Chapitre 3

Modules sur un anneau principal

Les principales applications de la théorie que nous allons développer dans ce chapitre seront la structure des groupes abéliens de type fini (cas de l'anneau principal $\mathbf{Z}$) et la structure des endomorphismes des espaces vectoriels de dimension finie (cas de l'anneau principal $K[X]$). Nous retrouverons des résultats déjà obtenus en L2 et L3, qui seront affinés et complétés.

3.1 Modules libres

3.1.1 Sous-modules d'un module libre

Rappelons que si le A-module L est libre de rang n et si $\mathcal{B} := (e_1, \ldots, e_n)$ en est une base, l'application $P \mapsto \mathcal{B}P$ est une bijection de $\mathrm{GL}_n(A)$ sur l'ensemble des bases de L.

Théorème 3.1.1 (de la base adaptée) *Soient L un A-module libre de rang n et $R \subset L$ un sous-module. Il existe alors une base $\mathcal{B} := (e_1, \ldots, e_n)$ de L et des éléments non nuls $d_1, \ldots, d_k$ de A avec $0 \leq k \leq n$, tels que :*

$$d_1 | \cdots | d_k \text{ et } (d_1 e_1, \ldots, d_k e_k) \text{ est une base de } R.$$

Preuve. - Il existe une preuve "géométrique" que l'on trouvera dans Lang et dans RW3. On va donner ici une preuve plus algorithmique, mais sous une hypothèse plus restrictive (anneau euclidien) : cependant, cette hypothèse sera satisfaite dans nos applications.
Comme A est noetherien (puisque principal), on sait *a priori* que R est de type fini. On choisit une base arbitraire $\mathcal{X} := (x_1, \ldots, x_n)$ de L (elle a nécessairement n éléments) et un système générateur fini $\mathcal{Y} := (y_1, \ldots, y_p)$ de R. L'écriture des y_j dans la base $\mathcal{X}$ se traduit par une relation $\mathcal{Y} = \mathcal{X}M$ où $M \in \mathrm{Mat}_{n,p}(A)$ (la j-ème colonne de M est formée des coordonnées de y_j dans la base $\mathcal{X}$).
D'après le théorème 3.1.5, que nous démontrerons plus loin, on a une *équivalence de matrices* :

$$M = PDQ^{-1}, \text{ où } P \in \mathrm{GL}_n(A), Q \in GL_p(A) \text{ et } D = \mathrm{Diag}(d_1, \ldots, d_k) \in \mathrm{Mat}_{n,p}(A), \text{ avec } d_1, \ldots, d_k \neq 0, d_1 | \cdots | d_k.$$

Exceptionnellement ici, la notation $\mathrm{Diag}(d_1, \ldots, d_k)$ désigne la matrice rectangulaire $(e_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ telle que $e_{i,j} = d_i$ si $i = j \in \{1, \ldots, k\}$ et $e_{i,j} = 0$ autrement.
De la relation $\mathcal{Y} = \mathcal{X}M$, on tire $\mathcal{Y}Q = \mathcal{B}D$, où $\mathcal{B} := \mathcal{X}P$ est bien entendu une base ; notons-la $(e_1, \ldots, e_n)$. La famille $\mathcal{Y}Q$ engendre $\mathcal{Y}QA^p = \mathcal{Y}A^p = R$ (puisque Q est inversible). On a visiblement $\mathcal{Y}Q = (d_1 e_1, \ldots, d_k e_k, 0, \ldots, 0)$, de sorte que la famille $(d_1 e_1, \ldots, d_k e_k)$ engendre R. Enfin, les d_i étant non nuls, il est facile de voir que c'est une famille libre. □

Exemple 3.1.2 Soit $A := \mathbf{Z}$, $L := \mathbf{Z}^2$, et R le sous-module engendré par $(-10,-8)$ et $(14,10)$. Si l'on note $\mathcal{X} = (x_1, x_2)$ la base canonique de L, on a donc une famille génératrice :

$$\mathcal{Y} = (y_1, y_2) = \mathcal{X} \begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}.$$

On vérifie facilement que :

$$\begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} \begin{pmatrix} 1 & 5 \\ 1 & 4 \end{pmatrix}^{-1}.$$

(On verra plus loin comment trouver cette décomposition.) En appliquant le raisonnement ci-dessus, on trouve d'abord une base de L :

$$(e_1, e_2) := (x_1, x_2) \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \Longrightarrow e_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \text{ et } e_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

puis une base de R :

$$(f_1, f_2) = (e_1, e_2) \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} = (2e_1, 6e_2) = (y_1, y_2) \begin{pmatrix} 1 & 5 \\ 1 & 4 \end{pmatrix}.$$

Corollaire 3.1.3 *L'idéal Ad_1 est maximum parmi tous les idéaux $\phi(R)$, où ϕ parcourt l'ensemble des formes linéaires sur L (c'est-à-dire, par définition, des morphismes de A-modules $\phi : L \to A$).*

Preuve. - Soit ϕ une telle forme linéaire. Alors $\phi(R)$ est un sous-module de A, donc un idéal. Avec les notations du théorème, on a pour tout $i = 1, \ldots, k$:

$$\phi(d_i e_i) = d_i \phi(e_i) \in Ad_i \subset Ad_1,$$

puisque $d_1 | d_i$. Comme $\phi(R)$ est engendré par les $\phi(d_i e_i)$, on a bien $\phi(R) \subset Ad_1$. Réciproquement, si l'on prend pour ϕ la forme linéaire "première coodonnée" $x_1 e_1 + \cdots +, x_n e_n \mapsto x_n$, il est immédiat que $\phi(R) = Ad_1$. □

On voit donc que Ad_1 est indépendant du choix de la base adaptée. C'est en fait vrai de tous les Ad_i mais notre preuve sera plus indirecte (voir la section 3.3).

Exercice 3.1.4 Le démontrer en étudiant les images des "formes k-linéaires alternées" sur L.

3.1.2 L'algorithme d'Euclide-Gauß

Le théorème de réduction matricielle qui a été invoqué se démontre à l'aide d'un algorithme qui généralise à la fois l'algorithme du pivot de Gauß et l'algorithme d'Euclide (pour le pgcd). Cet algorithme existe sous une forme très générale, valable pour tout anneau principal, et que l'on peut trouver dans "Basic Algebra" de Jacobson (chap. 3, §7). Nous en donnons ici une forme un peu simplifiée qui ne vaut que pour un anneau euclidien.

Théorème 3.1.5 (Algorithme du pivot sur un anneau euclidien) *Soient A un anneau principal et $M \in Mat_{n,p}(A)$. Il existe alors $P \in GL_n(A)$, $Q \in GL_p(A)$ et $d_1, \ldots, d_k \in A$ non nuls, $0 \leq k \leq \min(n,p)$, tels que $d_1 | \cdots | d_k$ et $M = PDQ^{-1}$, où $D = Diag(d_1, \ldots, d_k) \in Mat_{n,p}(A)$.*

Preuve. - La définition de $\mathrm{Diag}(d_1,\dots,d_k) \in \mathrm{Mat}_{n,p}(A)$ a déjà été expliquée. On va supposer que A est euclidien, *i.e.* qu'il admet un stathme euclidien $g : A\setminus\{0\} \to \mathbf{N}$, dont on rappelle les propriétés :

$$\forall x,x' \in A\setminus\{0\}\ ,\ g(x) \leq g(xx') \text{ et } \forall x \in A\ ,\ \forall y \in A\setminus\{0\}\ ,\ \exists q,r \in A\ :\ \begin{cases} x = qy + r, \\ r = 0 \text{ ou } g(r) < g(x). \end{cases}$$

(Dans $\mathbf{Z}$, on prendra $g(x) := |x|$. Dans $K[X]$, on prendra $g(P) := \deg P$.)
L'algorithme consiste à transformer M par opérations élémentaires sur les lignes et colonnes. Les opérations autorisées sont les permutations de lignes et de colonnes ; et les transvections, c'est-à-dire les opérations du type $L_i \leftarrow L_i + aL_j$ et $C_i \leftarrow C_i + aC_j$. Comme dans le cas de l'algèbre linéaire sur un corps, ces opérations équivalent à la multiplication à droite ou à gauche par une matrice de déterminant ± 1, donc inversible sur l'anneau. Comme pour l'algorithme du pivot de Gauß, il nous suffit donc de déterminer une succession de telles opérations qui transforme M en D.
Le "compteur" qui diminue à chaque étape et garantit la terminaison de l'algorithme est :

$\gamma(M) := \min\{g(m_{i,j}) \mid 1 \leq i \leq n, 1 \leq j \leq p, m_{i,j} \neq 0\}$. (On peut bien entendu supposer M non nulle.)

Première phase.

1. On choisit un *pivot* $m_{i,j}$, *i.e.* un coefficient de M tel que $\gamma(M) = g(m_{i,j})$. On le ramène en position $(1,1)$ par les transpositions $L_i \leftrightarrow L_1$ et $C_j \leftrightarrow C_1$.
2. On effectue les divisions euclidiennes $m_{1,j} = q_j m_{1,1} + r_j$ et $m_{i,1} = q'_i m_{1,1} + r'_i$; puis les transvections $C_j \leftarrow C_j - q_j C_1$ et $L_i \leftarrow L_i - q'_i L_1$.
3. S'il reste un élément $m \neq 0$ dans la première ligne ou la première colonne, on a $g(m) < g(m_{1,1})$. On le met en position $(1,1)$ et l'on recommence les divisions euclidiennes et les transvections.
4. Puisque $g(m_{1,1})$ diminue strictement chaque fois, le processus doit s'arrêter : on a alors une matrice de la forme $\begin{pmatrix} m_{1,1} & 0_{1,p-1} \\ 0_{n-1,1} & M' \end{pmatrix}$ où $M' \in \mathrm{Mat}_{n-1,p-1}(A)$ et où $g(m_{1,1})$ est strictement plus petit que le $\gamma(M)$ de départ.

Deuxième phase.

1. Si $m_{1,1}$ ne divise pas tous les coefficients de M', on remonte en première ligne un coefficient fautif (*i.e.* non multiple de $m_{1,1}$) à l'aide d'une opération $L_1 \leftarrow L_1 + L_i$. On recommence alors toute la première étape (divisions euclidiennes, transpositions, transvections) pour obtenir à nouveau une matrice de la forme $\begin{pmatrix} m_{1,1} & 0_{1,p-1} \\ 0_{n-1,1} & M' \end{pmatrix}$ avec une valeur de $g(m_{1,1})$ strictement plus petite.
2. Puisqu'à chaque fois l'entier naturel $g(m_{1,1})$ diminue strictement, le processus doit s'arrêter : on a alors une matrice de la forme $\begin{pmatrix} m_{1,1} & 0_{1,p-1} \\ 0_{n-1,1} & M' \end{pmatrix}$ où $m_{1,1}$ divise tous les coefficients de M'.

Troisième phase. On recommence l'ensemble des deux premières phases avec M', ce qui ne modifie pas la première ligne et la première colonne. On finit par obtenir une matrice diagonale dont chaque coefficient diagonal divise le suivant. □

Exemple 3.1.6 On part de $M := \begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}$. Voici une succession possible d'opérations et d'états de la matrice.

$$\begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix} \quad L_1 \leftrightarrow L_2 \quad \begin{pmatrix} -8 & 10 \\ -10 & 14 \end{pmatrix} \quad C_2 \leftarrow C_2 + C_1 \text{ , } L2 \leftarrow L_2 - L_1 \quad \begin{pmatrix} -8 & 2 \\ -2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} -8 & 2 \\ -2 & 2 \end{pmatrix} \quad C_1 \leftrightarrow C_2 \quad \begin{pmatrix} 2 & -8 \\ 2 & -2 \end{pmatrix} \quad C_2 \leftarrow C_2 + 4C_1 \text{ , } L2 \leftarrow L_2 - L_1 \quad \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} =: D.$$

Ces transformations se résument en l'égalité matricielle $P^{-1}MQ = D$, où :

$$P^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 1 & 4 \end{pmatrix}.$$

On n'a pas cherché à respecter rigoureusement les phases décrites ci-dessus. De toutes façons, l'algorithme n'est pas déterministe, et, selon les choix faits à chaque étape, on peut obtenir diverses valeurs de P, Q, D satisfaisant aux conditions du théorème. Les sections suivantes préciseront ce qui est invariant dans le résultat.

3.1.3 Vecteurs primitifs

Théorème 3.1.7 *Soit L un module libre de rang fini sur l'anneau principal A. Soit $x \in L \setminus \{0\}$. Les conditions suivantes sont alors équivalentes :*
(i) Le sous-module $R := Ax$ est un facteur direct de L.
(ii) Il existe une forme linéaire $\phi : L \to A$ telle que $\phi(x) = 1$.
(iii) L'élément x peut être complété en une base de L.
(iv) L'élément x est indivisible*, autrement dit, une égalité $x = dy$ dans L n'est possible que si $d \in A^*$.*
(v) Le module L/Ax est sans torsion.

Preuve. - Facile avec ce qui précède, et laissée au plaisir du lecteur ! □

Définition 3.1.8 On dit que $x \in L$ est un *vecteur primitif* ou un *élément primitif*[1] s'il satisfait aux conditions équivalentes du théorème.

En appliquant l'équivalence de (iii) et de (iv) lorsque $L := A^n$, on obtient la généralisation suivante du théorème de Bézout :

Corollaire 3.1.9 *Soit $(a_1, \ldots, a_n) \in A^n$ tel que les a_i soient premiers entre eux dans leur ensemble* (i.e. $\sum Ad_i = A$)*. Il existe alors une matrice inversible sur A dont ils constituent la première ligne (ou colonne).*

□

1. À ne pas confondre avec les "éléments primitifs" de la théorie des extensions séparables de corps.

3.2 Modules de type fini

Théorème 3.2.1 *Pour tout module de type fini sur l'anneau principal A, on a un isomorphisme :*

$$M \simeq A^r \times A/Ad_1 \times \cdots \times A/Ad_k,$$

où $d_1, \ldots, d_k \in A$ sont non nuls et non inversibles et tels que $d_1 | \cdots | d_k$. L'entier r et les idéaux Ad_i sont uniques.

Preuve. - Puisque M est de type fini, il y a une suite exacte $0 \to R \to L \to M \to 0$, où L est libre de rang fini (avec les notations du théorème,ce rang est $n+k$). Le choix d'une base adaptée donne des un isomorphisme $A^n \to L$ par lequel c'est $\{0\}^r \times Ad_1 \times \cdots \times Ad_k$ qui correspond à R, d'où un diagramme commutatif de suites exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{0\}^r \times Ad_1 \times \cdots \times Ad_k & \longrightarrow & A^n & \longrightarrow & A^r \times A/Ad_1 \times \cdots \times A/Ad_k & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & R & \longrightarrow & L & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Le lemme 2.1.5 fournit l'isomorphisme voulu.
Il est évident que $\mathrm{Tor}_A(M) = A/Ad_1 \times \cdots \times A/Ad_k$, donc que $M/\mathrm{Tor}_A(M)$ est libre de rang r : cela définit r de façon intrinsèque, d'où l'unicité. Le cas de $Ad_1, \ldots, Ad_k$ pourrait être traité ici mais le sera plus simplement comme conséquence des résultats sur les diviseurs élémentaires. □

Définition 3.2.2 L'entier r est le *rang* de M ; les idéaux Ad_i sont les *facteurs invariants* de M. Lorsqu'il existe un choix canonique de générateurs de ces idéaux (par exemple dans $\mathbf{Z}$: positifs ; ou dans $K[X]$: unitaires), ces générateurs sont par abus de langage appelés facteurs invariants.

Corollaire 3.2.3 *Tout module sans torsion de type fini sur un anneau principal est libre.*

Corollaire 3.2.4 *Tout module de torsion de type fini sur un anneau principal est produit de modules* cycliques *(c'est-à-dire monogènes et de torsion).*

Corollaire 3.2.5 *Tout module de de type fini sur un anneau principal est somme directe de son sous-module de torsion et d'un module libre.*

Preuve. - Plus précisément, la suite exacte $0 \to \mathrm{Tor}_A(M) \to M \to M/\mathrm{Tor}_A(M) \to 0$ est scindée et le terme droit est libre. □

Exercice 3.2.6 Soient $S := A \setminus \{0\}$ et $K := S^{-1}A$ le corps des fractions de A. Alors le rang de M est égal à la dimension du K-espace vectoriel $S^{-1}M$.

3.3 Diviseurs élémentaires

On va maintenant fixer un ensemble de représentants P de l'ensemble des éléments premiers de A pour la relation d'équivalence "être associé" ; autrement dit, tout idéal premier de A admet un générateur unique dans P. (Dans le cas de $\mathbf{Z}$, on prend l'ensemble des "nombres premiers" *i.e.* des premiers naturels ; dans le cas de $K[X]$, on prend l'ensemble des irréducibles unitaires.)

On va raisonner sur le cas d'un module de torsion M pas nécessairement de type fini. (Pour un module quelconque, ce qui suit peut donc être appliqué à son sous-module de torsion). On a donc une réunion *filtrante* :

$$M = \bigcup_{a \in A\setminus\{0\}} M(a) \text{ où l'on note } M(a) := \{x \in M \mid ax = 0_M\}.$$

Ici, "filtrante" signifie que deux quelconques des sous-modules $M(a)$ sont inclus dans un troisième : on vérifie en effet immédiatement que $M(a), M(b) \subset M(ab)$.

Lemme 3.3.1 (Forme abstraite du lemme des noyaux) *(i) Si $a \wedge b = 1$, on a $M(ab) = M(a) \oplus M(b)$.*
(ii) Si a n'est pas nul, $M(a) = \bigoplus_{p \in P} M(p^{v_p(a)})$.

Preuve. - (i) Puisque $M(a), M(b) \subset M(ab)$, on a déjà $M(a) + M(b) \subset M(ab)$. Soient $u, v \in A$ tels que $au + bv = 1$ (Bézout). Alors, pour tout $x \in M(a) \cap M(b)$:

$$x = uax + vbx = u0_M + v0_M = 0_M,$$

d'où $M(a) \cap M(b) = \{0\}$. D'autre part, pour tout $x \in M(ab)$:

$$x = uax + vbx \text{ et } \begin{cases} a(vbx) = v(abx) = v0_M = 0_M \Rightarrow vbx \in M(a), \\ b(uax) = u(abx) = u0_M = 0_M \Rightarrow uax \in M(b), \end{cases}$$

d'où $M(ab) = M(a) + M(b)$.
(ii) découle de (i) par récurrence. □

Définition 3.3.2 Pour tout $p \in P$, on appelle *composante p-primaire de M* le sous-module :

$$M_p := \bigcup_{n \geq 0} M(p^n).$$

(C'est bien un sous-module car réunion d'une suite croissante de sous-modules.)

Théorème 3.3.3 *Le module de torsion M est somme directe de ses composantes primaires :*

$$M = \bigoplus_{p \in P} M_p.$$

Preuve. - Cela découle formellement de l'égalité $M = \bigcup_{a \in A\setminus\{0\}} M(a)$ et du lemme. Tout d'abord, tout $x \in M$ appartient à l'un des $M(a)$, donc (lemme des noyaux) à $\sum_{p \in P} M(p^{v_p(a)}) \subset \sum_{p \in P} M_p$, d'où l'égalité $M = \sum_{p \in P} M_p$.
Pour montrer que la somme est directe (c'est-à dire que la décomposition d'un élément de M comme somme d'éléments des M_p est unique), il suffit selon le raisonnement standard de supposer $\sum_{p \in P} x_p = 0$ avec les $x_p \in M_p$ presque tous nuls, et de montrer qu'ils sont tous nuls. Mais on a $x_p \in M(p^{n_p})$ où les n_p sont presque tous nuls, et c'est donc une égalité dans $M(a)$, où $a = \prod_{p \in P} p^{n_p}$: on peut donc appliquer le lemme. □

Exemple 3.3.4 En appliquant le lemme chinois, on sait que $A/Aa \simeq \prod_{p\in P} A/Ap^{n_p}$. On vérifie facilement que la composante p-primaire du membre droit de cet isomorphisme est A/Ap^{n_p} (qui est donc trivial si $p \not| a$).

Application aux facteurs invariants. Si M est de plus de type fini, on a un isomorphisme $M \simeq A/Ad_1 \times \cdots \times A/Ad_k$ avec $d_1|\cdots|d_k$; et $A/Ad_i \simeq \prod_{p\in P} A/Ap^{v_p(d_i)}$, où donc :

$$\forall p \in P\ ,\ v_p(d_1) \leq \cdots \leq v_p(d_k).$$

La composante p-primaire M_p de M est isomorphe à $\prod_{i=1}^{k} A/Ap^{v_p(d_i)}$. Pour prouver l'unicité des facteurs invariants, il suffit donc de prouver que, dans un isomorphisme $N \simeq A/Ap^{r_1} \times \cdots \times A/Ap^{r_k}$, avec $r_1 \leq \cdots \leq r_k$, les r_i sont uniquement déterminés par N. Cela découle des deux remarques suivantes :

1. Si $N = N_1 \times \cdots \times N_k$, alors $N(p^s) = N_1(p^s) \times \cdots \times N_k(p^s)$.
2. Si $N = A/Ap^r$, alors la suite croissante des $N(p^s)$ stationne à partir de $s = r$ (et pas avant).

Définition 3.3.5 Soit M un module de torsion de type fini sur l'anneau principal A. Si $M \simeq A/Ad_1 \times \cdots \times A/Ad_k$ avec $d_1|\cdots|d_k$, les *diviseurs élémentaires* de M sont ceux des $Ap^{v_p(d_i)}$ (ou, par abus, des $p^{v_p(d_i)}$) qui ne sont pas triviaux.

3.4 Applications

3.4.1 Structure des groupes abéliens finis

Un groupe abélien fini G est un $\mathbf{Z}$-module de type fini (prendre pour ensemble générateur le groupe lui-même) et de torsion (théorème de Lagrange). Il est donc isomorphe à un produit de groupes cycliques dont les cardinaux sont totalement ordonnés pour la relation de divisibilité. Réciproquement, un $\mathbf{Z}$-module de type fini et de torsion étant isomorphe à un produit de groupes cycliques est fini.

Remarque 3.4.1 La structure des groupes abéliens de type fini s'en déduit immédiatement : un tel groupe est produit d'un facteur $\mathbf{Z}^r$ par un groupe abélien fini.

Comme déjà indiqué, on appellera facteurs invariants de G les entiers naturels $d_i \in \mathbf{N}^*$ tels que $G \simeq \mathbf{Z}/\mathbf{Z}d_1 \times \cdots \times \mathbf{Z}/\mathbf{Z}d_k$ avec $d_1|\cdots|d_k$ et diviseurs élémentaires de G les $p^{v_p(d_i)}$ non triviaux (*i.e.* $\neq 1$) les p étant des nombres premiers (*i.e.* des premiers naturels).

Pour reconstruire les facteurs invariants à partir des diviseurs élémentaires, on procède comme suit. Pour tout p, on les écrit comme une suite de puissances $p^{r_i(p)}$ avec des exposants décroissants $r_0(p) \geq r_1(p) \geq \cdots$, cette suite stationnant en la valeur 0. Alors $d_k = \prod_{p\in P} p^{r_0(p)}$, $d_{-1} = \prod_{p\in P} p^{r_1(p)}$, etc.

Exemple 3.4.2 Soit $G := \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z}$. Les facteurs invariants ne sont pas $8, 12, 18$ (ils ne se divisent pas les uns les autres). Par le lemme chinois, $G \simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times$

$\mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Les diviseurs élémentaires sont maintenant apparents : ce sont $8,4,3,9,2$. On les organise en suites $(8,4,2,1,\ldots)$ et $(9,3,1,\ldots)$ d'où les facteurs invariants $8.9 = 72$, $4.3 = 12$ et $2.1 = 2$.

Les suites de facteurs invariants (suites d'entiers naturels finies et croissantes pour la relation de divisibilité) peuvent être considérées comme un codage pour les structures possibles des groupes abéliens finis.

Exemple 3.4.3 Pour trouver, à isomorphisme près, tous les groupes abéliens d'ordre 18, on cherche toutes les suites $d_1|\cdots|d_k$ telles que $d_1 > 1$ et $d_1 \cdots d_k = 18$. Les seules possibilités sont $(3,6)$ et (18). Il n'y a donc que $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ et $\mathbf{Z}/18\mathbf{Z}$.
On peut également procéder à partir des diviseurs élémentaires. Pour 2, la seule possibilité est 2. Pour 3, les possibilités sont (9) et $(3,3)$. Les deux combinaisons possibles donnent les suites de facteurs invariants (18) et $(6,3)$.

Exercice 3.4.4 Pour tout entier naturel r, calculer le nombre de suites décroissantes d'entiers naturels $r_0 \geq r_1 \geq \cdots$ telles que $r = \sum r_i$. En déduire, pour tout $n \in \mathbf{N}$, le nombre de classes d'isomorphie de groupes abéliens de cardinal n.

3.4.2 Réduction des endomorphismes d'un espace vectoriel

Soient K un corps commutatif, V un K-espace vectoriel de dimension finie et ϕ un endomorphisme de K. Le $K[X]$-module M associé à (V,ϕ) est de type fini (toute base de V en est un système générateur) et de torsion (si μ_ϕ est le polynôme minimal de l'endomorphisme ϕ, on voit que $M = M(\mu_\phi)$).

L'isomorphisme $M \simeq A/A\mu_1 \times \cdots \times A/A\mu_k$, où $A = K[X]$ et où les $\mu_i \in K[X]$ sont des polynômes unitaires tels que $\mu_1|\cdots|\mu_k$, signifie que $V = V_1 \oplus \cdots \oplus V_k$, où chaque V_i est un sous-espace stable par ϕ, et où le $K[X]$-module associé à $(V_i, \phi_{|V_i})$ est isomorphe à $A/A\mu_i$. Cette dernière relation signifie que $(V_i, \phi_{|V_i})$ est cyclique : il admet une base $(e_i, \phi(e_i), \ldots, \phi^{n_i-1}(e_i))$ et μ_i est le polynôme minimal de $\phi_{|V_i}$ (donc $n_i = \deg \mu_i$). La matrice de $\phi_{|V_i}$ dans cette base est la matrice compagnon C_{μ_i} de μ_i. Dans la base obtenue par juxtaposition de ces bases cycliques, la matrice de ϕ est donc diagonale par blocs, de blocs les C_{μ_i}.

Exercice 3.4.5 Montrer que $\mu_\phi = \mu_1$ et que $\chi_\phi = \mu_1 \cdots \mu_k$ (polynôme caractéristique).

Remarque 3.4.6 On peut utiliser de même les diviseurs élémentaires pour retrouver la forme réduite de Jordan : voir Lang ou RW3.

Exercice 3.4.7 On suppose K algébriquement clos. Quel est le lien entre les composantes primaires de M et les sous-espaces caractéristiques de ϕ ?

3.5 Exercices sur le chapitre 3

Exercice 3.5.1 Étudier le système à inconnues entières $\begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ $(x,y,a,b \in \mathbf{Z})$.

Exercice 3.5.2 Discuter la résolubilité dans $\mathbf{Z}$ du système : $\begin{cases} 6x+8y+4z+20t = a, \\ 12x+12y+18z+30t = b, \\ 18x+4y+4z+10t = c. \end{cases}$

Exercice 3.5.3 (i) Appliquer le théorème de la base adptée à $L := \mathbf{Z}^n$ et à $R := \mathbf{Z}(a_1,\ldots,a_n)$.
(ii) Appliquer le théorème de la base adaptée à $L := \mathbf{Z}^2$ et à $R := \mathrm{Ker}\big((x,y) \mapsto (y-ax) \pmod{p}\big)$.

Exercice 3.5.4 Calculer les facteurs invariants de $\mathbf{Z}/a\mathbf{Z}$ en utilisant d'abord le seul générateur $\overline{1}$, puis en utilisant la famille génératrice $(\overline{1},\overline{b})$ $(b \in \mathbf{Z})$.

Exercice 3.5.5 Soient p,q,r des éléments premiers deux à deux distincts. Quels sont les diviseurs élémentaires du module dont les facteurs invariants sont pq, p^2qr et $p^3q^2r^2$? Quels sont les facteurs invariants du module dont les diviseurs élémentaires sont p, p^2, p^3, p^4, q^2, q^3, q^4, r^3, r^4 ?

Exercice 3.5.6 Démontrer le résultat suivant, dû à Gauß : dans un groupe abélien fini G, il existe un élément dont l'ordre est le ppcm des ordres de tous les éléments. En déduire que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Exercice 3.5.7 Démontrer que tous les groupes abéliens d'ordre quadratfrei (c'est-à-dire non divisible par un carré non trivial) sont cycliques.

Exercice 3.5.8 Combien y a-t-il de groupes abéliens d'ordre 12 ?

Exercice 3.5.9 Déterminer tous les groupes d'ordre p^2. (On sait *a priori* que ces groupes sont abéliens.)

Exercice 3.5.10 Si R est un supplémentaire de Aa dans le module libre L de rang n, les facteurs invariants de R dans L sont les $(n-1)$ idéaux $A,\ldots,A$.

Exercice 3.5.11 Quels sont les facteurs invariants de $A(a,b)+A(c,d) \subset A^2$?

Exercice 3.5.12 Montrer que le module des endomorphismes d'un module de torsion de type fini de facteurs invariants $Ad_1,\ldots,Ad_k$ tels que $d_1|\cdots|d_k$ est isomorphe à $\prod(A/Ad_i)^{2k-2i+1}$.

Exercice 3.5.13 (i) Pour $a \in A \setminus \{0\}$, montrer que A/Aa n'a qu'un nombre fini de sous-modules.
(ii) À l'aide des exercices de la feuille de TD précédente, en déduire que les A-modules artiniens et noetheriens sur A sont exactement les A-modules de torsion et de type fini.

Exemple 3.5.14 (Méthode de complétion de la matrice) Soit $a := (a_1,\ldots,a_n)$ un vecteur primitif de A^n. Il existe donc une forme linéaire $\phi(x_1,\ldots,x_n) := u_1x_1+\cdots+u_nx_n$ telle que $\phi(a) = u_1a_1+\cdots+u_na_n = 1$. On peut calculer les u_i en appliquant le théorème de Bézout à a_1 et a_2, puis à $a_1 \wedge a_2$ et a_3, etc.

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

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

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

Exercice 3.5.15 Vérifier l'affirmation sur les facteurs invariants de $\mathrm{Ker}\phi$ dans L.

Exercice 3.5.16 Compléter $a := (6, 15, 10) \in \mathbf{Z}^3$ en une matrice inversible.

Exercice 3.5.17 Soit L un module libre de rang fini. Montrer que le *contenu* de $x \in L$, c'est-à-dire le pgcd de ses coordonnées dans une base, est indépendant du choix de la base.