La classification des groupes abéliens de type fini

Johannes Huisman

18 octobre 2004

1 Groupes abélien de type fini

Définition 1.1. Un groupe G est *de type fini* s'il admet une partie génératrice finie.

Proposition 1.2. *Soit G un groupe abélien. Alors, G est de type fini si et seulement s'il existe un morphisme surjectif $f\colon \mathbb{Z}^n \to G$, pour un certain entier naturel n.*

Démonstration. Supposons qu'il existe un morphisme surjectif $f\colon \mathbb{Z}^n \to G$. Soit e_i le i-ième vecteur standard de $\mathbb{Z}^n$, pour $i = 1, \ldots, n$. Comme $\{e_1, \ldots, e_n\}$ engendre $\mathbb{Z}^n$, $\{f(e_1), \ldots, f(e_n)\}$ engendre $f(\mathbb{Z}^n)$. Comme f est surjectif, on a $f(\mathbb{Z}^n) = G$, et G est donc de type fini.

Réciproquement, supposons que G est de type fini, et soit $\{g_1, \ldots, g_n\}$ une partie génératrice de G. Soit $f\colon \mathbb{Z}^n \to G$ l'application définie par

$$f(a_1, \ldots, a_n) = a_1 g_1 + \cdots + a_n g_n.$$

Comme G est abélien, f est un morphisme de groupes. Comme $\{g_1, \ldots, g_n\}$ est génératrice, f est surjectif. $\square$

Corollaire 1.3. *Tout sous-groupe du groupe $\mathbb{Z}^n$ est de type fini.*

2 Sous-groupes de $\mathbb{Z}^n$

Proposition 2.1. *Soit $n \in \mathbb{N}$ et soit G un sous-groupe de $\mathbb{Z}^n$. Alors, il existe un entier naturel m et des élément $g_1, \ldots, g_m \in G$ tels que*

1. *$G = \langle g_1, \ldots, g_m \rangle$, et*
2. *$m \leq n$.*

Démonstration. Par récurrence sur n. □

Définition 2.2. Soit $f\colon G \to G'$ un morphisme de groupes abéliens. Le *conoyau* de f est le groupe quotient $G'/f(G)$.

Corollaire 2.3. *Soit G un groupe abélien de type fini. Alors, il existe des entiers naturels $m, n \in \mathbb{N}$ et un morphisme $f\colon \mathbb{Z}^m \to \mathbb{Z}^n$ tels que G est isomorphe au conoyau* $\operatorname{coker}(f)$ *de f.*

Démonstration. Comme G est abélien de type fini, il existe un morphisme surjectif $g\colon \mathbb{Z}^n \to G$ d'après Proposition 1.2. Le noyau $\ker(g)$ est un sous-groupe de $\mathbb{Z}^n$. D'après Corollaire 1.3, $\ker(g)$ est de type fini. D'après Proposition 1.2, il existe donc un morphisme surjectif $f\colon \mathbb{Z}^m \to \ker(g)$. Par conséquent, f, vu comme morphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$, a un conoyau isomorphe à G. □

3 Morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$

Soit $\operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$ l'ensemble des morphismes de groupes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$. Cet ensemble devient un groupe abélien lorsque on définit

$$(f+g)(x) = f(x) + g(x),$$

pour tout $x \in \mathbb{Z}^m$.

Soit $M_{n\times m}(\mathbb{Z})$ l'ensemble des matrices à n lignes et m colonnes à coefficients eniers. Cet ensemble est un groupe abélien sous l'addition matricielle.

Pour $a \in M_{n\times m}(\mathbb{Z})$, on définit une application

$$\Phi(a)\colon \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$$

par $\Phi(a)(x) = ax$, où ax est le produit matriciel de la matrice a et le vecteur x. Si $x \in \mathbb{Z}^m$, ax est bien un élément de $\mathbb{Z}^n$. Comme $a(x+x') = ax+ax'$, quels que soient $x, x' \in \mathbb{Z}^m$, l'application $\Phi(a)$ est un morphisme de groupes.

Proposition 3.1. *L'application*

$$\Phi\colon M_{n\times m}(\mathbb{Z}) \longrightarrow \operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$$

est un isomorphisme de groupes.

Démonstration. Comme $(a+a')x = ax+a'x$ pour tout $x \in \mathbb{Z}^m$ et quelles que soient les matrices a et a' dans $M_{n\times m}(\mathbb{Z})$, l'application Φ est un morphisme de groupes.

Si $\Phi(a) = 0$, on a $\Phi(a)(e_i) = 0$ pour tout $i = 1, \ldots, m$, où e_i est le vecteur standard de $\mathbb{Z}^m$ dont toutes les coordonnées sont nulles, sauf la i-ième qui est égale à 1. Mais, $\Phi(a)(e_i) = ae_i$ est égale à la i-ième colonne de a. Donc, toutes les colonnes de a sont nulles. Par conséquent a est nulle, et Φ est injectif.

Pour montrer que Φ est surjectif, soit f un morphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$. Soit a la matrice dans $M_{n\times m}(\mathbb{Z})$ dont la i-ième colonne est égale à $f(e_i)$, pour $i = 1, \ldots, m$. Comme $\Phi(a)(e_i) = f(e_i)$ et comme $\{e_1, \ldots, e_m\}$ est générateur de $\mathbb{Z}^m$, on a $\Phi(a) = f$. Cela montre la surjectivité de Φ. □

Proposition 3.2. *Soient $k, m, n \in \mathbb{N}$, $a \in M_{n\times m}(\mathbb{Z})$ et $b \in M_{m\times k}(\mathbb{Z})$. Alors, $ab \in M_{n\times k}(\mathbb{Z})$ et*

$$\Phi(ab) = \Phi(a) \circ \Phi(b).$$

Démonstration. C'est facile : si $x \in \mathbb{Z}^k$, $(\Phi(a) \circ \Phi(b))(x) = a(bx) = (ab)x = \Phi(ab)(x)$. □

Soit $n \in \mathbb{N}$. Le groupe $\mathrm{End}(\mathbb{Z}^n)$ est un anneau sous la composition d'endomorphismes. Son groupe multiplicatif est, par définition, $\mathrm{Aut}(\mathbb{Z}^n)$.

Le groupe $M_n(\mathbb{Z})$ des matrices carrées est un anneau sous la multiplication matricielle. Son groupe multiplicatif est, par définition,$\mathrm{GL}_n(\mathbb{Z})$.

Corollaire 3.3. *Soit $n \in \mathbb{N}$. Alors*

$$\Phi\colon M_n(\mathbb{Z}) \longrightarrow \mathrm{End}(\mathbb{Z}^n)$$

est un isomorphisme d'anneaux. En particulier, sa restriction $\Phi^\times$ à $\mathrm{GL}_n(\mathbb{Z})$ est un isomorphisme de groupes

$$\Phi^\times\colon \mathrm{GL}_n(\mathbb{Z}) \longrightarrow \mathrm{Aut}(\mathbb{Z}^n).$$

Proposition 3.4. *Soit $n \in \mathbb{N}$. On a*

$$\mathrm{GL}_n(\mathbb{Z}) = \{a \in M_n(\mathbb{Z}) \mid \det(a) = \pm 1\}.$$

Démonstration. Si $a \in \mathrm{GL}_n(\mathbb{Z})$, il existe $b \in M_n(\mathbb{Z})$ telle que $ab = 1_n$, où 1_n est la matrice identité dans $M_n(\mathbb{Z})$. On a donc $1 = \det(1_n) = \det(ab) = \det(a)\det(b)$. Comme $\det(a), \det(b) \in \mathbb{Z}$, $\det(a) \in \mathbb{Z}^\times = \{\pm 1\}$.

Réciproquement, si $a \in M_n(\mathbb{Z})$ est de déterminant 1, soit a' la matrice des cofacteurs de a. Evidemment, $a' \in M_n(\mathbb{Z})$. Comme $aa' = a'a = \det(a)1_n = \pm 1_n$, on a bien $a \in \mathrm{GL}_n(\mathbb{Z})$. □

4 Equivalence de matrices entières

Définition 4.1. Soient $n \in \mathbb{N}$ et $i, j \in \mathbb{N}$ tels que $i, j \leq n$. La *matrice $n \times n$ standard* e_{ij} est la matrice dont tous les coefficients sont nuls, sauf celui dans la i-ième ligne et j-ième colonne qui est égal à 1. Un *matrice $n \times n$ élémentaire* à coefficients dans $\mathbb{Z}$ est une matrice de la forme $1_n + qe_{i,j}$, où $i \neq j$, $q \in \mathbb{Z}$ et 1_n est la matrice $n \times n$ identité. On pose $e_{ij}(q) = 1_n + qe_{ij}$.

Proposition 4.2. *Soit $a \in M_{n\times m}(\mathbb{Z})$ et soit $q \in \mathbb{Z}$.*

1. *Soient $i, j \in \mathbb{N}$ avec $i, j \leq n$. La matrice $e_{ij}(q)a$ est la matrice obtenu à partir de a en effectuant l'opération élémentaire qui consiste en remplacer la i-ième ligne de a par la somme de la i-ième ligne de a et q fois la j-ième ligne de a.*
2. *Soient $i, j \in \mathbb{N}$ avec $i, j \leq m$. La matrice $ae_{ij}(q)$ est la matrice obtenu à partir de a en effectuant l'opération élémentaire qui consiste en remplacer la j-ième colonne de a par la somme de la j-ième colonne de a et q fois la i-ième colonne de a.* □

Définition 4.3. Soient $m, n \in \mathbb{N}$. Une *matrice diagonale $n \times m$ à coefficients dans $\mathbb{Z}$* est une matrice $a = (a_{ij})$, où $a_{ij} \in \mathbb{Z}$ pour $i = 1, \dots, n$ et $j = 1, \dots, m$ tels que $a_{ij} = 0$ lorsque $i \neq j$. Soit ℓ un entier naturel avec $\ell \leq m$ et $\ell \leq n$. Soient $d_1, \dots, d_\ell$ des entiers relatifs, on note $\mathrm{diag}_{m\times n}(d_1, \dots, d_\ell)$ ou, simplement, $\mathrm{diag}(d_1, \dots, d_\ell)$ la matrice diagonale $a = (a_{ij})$ de format $n \times m$ définie par $a_{ij} = 0$ si $i \neq j$, $a_{ii} = d_i$, pour $i = 1, \dots, \ell$, et $a_{ii} = 0$ pour $i > \ell$, i.e.

$$\mathrm{diag}(d_1, \dots, d_\ell) = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & d_\ell & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Théorème 4.4. *Soient $m, n \in \mathbb{N}$. Soit $a \in M_{n\times m}(\mathbb{Z})$.Il existe des matrices $u \in M_n(\mathbb{Z})$ et $v \in M_m(\mathbb{Z})$, $\ell \in \mathbb{N}$ et $d_1, \dots, d_\ell \in \mathbb{Z} \setminus \{0\}$ tels que*

1. *u et v sont des produits de matrices élémentaires,*
2. *$uav = \mathrm{diag}(d_1, \dots, d_\ell)$, et*
3. *d_i divise d_{i+1} pour $i = 1, \dots, \ell - 1$.*

Démonstration. Par récurrence sur n. Si $n = 0$, a est la matrice vide de format $0 \times m$, et l'énoncé est bien vrai. Supposons donc que l'énoncé est vrai au rang $n-1$, pour un certain $n \in \mathbb{N}$, $n > 0$. Soit a une matrice $n \times m$ à coefficients dans $\mathbb{Z}$. On doit montrer que l'énoncé est vrai pour a. On peut évidemment supposer que $a \neq 0$. On montre qu'il existe des matrices $u' \in M_n(\mathbb{Z})$ et $v' \in M_m(\mathbb{Z})$ telles que

$$u'av' = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{pmatrix},$$

où $d_1 \in \mathbb{Z} \setminus \{0\}$ divise tous les éléments de la matrice a' extraite de $u'av'$ en supprimant la première ligne et la première colonne, et où u' et v' sont des produits de matrices élémentaires. D'après l'hypothèse de récurrence, il y aura alors des matrices $u'' \in M_{n-1}(\mathbb{Z})$ et $v'' \in M_{m-1}(\mathbb{Z})$, produits de matrices élémentaires, telles que $u''a'v'' = \mathrm{diag}(d_2, \ldots, d_\ell)$, où $d_2, \ldots, d_\ell \in \mathbb{Z} \setminus \{0\}$, et d_i divise d_{i+1} pour $i = 2, \ldots, \ell - 1$. Soient

$$u = \begin{pmatrix} 1 & 0 \\ 0 & u'' \end{pmatrix} \cdot u' \quad \text{et} \quad v = v' \cdot \begin{pmatrix} 1 & 0 \\ 0 & v'' \end{pmatrix}.$$

Il est clair que u et v sont encore des produits de matrices élémentaires. On a

$$uav = \begin{pmatrix} 1 & 0 \\ 0 & u'' \end{pmatrix} \begin{pmatrix} d_1 & 0 \\ 0 & a' \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & v'' \end{pmatrix} = \mathrm{diag}(d_1, \ldots, d_\ell).$$

Comme d_1 divise tous les coefficients de a', d_1 divise aussi tous les coefficients de $u''a'v'' = \mathrm{diag}(d_2, \ldots, d_\ell)$. D'où d_i divise d_{i+1} pour $i = 1, \ldots, \ell - 1$. Par conséquent, il suffit de montrer l'existence des matrices u' et v' comme ci-dessus.

Quitte à multiplier a à gauche par une matrice élémentaire, on peut supposer que la première ligne de a est non nulle. D'après l'algorithme d'Euclide, il existe un produit de matrices élémentaires v_1 tel que tous les coefficients de la première ligne de av_1 sont nuls, sauf un qui est égal au pgcd des coefficients de la première ligne de a. Quitte à multiplier v_1 à droite par un produit de matrices élémentaires, on peut supposer que le coefficient non nul de la première ligne de av_1 est dans la première colonne, i.e., que

$$av_1 = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ \star & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ \star & \star & \cdots & \star \end{pmatrix},$$

où $c_1 \in \mathbb{Z} \setminus \{0\}$ est un pgcd des coefficients de la première ligne de a.

Ensuite, d'après l'algorithme d'Euclide, il existe un produit de matrices élémentaires u_1 tel que tous les coefficients de la première colonne de $u_1 a v_1$ sont nuls, sauf un qui est égal au pgcd des coefficients de la première colonne de av_1. Quitte à multiplier u_1 à gauche par un produit de matrices élémentaires, on peut supposer que le coefficient non nul de la première colonne de $u_1 a v_1$ est dans la première ligne, i.e., que

$$u_1 a v_1 = \begin{pmatrix} c_2 & \star & \cdots & \star \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{pmatrix},$$

où $c_2 \in \mathbb{Z} \setminus \{0\}$ est un pgcd des coeffcients de la première colonne de av_1. En particulier, c_2 divise c_1. On réitère. Ce procédé termine forcément, i.e., il existe des matrices u_2 et v_2, produits de matrices élémentaires, telles que

$$u_2 a v_2 = \begin{pmatrix} c_3 & 0 & \cdots & 0 \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{pmatrix},$$

où $c_3 \in \mathbb{Z} \setminus \{0\}$.

Si c_3 divise tous les coefficients de $u_2 a v_2$, on a terminé. Sinon, quitte à multiplier $u_2 a v_2$ à gauche par une matrice élémentaire, on peut supposer que le pgcd de la première ligne de $u_2 a v_2$ divise strictement c_3. Comme ci-dessus, il existe alors un produit de matrices élémentaires v_3 tel que tous les coefficients de la première ligne de $u_2 a v_3$ sont nuls sauf le premier qui est égal à ce dernier pgcd. Puis, il existe un produit de matrices élémentaires u_3 tel que

$$u_3 a v_3 = \begin{pmatrix} c_4 & 0 & \cdots & 0 \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{pmatrix},$$

où c_4 divise strictement c_3. Comme avant, ou bien c_4 divise tous les coefficients de $u_3 a v_3$, auquel cas on a terminé, ou bien il existe un coefficient qui n'est pas divisible par c_4, et on réitère. Il est clair que ce processus termine, c-à-d, qu'il existe des produits de matrices élémentaires u' et v' tels que $u' a v'$ est de la forme recherchée. $\square$

Exemple 4.5. Soit a la matrice de $M_2(\mathbb{Z})$ définie par

$$a = \begin{pmatrix} 30 & 42 \\ 70 & 105 \end{pmatrix} = \begin{pmatrix} 2\cdot 3\cdot 5 & 2\cdot 3\cdot 7 \\ 2\cdot 5\cdot 7 & 3\cdot 5\cdot 7 \end{pmatrix}.$$

On se propose d'effectuer l'algorithme ci-dessus sur a pour trouver des matrices u et v tel que uav est une matrice diagonale comme dans l'énoncé du théorème. Comme le pgcd des coefficients de a est égal à 1, et comme le déterminant de a est égal à 210, on peut affirmer a priori que a est équivalente à la matrice diagonale $\mathrm{diag}(1, 210)$. Et, en effet, si l'on effectue l'algorithme, on obtient la suite des opérations élémentaires suivantes :

$$\begin{pmatrix} 2\cdot 3\cdot 5 & 2\cdot 3\cdot 7 \\ 2\cdot 5\cdot 7 & 3\cdot 5\cdot 7 \end{pmatrix} \overset{C_2:=C_2-C_1}{\rightsquigarrow} \begin{pmatrix} 2\cdot 3\cdot 5 & 2\cdot 3\cdot 2 \\ 2\cdot 5\cdot 7 & 5\cdot 7 \end{pmatrix} \overset{C_1:=C_1-2C_2}{\rightsquigarrow}$$
$$\begin{pmatrix} 2\cdot 3 & 2\cdot 3\cdot 2 \\ 0 & 5\cdot 7 \end{pmatrix} \overset{C_2:=C_2-2C_1}{\rightsquigarrow} \begin{pmatrix} 2\cdot 3 & 0 \\ 0 & 5\cdot 7 \end{pmatrix} \overset{L_1:=L_1+L_2}{\rightsquigarrow}$$
$$\begin{pmatrix} 2\cdot 3 & 5\cdot 7 \\ 0 & 5\cdot 7 \end{pmatrix} \overset{C_2:=C_2-5C_1}{\rightsquigarrow} \begin{pmatrix} 6 & 5 \\ 0 & 35 \end{pmatrix} \overset{C_1:=C_1-C_2}{\rightsquigarrow}$$
$$\begin{pmatrix} 1 & 5 \\ -35 & 35 \end{pmatrix} \overset{C_2:=C_2-5C_1}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ -35 & 210 \end{pmatrix} \overset{L_2:=L_2+35L_1}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 0 & 210 \end{pmatrix}$$

On pose

$$u = \begin{pmatrix} 1 & 0 \\ 35 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 35 & 36 \end{pmatrix}$$

et

$$\begin{aligned} v &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 25 & -147 \\ -17 & 100 \end{pmatrix}. \end{aligned}$$

On a bien $uav = \mathrm{diag}(1, 210)$.

Définition 4.6. Soient $m, n \in \mathbb{N}$ et $a, b \in M_{n\times m}(\mathbb{Z})$. On dit que a et b sont *équivalentes* s'il existe des matrices $u \in \mathrm{GL}_n(\mathbb{Z})$ et $v \in \mathrm{GL}_m(\mathbb{Z})$ telles que $uav = b$.

Théorème 4.7. *Soient $m, n \in \mathbb{N}$ et $a \in M_{n\times m}(\mathbb{Z})$. Alors il existe un entier naturel ℓ et des entiers naturels non nuls $d_1, \ldots, d_\ell$ tels que*

1. *a est équivalente à la matrice* $\mathrm{diag}(d_1, \ldots, d_\ell)$, *et*
2. *d_i divise d_{i+1} pour $i = 1, \ldots, \ell - 1$.*

De plus, l'entier ℓ et les entiers $d_1, \dots, d_\ell$ sont uniquement déterminés par a.

Démonstration. Montrons d'abord l'existence. D'après le théorème précédent, il existe $u \in \mathrm{GL}_n(\mathbb{Z})$ et $v \in \mathrm{GL}_m(\mathbb{Z})$ telles que $uav = \mathrm{diag}(d_1, \dots, d_\ell)$ pour certains entiers relatifs non nuls $d_1, \dots, d_\ell$, où d_i divise d_{i+1}. Quitte à multiplier u à gauche par une matrice diagonale dans $\mathrm{GL}_n(\mathbb{Z})$ à coefficients diagonaux égaux à ± 1, on peut supposer que les entiers $d_1, \dots, d_\ell$ sont positifs. cela montre l'existence. On admettra l'unicité. $\square$

Définition 4.8. Avec la notation du Corollaire ci-dessus, ℓ est le *rang* de la matrice a et les entiers naturels non nuls $d_1, \dots, d_\ell$ sont les *facteurs invariants* de a.

Corollaire 4.9. *Soient $m, n \in \mathbb{N}$ et $a, b \in M_{n\times m}(\mathbb{Z})$. Les matrices a et b sont équivalentes si et seulement si elles ont même rang et mêmes facteurs invariants.*

5 Retour aux morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$

Corollaire 5.1. *Soient $m, n \in \mathbb{N}$ et soit $f \colon \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$ un morphisme de groupes. Il existe des automorphismes α et β de $\mathbb{Z}^n$ et $\mathbb{Z}^m$ respectivement, un entier naturel ℓ, et des entiers naturels non nuls $d_1, \dots, d_\ell$ tels que*

1. *la matrice de $\alpha \circ f \circ \beta$ est la matrice diagonale $\mathrm{diag}_{m\times n}(d_1, \dots, d_\ell)$, et*
2. *d_i divise d_{i+1} pour $i = 1, \dots, \ell - 1$.*

De plus, l'entier ℓ et les entiers $d_1, \dots, d_\ell$ sont uniquement déterminés par f.

Définition 5.2. Avec la notation du Corollaire ci-dessus, ℓ est le *rang* du morphisme f et les entiers naturels non nuls $d_1, \dots, d_\ell$ sont les *facteurs invariants* de f.

6 Classification des groupes abéliens de type fini

Théorème 6.1. *Soit G un groupe abélien de type fini. Alors, il existe des entiers naturels r et ℓ, et des entiers naturels $d_1, \dots, d_\ell$ tels que*

1. *G est isomorphe au groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z} \times \mathbb{Z}^r$,*
2. *d_i divise d_{i+1}, pour $i = 1, \dots, \ell - 1$, et*
3. *$d_i \geq 2$, pour $i = 1, \dots, \ell$.*

De plus, les entiers r, ℓ, et $d_1, \dots, d_\ell$ sont uniquement déterminés par G.

Démonstration. Montrons d'abord l'existence. Soit $f\colon \mathbb{Z}^m \to \mathbb{Z}^n$ un morphisme tel que $\operatorname{coker}(f) \cong G$. D'après le corollaire précédent, on peut supposer que la matrice de f est égale à $\operatorname{diag}(d_1, \ldots, d_\ell)$, où ℓ est un entier naturel et $d_1, \ldots, d_\ell$ sont des entiers naturels non nuls tels que d_i divise d_{i+1}. Cela veut dire que $f(e_i) = d_i e_i$ pour $i = 1, \ldots, \ell$ et que $f(e_i) = 0$ pour $i = \ell + 1, \ldots, m$. D'où

$$\operatorname{im}(f) = d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_\ell\mathbb{Z} \times \{0\}^r,$$

où $r = n - \ell$. Il s'ensuit que

$$\operatorname{coker}(f) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z} \times \mathbb{Z}^r.$$

On peut supposer que $d_i \neq 1$, i.e., que $d_i \geq 2$ pour tout i. L'unicité de ℓ et $d_1, \ldots, d_\ell$ découle facilement de l'unicité des entiers correspondants de f. □

Corollaire 6.2. *Tout groupe abélien de type fini est isomorphe à un produit de groupes monogènes.*

Corollaire 6.3. *Soit G un groupe abélien fini. Alors, il existe un entier naturel ℓ, et des entiers naturels $d_1, \ldots, d_\ell$ tels que*

1. *G est isomorphe au groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$,*
2. *d_i divise d_{i+1}, pour $i = 1, \ldots, \ell - 1$, et*
3. *$d_i \geq 2$, pour $i = 1, \ldots, \ell$.*

De plus, les entiers ℓ et $d_1, \ldots, d_\ell$ sont uniquement déterminés par G.

Corollaire 6.4. *Tout groupe abélien fini est isomorphe à un poduit de groupes cycliques.*

Définition 6.5. Avec la notation du Théorème précédent, l'entier natural r est le *rang* du groupe G, les entiers naturels non nuls $d_1, \ldots, d_\ell$ sont les *facteurs invariants* de G.

Définition 6.6. Soit G un groupe. Un élément de G est *de torsion* s'il est d'ordre fini. Soit G_{tors} le sous-ensemble de G des éléments de trosion. On dit que G est *sans torsion* lorsque $G_{\text{tors}} = \{1\}$. On dit que G est *de torsion* lorsque $G_{\text{tors}} = G$.

Proposition 6.7. *Soit G un groupe abélien. Alors G_{tors} est un sous-groupe de G. Le quotient G/G_{tors} est sans torsion.*

Démonstration. Exercice. □

Définition 6.8. Soit G un groupe abélien. Le sous-groupe G_{tors} est le *sous-groupe de torsion* de G.

Corollaire 6.9. *Soit G un groupe abélien de type fini. Si G est sans torsion, alors G est isomorphe à $\mathbb{Z}^r$, pour un certain $r \in \mathbb{N}$.*