{-1}M' \to S^{-1}M$ par $S^{-1}f(\frac{x}{s}) = \frac{f(x)}{s}$. Il faut, bien entendu, vérifier que $S^{-1}f$ est ainsi bien définie et est un homomorphisme de $S^{-1}A$-modules.

2.3 Suites exactes

2.3.1 Définition

Définition 2.3.1 *On dit qu'une suite d'homomorphismes de A-modules*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

est exacte si $\ker(g) = im(f)$.

Plus généralement, une suite

$$\cdots \to F_{i-1} \to F_i \to F_{i+1} \to \cdots$$

est exacte si toutes les sous-suites à 3 termes le sont.

Exemples :

1) La suite $0 \to G \xrightarrow{f} G'$ est exacte ssi f est injective.

2) La suite $G \xrightarrow{f} G' \to 0$ est exacte ssi f est surjective.

3) Suites exactes courtes :

La suite $0 \to F' \xrightarrow{f} F \xrightarrow{g} F'' \to 0$ est exacte ssi f est injective, g est surjective et $\ker(f) = \mathrm{im}(g)$.

Exemple : soit N un sous-module d'un A-module M, alors la suite $0 \to N \to M \to M/N \to 0$ est exacte. Il en est ainsi, par exemple, de la suite $0 \to IM \to M \to M/IM \to 0$.

Théorème 2.3.1 *Pour toute suite exacte de A-modules $0 \to F \xrightarrow{f} E \xrightarrow{g} G \to 0$, il y a équivalence de :*

i) $\phi : E \cong F \times G$ de telle sorte que le diagramme suivant commute

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F & \xrightarrow{f} & E & \xrightarrow{g} & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Id_F} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle Id_G} & & \\ 0 & \longrightarrow & F & \xrightarrow{i} & F \times G & \xrightarrow{\pi} & G & \longrightarrow & 0 \end{array}$$

où $i(x) = (x, 0)$ et $\pi((x, y)) = y$;

ii) il existe $r : E \to F$ telle que $rf = Id_F$;

iii) il existe $s : G \to E$ telle que $gs = Id_G$.

On dit alors que la suite exacte est scindée.

Preuve : i) $\Rightarrow$ ii) On définit r par pour tout $z \in E$, $r(z) = i^{-1}(\phi(z))$ qu'on vérifie être un homomorphisme. Alors, pour tout $x \in F$, $rf(x) = r(f(x)) = i^{-1}(\phi(f(x))) = i^{-1}(i \circ \mathrm{Id}_F)(x) = x$.

i) $\Rightarrow$ iii) De même, on peut définir $s : G \to F \times G \cong E$ par $s(y) = (0, y)$. Cela définit bien une section de g ie. $gs = \mathrm{Id}_G$.

ii) $\Rightarrow$ i) On définit s par $s(y) = \phi^{-1}((0,y))$ et on voit que, pour tout $y \in G$, $gs(y) = \mathrm{Id}_G(gs(y)) = \pi \circ \phi(s(y) = \pi \circ \phi(\phi^{-1}((0,y))) = y$.

iii) $\Rightarrow$ i) Soit donc s une section de g. Remarquons que s est alors injective (en effet, $s(x) = s(y) \Rightarrow x = gs(x) = gs(y) = y$). Définissons $\psi : F \times G \to E$ par $\psi((x,y)) = f(x) + s(y)$. Vérifions que c'est un homomorphisme de A-modules. On a $\psi((x,y)+(x',y)) = \psi(x+x', y+y') = f(x) + f(x') + s(y) + s(y') = \psi((x,y)) + \psi((x',y'))$.

On vérifie facilement que ψ est injectif et surjectif. En effet, ψ est injective : supposons $\psi((x,y)) = 0 \Leftrightarrow f(x)+s(y) = 0$, d'où en composant avec g, $0 = gf(x)+gs(y) = y$, d'où $f(x) = 0$ ce qui implique $x = 0$.

Pour ce qui est de la surjectivité, il suffit de remarquer que $\forall z \in E$, $z = z - sg(z) + sg(z)$ et $z - sg(z) \in \ker(g) = \mathrm{im}(f)$, d'où $z = f(x) + s(g(y))$ où $f(x) = z - sg(z)$.

Remarque : Pour une suite exacte de A-modules $0 \to F \xrightarrow{f} E \xrightarrow{g} G \to 0$, f rétractable équivaut à g sectionnable qui équivaut encore à $E \cong F \times G$ et on a $E = \mathrm{im}(f) \oplus \mathrm{im}(s)$ où s est une section de g.

2.3.2 Résultats

Proposition 2.3.1 *Si $M' \longrightarrow M \longrightarrow M"$ est une suite exacte de A-modules, alors $S^{-1}M' \longrightarrow S^{-1}M \longrightarrow S^{-1}M"$ est une suite exacte de $S^{-1}A$-modules.*

Preuve : Notons $\tilde{f}$ et $\tilde{g}$ les applications $S^{-1}f$ et $S^{-1}g$ respectivement.
Montrons que la suite obtenue est exacte :

* $g \circ f = 0 \Rightarrow \forall x, g(f(x)) = 0$, or $\tilde{g}(\tilde{f}(x/t)) = \frac{1}{t}(g \circ f)(x) = 0$, d'où $\tilde{g} \circ \tilde{f} = 0$; ce qui signifie que $\mathrm{im}(f) \subseteq \ker(g)$.

* prenons à présent un élément y/t de $S^{-1}M$ tel que $\tilde{g}(y/t) = 0$. Alors, $\frac{t}{1}\tilde{g}(\frac{y}{t}) = \tilde{g}(\frac{t}{1}\frac{y}{t}) = \frac{g(y)}{1} = 0$. Par conséquent, $\exists s \in S$ tel que $sg(y) = g(sy) = 0$. Autrement dit, $sy \in \mathrm{Im}(f)$, d'où $\exists x \in M'$ tel que $sy = f(x)$; mais alors, $y/t = f(x)/ts = \tilde{f}(\frac{x}{ts})$. D'où l'inclusion inverse.

Lemme 2.3.1 ***dit lemme du serpent*** *Si dans le diagramme commutatif suivant*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\alpha} & N & \xrightarrow{\beta} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\alpha'} & N' & \xrightarrow{\beta'} & P' & \longrightarrow & 0 \end{array}$$

les lignes sont exactes et si K_f, K_g, K_h (resp. C_f, C_g, C_h) désignent les noyaux (resp. conoyaux) de f, g, h, alors la suite

$$0 \longrightarrow K_f \longrightarrow K_g \longrightarrow K_h \xrightarrow{\partial} C_f \longrightarrow C_g \longrightarrow C_h \longrightarrow 0$$

est exacte.

La démonstration de ce lemme très utile se fera en TD.

2.4 Conditions de finitude

2.4.1 Conditions de chaîne

Définition 2.4.1 *Soit $(X, \leq)$ un ensemble ordonné (partiellement). Une suite croissante d'éléments de X, $a_0 \leq a_1 \leq \cdots \leq a_s \leq \cdots$, est stationnaire s'il existe n tel que $\forall m \geq n$, $a_m = a_n$.*

Proposition 2.4.1 *Soit $(X, \leq)$ un ensemble ordonné (partiellement). Les conditions suivantes sont équivalentes :*

(i) toute suite croissante est stationnaire

(ii) tout sous-ensemble non vide admet un élément maximal.

Preuve : (i) $\Rightarrow$ (ii) Supposons qu'il existe $T \subset X,\ T \neq \emptyset$, tel que T n'admette pas d'élément maximal. Soit alors $a_0 \in T$; a_0 n'est pas maximal, donc il existe $a_1 \in T$ tel que $a_0 < a_1$. Puis, par récurrence, on construit une suite non stationnaire, ce qui est exclu par (i) ;

(ii) $\Rightarrow$ (i) Soit $(a_i)_{i\in\mathbb{N}}$ une suite croissante et $T = \{a_0, a_1, \ldots\}$. Par hypothèse, T admet un élément maximal, soit a_n, d'où, quel que soit $m \geq n$, $a_m = a_n$.

Définition 2.4.2 *Un A-module M est dit noethérien si $(S(M), \subseteq)$ où $S(M)$ désigne l'ensemble des sous-modules de M vérifie l'une des conditions de la proposition. On dit aussi que M vérifie la condition de chaîne ascendante.*

Remarque : Un module M est dit *artinien* si $(S(M), \supseteq)$ vérifie la proposition. On dit aussi que M vérifie la condition de chaîne descendante.

Exemples : 1) Si G est un groupe abélien fini, c'est un $\mathbb{Z}$-module noethérien (et artinien). En effet, soit $G_0 \subseteq G_1 \subseteq \cdots$ une chaîne ascendante de sous-groupes, alors la suite des ordres $|G_0| \leq |G_1| \leq \cdots \leq |G|$ est une suite d'entiers majorés, donc stationnaire, d'où la conclusion.

2) $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion qui admet, pour tout entier n un unique sous-groupe d'ordre n, H_n (exercice). Alors la suite croissante "infinie" $H_0 \subset H_1 \subset \cdots$ montre que $\mathbb{Q}/\mathbb{Z}$ n'est pas noethérien (mais il est artinien).

3) (exercice) Soit G le sous-groupe de $\mathbb{Q}/\mathbb{Z}$ constitué des éléments d'ordre une puissance de p où p est un nombre premier fixé (vérifier que c'est bien un sous-groupe), alors G admet exactement un sous-groupe G_n d'ordre p^n pour chaque $n \geq 0$. D'où $G_0 \subsetneqq G_1 \subsetneqq \cdots$ est une suite croissante non stationnaire, donc G n'est pas noethérien (on peut montrer que G est artinien).

4) (exercice) Soit $H = \{\frac{m}{p^n} |\ m, n \in \mathbb{Z},\ n \geq 0\}$. C'est un sous-groupe de $\mathbb{Q}$. On a une suite exacte $0 \to \mathbb{Z} \to H \to G \to 0$. Alors H n'est pas artinien car $\mathbb{Z}$ ne l'est pas et H n'est pas noethérien car G ne l'est pas (voir proposition 2.4.3).

5) $\mathbb{Z}$ (comme $\mathbb{Z}$-module) vérifie la CCA (cond. de chaîne asc.) (par principalité), mais pas la CCD (car, si $a \in \mathbb{Z},\ a \neq 0$, alors $(a) \supset (a^2) \supset (a^3) \supset \cdots$).

6) De même, $k[X]$ est noethérien, mais non artinien.

6) Par contre, $k[X_1, X_2, \ldots]$ ne vérifie ni CCA (car $(X_1) \subset (X_1, X_2) \subset \cdots$ ne stationne pas), ni CCD (cf. exemple 5).

Proposition 2.4.2 *M est noethérien ssi tout sous-module de M est de type fini.*

Preuve : Supposons M noethérien et N un sous-module de M. Soit Σ l'ensemble des sous-modules de type fini de N. Alors Σ est non vide ($0 \in \Sigma$), donc admet un élément maximal N_0. Si $N_0 \neq N$, il existe $x \in N$ tel que $x \notin N_0$; alors $N_0 + Ax$ est un sous-module de N de type fini, d'où $N_0 + Ax \in \Sigma$ et $N_0 \subsetneqq N_0 + Ax$; ce qui contredit la maximalité de N_0. D'où $N = N_0$ est de type fini.

Inversement soit $M_1 \subseteq M_2 \subseteq \cdots$ une chaîne croissante de sous-modules de M. Alors $N = \cup M_n$ est un sous-module de M, donc de type fini, càd. $N =< x_1, \ldots, x_t >$ et $x_i \in \cup M_n$, donc il existe i tel que $x_i \in M_{n_i}$. Soit $n = \sup(n_i)$, alors, pour tout i, $x_i \in M_n$ et, subséquemment, $N =< x_1, \ldots, x_t >= M_n$ ie. la chaîne est stationnaire.

Proposition 2.4.3 *Soit $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M" \longrightarrow 0$ une suite exacte de A-modules. Alors M est noethérien ssi M' et $M"$ le sont.*

Preuve : Soit $M'_1 \subseteq M'_2 \subseteq \cdots$ une chaîne de sous-modules de M'. Alors $\alpha(M'_i)$ constitue une chaîne croissante de sous-modules de M, donc stationnaire, d'où il existe n tel que $\alpha(M'_{n+k}) = \alpha(M'_n), \forall k \geq 0$. Par injectivité de α, on conclut alors que $M'_{n+k} = M'_n$.

De même, si $M"_0 \subseteq M"_1 \subseteq \cdots$ est une chaîne dans $M"$, les $\beta^{-1}(M"_j)$ forment une chaîne croissante dans M qui stationne, d'où : la suite des $M"_j$ stationne.

Inversement, Supposons M' et $M"$ noethériens. Soit alors $M_0 \subseteq M_1 \subseteq \cdots$ une chaîne de sous-modules de M. La chaîne des $\alpha^{-1}(M_i)$ est une chaîne croissante de sous-modules de M' et les $\beta(M_i)$ forment une chaîne croissante de sous-modules de $M"$. Ces deux chaînes stationnent, et, pour $n >> 0$, elles stationnent simultanément, ie. il existe n tel que $\forall k \geq 0$, $\alpha^{-1}(M_{n+k}) = \alpha^{-1}(M_n)$ et $\beta(M_{n+k}) = \beta(M_n)$. Par conséquent, $M_{n+k} = M_n$ (en effet : d'une part, $M_n \subset M_{n+k}$ et, d'autre part, si $x \in M_{n+k}$, $\beta(x) \in \beta(M_{n+k}) = \beta(M_n)$, x peut s'écrire $x = y_n + \alpha(m')$, $m' \in M'$, $y_n \in M_n$. Or, $\alpha(m') = x - y_n \in M_{n+k}$, donc $m' \in \alpha^{-1}(M_{n+k}) = \alpha^{-1}(M_n)$ càd. $\alpha(m') \in M_n$, d'où $x = y_n + \alpha(m') \in M_n$).

Corollaire 2.4.1 *Si M et N sont noethériens, alors $M \times N$ (ou $M \oplus N$) le sont.*

Remarquant que la suite $0 \to M \to M \times N \to N \to 0$ est une suite exacte, c'est une conséquence directe de la proposition.

2.4.2 Anneaux noethériens

Définition 2.4.3 *Un anneau est noethérien (resp. artinien) s'il est noethérien (resp. artinien) en tant que module sur lui-même.*

Les propositions 2.4.1 et 2.4.2 se réécrivent alors

Proposition 2.4.4 *A est noethérien ssi A satisfait l'une des conditions équivalentes suivantes :*
(i) toute chaîne croissante d'idéaux est stationnaire
(ii) tout ensemble non vide d'idéaux de A admet un élément maximal
(iii) tout idéal de A est engendré par un nombre fini d'éléments.

Exemples 1) Tout corps est noethérien (et artinien).

2) $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ ou, plus généralement, tout anneau principal est noethérien (remarquons au passage que $\mathbb{Z}$ n'est pas artinien, mais $\mathbb{Z}/n\mathbb{Z}$ l'est).

3) $\mathcal{C}^0([0,1])$ n'est pas noethérien (prendre $I_n = \{f |\ f_{|[0,1/n]} \equiv 0\}$; c'est une suite croissante d'idéaux non stationnaire).

Proposition 2.4.5 *Si A est noethérien et M un A-module de type fini, alors M est noethérien.*

Preuve : C'est une conséquence de la proposition 2.4.3 sachant que, si M est engendré par n éléments, on peut construire une surjection $A^n \to M$ et A^n est noethérien par application récurrente du même théorème.

Corollaire 2.4.2 *Soit $A \subseteq B$ un sous-anneau. Si A est noethérien et B un A-module de type fini, alors B est noethérien.*

Attention Un sous-anneau d'un anneau noethérien *n'est* pas en général noethérien ! Exemple : l'anneau de valuation d'une valuation à groupe de valeur $\neq \mathbb{Z}$ ie. une valuation de rang > 1 donne un sous-anneau de $\mathbb{C}(x,y)$ non noethérien. Autre exemple : $\mathbb{C}[xy, x^2y, x^3y, \ldots]$ est un sous-anneau de $C[x,y]$ qui est isomorphe à $\mathbb{C}[x_1, x_2, \ldots]$ (les $x^k y$ sont algébriquement indépendants !) qui n'est donc pas noethérien.

Proposition 2.4.6 *Un quotient d'un noethérien est noethérien.*

C'est encore une conséquence de la proposition 2.4.3.

Rappelons encore le

Théorème 2.4.1 de la base de Hilbert *Si A est un anneau noethérien, alors l'anneau de polynôme $A[X]$ est noethérien.*

Preuve : Soit I un idéal de $A[X]$, il s'agit de montrer que I est de type fini. Soit $\mathcal{E}$ l'ensemble des coefficients des termes de plus haut degré des éléments de I. Alors $\mathcal{E}$ est clairement un idéal de A, donc de type fini. Soient $\{a_1, \ldots, a_n\}$ un système de générateurs et considérons les $f_i = a_i X^{r_i} + (\text{ termes de degré } < r_i) \in I$ qui ont donné naissance aux a_i. Soit encore $r = \max r_i$ et $J \subset I$ l'idéal de $A[X]$ engendré par $f_1, \ldots, f_n$.

• Montrons que, $\forall f \in I$, $f = g + h$ où $h \in J$ et $g \in I$ de degré $< r$. Si $d^\circ f < r$, il n'y a rien à démontrer. On peut donc supposer $m = d^\circ f \geq r$. Alors $f = ax^m + (d^\circ < m)$. Or $a \in \mathcal{E}$, donc $a = \sum_i a_i u_i$.

Posons alors $g_1 = f - \sum_i u_i f_i X^{m-r_i}$. Ainsi $g_1 \in I$ et son degré $d^\circ g_1 < m$, d'où, par récurrence descendante sur m, on peut écrire $f = g_j + h$ où $h \in J$ et $d^\circ g_j < r$. Il suffit alors de poser $g = g_j$.

• Soit $M = A + AX + AX^2 + \ldots + AX^{r-1}$; c'est un A-module de type fini, donc noethérien et on a $I = J + I \cap M$. Or J est de type fini, donc I est de type fini.

Corollaire 2.4.3 *Si A est noethérien, alors $A[X_1, \ldots, X_n]$ l'est.*

2.5 Application aux modules sur les anneaux principaux

2.5.1 Rappels

Rappelons quelques résultats essentiels sur les modules sur les anneaux principaux (voir par exemple, le cours de premier semestre, le chapitre 2 de mon cours de licence sur les groupes ou [6]).

Théorème 2.5.1 *Soit A un anneau principal, M un A-module libre de rang m et N un sous-module de M. Alors :*

(i) N est libre de rang $k \leq m$;

(ii) il existe une base $\{e_1, \ldots, e_m\}$ de M et des éléments $a_1, \ldots, a_k$ de A tels que :

1. $\{a_1 e_1, \ldots, a_k e_k\}$ forme une base de N ;

2. pour tout i, a_i divise a_{i+1}.

Preuve : On va démontrer ce théorème en 5 étapes. Soit d'abord $\{e_1, \ldots, e_m\}$ une base de M.

(1) L'ensemble $\{u(N); u \in M^* = \mathrm{Hom}_A(M, A)\}$ est un ensemble d'idéaux de A. Comme celui-ci est principal, donc noethérien, il admet un élement maximal, qui est un idéal monogène ; il existe donc un $u \in M^*$ tel que Aa_u soit maximal. Comme on peut supposer $N \neq 0$ (sinon il n'y a rien à prouver), on en déduit que $Aa_u \neq 0$ (en effet : soit $0 \neq x \in N$ alors x peut s'écrire $x = \sum_{i=1}^n a_i x_i$ où l'un au moins des a_i n'est pas nul, mais alors l'homomorphisme $M \to A$ tel que $e_i \mapsto 1$ vérifie $u(N) \neq 0$). Soit alors $e' \in N$ tel que $u(e') = a_u$.

(2) Pour tout $v \in M^*$, a_u divise $v(e')$. En effet, soit $d = \mathrm{pgcd}(a_u, v(e'))$, alors, par Bezout, $d = ba_u + cv(e') = bu(e') + cv(e') = (bu + cv)(e')$. Mais $w = bu + cv \in M^*$. Comme $d = w(e') \in w(N)$, $Ad \subset w(N)$, d'où $Aa_u \subset Ad$ (par division)$\subset w(N)$. Mais par maximalité de Aa_u, on en déduit $Aa_u = w(N)$ et donc $Ad = Aa_u$, d'où $a_u | d | v(e')$.

(3) Considérons, pour tout $i = 1, \ldots, n$, l'application de projection $p_i : M \to A$ définie par $x = \sum_i \alpha_i e_i \mapsto \alpha_i$ (autrement dit, l'application linéaire $e_j \mapsto 0$ si $j \neq i$, $e_i \mapsto 1$). Alors $p_i \in M^*$,

pour tout i, d'où par (2), $a_u|p_i(e')$ pour tout i, càd. il existe β_i tel que $p_i(e') = \beta_i a_u$. Or $e' = \sum_i p_i(e')e_i = \sum_i \beta_i a_u e_i = a_u(\sum_i \beta_i e_i)$. Posons $e = \sum_i \beta_i e_i$. Comme $e' = a_u e$, on en déduit que $a_u = u(e') = a_u u(e)$, d'où $u(e) = 1$.

(4) Tout $x \in M$ peut s'écrire $x = u(x)e + (x - u(x)e)$. Or $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, donc $x - u(x)e \in \ker(u)$. De plus, $Ae \cap \ker(u) = 0$ (car $u(\alpha e) = \alpha(u(e)) = 0 \Rightarrow \alpha = 0$). Conclusion :

$$M = Ae \oplus \ker(u) \quad (*).$$

Or, si $y \in N$, on a $u(y) = ba_u \Rightarrow y = u(y)e + (y - u(y)e) = ba_u(e) + (y - ba_u e) = be' + (y - be')$, par définition de e' et $y - be' \in N$, d'où

$$N = Ae' \oplus (N \cap \ker(u)) \quad (**).$$

(5) Pour prouver i), on procède par récurrence sur le rang de N. Si $\mathrm{rg}(N) = 0$, alors $N = 0$ et il n'y a rien à démontrer. Supposons donc $\mathrm{rg}(N) = k > 0$. Alors de (4), on déduit que $N \cap \ker(u)$ est de rang $k - 1$, donc libre par récurrence et du fait que $N = Ae' \oplus (N \cap \ker(u)$, les deux facteurs étant libres, on en déduit que N est libre de rang k.

Pour prouver ii), on procède par récurrence sur le rang de M. Là encore, si $M = 0$, il n'y a rien à montrer. Supposons donc que le rang m de M est > 0. Soit alors a_u comme dans (1), càd. tel que Aa_u soit maximal. Alors, on peut décomposer $M = Ae \oplus \ker(u)$. $\ker(u)$ est libre par i) de rang $n - 1$; on applique alors l'hypothèse de récurrence au couple $(N \cap \ker(u) \subset \ker(u))$.

On sait donc qu'il existe $k \leq m-1$, une base $\{e_2, \ldots, e_m\}$ de $\ker(u)$, des éléments $a_2, \ldots, a_k$ tels que $\{a_2e_2, \ldots, a_ke_k\}$ soit une base de $N \cap \ker(u)$ et que, pour tout $i \geq 2$, $a_i|a_{i+1}$.

Posons alors $a_1 = a_u$, $e_1 = e$. Alors $\{e_1, \ldots, e_m\}$ est bien une base de M (par (4)(*)) et $\{a_1e_1, \ldots, a_ke_k\}$ une base de N (par (4)(**)).

Il reste à montrer que $a_1|a_2$. Or, soit $v \in M^*$ tel que $v(e_1) = v(e_2) = 1$ et $v(e_i) = 0$ pour $i \neq 1, 2$. Alors, $v(a_1e_1) = v(a_ue) = v(e') \in v(N)$, d'où $Aa_u \subset v(N)$, et, par maximalité de Aa_u, on en déduit que $Aa_u = v(N)$. Or $a_2 = v(a_2e_2) \in v(N) \Rightarrow a_2 \in Aa_u = Aa_1$. □

Remarque : cela implique, en particulier, que, sur un anneau **principal**, tout sous-module d'un libre est libre.

Corollaire 2.5.1 Décomposition en modules monogènes *Soit M un A-module de type fini sur un anneau principal A, alors*

$$M \cong \frac{A}{\mathcal{I}_1} \times \cdots \times \frac{A}{\mathcal{I}_n}$$

*où $\mathcal{I}_1 \supset \mathcal{I}_2 \supset \cdots \supset \mathcal{I}_n$ est une suite d'idéaux de A. De plus, ces idéaux, appelés **facteurs invariants** de M, sont uniquement déterminés par M.*

Preuve : il suffit de remarquer que M peut être engendré par un nombre fini d'éléments $x_1, \ldots, x_n$, d'où on peut construire un homomorphisme surjectif $\phi : A^n \to M$.

Le noyau $\ker(\phi)$ est un sous-module du module libre A^n. D'après le théorème précédent, on peut donc trouver une base $e_1, \ldots, e_n$ de A^n, un entier $k \leq m$, des éléments $a_1|a_2|\cdots|a_k$ de A tels que $a_1e_1, \ldots, a_ke_k$ soit une base de $\ker(\phi)$. En écrivant $A^n = Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_n$, on a $\ker(\phi) = Aa_1e_1 \oplus Aa_2e_2 \oplus \cdots \oplus Aa_ke_k$ où $Aa_ie_i \subset Ae_i$ facteur à facteur. Par conséquent, M est isomorphe à

$$M \cong \frac{Ae_1}{Aa_1e_1} \oplus \cdots \oplus \frac{Ae_k}{Aa_ke_k} \oplus Ae_{k+1} \oplus \cdots \oplus Ae_m.$$

Remarquant que $\frac{Ae_i}{Aa_ie_i} \cong \frac{A}{Aa_i}$, on obtient le résultat énoncé en posant $I_i = Aa_i$, pour $i = 1, \ldots, k$ et $I_i = 0$ pour $i > k$.

Remarque : Par construction, les idéaux $\mathcal{I}_i = a_iA$. Les divisions se traduisant alors par des inclusions $I_{i+1} \subset I_i$.

Définition 2.5.1 *Un élément $x \neq 0$ d'un A-module M est dit "de torsion" s'il existe $a \neq 0$ dans A tel que $ax = 0$. Si un module ne contient aucun élément de torsion, on dit qu'il est "sans torsion".*

Rappelons encore les deux résultats suivants :

Tout A-module libre est sans torsion

Si A est un anneau principal et M un A-module de type fini sans torsion, alors M est libre(en effet, tous les modules de la décomposition ci-dessus sont de torsion lorsque $I_k \neq 0$).

Définition 2.5.2 *Soit p un élément irréductible de A. Un A-module M est dit p-primaire si tous ses éléments sont annulés par une puissance de p.*

Exemple : $\mathbb{Z}/pZ$ est un module p-primaire **et** monogène. Mais $\mathbb{Z}/2Z \times \mathbb{Z}/2\mathbb{Z}$ est 2-primaire sans être monogène.

Rappelons (et donnons-en une preuve succincte) d'abord le théorème des restes chinois :

Théorème 2.5.2 *Soit A un anneau, $I_1, \ldots, I_n$ des idéaux de A tels que $I_i + I_j = A$ pour tout couple $i \neq j$. Alors l'application naturelle*

$$\frac{A}{\bigcap_{i=1}^n I_i} \to \prod_{i=1}^n \frac{A}{I_i}$$

qui envoie $x + \bigcap_{i=1}^n I_i$ sur $(x + I_1, \ldots, x + I_n)$ est un isomorphisme d'anneaux.

Preuve : on procède par récurrence sur n. Si $n = 2$, $I_1 + I_2 = A$ se traduit par l'existence de $a_1 \in I_1$ et $a_2 \in I_2$ tels que $a_1 + a_2 = 1$. Mais alors, l'application $\phi : A \to A/I_1 \times A/I_2$ définie par $x \mapsto (x + I_1, x + I_2)$ donne $a_1 \mapsto (0, 1)$, $a_2 \mapsto (1, 0)$, d'où, si $x = x_2a_1 + x_1a_2$, $\phi(x) = (x_1 + I_1, x_2 + I_2)$. Ce qui montre la surjectivité de ϕ et il suffit alors de remarquer que le noyau de ϕ est précisément $I_1 \cap I_2$.

Pour passer au cas général, il suffit de montrer que $(\bigcap_{i=2}^n I_i) + I_n = A$. Pour cela, prenons $a_i + b_i = 1$ pour $i = 2, \ldots, n$, où $a_i \in I_1,\ b_i \in I_i$. Alors le produit $1 = \prod_i (a_i + b_i) \in I_1 + \prod_{i=2}^n I_i$, d'où le résultat et il n'y a plus qu'à appliquer l'hypothèse de récurrence et le cas $n = 2$ pour conclure.

En revenant au cas d'un anneau intègre, on décompose a en facteurs premiers $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et on obtient alors une décomposition de A/aA en modules p_s-primaires (ie. annulés par une puissance de p_s), $s = 1, \ldots, n$,

$$\frac{A}{aA} \cong \frac{A}{p_1^{\alpha_1}A} \times \cdots \times \frac{A}{p_n^{\alpha_n}A}.$$

On obtient ainsi le

Corollaire 2.5.2 Décomposition en modules primaires *Tout module de torsion (ie. tel que tout élément de ce module est de torsion) de type fini sur un anneau principal se décompose en un produit de modules primaires cycliques. (en fait, de manière unique, ce qu'on admettra ici).*

Preuve : on utilise l'existence d'une décomposition en modules monogènes $M = A/I_1 \times \cdots \times A/I_n$ avec $I_k = Aa_k$ et on décompose a_k en facteurs premiers.

2.5.2 Espaces vectoriels sur k et $k[t]$-modules

Soit V un k-espace vectoriel de dimension finie n et $u : V \to V$ un endomorphisme. On définit sur V (qui a déjà une structure de groupe abélien par l'addition de vecteurs), une multiplication "externe" par les éléments de $k[t]$ de la manière suivante :

$$\forall x \in V,\ \forall P \in k[t],\ P(t) \cdot x := P(u)(x).$$

Plus précisément, si $P(t) = a_0 + a_1 t + \cdots + a_d t^d$, $P(u)$ est l'endomorphisme de k-ev de V défini par $P(u) = a_0 \mathrm{Id} + a_1 u + \cdots + a_d u^d$.

On vérifie immédiatement que, muni de cette multiplication, V est un $k[t]$-module. Comme $k[t]$ est un anneau principal, on peut appliquer à V les résultats ci-dessus rappelés.

Proposition 2.5.1 *Si V est de dimension finie sur k, alors V est un $k[t]$-module de type fini et de torsion. De plus, $Ann_{k[t]}(V)$ est l'idéal de $k[t]$ engendré par le polynôme minimal q_u de u.*

Preuve : V est de type fini car déjà engendré sur k par les éléments d'une base, donc a fortiori sur $k[t]$. Il est tout aussi immédiat que V est de torsion puisqu'il existe un polynôme (par exemple caractéristique) P tel que, $\forall x \in V$, $P(t)x = 0$, autrement dit, tout élément de V est de torsion.

De plus, l'annulateur $\mathrm{Ann}_{k[t]}(V) = \{P \in k[t] | P(t)x = 0,\ \forall x \in V\} = \{P \in k[t] | P(u) \equiv 0\}$ est un idéal de $k[t]$, donc est engendré par un élément q_u, qu'on peut choisir unitaire, et celui-ci est ainsi le plus petit polynôme qui annule u, donc est le polynôme minimal de u.

Remarque : On peut aussi voir la structure de $k[t]$-module de V comme induite de la structure de $\mathrm{End}_k(V)$-module (à gauche) par l'homomorphisme d'anneaux $\phi_u : k[t] \to \mathrm{End}_k(V)$ qui envoie P sur $P(u)$. Ainsi d'ailleurs, $q_u k[t]$ est le noyau de ϕ_u.

2.5.3 Matrices à coefficients dans un anneau

On pourrait bien sûr retraduire directement les résultats de la première partie et en déduire (décomposition en modules primaires cycliques) l'existence d'une réduction de Jordan lorsque le polynôme minimal peut s'écrire dans $k[t]$ comme produit de facteurs du premier degré. C'est là un excellent exercice.

Cependant, on a choisi ici une autre présentation, suivant en cela, par exemple [6].

i. Généralités

Soit A un anneau (commutatif). Une matrice à m lignes et n colonnes à coefficients dans A est un tableau

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix},\ a_{ij} \in A.$$

On met sur l'ensemble des matrices $m \times n$ une structure de A-module par $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ et $\forall \alpha \in A,\ \alpha(a_{ij}) = (\alpha a_{ij})$. De plus, on peut, de la manière habituelle, multiplier une matrice $m \times n$ par une matrice $n \times p$.

Si $m = n$, cette multiplication devient une loi *interne* à l'ensemble des matrices carrées $M_n(A)$ qui devient alors une A-algèbre (càd. muni d'une structure d'anneau, de A-module et vérifiant $\alpha(M \cdot N) = (\alpha M) \cdot N = M \cdot (\alpha N)$, pour tous $\alpha \in A$ et $M, N \in M_n(A)$.

Correspondance matrices-homomorphismes Soient $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de A^n et $\mathcal{E}' = \{e'_1, \ldots, e'_m\}$ une base de A^m. A toute matrice $M = (a_{ij})$, on peut associer un A-homomorphisme $f : A^n \to A^m$ défini par $f(e_i) = \sum_{j=1}^m a_{ji} e'_j$.

Remarque Toute application A-linéaires d'un A-module libre de rang fini est déterminée par ses valeurs sur une base.

ii. Déterminants

Définition 2.5.3 *Soit $M = (a_{ij}) \in M_n(A)$ une matrice carrée, le déterminant est défini par* $\det(M) = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\epsilon(\sigma)} a_{1\sigma(1)} \cdots a_{n\sigma(n)}$*, où $\mathfrak{S}_n$ est le groupe des permutations de n éléments.*

Ainsi défini, le déterminant d'une matrice est donc un élément de A (c'est une somme de produits d'éléments de A).

La plupart des résultats sur les déterminants qui n'utilisent pas dans leur démonstration la nécessité de **"diviser"** (càd multiplier par l'inverse) par des éléments (a priori non inversibles) de A se transposent tels quels aux déterminants de matrices à coefficients dans A. Ainsi par exemple :

- $\det(MN) = \det(M)\det(N)$, le déterminant d'un produit est égal au produit des déterminants ;
- on peut calculer un déterminant en développant par rapport à une ligne ou une colonne ;
- la formule $M\mathrm{Com}(M)^t = \det(M)I$, I étant la matrice identité $n \times n$ est encore valide pour $M \in M_n(A)$ où $\mathrm{Com}(M)$ désigne la matrice des cofacteurs de M ; d'où l'on déduit immédiatement

Lemme 2.5.1 *Une matrice carrée $M \in M_n(A)$ est inversible ssi* $\det(M)$ *est un élément inversible de A.*

Preuve : Si M est inversible, il existe N telle que $MN = I$, matrice identité. Alors $1 = \det(I) = \det(M)\det(N)$, d'où $\det(M)$ (et $\det(N)$) est inversible.

Inversement, d'après la formule ci-dessus, $M \cdot \det(M)^{-1}\mathrm{Com}(M)^t = I$, d'où $M^{-1} = \det(M)^{-1}\mathrm{Com}(M)^t$, formule bien connue pour les matrices à coefficients dans un corps.

iii. Matrices équivalentes

Définition 2.5.4 *On dit que deux matrices M et N sont équivalentes si elles représentent le même homomorphisme $f : A^n \to A^m$.*

De manière équivalente, s'il existe P, matrice $n \times n$ inversible, Q matrice $m \times m$ inversible telles que $M = QNP^{-1}$ (il suffit, en effet, de faire un changement de base dans A^n, de matrice P, dans A^m de matrice Q).

Exercice : pourquoi une matrice de changement de base est-elle inversible ?

Il y a 3 types d'opération élémentaire sur les lignes (ou colonnes) d'une matrice :

- échanger deux lignes (ou colonnes) ;
- multiplier une ligne (colonne) par un élément **inversible** de l'anneau A ;
- ajouter à une ligne (colonne) le produit d'une autre ligne (colonne) par un élément de A.

Une telle opération correspond à la multiplication (à gauche pour les lignes, à droite pour les colonnes) par une matrice élémentaire **inversible**. Par exemple, multiplier la ligne i d'une matrice $m \times n$ par a, élément inversible de A, revient à multiplier à gauche par la $m \times m$ matrice diagonale dont les éléments sont $1, \ldots, 1, a, 1 \ldots, 1$ où a se trouve à la i-ème place. Bien entendu le déterminant de cette matrice qui, précisément est a, est alors inversible.

Le théorème suivant est vrai sur un anneau principal quelconque. Cependant, il est nécessaire pour le prouver d'introduire la notion d'opération secondaire. On se limitera donc aux anneaux $\mathbb{Z}$ et $k[t]$ qui ont l'avantage de posséder une division euclidienne (ce sont des anneaux dits *euclidiens* et la démonstration reste correcte pour tout anneau euclidien).

Théorème 2.5.3 *Toute matrice, de rang r, à coefficients dans $\mathbb{Z}$ ou $k[t]$ est équivalente à une matrice de la forme*

$$\begin{bmatrix} L & 0 \\ 0 & 0 \end{bmatrix}$$

où L est une matrice diagonale de type (r,r) telle que ses termes diagonaux, tous non nuls, vérifient $\delta_1|\delta_2|\cdots|\delta_r$.

Preuve : Il faut d'abord remarquer qu'on peut, par des manipulations élémentaires, ramener toute matrice $M = (a_{ij})$ à la forme

$$\begin{pmatrix} \delta & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

où δ divise tous les éléments de N.

Remarquons d'abord que, par des échanges de lignes et de colonnes, on peut supposer que $a_{11} \neq 0$.

i) la matrice M est équivalente à une matrice dont la première ligne est de la forme $(\ d \quad 0 \quad b_{13} \quad \cdots \quad b_{1n}\ )$ où $d = \text{pgcd}(a_{11}, a_{12})$. Posons $a = a_{11},\ b = a_{12}$ par commodité.

En effet, supposons $a_{11} > a_{12}$ (sinon on échange les deux premières colonnes). Alors, par division euclidienne, $a_{11} = a_{12}q + r$ avec r "plus petit" au sens de la division euclidienne (si $A = \mathbb{Z}$, c'est $|r| < |b|$, si $A = k[t]$, c'est au sens des degrés).

Alors, en retranchant à la première colonne, q fois la deuxième, la matrice M est équivalente à une matrice dont la première ligne est $(\ r \quad b \quad a_{13} \quad \cdots \quad a_{1n}\ )$; puis, on échange les deux premières colonnes et on recommence avec les éléments b et r, càd. $b = rq_1 + r_1$, et on se retrouve avec le coin remplacé par r_1, etc... En poursuivant le procédé, on retrouve l'algorithme de calcul du pgcd, d. Le deuxième élément de la première ligne est alors un multiple kd, et en retranchant k fois la première colonne à la deuxième, on annule ce deuxième élément. D'où l'affirmation.

ii) En réitérant le procédé i), on annule ainsi tous les termes de la ligne. Mais, de plus, le coin ainsi obtenu, notons-le δ, divise tous les a_{1j}, en particulier, $(a_{11}) \subset (\delta)$ et $(d) \subset (\delta)$. On obtient ainsi une matrice dont la première ligne est $(\ \delta \quad 0 \quad 0 \quad \cdots \quad 0\ )$.

iii) On fait de même pour les éléments de la première colonne, quitte à remettre des éléments non nuls sur la première ligne. Pour finir, on obtient alors une matrice dont la première colonne est du type $(\ \delta' \quad 0 \quad 0 \quad \cdots \quad 0\ )$, mais avec $(\delta) \subset (\delta')$. On recommence alors le procédé pour faire apparaître des zéros dans la première ligne, d'où un coin qui devient δ" tel que $(a) \subset (\delta) \subset (\delta') \subset (\delta")$.

iv) On itère les processus i) à iii) autant que nécessaire. L'anneau étant noethérien, La suite $(a) \subset (\delta) \subset (\delta') \subset (\delta") \subset \cdots$ s'arrête, càd. pour un certain s, $\delta^{(s)} = \delta^{(s+1)}$, mais cela signifie alors que $\delta^{(s)}$ divise tous les termes de la première ligne (ou première colonne) et, en retranchant le nombre de fois nécessaire, la première colonne (ou ligne) on fait apparaître les zéros dans toute la ligne (ou colonne) sans toucher à ceux de la première colonne (ou ligne).

v) Il reste à montrer qu'on peut encore supposer que le coin, appelons-le δ, ainsi obtenu divise tous les éléments de N. Supposons qu'il existe un élément de N que δ ne divise pas. On ajoute alors la ligne qui contient cet élément à la première, et on réitère tout le processus ci-dessus. Comme le nouveau coin est obtenu comme pgcd du coin précédent et des termes de la ligne, ce nouveau coin va donc diviser l'élément en question. On recommence autant que nécessaire. Comme les coins ainsi obtenus engendrent des idéaux en ordre croissant, pour la même raison que ci-dessus, on est sûr que le processus s'arrête.

Il reste à conclure par une récurrence sur la dimension de la matrice M.

2.5.4 Calcul des facteurs invariants

Soit V un A-module de type fini. Alors, si $e_1, \ldots, e_m$ est un système de générateurs de V, il existe un A-homomorphisme surjectif (épimorphisme) $f : A^m \to V$. Le noyau K de f est lui aussi un A-module de type fini, par conséquent, par choix d'un système de n générateurs, il existe un épimorphisme $h : A^n \to K$. D'où $g : A^n \to A^m$ composée de l'inclusion naturelle de K dans A^m et de h.

On obtient ainsi la suite exacte $A^n \xrightarrow{g} A^m \xrightarrow{f} V \longrightarrow 0$, autrement dit, V est le conoyau de g.

Notons M la matrice définie par g dans les bases canoniques de A^n et A^m. Comme deux matrices équivalentes correspondent à la même application A-linéaire, elles définissent le même conoyau.

Si A est euclidien, on peut donc choisir des bases de A^n et A^m telles que la matrice soit de la forme

$$\begin{bmatrix} L & 0 \\ 0 & 0 \end{bmatrix}$$

où L est une matrice diagonale de type (r, r) telle que ses termes diagonaux, tous non nuls, vérifient $\delta_1|\delta_2|\cdots|\delta_r$ (on peut même se contenter de A principal, si on admet, moyennant des opérations "secondaires", le théorème 2.5.3 dans le cas général).

Bien entendu, si A est un anneau principal, K lui-même, comme sous-module d'un module libre, est libre. On peut donc prendre $K = A^n$, ce qui revient à avoir une matrice du type $\begin{bmatrix} L \\ 0 \end{bmatrix}$.

Dans ce cas, l'image de g est $\delta_1 A \oplus \delta_2 A \oplus \cdots \oplus \delta_r A$ dans $A \oplus A \oplus \cdots \oplus A$, d'où un quotient de la forme

$$\frac{A}{\delta_1 A} \oplus \frac{A}{\delta_2 A} \oplus \cdots \oplus \frac{A}{\delta_r A} \oplus A \oplus \cdots \oplus A.$$

Bien entendu, $\delta_i = 1 \Rightarrow \frac{A}{\delta_i A} = 0$. Les idéaux $\delta_1 A \supset \delta_2 A \supset \cdots \supset \delta_r A$ ainsi obtenus sont les **facteurs invariants** de V et ce qui précède constitue une nouvelle preuve de la décomposition en modules monogènes, qui engendre la décomposition en modules primaires cycliques.

2.5.5 Retour aux espaces vectoriels

Tout ceci s'applique bien sûr au cas où $u : V \to V$ est un endomorphisme de k-espaces vectoriels, donnant ainsi à V une structure de $k[t]$-module. Et on obtient ainsi le

Théorème 2.5.4 *Soit u un endomorphisme du k-espace vectoriel V de dimension finie n de matrice $M = (a_{ij})$ dans la base $\mathcal{V} = \{v_1, \ldots v_n\}$. Alors V peut être défini comme le conoyau d'une application $k[t]$-linéaire $k[t]^n \to k[t]^n$ dont la matrice dans la base canonique est diagonale d'éléments $\delta_1|\delta_2|\ldots|\delta_n$, le polynôme caractéristique de u est le produit $\delta_1 \cdots \delta_n$, le polynôme minimal est δ_n, on a un isomorphisme*

$$V \cong \frac{k[t]}{\delta_1} \times \cdots \times \frac{k[t]}{\delta_n}$$

où u correspond à la multiplication par t.

On peut trouver une base de V dans laquelle la matrice de u est "somme directe" de matrices compagnons.

Lorsque δ_n est scindé (par exemple, si k est algébriquement clos), on peut trouver une base de V dans laquelle la matrice de u est sous forme de Jordan.

Preuve : De ce qui précède, on peut immédiatement conclure que V est un $k[t]$-module, conoyau d'une application $k[t]^s \to k[t]^n$. Pour cela, il suffit de remarquer que $\mathcal{V}$ est aussi un système de générateurs de V sur $k[t]$ et, par conséquent, on peut définir un A-homomorphisme $p : k[t]^n \to V$ par $e_i \mapsto v_i$, pour tout $i = 1, \ldots, n$, où on désigne par $\mathcal{E} = \{e_1, \ldots, e_n\}$ la base canonique de $k[t]^n$.

Le noyau K de p est lui-même de type fini (comme sous-module d'un module de type fini sur un anneau noethérien, par exemple ; on peut même remarquer que comme sous-module d'un libre sur un anneau principal, il est libre) ; on peut alors prendre un système de générateurs de K et recommencer la même opération que ci-dessus.

Cependant, avant de le faire, nous remarquons qu'on peut engendrer K par exactement n éléments, ce qui permettra de prendre $s = n$. En effet, $u(v_j) = \sum_i a_{ij} v_i$. Posons alors $w_j = te_j - \sum_i a_{ij} e_i \in k[t]^n$. Par $k[t]$-linéarité, on a $p(w_j) = t \cdot p(e_j) - \sum a_{ij} p(e_i) = u(v_j) - \sum_i a_{ij} v_i = 0$. Par conséquent, $w_1, \ldots, w_n \in K$; notons W le sous-espace de $k[t]^n$ engendré par les w_j. On a donc $W \subset K$.

Mais, modulo W, un élément $R = \sum_s \alpha_s(t) e_s$ se réduit à $R = \sum_r \beta_r e_r$ où $\beta_r \in k$, autrement dit $R = \sum_r \beta_r e_r + w,\ w \in W$ (en effet, pour tout j, $t \cdot e_j = \sum_i a_{ij} e_i + w_j$ et par récurrence, on en déduit que, pour tout entier s, $t^s \cdot e_j$ est combinaison linéaire à coefficients dans k modulo W, d'où $\alpha_s(t) e_s$ aussi, etc...) Il en ressort que $p(R) = 0 \Leftrightarrow p(\sum_r \beta_r e_r) = \sum_r \beta_r p(e_r) = \sum_r \beta_r v_r = 0 \Leftrightarrow R \equiv 0$ modulo W ($\mathcal{V}$ étant une base, il n'y a pas de combinaison linéaire, à coefficients dans k, non triviale entre les v_i), autrement dit, $R \in W$. Conclusion $K = W$. Soit donc l'application $f : k[t]^n \to k[t]^n$ définie par $f(e_j) = -w_j$ et ainsi la suite

$$k[t]^n \xrightarrow{f} k[t]^n \xrightarrow{p} V \longrightarrow 0$$

est exacte.

L'application f étant donnée par $f(e_j) = -te_j + \sum_i a_{ij} e_i$, la matrice de f dans la base $\mathcal{E}$ est alors simplement $M - tI$ (I désignant la matrice unité $n \times n$).

Le paragraphe précédent a montré que cette matrice pouvait se réduire, en faisant des changements de base définis par les matrices P et Q, comme dans le diagramme suivant :

$$\begin{array}{ccccccc} k[t]^n & \xrightarrow{f} & k[t]^n & \xrightarrow{p} & V & \longrightarrow & 0 \\ {\scriptstyle P^{-1}}\downarrow & & \downarrow{\scriptstyle Q} & & \downarrow{\scriptstyle \psi} & & \\ k[t]^n & \xrightarrow{g} & k[t]^n & \longrightarrow & \prod_i \dfrac{k[t]}{\delta_i} & \longrightarrow & 0 \end{array}$$

à une matrice équivalente diagonale de termes $\delta_1 | \delta_2| \cdots | \delta_n$, dont aucun n'est nul.

Le déterminant de $M - tI$, qui n'est autre que le polynôme caractéristique de u, n'est donc pas nul (et la matrice est de rang n) et est aussi celui de la matrice diagonale équivalente, d'où égal au produit des δ_i. De plus, δ_n, multiple de tous les δ_i, annule tous les facteurs $k[t]/\delta_i$, donc V ; et, clairement, comme chacun des facteurs du produit est annulé exactement par l'un des δ_i, aucun polynôme de degré inférieur n'annule $k[t]/\delta_n$, donc δ_n est le polynôme minimal de u (on aura pris soin de prendre les δ_i, et en tous cas δ_n, unitaires).

Une k-base d'un module du type $\dfrac{k[t]}{\delta}$ est constituée par $1, t, t^2, \ldots, t^{d-1}$ où d est le degré de δ. La matrice de l'endomorphisme "multiplication par t" est alors clairement la *matrice compagnon* de δ comme on le vérifie aisément. Pour obtenir une base de V, il suffit alors de prendre son image par ψ^{-1}. En remarquant que u correspond à la multiplication par t. Pour cela, on remonte les calculs : 1, comme $k[t]$-générateur de $k[t]/\delta_j$, est l'image du j-ième vecteur e'_j de la base canonique de $k[t]^n$. En faisant le changement de base de matrice Q^{-1} dans $k[t]^n$,

on se ramène à $k[t]^n = p^{-1}(V)$, puis on prend l'image de $Q^{-1}e'_j$ par p (qui est, rappelons-le $k[t]$-linéaire), cela donne un vecteur $v \in V$ qui engendre un système $v, u(v), u^2(v), \ldots$, partie d'une base cherchée.

En faisant cela pour tous les δ_i, on obtient comme base de V, les vecteurs

$$v_1, u(v_1), u^2(v_1), \ldots, v_2, u(v_2), \ldots, v_n, u(v_n), \ldots$$

dans laquelle la matrice de u est somme directe de matrices compagnons.

De même, si δ_n est scindé, tous les δ_i sont décomposables en facteurs de degré 1 et V est un produit de $k[t]$-modules cycliques primaires de la forme $k[t]/(t-a)^n$. En effet, $t(t-a)^k = (t-a)^{k+1} + a(t-a)^k$. Mais, pour un tel module, la base $1, t-a, (t-a)^2, \ldots$ constitue une base de Jordan pour l'endomorphisme "multiplication par t". Rappelons que les facteurs premiers qui interviennent dans la décomposition en modules primaires cycliques de V sont les **diviseurs élémentaires** du $k[t]$-module V).

Pour remonter aux e'_j, il faut cependant utiliser ici l'isomorphisme (théorème chinois) :

$$\frac{k[t]}{(t-a)^\alpha (t-b)^\beta} \cong \frac{k[t]}{(t-a)^\alpha} \times \frac{k[t]}{(t-b)^\beta}$$

lorsque $a \neq b$.

Pour trouver une base de Jordan de V, on doit prendre les images inverses de générateurs du $k[t]$-module de droite. On obtient ainsi des générateurs de $\dfrac{k[t]}{(t-a)^\alpha (t-b)^\beta}$ dont on prend les images inverses par ψ. Pour ce faire, comme ci-dessus, on les remonte par Q^{-1} et dont on prend l'image par p dans V. Il faut ensuite prendre ces vecteurs et leurs images successives par $u - a\mathrm{Id}$ (ou $u - b\mathrm{Id}$). On obtient ainsi une base de Jordan de V.

Corollaire 2.5.3 *Deux matrices carrées M et N à coefficients dans k sont semblables ssi les matrices $M - tI$ et $N - tI$ sont équivalentes sur $k[t]$.*

Preuve : Les deux matrices $M - tI$ et $N - tI$ sont toutes deux équivalentes à la même matrice diagonale (qui ne dépendait que du couple (V, u) ; elles sont donc équivalentes.

Inversement, deux matrices équivalentes définissent le même $k[t]$-module V, et $\forall v \in V,\ t \cdot v = M \cdot v$ ou $= N \cdot v$, selon que V est le conoyau de $M - tI$ ou $N - tI$. M et N représentent donc le même endomorphisme $u = \times t$, et sont donc semblables.

2.5.6 Exemples

Nous allons traiter ici un exemple très simple : il s'agit de jordaniser la matrice 3×3

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

La matrice caractéristique

$$M - tI = \begin{pmatrix} 1-t & 1 & 1 \\ 0 & 1-t & 1 \\ 0 & 0 & 1-t \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1-t \\ 1-t & 1 & 0 \\ 0 & 1-t & 0 \end{pmatrix}$$

par échange de colonnes

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 1-t & t & -(1-t)^2 \\ 0 & 1-t & 0 \end{pmatrix}$$

, puis en faisant $L_2 := L_2 - (1-t)L_1$ ce qui correspond à la matrice inverse de

$$Q_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1-t & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

, on obtient la matrice

$$M - tI \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & t & -(1-t)^2 \\ 0 & 1-t & 0 \end{pmatrix}.$$

Puis, en faisant $L_2 := L_2 + L_3$ de matrice inverse

$$Q_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},$$

$M - tI$ est encore équivalente à

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -(1-t)^2 \\ 0 & 1-t & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1-t & (1-t)^3 \end{pmatrix}$$

par $C_3 := C_3 + (1-t)^2 C_2$.

Enfin, on obtient

$$M - tI \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (1-t)^3 \end{pmatrix}$$

(où l'on a bien $1|1|(1-t)^3$) par changement $L_3 := L_3 - (1-t)L_2$ de matrice inverse

$$Q_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1-t & 1 \end{pmatrix}.$$

On remarque donc que le polynôme caractéristique de M est $\chi = (1-t)^3 = -\mu$, polynôme minimal.

La matrice Q^{-1} est le produit des trois matrices correspondant aux changements affectant les lignes, càd.

$$Q^{-1} = Q_1^{-1}Q_2^{-1}Q_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1-t & t & -1 \\ 0 & 1-t & 1 \end{pmatrix}.$$

Si $\{e_1', e_2', e_3'\}$ (rappelons que $E_i' = Qe_i$) désigne la base canonique de $k[t]^3$, on a la projection naturelle

$$\pi : k[t]^3 \to C = k[t]/(t-1)^3$$

qui envoie $e_1' \mapsto 0, e_2' \mapsto 0, e_3' \mapsto 1$.

Une base de Jordan du module $k[t]/(t-1)^3$ est alors donnée par $1, t-1, (t-1)^2$ et il faut la remonter (par l'isomorphisme ψ^{-1}) en une base de Jordan de k^3. Or, ψ^{-1} est défini par : pour tout $x \in C$, $\psi^{-1}(x) = p(Q^{-1}y)$ où y est n'importe quel antécédent par π de x. Ainsi pour $x = 1 \in C$, sachant que $\pi(e_3') = 1$, $w_1 := \psi^{-1}(1) = p(Q^{-1}e_3') = p(-e_2 + e_3) = -v_2 + v_3 = (0, -1, 1)$. Et, on obtient alors $w_1, w_2 := (u - \mathrm{Id})(w_1), w_3 := (u - \mathrm{Id})(w_2)$ forment une base de Jordan de V (il est aisé d'ailleurs de vérifier que w_3 est vecteur propre de u).

Exercice : L'exercice suivant est plus long, mais plus complet : jordaniser la matrice 4×4

$$\begin{pmatrix} -7 & 3 & 1 & -6 \\ -6 & 2 & 1 & -6 \\ 0 & 0 & 2 & 0 \\ 6 & -3 & -1 & 5 \end{pmatrix}.$$

Bibliographie

[1] S. LANG, Algèbre, Addison-Wesley.

[2] M.F. ATIYAH, I.G. MACDONALD, Introduction to Commutative Algebra, Addison Wesley Publishing.

[3] R. GODEMENT, Cours d'Algèbre, Herrmann

[4] H. MATSUMURA, Commutative Algebra, Benjamin.

[5] N. BOURBAKI, Algèbre

[6] S. MAC LANE, G. BIRKHOFF, Algèbre 2, les Grands Théorèmes, Gauthier-Villars.

[7] J.P. SERRE, Représentation linéaire des groupes finis.

[8] FULTON, HARRIS, Representations, Springer.

[9] O. ZARISKI, P. SAMUEL, Commutative Algebra, Van Nostrand.

Table des matières

2 Modules sur un anneau **11**

2.1 Modules et homomorphismes . . . 11
2.1.1 Définition : . . . 11
2.1.2 Homomorphismes . . . 11
2.1.3 Opérations sur les sous-modules . . . 12
2.1.4 Modules quotients . . . 13
2.1.5 Propriétés . . . 13
2.1.6 Produit de modules . . . 14
2.1.7 Compléments . . . 14
2.1.8 Exemple des espaces vectoriels sur un corps . . . 15
2.2 Modules de fractions . . . 15
2.3 Suites exactes . . . 16
2.3.1 Définition . . . 16
2.3.2 Résultats . . . 17
2.4 Conditions de finitude . . . 17
2.4.1 Conditions de chaîne . . . 17
2.4.2 Anneaux noethériens . . . 19
2.5 Application aux modules sur les anneaux principaux . . . 20
2.5.1 Rappels . . . 20
2.5.2 Espaces vectoriels sur k et $k[t]$-modules . . . 23
2.5.3 Matrices à coefficients dans un anneau . . . 23
2.5.4 Calcul des facteurs invariants . . . 26
2.5.5 Retour aux espaces vectoriels . . . 26
2.5.6 Exemples . . . 28