LE THÉORÈME PRINCIPAL SUR LES MODULES DE TYPE FINI D'UN DOMAINE PRINCIPAL

ABRAHAM BROER

Introduction

Dans ces notes on donne une autre présentation de quelques résultats du chapitre 12 du manuel [1].

1. Forme normale d'une matrice sur un domaine principal

Soit R un anneau commutatif unitaire. On va considérer des matrices avec coefficients dans l'anneau R. On dit que deux matrices $A, A' \in \mathrm{Mat}(n \times m, R)$ sont *équivalentes* s'il existe deux matrices inversible $P \in \mathrm{GL}(n, R)$ et $Q \in \mathrm{GL}(m, R)$ telles que

$$A' = PAQ.$$

Si R est un corps, on a vu dans le cours de l'algèbre linéaire que chaque matrice est équivalente à une matrice quasi-diagonal de la forme

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & \dots & 0 \\ 0 & \ddots & 0 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 0 & 0 & \ddots & \ddots & \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & & & 0 \end{pmatrix}$$

où le nombre des 1's est exactement le rang de la matrice.

Pour un domaine principal on connaît encore une forme normale, mais pour an anneau quelconque une forme normale n'est pas connu. Dans cette première section on va décrire cette forme normale, si l'anneau est un domaine principal.

1.1. **Idéaux de Fitting d'une matrice.** Si deux matrices sont équivalentes, ces idéaux de Fitting coincident. Soit $A \in \mathrm{Mat}(n \times m, R)$ et $r \geq 1$. On définit $I_r(A)$, le r-ième *idéal de Fitting*, comme étant l'idéal de R engendré tous les $r \times r$ sous-déterminants de A. En particulier, $I(A) := I_1(A)$ est l'idéal engendré par les coefficients de A.

Lemme 1.1. *Supposons A et $A' \in \mathrm{Mat}(n \times m, R)$ sont équivalentes. Alors leurs idéaux de Fitting coincident, c.-à-d. pour chaque r on a que $I_r(A) = I_r(A')$.*

Preuve. On commence avec le cas $r = 1$. Soit $P \in \mathrm{GL}(n, R)$. Alors

$$(PA)_{ij} = \sum_k P_{ik} A_{kj} \in I_1(A),$$

donc $I_1(PA) \subseteq I_1(A)$. Et

$$A_{ij} = \sum_k (P^{-1})_{ik}(PA)_{kj} \in I_1(PA)$$

donc $I_1(A) \subseteq I_1(PA)$, et on conclut $I_1(A) = I_1(PA)$. Clairement $I_r(A^t) = I_r(A)$ où A^t est la matrice transposée de A. Donc si $Q \in \mathrm{GL}(m, R)$ on a

$$I_1(A) = I_1(PA) = I_1((PA)^t) = I_1(Q^t(PA)^t) = I_1((PAQ)^t) = I_1(PAQ).$$

Si $A \in \mathrm{Mat}(n \times m, R)$, $\mathcal{I} = (i_1 < i_2 < \ldots < i_r)$ et $\mathcal{J} = (j_1 < j_2 < \ldots < j_r)$ on définit (où on suppose que $i_r \leq n$ et $j_r \leq m$) la sous-matrice $A(\mathcal{I}|\mathcal{J})$ de taille $r \times r$ définie par les lignes I et les colonnes J par

$$(A(\mathcal{I}|\mathcal{J}))_{s,t} := A_{i_s,j_t}.$$

Soit C une autre matrice, disons de taille $p \times n$. Fixons r et considérons la formule suivante

$$\det\left((CA)(\mathcal{I}|\mathcal{J})\right) = \sum_{\mathcal{K}} \det\left(C(\mathcal{I}|\mathcal{K})\right) \det\left(A(\mathcal{K}|\mathcal{J})\right),$$

où la somme est sur les $\mathcal{K} = (k_1 < k_2 < \ldots < k_r)$, et $i_r \leq p$, $k_r \leq n$, $j_r \leq m$. Si R est un domaine d'intégrité, soit $\mathbb{F}$ le corps des fractions de R. Il suffit clairement de montrer la formule où R est un corps. Puis il suffit de montrer la formule si C ou A est une matrice élémentaire $E_{ij}(c)$, $E_i(c)$, E_{ij} comme défini à l'algèbre linéaire; ce qui se fait directement. On acceptera cette formule si R n'est pas intègre.

En revenant dans notre situation, soit $P \in \mathrm{GL}(n, R)$. Alors un générateur de $I_r(PA)$ s'écrit comme

$$\det\left((PA)(\mathcal{I}|\mathcal{J})\right) = \sum_{\mathcal{K}} \det\left(P(\mathcal{I}|\mathcal{K})\right) \det\left(A(\mathcal{K}|\mathcal{J})\right) \in I_r(A),$$

donc $I_r(PA) \subseteq I_r(A)$. Un générateur de $I_r(A)$ s'écrit comme

$$\det\left((A)(\mathcal{I}|\mathcal{J})\right) = \sum_{\mathcal{K}} \det\left(P^{-1}(\mathcal{I}|\mathcal{K})\right) \det\left(PA(\mathcal{K}|\mathcal{J})\right) \in I_r(PA),$$

donc $I_r(A) \subseteq I_r(PA)$. Et on conclut comme dans le cas $r = 1$. □

1.2. **Un cas spécial.** Dans le restant du section on supposera que R est un domaine principal.

On veut donner une forme normale d'une matrice $n \times m$. On commence par le cas spécial où $m = 1$.

Lemme 1.2. *R est un domaine principal. Soient $a_1, a_2, \ldots, a_n$ et $d \in R$, tels que (d) est l'idéal de R engendré par $a_1, \ldots, a_n$. Alors il existe une matrice inversible $P \in \mathrm{GL}(n, R)$, telle que*

$$P \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Preuve. On utilise l'induction sur n. Pour $n = 1$ on a $(a_1) = (d)$, donc il existe un unité $c \in R^\times$ tel que $ca_1 = d$. Donc on peut utiliser la matrice $P = (c)$ de taille 1×1.

Soit $n \geq 2$ et supposons le résultat est vrai pour les colonnes de dimension $n-1$. Soit $d_2 \in R$ un générateur de l'idéal engendré par $a_2, \ldots, a_n$, qui existe car R est principal. Alors par induction il existe une matrice inversible $P' \in \mathrm{GL}(n-1, R)$ telle que

$$P' \begin{pmatrix} a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

En ajoutant une ligne et un colonne à P', on obtient la matrice inversible $P'' \in \mathrm{GL}(n, R)$:

$$P'' := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & P' & \\ 0 & & & \end{pmatrix}.$$

Donc

$$P'' \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ d_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

On a que

$$(d) = (a_1) + (a_2, \ldots, a_n) = (a_1) + (d_2) = (a_1, d_2).$$

Il suit qu'ils existent $a', b', u, v \in R$ tels que

$$a_1 = a'd, d_2 = b'd, d = ua_1 + vd_2, b'a_1 = a'd_2, 1 = ua' + vb'.$$

On obtient

$$\begin{pmatrix} u & v \\ -b' & a' \end{pmatrix} \begin{pmatrix} a_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix} \text{ et } \begin{pmatrix} u & v \\ -b' & a' \end{pmatrix}^{-1} = \begin{pmatrix} a' & -v \\ b' & u \end{pmatrix}$$

Donc si on prend

$$\tilde{P} := \begin{pmatrix} u & v & 0 & \ldots & 0 \\ -b' & a' & 0 & \ldots & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

et $P := \tilde{P}P''$, alors on aura que P est inversible et

$$P \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \tilde{P} \begin{pmatrix} a_1 \\ d_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Et on est prêt. □

Remarque. Si dans la situation du lemme l'anneau R est une domaine euclidien, alors on peut prendre pour P le produit d'une suite de matrices élémentaires de l'algèbre linéaire, $E_{ij}(c)$ $(c \in R)$, $E_i(c)$ $(c \in R^\times)$ et E_{ij}.

1.3. **La forme normale.** Dans le théorème qui suit on montre que dans la classe d'équivalence d'une matrice matrice $n \times m$ il existe une matrice quasi-diagonale où les éléments non-zéro satisfont des relations de divisibilité.

Théorème 1.1. *Soit $A \in \mathrm{Mat}(n \times m, R)$ une matrice avec coefficients dans un domaine principal R.*

(i) Ils existent des matrices inversibles $P \in \mathrm{GL}(n, R)$ et $Q \in \mathrm{GL}(m, R)$ telles que

$$PAQ = \begin{pmatrix} d_1 & 0 & 0 & 0 & \dots & \dots \\ 0 & d_2 & 0 & 0 & \dots & \dots \\ 0 & 0 & d_3 & 0 & \dots & \dots \\ 0 & 0 & 0 & d_4 & \ddots & \ddots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

où on a en plus que

$$(d_1) \supseteq (d_2) \supseteq (d_3) \dots .$$

(ii) En fait, on a que $(d_1) = I_1(A)$ est l'idéal engendré par les coefficients de A.

(iii) Plus généralement $(d_1 d_2 \cdots d_r) = I_r(A)$ est l'idéal engendré par tous les $r \times r$-sous-déterminants de A. En particulier, les idéaux (d_r) sont uniques, et ne dépendent pas de P et Q.

Preuve. (i) et (ii). On procède par induction. Si $m = 1$ alors (i) suit du lemme 1.2 et (ii) du lemme 1.1. Si $n = 1$ on prends les matrices transposées, et on retombe dans le cas $m = 1$.

Soit maintenant A une matrice $n \times m$ où $n \geq 1$ et $m \geq 1$ et supposons le théorème vrai pour les matrices de taille $n - 1 \times m - 1$. Posons $I = I_1(A)$ pour l'idéal engendré par les coefficients de A. On va procéder en plusieurs étapes.

(1) Si $(a_{11}) \neq I$ on va montrer que A est équivalente à une matrice A' telle que l'idéal (a'_{11}) est strictement plus grand que (a_{11}).

Si dans le premier colonne il existe un a_{i1} pas inclus dans (a_{11}) on utilise le lemme. 1.2 et on est prêt. Pareil, si un coefficient dans la première ligne n'est pas dans (a_{11}). Si a_{ij} n'est pas dans (a_{11}) mais a_{i1} et a_{1j} sont dans (a_{11}), disons $a_{1i} = ca_{11}$ alors on multiplie à droite par la matrice élémentaire $E_{ij}(-c)$ et après par $E_{ji}(1)$. Si A' est la matrice obtenue, on a $a'_{11} = a_{11}$ et $a'_{i1} = a_{ij} + (1 - c)a_{i1}$. Donc $a'_{i1} \notin (a'_{11})$ et on est dans le cas précédent, et on conclut.

Par exemple, si $i = 2 = j = n = m$

$$\begin{aligned} A' &= \begin{pmatrix} a_{11} & ca_{11} \\ a_{21} & a_{22} \end{pmatrix} E_{12}(-c)E_{21}(1) \\ &= \begin{pmatrix} a_{11} & ca_{11} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} - ca_{21} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & 0 \\ a_{22} + (1-c)a_{21} & a_{22} - ca_{21} \end{pmatrix} \end{aligned}$$

(2) En répétant l'étape (1) on trouve des matrices équivalentes $A, A', A'', \ldots$ et une suite stricte d'idéaux

$$(a_{11}) \subset (a'_{11}) \subset (a''_{11}) \subset \ldots.$$

Par la propriété de Noether pour R une telle suite d'idéaux infinie ne peut pas exister. Donc après répéter l'étape (1) un nombre fini de fois, on arrive à une matrice équivalente à A, disons A', telle que $I_1(A) = I_1(A') = (a'_{11})$. Donc tous les coefficients de A' sont divisible par a'_{11}.

(3) En multipliant à gauche par des matrices élémentaires $E_{i1}(c)$ et à droite par des matrices $E_{1i}(c)$ on obtient une matrice A' équivalente à A telle que encore $a'_{11} = I$, et donc $a'_{ij} \in (a'_{11})$ pour chaque i, j, et maintenant en plus que $a'_{i1} = a'_{1j} = 0$ pour chaque $i \neq 1$ et $j \neq 1$.

(4) Soit A'' la matrice $n-1 \times m-1$ telle que

$$A' = \begin{pmatrix} a'_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{pmatrix},$$

où A' est la matrice obtenue en (3). Par induction ils existent des matrices P'' et Q'' tel que

$$P''A''Q'' = \begin{pmatrix} d_2 & 0 & 0 & 0 & \ldots & \ldots \\ 0 & d_3 & 0 & 0 & \ldots & \ldots \\ 0 & 0 & d_4 & 0 & \ldots & \ldots \\ 0 & 0 & 0 & d_5 & \ddots & \ddots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

ou

$$(d_2) \supseteq (d_3) \supseteq (d_4) \ldots,$$

et (d_2) est l'idéal engendré par les coefficients de A''.

Posons $d_1 := a'_{11}$, alors $(d_1) = I$ et $(d_1) \supseteq (d_2)$. On pose

$$P' := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & P'' & \\ 0 & & & \end{pmatrix}, Q' := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & Q'' & \\ 0 & & & \end{pmatrix}$$

et on obtient

$$P'A'Q' = \begin{pmatrix} d_1 & 0 & 0 & 0 & \dots & \dots \\ 0 & d_2 & 0 & 0 & \dots & \dots \\ 0 & 0 & d_3 & 0 & \dots & \dots \\ 0 & 0 & 0 & d_4 & \ddots & \ddots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

Donc ça conclut la preuve de (i) et (ii).

(iii) Si $A' = PAQ$ est la matrice

$$A' := \begin{pmatrix} d_1 & 0 & 0 & 0 & \dots & \dots \\ 0 & d_2 & 0 & 0 & \dots & \dots \\ 0 & 0 & d_3 & 0 & \dots & \dots \\ 0 & 0 & 0 & d_4 & \ddots & \ddots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

où $(d_1) \supseteq (d_2) \supseteq (d_3) \supseteq (d_4) \dots$, alors on voit directement que

$$I_r(A') = (d_1 d_2 \dots d_r).$$

Donc par le lemme aussi $I_r(A) = (d_1 d_2 \dots d_r)$. □

Remarque. Si R est un domaine euclidien on peut faire tous les modifications avec les trois types des matrices élémentaires classiques.

(1) Par opérations élémentaires lignes/colonnes on peut réduire A à une matrice où le coefficient A_{11} divise tous les autres coefficients.

(2) Par opérations élémentaires lignes/colonnes on peut réduire A à une matrice où le coefficient A_{11} divise tous les autres coefficients et en plus que tous les autres coefficients de la première ligne et le premier colonne sont 0.

(3) Puis on va ce concentrer sur la sous-matrice obtenue en éliminant la première ligne et le premier colonne. Et cetera.

1.4. **Matrices inversibles.** Soit R encore un domaine principale. Considérons le cas où $A \in \mathrm{Mat}(n \times n, R)$ est une matrice carré. Alors A est inversible $\iff$ A est équivalente à la matrice identité 1_n $\iff$ on a $(d_r) = (1) = R$, pour chaque $1 \leq r \leq n$ $\iff$ $(d_1 d_2 \cdots d_n) = (1) = R$ $\iff$ le déterminant de A est un unité dans R.

2. Présentations finies

Soit R un anneau commutatif unitaire noetherien et M un R-module finiment engendré. On va voir que M est (à isomorphisme près) déterminé par une classe d'equivalence de matrices A avec coefficients dans R. Si R est un domaine principal, la forme normale des matrices donne comme conséquence aussi une forme normale des R-modules de type fini. Ainsi on peut facilement décrire tous les R-modules de type fini.

Le choix d'un système de générateurs, disons $m_1, \ldots, m_n$, induit un R-module homomorphism surjectif

$$\phi_0 : R^n \to M : \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^{n} a_i m_i.$$

Le R-module R^n est noetherien aussi, donc le noyau $\operatorname{Ker} \phi_0$ est aussi un R-module finiment engendré. On dit que $\operatorname{Ker} \phi_0$ est le *module des relations* parmi les générateurs, car

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \operatorname{Ker} \phi_0 \iff \sum_{i=1}^{n} a_i m_i = 0 \text{ (i.e., une relation).}$$

Soit $r_1, \ldots, r_m$ un système de générateurs du $\operatorname{Ker} \phi_0$. On définit la matrice $A \in \operatorname{Mat}(n \times m, R)$ avec le vecteur r_j comme colonne j, et un R-morphisme

$$\phi_1 : R^m \to R^n : \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \mapsto \sum_{j=1}^{m} b_j r_j,$$

ou $\phi_1(v) = Av$, en termes de la multiplication matricielle.

Par construction, $\operatorname{Ker} \phi_0 = \operatorname{Im} \phi_1$ et ϕ_0 est surjectif. On dit que

$$R^m \xrightarrow{\phi_1} R^n \xrightarrow{\phi_0} M$$

est *une présentation finie* de M. On retrouve le système des générateurs de M comme l'image par ϕ_0 de la base canonique de R^n. Et on retrouve M comme

$$M \simeq R^n / \operatorname{Ker} \phi_0 = R^n / \operatorname{Im} \phi_1$$

et $\operatorname{Im} \phi_1$ est l'espace colonne de la matrice A. Donc avec la matrice A donnée on peut reconstruire M (à isomorphisme près) comme R^n modulo l'espace colonne de A. Si A' est équivalente à A, alors il existe une autre présentation de M avec matrice A', comme on verra.

Exemple 2.1. Supposons on a une présentation de M telle que la matrice A est

$$\begin{pmatrix} a & 0 \\ 0 & b \\ 0 & 0 \end{pmatrix}.$$

Posons

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 := \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Alors l'espace colonne est

$$Rae_1 \oplus Rbe_2 \oplus 0e_3 \subset Re_1 \oplus Re_2 \oplus Re_3,$$

donc

$$M \simeq (Re_1 \oplus Re_2 \oplus Re_3,) \,/\, (Rae_1 \oplus Rbe_2 \oplus 0e_3) \simeq R/(a) \oplus R/(b) \oplus R.$$

2.1. **Changement des bases.** Si on change les bases de R^n et R^m on obtient une autre présentation finie du même module, qui peut être plus convenable.

Proposition 2.1. *Soient R un anneau commutatif unitaire, M un R-module finiment engendré et*

$$R^m \xrightarrow{\phi_1} R^n \xrightarrow{\phi_0} M$$

une présentation finie de M, c.-à-d., ϕ_0 est surjectif et $\operatorname{Ker}\phi_0 = \operatorname{Im}\phi_1$. Et soient $\psi_2 : R^m \to R^m$ et $\psi_1 : R^n \to R^n$ deux R-module automorphismes. Alors

$$\phi_1' = \psi_1 \circ \phi_1 \circ \psi_2^{-1} : R^m \to R^n \quad \text{et } \phi_0' = \phi_0 \circ \psi_1^{-1} : R^n \to M$$

définissent une autre présentation finie, c.-à-d., ϕ_0' est surjectif et $\operatorname{Ker}\phi_0' = \operatorname{Im}\phi_1'$.

$$\begin{array}{ccccc} R^m & \xrightarrow{\phi_1} & R^n & \xrightarrow{\phi_0} & M \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle =} \\ R^m & \xrightarrow{\phi_1'} & R^n & \xrightarrow{\phi_0'} & M \end{array}$$

Preuve. Les morphismes ϕ_0 et ψ_1^{-1} sont surjectifs, donc la composition $\phi_0' = \phi_0 \circ \psi_1^{-1}$ est aussi surjectif.

$$\begin{aligned} \operatorname{Ker}\phi_0' &= \{v \in R^n; \phi_0(\psi_1^{-1}(v)) = 0\} \\ &= \{v \in R^n; \psi_1^{-1}(v) \in \operatorname{Ker}\phi_0\} \\ &= \{v \in R^n; \psi_1^{-1}(v) \in \operatorname{Im}\phi_1\} \\ &= \{v \in R^n; v \in \operatorname{Im}\psi_1 \circ \phi_1\} \\ &= \{v \in R^n; v \in \operatorname{Im}\phi_1' \circ \psi_2\} \\ &= \{v \in R^n; v \in \operatorname{Im}\phi_1'\} \\ &= \operatorname{Im}\phi_1' \end{aligned}$$

Donc la paire (ϕ_1', ϕ_0') est aussi une présentation fini de M. □

2.2. **Exemple d'une présentation finie.** Soit $\mathbb{F}$ un corps et $R := \mathbb{F}[t]$ l'anneau de polynômes. Un R-module est la même chose comme un espace vectoriel avec un endomorphisme $\mathbb{F}$-linéaire fixé, disons $\eta : V \to V$. Alors la structure de R-module sur V est donnée par $f(t) \cdot v := f(\eta)(v)$, en particulier par définition

$$t \cdot v = \eta(v).$$

Supposons que V est de dimension finie, vu comme espace vectoriel sur $\mathbb{F}$. Fixons une $\mathbb{F}$-base $\mathcal{B} = \{b_1, \ldots, b_n\}$ de V. Sur cette base l'endomorphisme $\eta : V \to V$ est représenté par une matrice, disons $B \in \operatorname{Mat}(n \times n, \mathbb{F})$, telle que

$$t \cdot b_j = \eta(b_j) = \sum_{i=1}^{n} B_{ij} b_i.$$

Un automorphisme $\alpha : V \to V$ de R-modules est une application bijective telle que

$$\alpha(v_1 + v_2) = \alpha(v_1) + \alpha(v_2), \quad \text{et } \alpha(f(t) \cdot v) = f(t) \cdot \alpha(v),$$

pour $v, v_1, v_2 \in V$, $f(t) \in \mathbb{F}[t]$. C'est la même chose comme un automorphisme α d'espace vectoriel sur $\mathbb{F}$ tel que $\alpha \circ \eta = \eta \circ \alpha$.

La base $\mathcal{B}$ va nous aussi servir comme ensemble générateur de V comme R-module. Posons $\{e_1, \ldots, e_n\}$ pour la base canonique de R^n. Ainsi on obtient l'épimorphisme de R-module

$$\phi_0 : R^n \to V : \sum_i f_i(t) e_i \mapsto \sum_i f_i(t) \cdot b_i.$$

Cherchons maintenant des générateurs du noyau de ϕ_0, ou des R-relations entre les b_i's. Posons

$$f_j := te_j - \sum_{i=1}^{n} B_{ij} e_i \in R^n.$$

Alors $\phi_0(f_j) = t \cdot b_j - \sum_{i=1}^n B_{ij} b_i = 0$ et donc les $f_j \in \mathrm{Ker}(\phi_0)$. On montre que les f_j engendrent le noyau de ϕ_0 déjà.

Lemme 2.1. *Le noyau de ϕ_0 est le sous-R-module de R^n engendré par $f_1, \ldots, f_n$.*

Preuve. Soit $x = \sum_j F_j(t) e_j \in R^n$. Écrivons $F_j(t) = c_j + G_j(t) \cdot t$, où $c_j \in \mathbb{F}$. En utilisant $te_j = f_j + \sum_{i=1}^n B_{ij} e_i$ on obtient

$$\begin{aligned} \sum_j F_j(t) e_j &= \sum_j c_j e_j + \sum_j G_j(t) \cdot t \cdot e_j \\ &= \sum_j c_j e_j + \sum_j G_j(t) \cdot f_j + \sum_{i,j} B_{ij} G_j(t) \cdot e_j. \end{aligned}$$

En continuant comme ça on arrive à montrer qu'on peut écrire

$$x = \sum_j F_j(t) e_j = \sum_j a_j e_j + \sum_j H_j(t) f_j,$$

où $a_j \in \mathbb{F}$ et $H_j(t) \in R$. On obtient que

$$\phi_0(x) = \sum_j a_j b_j.$$

Donc $x \in \mathrm{Ker}(\phi_0)$ si et seulement si $\sum_j a_j b_j = 0$ si et seulement $a_1 = a_2 = \ldots = a_n = 0$ (car les b_i's font une $\mathbb{F}$-base). Il suit que

$$\mathrm{Ker}(\phi_0) =< f_1, f_2, \ldots, f_n > .$$

□

On obtient ainsi une présentation finie

$$R^n \xrightarrow{\phi_1} R^n \xrightarrow{\phi_0} V$$

où la matrice de ϕ_1 par rapport à la base canonique $e_1, \ldots, e_n$ est

$$A := \begin{pmatrix} t-b_{11} & -b_{12} & -b_{13} & \ldots & -b_{1n} \\ -b_{21} & t-b_{22} & -b_{23} & \ldots & -b_{2n} \\ -b_{31} & -b_{32} & t-b_{33} & & \vdots \\ \vdots & \vdots & & \ddots & -b_{n-1,n} \\ -b_{n1} & -b_{n2} & \ldots & -b_{n,n-1} & t-b_{nn} \end{pmatrix} = t1_n - B$$

Remarquer que les colonnes sont les relations f_i écrites sur la R-base des e_i. On a rencontré cette matrice déjà une fois dans le cours de l'algèbre linéaire. Son déterminant est le polynôme caractéristique de B, qu'on utilise pour trouver les valeurs propres de B.

Maintenant on va trouver une meilleure présentation de la même V. Par le th. 1.1 il existe des matrices inversibles $P, Q \in \mathrm{GL}(n, \mathbb{F}[t])$ (avec coefficients dans R) telles que

$$PAQ = \mathrm{diag}\,(d_1(t), d_2(t), \ldots, d_n(t))$$

où on a en plus que $d_i(t)$ est un polynme unitaire (possiblement 1), $d_i(t)|d_j(t)$ si $i < j$, $d_1(t)$ est le plus grand commun diviseur des coefficient de A et $d_1 d_2 \cdots d_n = \det(A)$ est le polynôme caractéristique de B. Les $d_i(t)$ sont appelés les *facteurs invariants* de la matrice B. Ils sont uniques.

La matrice inversible P définit un automorphism ψ_1 de R^n et l'inverse Q^{-1} définit un automorphisme ψ_2 de R^n. On obtient une autre présentation finie (ϕ_1', ϕ_0') de V, où la matrice associé à ϕ_1' est $\mathrm{diag}\,(d_1(t), d_2(t), \ldots, d_n(t))$. Les nouvelles générateurs comme R-module sont les

$$b_j' := \phi_0'(e_j) = \phi_0(\sum_j [P^{-1}]_{ij} e_i) = \sum_j [P^{-1}]_{ij} \cdot b_i.$$

On a

$$V = Rb_1' \oplus Rb_2' \oplus \ldots \oplus Rb_n'$$

et

$$Rb_i' \simeq \mathbb{F}[t]/(d_i(t))$$

. Donc on a un isomorphisme de $\mathbb{F}[t]$-module

$$V \simeq \mathbb{F}[t]/(d_1(t) \oplus \mathbb{F}[t]/(d_2(t)) \oplus \ldots \oplus \mathbb{F}[t]/(d_3(t)).$$

Soit $F(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots + a_{n-1} t + a_n$ un polynôme unitaire dans $\mathbb{F}[t]$. Considérons $\mathbb{F}[t]/(F(t))$ comme $\mathbb{F}[t]$ module. Comme espace vectoriel une base est $1, \bar{t}, \ldots, \bar{t}^{n-1}$. On a

$$\overline{t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots + a_{n-1} t + a_n} = 0,$$

donc

$$t \cdot \bar{t}^i = \begin{cases} \bar{t}^{i+1} & \text{si } i < n-1 \\ \bar{t}^n = -a_n - a_{n-1}\bar{t} - \ldots - a_1 \bar{t}^{n-1} & \text{si } i = n-1. \end{cases}$$

Sur cette base la multiplication par t est donnée par la *matrice de compagnon*

$$C(F(t)) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_n \\ 1 & 0 & 0 & \dots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \dots & 0 & -a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}$$

La matrice de compagnon a la propriété que $F(t)$ est le polynôme caractéristique et le polynôme minimal de $C(F(t))$.

2.3. **Forme canonique rationnelle.** Soit $\delta_i := \deg(d_i(t)$. Alors

$$b'_1, t \cdot b'_1, \dots, t^{\delta_1 - 1} \cdot b'_1, b'_2, t \cdot b'_2, \dots, t^{\delta_2 - 1} \cdot b'_2, \dots, t^{\delta_n - 1} \cdot b'_n$$

est une nouvelle base de V et sur cette base la matrice B sera représentée par la matrice bloc-diagonale avec les matrices compagnon des facteurs invariants comme blocs

$$\operatorname{diag}\left(C(d_1(t), C(d_2(t)), \dots, C(d_n)\right).$$

Théorème 2.1. *Soit $\mathbb{F}$ un corps et $B \in \operatorname{Mat}(n \times n, \mathbb{F})$. Alors il existe une matrice inversible $P \in \operatorname{GL}(n, \mathbb{F})$ telle que PBP^{-1} est de la forme canonique rationnelle :*

$$PBP^{-1} = \operatorname{diag}\left(C(d_1(t), C(d_2(t)), \dots, C(d_n)\right),$$

où $C(d_i(t))$ est la matrice compagnon du facteur invariant $d_i(t)$.

Ici, $d_1 | d_2 | \dots | d_n$, $d_1 d_2 \cdot d_n$ est le polynôme caractéristique de B, d_n est le polynôme minimal de B et $d_1 = 1$ si et seulement si B n'est pas une matrice scalaire.

2.4. **Forme canonique de Jordan.** Pour les nombres complexes $\mathbb{C}$ il y a une autre forme normale. Soit $F(t) \in \mathbb{C}[t]$ un polynôme unitaire. Alors ils existent des $\alpha_i \in \mathbb{C}$ ($\alpha_i \neq \alpha_i$ si $i \neq j$) et $n_i \geq 1$ tels que

$$F(t) = \prod_i (t - \alpha_i)^{n_i}.$$

Par le théorème chinois il existe un isomorphisme (de $\mathbb{C}[t]$-module et d'anneau)

$$\mathbb{C}[t]/(F(t)) \simeq \mathbb{C}[t]/((t-\alpha_1)^{n_1}) \oplus \mathbb{C}[t]/((t-\alpha_2)^{n_2}) \oplus \mathbb{C}[t]/((t-\alpha_r)^{n_r})$$

Une autre base naturelle sur $\mathbb{C}[t]/((t-\alpha)^n)$ est

$$1, (\overline{t-\alpha}), (\overline{t-\alpha})^2, \dots, (\overline{t-\alpha})^{n-1}.$$

On a

$$t \cdot (\overline{t-\alpha})^i = (\overline{t-\alpha})^{i+1} + \alpha(\overline{t-\alpha})^i$$

Multiplication par t est représentée sur cette base par *la matrice de Jordan*

$$J(n,\alpha) = \begin{pmatrix} \alpha & 0 & \cdots & & \cdots & 0 \\ 1 & \alpha & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \alpha & 0 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & 0 & 1 & \alpha & 0 \\ 0 & 0 & \cdots & 0 & 1 & \alpha \end{pmatrix}$$

Théorème 2.2. *Soit $B \in \mathrm{Mat}(n \times n, \mathbb{C})$. Alors il existe une matrice inversible $P \in \mathrm{GL}(n,\mathbb{C})$ telle que PBP^{-1} est bloc diagonal où chaque bloc est une matrice de Jordan $J(n,\alpha)$. Le nombre de fois que $J(n,\alpha)$ apparaît comme bloc est le nombre de i où α est une racine du facteur invariant $d_i(t)$ avec multiplicité exactement n. En particulier α est une racine du polynôme caractéristique, donc une valeur propre de B.*

3. Forme normal des modules de type fini sur un domaine principal.

3.1. **Torsion.** Soit R un domaine d'intégrité et M un R-module finiment engendré. On définit

$$\mathrm{Tor}(M) := \{m \in M; \exists r \in R, r \neq 0, rm = 0\}.$$

Il est facile à voir que $\mathrm{Tor}(M)$ (*la torsion de M*) est un sous module de M. On dit que M est *un module de torsion* si $M = \mathrm{Tor}(M)$ et on dit que M est *torsion libre* si $\mathrm{Tor}(M) = \{0\}$.

Par exemple, $\mathrm{Tor}(M)$ est un module de torsion et $M/\mathrm{Tor}(M)$ est torsion libre. Si r est le rang de M et $m_1, \ldots, m_r$ sont R-linéairement indépendant, alors $M/ < m_1, \ldots, m_r >$ est un module de torsion.

L'annulateur $\mathrm{Ann}(M)$ de M est l'idéal

$$\mathrm{Ann}(M) = \{r \in R; \forall m \in M : \ rm = 0\}.$$

Si M est torsion libre, alors $\mathrm{Ann}(M) = (0)$; si M est module de torsion (de type fini) alors $\mathrm{Ann}(M) \neq (0)$.

Par exemple, soit $R = \mathbb{R}[x^2, x^3]$ le sous-algèbre réelle de $\mathbb{R}[x]$ engendrée par x^2 et x^3. Considérons $M := \mathbb{R}[x]$ comme R-module. Alors M est un R-module torsion libre, mais pas libre. Le rang de M est un et $M =< 1, x >$. Le module $M/ < 1 >$ est un module de torsion avec annulateur l'idéal maximal $I = (x^2, x^3) \subset R$. L'idéal I est un sous-module de R de rang un, mais I n'est pas libre. Remarquons que R est un domaine d'intégrité (et noetherien), mais pas un domain principal. Un domaine principal a des meilleures propriétés: dans ce cas un module de type fini est libre si et seulement si c'est torsion libre, et chaque module de type fini est la somme directe de son sous-module de torsion et un module libre. Ce sera montré dans le théorème principal.

3.2. **Théorème fondamental des modules de type fini sur un domain principal.** Nous sommes maintenant prêt à formuler et montrer le théorème fondamental.

Théorème 3.1. *Soit R un domaine principal et $M \neq \{0\}$ un R-module finiment engendré de rang r.*

(i) Il existe un $s \geq 0$, des idéaux principaux uniques

$$R \neq (d_1) \supseteq (d_2) \supseteq (d_3) \supseteq \ldots \supseteq (d_s) \neq (0)$$

et un isomorphisme de R-modules

$$M \simeq R^r \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_s).$$

(ii) $M \simeq R^r \oplus \mathrm{Tor}(M)$, et (d_s) est l'annulateur de $\mathrm{Tor}(M)$.

(ii) Chaque sous-module N d'un module libre M de rang fini est libre, et le rang de N n'est pas plu grand que le rang de M.

Preuve. (i) Choisissons une présentation finie de M

$$R^m \xrightarrow{\phi_1} R^n \xrightarrow{\phi_0} M$$

et soit $A \in \mathrm{Mat}(n \times m, R)$ la matrice associée à ϕ_1, par rapport aux bases canonique de R^n et R^m.

Par le th. 1.1 ils existent $P \in \mathrm{GL}(n, R)$, $Q \in \mathrm{GL}(m, R)$ et

$$(d_1) \supseteq (d_2) \supseteq (d_3) \supseteq \ldots \supseteq$$

tels que

$$A' := PAQ = \begin{pmatrix} d_1 & 0 & 0 & 0 & \ldots & \ldots \\ 0 & d_2 & 0 & 0 & \ldots & \ldots \\ 0 & 0 & d_3 & 0 & \ldots & \ldots \\ 0 & 0 & 0 & d_4 & \ddots & \ddots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

Si $n > m$ on pose $d_i = 0$ pour $i > m$.

Définissons les automorphismes

$$\psi_1 : R^n \to R^n : \psi_1(v) := Pv$$

et

$$\psi_2 : R^m \to R^m : \psi_2(w) := Q^{-1}w.$$

Par la prop. 2.1 on obtient une autre présenation finie

$$R^m \xrightarrow{\phi_1'} R^n \xrightarrow{\phi_0'} M$$

et la matrice plus haute $A' \in \mathrm{Mat}(n \times m, R)$ est exactement la matrice associée à ϕ_1'. Si $e_1, \ldots, e_n$ est la base canonique, alors l'espace colonne de A' est engendré par $d_1e_1, d_2e_2, \ldots . d_ne_n$. Donc $\mathrm{Ker}\,\phi_0' = \mathrm{Im}\,\phi_1' =< d_1e_1, d_2e_2, \ldots, d_ne_n >$. Par le premier théorème d'isomorphisme, on a (car ϕ_0' est surjectif)

$$\begin{aligned} M &\simeq R^n/\,\mathrm{Ker}\,\phi_0' = R^n/\,\mathrm{Im}\,\phi_1' \\ &\simeq R^n/ < d_1e_1, d_2e_2, \ldots, d_ne_n > \\ &\simeq (Re_1 \oplus Re_2 \oplus \ldots \oplus Re_n)\,/Rd_1e_1 \oplus Rd_2e_2 \oplus \ldots \oplus Rd_ne_n, \\ &\simeq (Re_1/Rd_1e_1) \oplus (Re_1/Rd_1e_1) \oplus \ldots \oplus (Re_n/Rd_ne_n) \\ &\simeq R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_n). \end{aligned}$$

Si $(d_1) = R$ on a $R/(d_1) = \{0\}$, on peut enlever le terme et on peut donc supposer que $(d_1) \neq \{0\}$. Si $(d_s) \neq (0)$ et $(d_{s+1}) = (d_{s+2}) = \ldots = (d_n) = (0)$, alors $R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_s)$ est annulé par (d_s) et $M \simeq R^{n-s} \oplus R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_s$. Donc le rang de M est $n-s$, i.e., $r = n-s$.

La torsion de M est donc isomorphe à

$$R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_s)$$

où les $(d_i) \neq \{0\}$ et l'annulateur de $\mathrm{Tor}(M)$ est (d_s). Donc $M \simeq R^r \oplus \mathrm{Tor}(M)$, et (ii) est montré.

Il reste à montrer l'unicité. Il suffit de montrer que si $M_1 \simeq M_2$ où

$$M_1 = R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_s)$$

$(d_1|d_2|d_3 \cdots$ et $(d_s) \neq (0))$ et

$$M_2 = R/(d'_1) \oplus R/(d'_2) \oplus \ldots \oplus R/(d'_{s'}),$$

$(d'_1|d'_2|d'_3 \cdots$ et $(d'_{s'}) \neq (0))$, alors $s = s'$ et $(d_i) = (d'_i)$.

On va utiliser le résultat suivant simple. Soit $p \in R$ premier et $M := R/(d)$. Alors $\kappa(p) = R/(p)$ est un corps

$$M/pM \simeq \begin{cases} (0) & \text{si } p \not| d, \\ \kappa(p) & \text{si } p|d. \end{cases}$$

And si $p|d$ alors $pM \simeq R/(d_1/p)$.

On utilise l'induction sur le nombre de facteurs premier de $d_s d_{s'}$. Si $d_s d_{s'}$ a zero facteurs alors $M_1 = M_2 = (0)$.

Soit $p|d_1$, alors $p|d_i$ pour chaque i, et donc $\dim_{\kappa(p)} M_1/pM_1 = s$ et

$$\dim_{\kappa(p)} M_2/pM_2 = \#\{1 \leq i \leq s'; p|d'_i\} \leq s'.$$

Donc $s \leq s'$. Si on utilise $p|d'_1$ il suit que $s' \leq s$. Donc $s = s'$ et un premier p divise tous les d'_i's et tous les d_i's

On a $pM_1 \simeq R/(d_1/p) \oplus R/(d_2/p) \oplus \ldots \oplus R/(d_s/p)$, $pM_2 \simeq R/(d'_1/p) \oplus R/(d'_2/p) \oplus \ldots \oplus R/(d'_s/p)$. Par induction il suit que $(d_i/p) = (d'_i/p)$ et donc aussi $(d_i) = (d'_i)$. Ce qui finit la preuve de l'unicité.

(iii) Soit N un sous-module de R^n. Soit A la matrice $m \times n$ avec des générateurs de N comme colonnes. En changeant la base de R_n et les générateurs de N on peut supposer que la matrice est de la forme quasi diagonale. Donc sur la nouvelle base $f_1, \ldots, f_n$ de R^n les générateurs de N sont $d_1 f_1, d_2 f_2, \ldots d_m f_m$. On peut supposer que les $d_i \neq 0$ (sinon on jette ces générateurs). On a donc un isomorphisme naturel $R^m \simeq N$ et donc N est libre et son rang n'est pas plus grand que n. □

3.3. **Application aux groupes abéliens.** Un $\mathbb{Z}$-module est la même chose comme un groupe abélien.

Corollaire 3.1. *Soit A un groupe abélien fini. Alors ils existent des (uniques) entiers $s \geq 1$ et*

$$0 < d_1 \leq d_2 \leq \ldots \leq d_s$$

tels que $d_i|d_j$ si $i \leq j$ et il existe un isomorphisme de groupe

$$A \simeq \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \ldots \times \mathbb{Z}/(d_s).$$

3.4. **Application aux τ-groupes.** Un τ-groupe est un groupe abélien avec un automorphisme de groupe $\tau : A \to A$ tel que $\tau^2 = -1$. Un homomorphisme de τ-groupe $f : A_1 \to A_2$ est un homomorphisme de groupe tel que $f(\tau(a_1)) = \tau(f(a_1)$. Par exemple, si $0 \neq (d) \subset \mathbb{Z}[i]$, alors $\mathbb{Z}[i]/(d)$ est un groupe abélien fini avec $\tau\left(\overline{a+bi}\right) := \overline{-b+ai}$.

Corollaire 3.2. *Soit A un τ-groupe fini. Alors ils existent $s \geq 1$ et des entiers de Gauss*

$$d_1, d_2, \ldots, d_s$$

tels que $d_i | d_j$ si $i \leq j$ et il existe un isomorphisme de τ-groupe

$$A \simeq \mathbb{Z}[i]/(d_1) \times \mathbb{Z}[i]/(d_2) \times \ldots \times \mathbb{Z}[i]/(d_s).$$

Preuve. Un τ-groupe n'est rien d'autre qu'un $\mathbb{Z}[i]$-module (τ est la multiplication par i), et $\mathbb{Z}[i]$ est un domaine principal. □

Références

[1] D.S. Dummit et R.M. Foote, *Abstract Algebra. Third edition*, John Wiley & Sons, Inc., Hoboken, N.J., 2004