Chapitre 4

Groupes abéliens

4.1 Sommes directes et bases

4.1.1 Définition. — Soit $(M_i)_{i\in I}$ une famille de groupes abéliens. On note $\bigoplus_{i\in I} M_i$, et on appelle *somme directe* des M_i, l'ensemble de toutes les familles $(x_i)_{i\in I}$, $x_i \in M_i$, ne comportant qu'un nombre *fini* de termes non nuls (ce que l'on exprime souvent en disant que les x_i sont "presque tous nuls"). C'est un groupe abélien pour l'addition terme à terme.

Pour tout $i \in I$ fixé, on identifie M_i au sous-groupe abélien de $\bigoplus_{i\in I} M_i$ formé des familles dont tous les termes sont nuls sauf peut-être celui d'indice i. Il est clair alors que le groupe $\bigoplus_{i\in I} M_i$ est *engendré* par la réunion des M_i ; si $x = (x_i) \in \bigoplus_{i\in I} M_i$, alors x s'écrit $x = \sum_{i\in I} x_i$, $x_i \in M_i$ (où la somme a un sens parce que les x_i sont presque tous nuls.)

4.1.2 Remarques. — *(a)* Si, comme cela arrive souvent, l'ensemble I est *fini*, il n'y a pas de restriction sur les familles (x_i) ; dans ce cas, $\bigoplus_{i\in I} M_i$ s'identifie donc à l'ensemble produit $\prod_{i\in I} M_i$, avec sa loi de groupe habituelle, et la some directe est simplement une autre notation pour le produit.

(b) Un autre cas particulier que nous rencontrerons est celui où tous les M_i sont égaux à un même groupe abélien M. On note alors souvent $M^{(I)}$ au lieu de $\bigoplus_{i\in I} M_i$; c'est simplement l'ensemble de toutes les fonctions de I vers M, à support fini (*i.e.* nulles sauf au plus en un nombre fini de points), muni de l'addition habituelle des fonctions à valeurs dans un groupe abélien. Dans ce cas, il faut considérer que chaque M_i est une copie du groupe M, et que $M^{(I)}$ est la somme directe de ces copies.

(c) Si V est un espace vectoriel sur un corps commutatif k, toute décomposition $V = V_1 \oplus V_2$ (ou plus généralement $V = \bigoplus_{i\in I} V_i$) de V en somme directe d'une famille de sous-espaces vectoriels définit une décomposition du *groupe abélien* V en somme directe de sous-groupes abéliens. On peut dire que la notion de somme directe d'espaces vectoriels est un enrichissement de la notion de somme directe de groupes abéliens (mais bien sûr l'intérêt de la définition 4.1.1 est qu'elle s'applique dans des contextes où l'on n'a pas de structure d'espace vectoriel).

4.1.3. La propriété fondamentale des sommes directes, dont le lecteur a certainement déjà rencontré l'analogue dans le cas des espaces vectoriels, est la possibilité de décrire tous les homomorphismes au départ d'une somme directe en termes de ses facteurs :

Proposition. — Soit $(M_i)_{i\in I}$ une famille de groupes abéliens, M' un autre groupe abélien. Supposons donné pour chaque $i \in I$ un homomorphisme $\varphi_i : M_i \to M'$, et identifions comme en 4.1.1 chaque M_i à un sous-groupe abélien de $\bigoplus_{i\in I} M_i$. Alors il existe un unique homomorphisme $\varphi : \bigoplus_{i\in I} M_i \to M'$ tel que $\varphi|_{M_i} = \varphi_i$ pour tout $i \in I$.

Démonstration. — L'unicité est claire puisque les M_i engendrent $\bigoplus_{i\in I} M_i$. Pour l'existence, il suffit de poser $\varphi((x_i)) = \sum_{i\in I} \varphi_i(x_i)$.

4.1.4 Définition. — Soit M un groupe abélien, et soit $(N_i)_{i\in I}$ une famille de sous-groupes abéliens de M. Soit $\varphi : \bigoplus_{i\in I} N_i \to M$ l'homomorphisme défini par $\varphi((x_i)) = \sum_{i\in I} x_i$ (c'est l'homomorphisme associé aux injections canoniques $N_i \to M$ par la prop. 4.1.3).

(a) On dit que les N_i sont en somme directe dans M, si l'homomorphisme φ est *injectif*; il revient au même de demander que si $\sum_{i\in I} x_i = 0$ dans M, avec $x_i \in N_i$ presque tous nuls, alors $x_i = 0$ pour tout i.

(b) On dit que M est somme directe des sous-groupes N_i, si l'homomorphisme φ est *bijectif*; il revient au même de demander que tout $x \in M$ possède une unique écriture $x = \sum_{i\in I} x_i$, $x_i \in N_i$ presque tous nuls. Dans ce cas, on utilise l'homomorphisme φ pour identifier M et $\bigoplus_{i\in I} N_i$, et on écrit par abus de notation $M = \bigoplus_{i\in I} N_i$.

4.1.5 Remarque. — Il est important de ne pas confondre la notion de somme directe "concrète" de la déf. 4.1.4, qui concerne la décomposition d'un groupe abélien donné en somme directe d'une famille de sous-groupes, avec celle de somme directe "abstraite" définie en 4.1.1, qui est la construction d'un nouveau groupe abélien à partir d'une famille de groupes abéliens donnés. Le lien entre les deux est que la somme directe abstraite $\bigoplus_{i\in I} M_i$ est somme directe concrète, au sens de la déf. 4.1.4, de ses sous-groupes identifiés aux M_i.

4.1.6. Rappelons que dans un groupe abélien noté additivement, le sous-groupe engendré par un élément x est l'ensemble des nx, $n \in \mathbf{Z}$. Il est donc naturel de noter $\mathbf{Z}x$ ce groupe.

Définition. — Soit M un groupe abélien. On dit qu'une famille $(e_i)_{i\in I}$ d'éléments de M est une *base* de M, si tout $x \in M$ possède une unique écriture

$$x = \sum_{i\in I} n_i e_i \qquad \text{avec } n_i \in \mathbf{Z} \text{ presque tous nuls}$$

On dit alors que les n_i sont les coefficients de x dans la base (e_i). Il revient au même de dire que chaque e_i est d'ordre infini dans M (ou encore, que chaque groupe $\mathbf{Z}e_i$ est isomorphe à $\mathbf{Z}$), et que M est la somme directe des sous-groupes $\mathbf{Z}e_i$.

On dit qu'un groupe abélien est *libre*, s'il possède une base.

4.1.7 Remarques. — *(a)* Le groupe $\mathbf{Z}$ est évidemment libre. Pouvez-vous en déterminer toutes les bases ? De même, $\mathbf{Z}^n$ est libre pour tout $n \geq 0$.

(b) Par convention, le groupe trivial $\{0\}$ est libre, de base $\emptyset$.

(c) Un groupe abélien *fini*, non réduit à $\{0\}$, n'est jamais libre (exercice.)

(d) Plus généralement, pour tout groupe abélien M, notons M_{tor} l'ensemble des $x \in M$ tels qu'il existe $n \neq 0$ dans $\mathbf{Z}$ tel que $nx = 0$ (en d'autres termes, M_{tor} est l'ensemble des éléments d'ordre fini de M, ou, comme on le dit aussi, l'ensemble des éléments de torsion de M.) On voit facilement (exercice) que M_{tor} est un sous-groupe de M. Disons que M est *sans torsion*, si $M_{\mathrm{tor}} = \{0\}$. Alors on voit encore facilement qu'un groupe libre est toujours sans torsion.

(e) Le groupe additif $(\mathbf{Q}, +)$ est sans torsion, mais n'est pas libre ; le groupe multiplicatif $(\mathbf{Q}_+, .)$, en revanche, est libre (exercice).

(f) Un groupe libre de base $(e_i)_{i\in I}$ est clairement isomorphe à $\mathbf{Z}^{(I)}$. Ceci montre en particulier que deux groupes libres qui possèdent des bases de même cardinal sont isomorphes entre eux.

4.1.8 Proposition. — *Soit M un groupe abélien libre, $(e_i)_{i\in I}$ une base de M, et soit M' un autre groupe abélien. Alors pour toute famille $(y_i)_{i\in I}$ d'éléments de M', il existe un unique $\varphi \in \mathrm{Hom}\,(M, M')$ tel que $\varphi(e_i) = y_i$ pour tout $i \in I$.*

Démonstration. — L'unicité est claire car les e_i engendrent M. Pour l'existence, il suffit de poser $\varphi(x) = \sum_{i\in I} n_i y_i$, si les n_i sont les coefficients de x dans la base (e_i).

4.2 Groupes abéliens libres de type fini

4.2.1 Définition. — Nous dirons qu'un groupe abélien M est *libre de type fini*, si M possède une base finie. Il revient au même de dire que M est isomorphe à un groupe $\mathbf{Z}^n$, pour un certain $n \in \mathbf{N}$.

4.2.2. Soit $n \in \mathbf{N}$. Disons que des vecteurs $v_1, \ldots, v_s$ dans $\mathbf{Q}^n$ sont linéairement indépendants sur $\mathbf{Z}$, si l'égalité $\sum_{i=1}^{s} n_j v_j$, $n_j \in \mathbf{Z}$, implique $n_j = 0$ pour tout $1 \leq j \leq s$.

Lemme. — Soit $n \in \mathbf{N}$. Alors $v_1, \ldots, v_s \in \mathbf{Q}^n$ sont linéairement indépendants sur $\mathbf{Z}$ si et seulement si ils sont linéairement indépendants sur $\mathbf{Q}$.

Démonstration. — Clairement, des vecteurs linéairement indépendants sur $\mathbf{Q}$ le sont sur $\mathbf{Z}$. Réciproquement, soient $v_1, \ldots, v_s$ linéairement indépendants sur $\mathbf{Z}$, et soit

$$\sum_{j=1}^{s} a_j v_j = 0$$

avec $a_j \in \mathbf{Q}$. Ecrivons $a_j = p_j/q_j$ avec p_j, $q_j \in \mathbf{Z}$, $q_j > 0$ et p_j, q_j premiers entre eux. Soit q le produit des q_j. Alors on a encore

$$q \sum_{j=1}^{s} a_j v_j = \sum_{j=1}^{s} (q a_j) v_j = 0$$

et $qa_j \in \mathbf{Z}$ pour tout j, donc $qa_j = 0$ et $a_j = 0$.

4.2.3 Proposition. — *Soit M un groupe abélien libre de type fini. Alors toutes les bases de M ont même cardinal, appelé* rang *de M, et noté* $\operatorname{rg} M$.

Démonstration. — On peut supposer que $M = \mathbf{Z}^n \subset \mathbf{Q}^n$. Alors d'après le lemme, toute famille $v_1, \ldots, v_s$ d'éléments de M linéairement indépendants sur $\mathbf{Z}$ est libre dans $\mathbf{Q}^n$; cela n'est possible que si $s \leq n$. Or toute partie d'une base d'un groupe abélien est linéairement indépendante ; donc les bases de M ont au plus n éléments, et en particulier sont finies (ce qui n'était pas entièrement évident *a priori*.) Par hypothèse, M possède une base avec n éléments ; s'il en possédait une autre avec $m < n$ éléments, on aurait aussi $M \simeq \mathbf{Z}^m$ et on aurait une contradiction en échangeant les rôles de m et n.

4.2.4 Proposition. — *Soit M un sous-groupe de $\mathbf{Z}$. Alors il existe un unique entier $d \geq 0$ tel que $M = \mathbf{Z}d$.*

Démonstration. — Si $M = \{0\}$, il est clair que $d = 0$ est le seul choix possible. Sinon, M contient $x \neq 0$, et quitte à remplacer x par $-x$, on voit que M contient des éléments > 0. Soit d le plus petit élément > 0 de M. Alors si $x \in M$ est quelconque, il existe $q \in \mathbf{Z}$ et $0 \leq r < d$ uniques tels que $x = dq + r$ (division euclidienne). Mais alors $r = x - dq \in M$, donc par définition de d on doit avoir $r = 0$, ce qui prouve que $M = \mathbf{Z}\, d$. Réciproquement, si $M = \mathbf{Z}\, d$, avec $d > 0$, il est clair que d est le plus petit élément > 0 de M, d'où l'unicité.

4.2.5 Théorème. — *Soit M un groupe abélien libre de type fini. Alors tout sous-groupe $N \subset M$ est encore libre de type fini, et vérifie* $\operatorname{rg} N \leq \operatorname{rg} M$.

Démonstration. — On peut supposer que $M = \mathbf{Z}^n$, et faire une récurrence sur n. Si $n = 0$, il n'y a rien à démontrer ; si $n = 1$, le résultat découle aussitôt de la prop. 4.2.4. On peut donc supposer $n > 1$. Soit $M_1 = \mathbf{Z}e_1 \oplus \ldots \oplus \mathbf{Z}e_{n-1} \simeq \mathbf{Z}^{n-1}$, et $N_1 = N \cap M_1$. Alors $M = M_1 \oplus \mathbf{Z}e_n$, et $M/M_1 \simeq \mathbf{Z}$ est libre de rang 1.

Si $N_1 = N$, on a $N \subset M_1$, et on conclut par hypothèse de récurrence. Sinon, N/N_1 est un sous-groupe non nul de M/M_1, donc libre de rang 1 d'après la prop. 4.2.4. Soit a une base de N/N_1, et soit $v \in N$ un représentant de a. Alors si $\pi : N \to N/N_1$ est la surjection canonique, pour tout $x \in N$ il existe un unique $n \in \mathbf{Z}$ tel que $\pi(x) = na$; mais alors $\pi(x - nv) = 0$, ce qui prouve que $x - nv \in N_1$. Donc tout $x \in N$ s'écrit de manière unique $x = x_1 + nv$, $x_1 \in N_1$, $n \in \mathbf{Z}$, ce qui prouve que $N = N_1 \oplus \mathbf{Z}v$. Par hypothèse de récurrence, N_1 est libre de rang $\leq \operatorname{rg} M_1 = n - 1$, donc N est libre de rang $\operatorname{rg} N_1 + 1 \leq n$.

4.2.6. Une des choses qui différencie la théorie des groupes abéliens de celle des groupes généraux est le fait que si M, N sont deux groupes abéliens, il y a une structure naturelle de groupe abélien sur l'ensemble $\operatorname{Hom}(M, N)$, définie simplement en posant $(\varphi+\psi)(x) = \varphi(x) + \psi(x)$. De la prop. 4.1.8 on déduit facilement que le groupe abélien $\operatorname{Hom}(\mathbf{Z}^m, \mathbf{Z}^n)$ est libre de rang mn ; en fait il s'identifie naturellement à $\mathbf{M}_{n,m}(\mathbf{Z})$ (matrices $n \times m$ à coefficients dans $\mathbf{Z}$) en associant à $\varphi \in \operatorname{Hom}(\mathbf{Z}^m, \mathbf{Z}^n)$ la matrice dont les colonnes sont les $\varphi(e_i)$, $1 \leq i \leq m$. Cette identification est compatible avec la composition des

homomorphismes : si p est un troisième entier, $\varphi \in \mathrm{Hom}\,(\mathbf{Z}^m, \mathbf{Z}^n)$, $\psi \in \mathrm{Hom}\,(\mathbf{Z}^n, \mathbf{Z}^p)$, alors la matrice de $\psi \circ \varphi \in \mathrm{Hom}\,(\mathbf{Z}^m, \mathbf{Z}^p)$ est simplement le produit de la matrice de ψ par celle de φ.

Si on considère maintenant le cas des endomorphismes d'un groupe abélien M, on voit que l'addition définie ci-dessus et la composition des endomorphismes munissent $\mathrm{End}\,(M)$ d'une structure d'*anneau* (non commutatif en général.) En particulier, l'anneau $\mathrm{End}\,(\mathbf{Z}^n)$ s'identifie à $\mathbf{M}_n(\mathbf{Z})$; et le groupe des automorphismes de $\mathbf{Z}^n$, qui n'est autre que le groupe des éléments inversibles de $\mathrm{End}\,(\mathbf{Z}^n)$, s'identifie donc à $\mathbf{GL}(n, \mathbf{Z})$.

4.2.7 Théorème. — *Soit M un groupe abélien libre de type fini, N un sous-groupe de M. Alors il existe un unique entier s tel que $0 \leq s \leq n$, des entiers > 0 uniques $d_1, \ldots, d_s$ avec $d_1 | d_2 | \ldots | d_s$ et une base $v_1, \ldots, v_n$ de M (non unique en général), tels que les $v'_j = d_j v_j$, $1 \leq j \leq s$, soient une base de N. Dans cette écriture, s est le rang de N, et $d_1, \ldots, d_s$ sont appelés les* facteurs invariants *de N.*

Démonstration. — Tout d'abord, il est clair que s'il existe une base $v_1, \ldots, v_n$ et des entiers $d_1, \ldots, d_s$ avec les propriétés de l'énoncé, s est égal au rang du sous-groupe N ; il est donc unique. Nous nous contenterons pour l'instant de prouver l'*existence* ; l'unicité des entiers $d_1, \ldots, d_s$ sera prouvée à la fin de la section suivante (cf. 4.3.11).

Nous allons en fait donner un algorithme permettant de construire une base adaptée en partant d'un système de générateurs du groupe N (nous savons d'après le thm. 4.2.5 que le groupe N est libre, donc nous pourrions partir d'une base de N, mais en pratique il n'est pas toujours facile d'avoir directement une base ; notre algorithme résoud donc aussi ce problème d'obtenir une base d'un sous-groupe de M à partir d'un système de générateurs.)

Choisissons une base $e_1, \ldots, e_n$ de M. Soit $w_1, \ldots, w_m$ un système de générateurs de N, et représentons ce système par la matrice rectangulaire $A = (a_{i,j}) \in \mathbf{M}_{n,m}(\mathbf{Z})$ dont les colonnes sont les coordonnées des w_j dans la base (e_i). Nous allons effectuer sur A une suite d'opérations élémentaires des quatre types suivants :

(a) Retrancher à la colonne j un multiple entier d'une colonne k, $k \neq j$; cela revient à remplacer le générateur w_j par $w_j - cw_k$.

(b) Retrancher à la ligne i un multiple entier d'une ligne k, $k \neq i$; cela revient à remplacer le vecteur de base e_k par $e_k + ce_i$.

(c) Changer le signe d'une ligne ou d'une colonne ; cela revient à changer le signe d'un vecteur de base e_i ou d'un générateur w_j.

(d) Permuter les lignes, ou les colonnes, de A ; cela revient à permuter les vecteurs de base, ou les générateurs.

On aura donc prouvé le théorème si l'on parvient à trouver une suite d'opérations des quatre types précédents qui transforme la matrice A en une matrice $A' = (a'_{i,j})$ dont tous les coefficients sont nuls sauf les $a'_{j,j} = d_j$, $1 \leq j \leq s$, et que l'on ait $d_j > 0$ et $d_1 | d_2 | \ldots | d_s$ (noter que l'on a toujours $s = \mathrm{rg}\,(N) \leq \inf(n, m)$). Ces opérations se traduiront par une suite de changements de base dans M et de système générateur dans N ; la base $(v_1, \ldots, v_n)$ cherchée sera la base de M obtenue á la fin du processus, et les $v'_j = d_j v_j$, $1 \leq j \leq s$, sont alors le système générateur de N obtenu à la fin du processus

(il est clair que les v'_j sont indépendants sur $\mathbf{Z}$, donc ce système générateur sera en fait une base). Les colonnes nulles indiquent simplement que l'on n'était pas parti du plus petit nombre possible de générateurs ; on peut éliminer les colonnes nulles au fur et à mesure de leur apparition dans le processus.

Le procédé est une variante "sur $\mathbf{Z}$" du pivotage de Gauss ; dans le cas d'un corps elle aboutirait à une matrice avec $d_j = 1$ pour tout j, ce qui traduit simplement le théorème de la base incomplète. Le fait que dans $\mathbf{Z}$ on ne puisse pas toujours diviser rend les choses plus délicates (mais aussi plus intéressantes).

Il s'agit donc maintenant simplement d'un problème sur les matrices rectangulaires de nombres entiers ; nous allons le résoudre par récurrence sur n. Si tous les coefficients de A sont nuls, $N = 0$, $s = 0$, et il n'y a rien à démontrer. Sinon, soit $a = \inf\{|a_{i,j}|, a_{i,j} \neq 0\}$, et faisons encore une récurrence sur a. En permutant au besoin les lignes et les colonnes, on peut supposer que $|a_{1,1}| = a$; et quitte à changer le signe de la première colonne, que $a_{1,1} = a$. Si $n > 1$, effectuons alors pour $i > 1$ la division euclidienne de $a_{i,1}$ par a :

$$a_{i,1} = qa + r \qquad q \in \mathbf{Z},\ 0 \leq r < a$$

En retranchant q fois la ligne 1 à la ligne i, et en faisant cela pour chaque i, on obtient une matrice dont la première colonne est formée d'entiers ≥ 0, $a_{1,1} = a$ et $a_{i,1} < a$ si $i > 1$. Si l'un des $a_{i,1}$ est > 0, on peut donc appliquer l'hypothèse de récurrence. Sinon, on obtient une matrice de la forme :

$$\begin{pmatrix} a & a_{1,2} & \dots & a_{1,m} \\ 0 & a_{2,2} & \dots & a_{2,m} \\ \vdots & \vdots & & \vdots \\ 0 & a_{2,n} & \dots & a_{n,m} \end{pmatrix}$$

(bien sûr les $a_{i,j}$ ci-dessus ne sont plus ceux de la matrice de départ ; pour alléger les écritures nous continuons de noter $a_{i,j}$ les coefficients de toutes les matrices obtenues au cours du processus). On fait maintenant de même sur la première ligne : si l'un des $a_{1,j}$, $j > 1$, n'est pas divisible par a, on obtient une matrice avec un coefficient > 0 et $< a$, et on applique l'hypothèse de récurrence ; sinon, tous les $a_{1,j}$ sont divisibles par a, et en retranchant des multiples appropriés de la première colonne, on aboutit à une matrice :

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a_{2,2} & \dots & a_{2,m} \\ \vdots & \vdots & & \vdots \\ 0 & a_{2,n} & \dots & a_{n,m} \end{pmatrix}$$

(notons en passant que si $a = 1$ on n'a jamais de reste dans les divisions euclidiennes, et on arrive donc directement à la forme ci-dessus par des soustractions de lignes et de colonnes.) Si $n = 1$, ceci est déjà la forme voulue ; le lecteur se convaincra aisément que dans ce cas (où le problème revient simplement à trouver un générateur du sous-groupe de $\mathbf{Z}$ engendré par m entiers $a_1, \dots, a_m$), le nombre a trouvé au bout de ce processus (donc après avoir fait appel autant de fois que nécessaire à l'hypothèse de récurrence) est

simplement le pgcd des a_j, construit par l'algortihme d'Euclide (c'est évident puisqu'il est bien connu que ce pgcd est l'unique générateur > 0 du sous-groupe de $\mathbf{Z}$ engendré par les a_j, que l'on peut supposer $\neq 0$).

Si maintenant $n > 1$, et qu'il existe un $a_{i,j}$, $i, j > 1$, non divisible par a, on peut par exemple ajouter la ligne i à a ligne 1, et reprendre le processus : on tombera sur un reste non nul, donc sur une matrice à laquelle on peut applique l'hypothèse de récurrence. Ainsi, on peut de plus supposer que a divise en fait tous le $a_{i,j}$; notons alors d_1 la valeur de a obtenue à ce stade de l'algorithme. Notons B la matrice $(a_{i,j})_{i,j\geq 2}$, qui d'après ce qui précède s'écrit donc $B = d_1 B_1$, $B_1 \in \mathbf{M}_{n-1,m-1}(\mathbf{Z})$. On peut maintenant faire jouer l'hypothèse de récurrence sur n : si $B = 0$, c'est que $s = 1$ et on a abouti à la forme voulue. Sinon, par une suite finie d'opérations élémentaires ne portant plus que sur les lignes et les colonnes d'indice > 1, on peut transformer B_1 en une matrice B_1' de la forme voulue :

$$\begin{pmatrix} d_2' & 0 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & 0 & d_s' & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

avec $1 \leq d_2' | \dots | d_s'$. On pose alors $d_j = d_1 d_j'$ pour $j > 1$; par la même suite d'opérations que pour B_1, la matrice B se transforme en

$$\begin{pmatrix} d_2 & 0 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & 0 & d_s & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

et on a gagné.

4.2.8 Remarques. — *(a)* Les lecteurs intéressés par la programmation n'auront pas de mal à mettre la procédure ci-dessus sous la forme d'un programme récursif permettant le calcul des facteurs invariants et d'une base adaptée à partir de la donnée d'un système de générateurs. Précisons que de ce point de vue l'ordre dans lequel nous faisons les opérations ici n'est pas forcément le plus efficace ; l'appel récursif qui correspond à "faire jouer l'hypothèse de récurrence" peut en déclencher toute une motagne d'autres qu'il n'est pas forcément commode de maîtriser. Le calcul de bases adaptées est notamment à la base des systèmes informatiques tournés vers la théorie algébrique des nombres, mais les groupes abéliens interviennent aussi par exemple dans les questions de codes correcteurs d'erreurs.

(b) On se convainc facilement qu'au cours des opérations élémentaires composant la procédure ci-dessus, le sous-groupe de $\mathbf{Z}$ engendré par l'ensemble de tous les coefficients

de la matrice A ne change pas. Comme à la fin du processus ce sous-groupe est trivialement engendré par d_1, on en déduit que d_1 est simplement le pgcd des coefficients $a_{i,j}$ de la matrice de départ. Une façon d'aborder l'unicité des d_k est de prouver que $d_1 \dots d_k$ est le pgcd de l'ensemble des mineurs de taille k de la matrice de départ, en prouvant que le sous-groupe de $\mathbf{Z}$ engendré par ces mineurs ne change pas non plus au cours de la construction (ce qui en fait n'est pas très difficile.) Nous avons préféré déduire cette unicité d'une étude soigneuse de la structure des groupes abéliens finis.

(c) Lorsque nous aurons étudié les anneaux principaux, le lecteur intéressé pourra énoncer et démontrer les analogues de tous les résultats de cette section, et notamment du théorème de la base adaptée, pour les modules libres de type fini sur un anneau principal quelconque (un cas particulièrement intéressant étant celui des polynômes à une indéterminée sur un corps.) La difficulté principale dans l'approche que nous avons prise ici consiste à trouver un substitut pour la récurrence sur a.

4.2.9 Exercice. — Soit M un groupe abélien libre de type fini, et soient N, N' deux sous-groupes de M. Montrer qu'il existe un automorphisme u de M tel que $u(N) = N'$ si et seulement si N et N' ont même rang et mêmes facteurs invariants.

4.3 Structure des groupes abéliens de type fini

4.3.1. Nous allons maintenant nous intéresser à la structure d'un groupe abélien de type fini quelconque (non nécessairement libre.) Soit M un tel groupe, et soit $S = \{x_1, \dots, x_n\}$ un ensemble de générateurs de M. Dire que S est générateur est exactement équivalent au fait que l'application $\varphi : \mathbf{Z}^n \to M$ définie par

$$\varphi(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i x_i$$

est surjective. En d'autres termes, *tout groupe abélien de type fini est quotient d'un groupe abélien libre de type fini.* Cette remarque fondamentale a plusieurs conséquences importantes.

4.3.2 Théorème. — *Tout sous-groupe et tout quotient d'un groupe abélien de type fini M est encore de type fini.*

Démonstration. — C'est évident pour les quotients : si S est un ensemble de générateurs de M, l'image de S par l'application canonique dans tout quotient de M sera un ensemble générateur du quotient. Soit maintenant N un sous-groupe de M. Soit $\varphi : \mathbf{Z}^n \to M$ une surjection comme en 4.3.1. Alors $Q = \varphi^{-1}(N)$ est un sous-groupe de $\mathbf{Z}^n$, donc libre de type fini d'après le thm. 4.2.5 ; mais $N = \varphi(Q)$ est un quotient de Q, donc de type fini d'après le début de la démonstration.

4.3.3 Lemme. — *Soit M un groupe abélien de la forme $M = \bigoplus_{i\in I} M_i$, et soit, pour chaque $i \in I$, N_i un sous-groupe de M_i. Soit $N = \bigoplus_{i\in I} N_i \subset M$. Alors on a une*

décomposition canonique :

$$M/N = \bigoplus_{i\in I} M_i/N_i$$

Démonstration. — C'est facile : tout d'abord, on a $N \cap M_i = N_i$, puisque si $(x_j)_{j\in I} \in N \cap M_i$, on a à la fois $x_j \in N_j$ pour tout j, et $x_j = 0$ si $j \neq i$. Donc l'image de M_i dans M/N s'identifie à M_i/N_i. Ces images engendrent le quotient, puisque les M_i engendrent M. Reste à prouver qu'elles sont en somme directe. Or si

$$\sum_{i\in I} \pi(x_i) = \pi\left(\sum_{i\in I} x_i\right) = 0$$

avec $x_i \in M_i$, on a $\sum_{i\in I} x_i \in N$, donc $x_i \in N_i$ pour tout $i \in I$, d'où $\pi(x_i) = 0$ pour tout i.

4.3.4 Théorème. — *Soit M un groupe abélien de type fini. Alors M est isomorphe à la somme directe d'une somme directe finie de groupes cycliques finis et d'un groupe abélien libre de type fini :*

$$M \simeq \mathbf{Z}/m_1\mathbf{Z} \oplus \ldots \mathbf{Z}/m_r\mathbf{Z} \oplus \mathbf{Z}^l \qquad \text{avec } 1 < m_1|m_2| \ldots |m_r$$

Dans cette écriture, $\mathbf{Z}/m_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/m_r\mathbf{Z}$ est le sous-groupe M_{tor} des éléments d'ordre fini de M (cf. rem. 4.1.7 (d)), et $\mathbf{Z}^l$ est donc isomorphe à M/M_{tor}.

Démonstration. — Ceci résulte directement de la partie existence, déjà démontrée, du théorème de la base adaptée 4.2.7. Soit en effet $\varphi : \mathbf{Z}^n \to M$ une surjection, et soit $N = \operatorname{Ker}\varphi$. Remplaçons la base canonique de $\mathbf{Z}^n$ par une base $v_1, \ldots, v_n$ adaptée à N. Cela donne une décomposition $\mathbf{Z}^n = \mathbf{Z}v_1 \oplus \ldots \oplus \mathbf{Z}v_n$ pour laquelle

$$N = d_1\mathbf{Z}v_1 \oplus \ldots \oplus d_s\mathbf{Z}v_s \oplus 0 \oplus \ldots \oplus 0$$

D'après le lemme, en identifiant comme on peut le faire chaque $\mathbf{Z}v_j$ à $\mathbf{Z}$, on a donc une décomposition :

$$M = \mathbf{Z}/d_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/d_s\mathbf{Z} \oplus \mathbf{Z} \oplus \ldots \oplus \mathbf{Z}$$

Dans cette décomposition, on peut supprimer les facteurs $\mathbf{Z}/d_j\mathbf{Z}$ pour lesquels $d_j = 1$; il reste donc bien une écriture de la forme voulue, où r est le nombre de $d_j > 1$, et où $l = n - s$.

Comme nous l'avons signalé dans la remarque 4.1.7 *(d)*, un groupe abélien libre est sans torsion ; par conséquent, dans la décomposition ci-dessus, un élément d'ordre fini de M ne peut pas avoir de composante $\neq 0$ dans $\mathbf{Z}^l$, et est donc dans $\mathbf{Z}/m_1\mathbf{Z} \oplus \ldots \mathbf{Z}/m_r\mathbf{Z}$. Inversement, ce dernier est un groupe fini, donc tous ses éléments sont d'ordre fini, ce qui donne bien l'égalité voulue.

4.3.5 Corollaire. — *Un groupe abélien de type fini est libre si et seulement si il est sans torsion.*

4.3.6 Remarque. — Comme le montre l'exemple du groupe $(\mathbf{Q}, +)$ (cf. rem. 4.1.7 *(e)*), ce résultat devient tout à fait faux si l'on ne suppose plus que le groupe est de type fini.

4.3.7. Intéressons-nous maintenant à la question d'unicité dans le théorème 4.3.4. Puisque $\mathbf{Z}^l \simeq M/M_{\mathrm{tor}}$, on voit déjà que $l = \mathrm{rg}\,(M/M_{\mathrm{tor}})$ est bien défini. Quitte à remplacer M par M_{tor}, on peut donc dorénavant supposer que M est un groupe abélien fini. Nous allons considérer les réductions de M modulo un nombre premier p. Elles sont définies de la façon suivante : la multiplication par p définit un endomorphisme du groupe abélien M, d'image pM ; le quotient M/pM est la réduction de M modulo p. Il est clair que pour tout $x \in M/pM$ fixé, l'homomorphisme $\varphi_x : \mathbf{Z} \to M/pM$ défini par $\varphi_x(n) = nx$ passe au quotient par $p\mathbf{Z}$; on vérifie facilement (exercice) que l'application $(\lambda, x) \to \lambda x$ de $\mathbf{Z}/p\mathbf{Z} \times M/pM \to M/pM$ ainsi définie munit canoniquement M/pM d'une structure d'*espace vectoriel* sur le corps fini $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

4.3.8 Lemme. — *Soit M un groupe abélien fini, p un nombre premier. Alors les conditions suivantes sont équivalentes :*

(i) *la multiplication par p n'est pas injective de M dans M ;*

(ii) *la multiplication par p n'est pas surjective de M dans M ;*

(iii) *$M/pM \neq 0$.*

(iv) *p divise $|M|$.*

Démonstration. — L'équivalence de *(i)* et *(ii)* est vraie pour toute fonction d'un ensemble fini dans lui-même ; *(iii)* est trivialement équivalent à *(ii)*. Or l'application $\varphi : x \to px$ de M dans lui-même est évidemment un homomorphisme de groupes ; donc elle est injective si et seulement si $\mathrm{Ker}\,\varphi = \{0\}$, ce qui revient à dire que M n'a pas d'éléments d'ordre p. Clairement, si M a des éléments d'ordre p, p divise $|M|$. Si p divise $|M|$, nous avons vu au chap. 2, lemme 2.3.2, que M contient des éléments d'ordre p.

4.3.9 Lemme. — *Soit M un groupe abélien fini, écrit sous la forme*

$$M = \mathbf{Z}/m_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/m_r\mathbf{Z}$$

(sans condition de divisibilité sur les m_j.) Soit p un nombre premier. Alors la dimension du $\mathbf{F}_p$-espace vectoriel M/pM est égale au nombre d'indices j tels que $p|m_j$.

Démonstration. — L'homomorphisme de multiplication par p respecte tous les sous-groupes de M ; donc si l'on note $C_j = \mathbf{Z}/m_j\mathbf{Z}$ dans la décomposition ci-dessus, on a $pM = \bigoplus_{j=1}^r pC_j$. Mais alors d'après le lemme 4.3.3, $M/pM = \bigoplus_{j=1}^r C_j/pC_j$, et d'après le lemme 4.3.8, $C_j/pC_j \neq 0$ si et seulement si p divise $|C_j| = m_j$. Puisque le groupe C_j est cyclique, il est engendré par un unique élément, donc il en va de même pour le $\mathbf{F}_p$-espace vectoriel C_j/pC_j, ce qui prouve que si $C_j/pC_j \neq 0$, il est exactement de dimension 1. Donc $\dim_{\mathbf{F}_p}(M/pM)$ est exactement le nombre d'indices j tels que $p|m_j$.

4.3.10 Théorème. — *Le nombre r et les entiers $m_1|\ldots|m_r$ apparaissant dans le théorème 4.3.4 sont uniques. Par abus de langage, nous dirons encore que les m'_j sont les facteurs invariants de M.*

Démonstration. — Il résulte du lemme 4.3.9 que pour tout nombre premier p on a $\dim_{\mathbf{F}_p}(M/pM) \leq r$, avec égalité si et seulement si p divise m_1. Donc

$$r = \sup_p \dim_{\mathbf{F}_p}(M/pM)$$

est unique. Pour l'unicité des m_j, faisons une récurrence sur $|M|$. Si $|M| = 1$, il n'y a rien à démontrer. Sinon, choisissons un nombre premier p tel que $p|m_1$; d'après ce qui précède, l'ensemble de ces nombres premiers ne dépend pas du choix de la décomposition. Alors, dans les notations de la démonstration du lemme 4.3.9, et compte tenu du fait (exercice) que tout sous-groupe d'un groupe cyclique est encore cyclique, on a

$$pM = pC_1 \oplus \ldots \oplus pC_r \simeq \mathbf{Z}/m_1'\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/m_r'\mathbf{Z}$$

avec $m_j' = m_j/p$ pour $1 \leq j \leq r$. C'est encore une décomposition du type voulu, à ceci près que certains entiers m_j' pourraient être égaux à 1 ; les $m_j' > 1$ sont les facteurs invariants de pM. Donc, si aucun des m_j' n'est égal à 1, les m_j sont simplement les pm_j', et comme les m_j' sont uniques par hypothèse de récurrence, les m_j le sont aussi. Sinon, il y a $r - r'$ facteurs m_j égaux à p, où r' est le nombre de termes dans la décomposition canonique de pM (on notera d'ailleurs que dans ce cas il n'y a qu'un seul choix possible pour p) ; les autres m_j sont les pm_j', $m_j' > 1$, et sont donc encore uniques.

4.3.11. Venons-en maintenant à la question de l'unicité des facteurs invariants dans le théorème 4.2.7. Soit t le plus grand entier j tel que $d_j = 1$. Comme on l'a vu, on a alors :

$$M/N = \bigoplus_{j=t+1}^{s} \mathbf{Z}/d_j\mathbf{Z} \oplus \mathbf{Z}^l$$

avec $l = n - s$, d'où $(M/N)_{\mathrm{tor}} \simeq \bigoplus_{j=t+1}^{s} \mathbf{Z}/d_j\mathbf{Z}$. Comme $1 < d_{t+1}| \ldots |d_s$, ceci est la décomposition canonique du groupe $(M/N)_{\mathrm{tor}}$ donnée par le théorème 4.3.10. Donc $r = s - t$ et les $d_j > 1$ sont uniques. Mais comme $s = \mathrm{rg}\,(N)$ est également unique, t est unique, et donc tous les d_j sont uniques.