Groupes abéliens de type fini

Nicolas Tosel

En algèbre, le point de vue « structurel » conduit naturellement à la détermination « à isomorphisme près » de tous les objets vérifiant une liste d'axiomes donnée. À vrai dire, un tel objectif est le plus souvent chimérique et il est ainsi illusoire d'espérer classer les groupes finis, les anneaux commutatifs finis ...

Certains objets simples sont cependant susceptibles d'une telle description. Ainsi, deux espaces vectoriels de dimension finie sur le corps $\mathbb{K}$ sont isomorphes si et seulement s'ils ont même dimension. Ce texte est consacré à un théorème de cette nature, sensiblement plus délicat, la classification à isomorphisme près des groupes abéliens de type fini. L'ubiquité de ces groupes (arithmétique des corps de nombres) rend le résultat précieux.

La présentation suivie n'est pas économique. On élucide en premier lieu la structure des groupes abéliens finis en utilisant la notion d'exposant et un argument de dualité (prolongement des caractères). On passe ensuite au cas général. La méthode suivie due à Frobenius et Stickelberger (1879), repose sur la « forme normale de Smith » des matrices entières », découverte par H.J. Smith en 1861. Les paragraphes **2** et **3**, qui établissent cette généralisation, peuvent pour l'essentiel être lus indépendamment du paragraphe **1**.

Un groupe abélien n'est rien d'autre qu'un $\mathbb{Z}$-module. Pour souligner l'importance de la linéarité, la loi de groupe est notée ici additivement. On utilise librement le vocabulaire de base concernant les modules : somme, somme directe. En particulier, si H est un sous-groupe d'un groupe abélien G, on dit que *H est facteur direct dans G* si et seulement s'il existe un sous-groupe K de G tel que : $H \oplus K = G$.

Signalons pour terminer que les démonstrations s'adaptent immédiatement (resp. avec des modifications mineures dans les preuves) pour fournir la structure des modules de type fini sur un anneau euclidien (resp. principal). Cette généralisation, qui est la clé de la théorie des invariants de similitude d'un endomorphisme, n'est pas abordée ici.

1 Les groupes abéliens finis

Une des grandes différences entre la théorie des modules et celle des espaces vectoriels est qu'un sous-module n'est pas facteur direct en général. Néanmoins on a le résultat très simple suivant.

Lemme 1. *Soient $(G,+)$ un groupe abélien, G_1 un sous-groupe de G et H un groupe. Supposons qu'il existe un élément Φ de $Hom\,(G,H)$ induisant un isomorphisme de G_1 sur $\Phi(G)$. Alors : $G_1 \oplus Ker\ \Phi = G$.*

Preuve. Soit g dans G. Il suffit de vérifier qu'il existe un unique g_1 dans G_1 tel que $g - g_1$ appartienne à Ker Φ c'est-à-dire tel que : $\Phi(g) = \Phi(g_1)$. Mais $\Phi(g)$ a un unique antécédent par Φ dans G_1, d'où le résultat.

Nous noterons g.a.f pour « groupe abélien fini ». Ce paragraphe est dévolu à la preuve du théorème de structure ci-après, dû à Kronecker.

Théorème 1. *Soit $(G, +)$ un g.a.f. non nul. Alors :*

i) il existe $r \in \mathbb{N}^*$, des entiers $d_1, \ldots, d_r$ supérieurs ou égaux à 2 tels que $d_1|d_2|\cdots|d_r$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$;

ii) les entiers $r, d_1, \ldots, d_r$ sont déterminés par G.

Un g.a.f est ainsi produit direct de groupes cycliques, la condition de divisibilité sur les d_i assurant l'unicité de l'écriture.

La démonstration suivie ici part de la mise en évidence du facteur $\mathbb{Z}/d_r\mathbb{Z}$. Le lemme suivant nous sera utile.

Lemme 2. *Soient a et b deux éléments d'un groupe G, d'ordres finis respectifs u et v. Si a et b commutent et u et v sont premiers entre eux, alors ab est d'ordre uv.*

Preuve. Puisque $ab = ba$, on voit facilement que $(ab)^{uv} = e$: ab est d'ordre fini w divisant uv. Par ailleurs, on a $e = (ab)^w = a^w b^w, a^w = b^{-w}$. Or, on dispose de x et y dans $\mathbb{Z}$ tels que $ux + vy = 1$. En élevant la dernière relation à la puissance yv, il vient $a^w = e$, ce qui montre que u divise w. Par symétrie, v divise w et donc uv divise w, ce qui achève la preuve.

On nomme *exposant* du g.a.f G le ppcm des ordres des éléments de G ; on a alors la proposition suivante, qui serait évidente si le théorème était établi, mais qui nous servira ici de point de départ.

Lemme 3. *Si $(G, +)$ est un g.a.f, il existe un élément de G dont l'ordre est l'exposant de G.*

Preuve. Soit d l'exposant de G : $d = \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i sont premiers deux à deux distincts et les α_i sont dans $\mathbb{N}^*$. Par définition de d, il existe $g_i \in G$ d'ordre ω_i multiple de $p_i^{\alpha_i}$. Ecrivons : $\omega_i = q_i p_i^{\alpha_i}$ et observons que $h_i = q_i g_i$ est d'ordre $p_i^{\alpha_i}$. Le lemme précédent montre que $h = h_1 \cdots h_r$ est d'ordre d.

Pour établir l'existence de la décomposition dans le théorème, il suffit, moyennant une récurrence facile, de montrer que tout sous-groupe cyclique d'un g.a.f. G dont l'ordre est l'exposant de G est facteur direct dans G. Pour ce faire, nous utiliserons les *caractères* de G, c'est-à-dire les morphismes de G dans le groupe multiplicatif $(U, \times)$ des complexes de module 1. L'ensemble des caractères de G sera noté $\widehat{G}$.

Les caractères ont beaucoup d'applications, mais, ici, nous utiliserons seulement le lemme de prolongement :

Lemme 4. *Soient $(G, +)$ un g.a.f, H un sous-groupe de G, φ dans $\widehat{H}$. Il existe au moins un élément de $\widehat{G}$ prolongeant φ.*

Preuve. Si $H = G$, c'est terminé. Sinon, soient $x \in G \setminus H$ et K le sous-groupe de G engendré par x et H : $K = H + \mathbb{Z}x$. On va prolonger φ en un élément de $\widehat{K}$. Le lemme sera alors établi car, en répétant un nombre fini de fois cette opération, on aura prolongé φ en un élément de $\widehat{G}$. On considère naturellement $\{k \in \mathbb{Z},\ kx \in H\}$, qui est un sous-groupe non trivial de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}^*$. On a : $mx \in H$, on pose $\gamma = \varphi(mx)$ et on choisit $\alpha \in U$ tel que $\alpha^m = \gamma$. Pour $h \in H$ et $k \in \mathbb{Z}$, on définit : $\psi(kx + h) = \alpha^k \varphi(h)$. On laisse au lecteur le soin de vérifier que ψ est bien définie, à valeurs dans U, prolonge φ, et est dans $\widehat{K}$. Le résultat suit.

Le lemme ci-après complète la démonstration de la partie « existence » dans le théorème de structure des g.a.f.

Lemme 5. *Soient $(G, +)$ un g.a.f, x un élément de G dont l'ordre d est l'exposant de G. Alors $\mathbb{Z}x$ est facteur direct dans G.*

Preuve. On pose, pour k dans $\mathbb{Z}$: $\varphi(kx) = e^{2ik\pi/d}$. On vérifie que φ est bien définie et réalise un isomorphisme du sous-groupe de G engendré par x sur le sous-groupe U_d des racines d-ièmes de l'unité. On prolonge φ en un caractère ψ de G. Pour g dans G alors $dg = 0$ et $\psi(g) \in U_d$, donc $\psi \in \mathrm{Hom}\,(G, U_d)$. Il reste à appliquer le premier lemme du paragraphe pour obtenir le résultat avec $H = \mathrm{Ker}\ \psi$.

Prouvons à présent l'unicité dans le théorème de structure des g.a.f. Il s'agit de démontrer que si :

$$(G,\ +) = (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z},\ +)\,,$$

où r et les d_i sont comme dans l'énoncé, on lit r et les d_i dans la structure de groupe de G. Soient $p_1, \ldots, p_s$ les facteurs premiers de $|G|$. Si $1 \leq j \leq r$, d_j s'écrit :

$$d_j = \prod_{i=1}^{s} p_i^{\alpha_{i,j}} \qquad \text{où } \alpha_{i,j} \in \mathbb{N}, \quad \text{et} \quad \alpha_{i,1} \leq \cdots \leq \alpha_{i,r}\ .$$

Il suffit de montrer que les $\alpha_{i,j}$ sont également déterminés par G. Or, en appliquant le théorème chinois à chaque $\mathbb{Z}/d_j\mathbb{Z}$, il vient :

$$G \simeq G_1 \times \cdots \times G_s \quad \text{où} \quad G_i = \prod_{j=1}^{r} \mathbb{Z}/p_i^{\alpha_{i,j}}\mathbb{Z}\ .$$

Comme G_i s'identifie au sous-groupe des éléments de $G_1 \times \cdots \times G_s$ dont l'ordre est une puissance de p_i, G_i est déterminé par $G_1 \times \cdots \times G_s$. Reste alors à montrer que les $(\alpha_{i,j})_{1 \leq j \leq r}$ sont déterminés par G_i, ce qui découle du :

Lemme 6. *Soient p un nombre premier, $q \in \mathbb{N}^*$, et*

$$H = (\mathbb{Z}/p\mathbb{Z})^{n_1} \times \cdots \times (\mathbb{Z}/p^q\mathbb{Z})^{n_q}$$

où les n_i sont dans $\mathbb{N}$. Alors les n_i sont déterminés par H.

Preuve. Si $1 \leq i \leq q$, le nombre d'élément de H dont l'ordre divise p^i est :

$$p^{n_1 + 2n_2 + \cdots + in_i + in_{i+1} + \cdots + in_q}.$$

Ainsi les nombres :

$$\begin{cases} n_1 + 2n_2 + \cdots + qn_q \\ n_1 + 2n_2 + \cdots + (q-1)n_{q-1} + (q-1)n_q \\ \quad \vdots \\ n_1 + n_2 + \cdots + n_q \end{cases}$$

sont déterminés par H. Les n_i le sont donc également.

Le théorème de structure contient virtuellement toute la théorie des g.a.f. Les exercices suivants en indiquent quelques applications.

Exercice 1. *Soit G un g.a.f. À quelle condition existe-t-il deux g.a.f. non triviaux G_1 et G_2 tels que G soit isomorphe à $G_1 \times G_2$? (On dit alors que G est décomposable.)*

Exercice 2. *Soient G un g.a.f d'ordre n, d un diviseur de n. Montrer que G a un sous-groupe d'ordre d.*

Exercice 3. *Montrer que deux g.a.f sont isomorphes si et seulement s'ils ont, pour tout d de $\mathbb{N}^*$, même nombre d'éléments d'ordre d.*

Exercice 4. *Soit G un g.a.f. Montrer que $Aut\,(G)$ est abélien si et seulement si G est cyclique.*

Exercice 5. *On note φ l'indicateur d'Euler. Si G est un g.a.f, montrer que $|Aut\,(G)|$ est minoré par $\varphi(|G|)$. Cas d'égalité ?*

2 G.a.t.f et g.a.l.t.f

Un groupe est dit de type fini si et seulement s'il admet une famille génératrice finie. On abrègera *groupe abélien de type fini* en g.a.t.f. Les g.a.t.f sont exactement les $\mathbb{Z}$-modules de type fini.

Exemples. Tout g.a.f. est un g.a.t.f ; si $n \in \mathbb{N}^*$, $(\mathbb{Z}^n, +)$ est un g.a.t.f ; le produit de deux g.a.t.f est un g.a.t.f. On montrera que tous les g.a.t.f s'obtiennent en combinant ces trois assertions.

Soient $(G, +)$ un g.a.t.f, $(a_1, \ldots, a_n)$ une famille génératrice de G. Le morphisme :

$$\begin{array}{rccc} \varphi\ : & \mathbb{Z}^n & \to & G \\ & (\lambda_1, \ldots, \lambda_n) & \mapsto & \displaystyle\sum_{i=1}^{n} \lambda_i a_i \end{array} .$$

est surjectif et G est isomorphe au quotient de $\mathbb{Z}^n$ par $\ker \varphi$. Pour comprendre la structure de G on est ainsi amené à étudier les sous-groupes de $\mathbb{Z}^n$. Introduisons à cet effet un peu de terminologie.

1. Soit $(G, +)$ un groupe abélien. On appelle $\mathbb{Z}$-*base* de G toute famille $\mathbb{Z}$-libre et $\mathbb{Z}$-génératrice de G, c'est-à-dire toute famille $(g_i)_{i \in I}$ de G telle que tout élément de G s'écrive d'une unique façon :

$$\sum_{i \in I} \lambda_i g_i$$

où $(\lambda_i)_{i \in I}$ est une famille presque nulle d'éléments de $\mathbb{Z}$.

2. On appelle *groupe abélien libre* tout groupe abélien possédant une $\mathbb{Z}$-base. Par exemple, si X est un ensemble, le groupe additif $\mathbb{Z}^{(X)}$ des fonctions à support fini de X dans $\mathbb{Z}$ est libre et la famille des fonctions caractéristiques des singletons en est une $\mathbb{Z}$-base. Un groupe abélien libre de base B est d'ailleurs isomorphe à $\mathbb{Z}^{(B)}$

Par définition même, un groupe abélien libre possédant une $\mathbb{Z}$-base indexée par l'ensemble I est isomorphe au $\mathbb{Z}$-module $Z^{(I)}$ des familles presques nulles indexées par I. Si I est infini, ce module ne peut évidemment pas être de type fini. Les groupes abéliens libres de type fini (abréviativement g.a.l.t.f) sont donc les groupes isomorphes à $(\mathbb{Z}^n, +)$ pour un certain n de $\mathbb{N}$.

Il est naturel à ce stade de vérifier que l'isomorphisme de $(\mathbb{Z}^n, +)$ et $(\mathbb{Z}^m, +)$ avec $(n, m) \in \mathbb{N}^2$ implique $n = m$, autrement dit que la structure de groupe de $(\mathbb{Z}^n, +)$ détermine n. Voici l'argument essentiel.

Lemme 7. *Si le g.a.t.f G possède une famille génératrice de cardinal $n \in \mathbb{N}^*$, toute famille $\mathbb{Z}$-libre de G est finie de cardinal au plus n.*

Preuve. Toute famille $\mathbb{Z}$-libre de $\mathbb{Z}^n$ est une famille $\mathbb{Q}$-libre du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$, donc finie de cardinal majoré par n. Le résultat s'en déduit aisément.

Soit r dans $\mathbb{N}$. On dit qu'un groupe abélien G est de *rang* r si et seulement si r est le cardinal maximal d'une famille $\mathbb{Z}$-libre d'éléments de G. En utilisant le lemme précédent et en observant que la $\mathbb{Z}$-base canonique de $\mathbb{Z}^n$ est $\mathbb{Z}$-libre, on obtient le :

Lemme 8. *Si $n \in \mathbb{N}^*$, le g.a.l.t.f $(\mathbb{Z}^n, +)$ est de rang n. L'entier n est donc déterminé par la structure de groupe de $(\mathbb{Z}^n, +)$.*

Remarques

1. L'étude des g.a.l.t.f, cas particulier de celle des modules, a de nombreux points communs avec celle des espaces vectoriels. Le lemme précédent montre ainsi que toutes les $\mathbb{Z}$-bases d'un g.a.l.t.f G ont même cardinal. Il y a cependant d'importantes différences : une famille $\mathbb{Z}$-libre de cardinal n de $(\mathbb{Z}^n, +)$ n'est pas forcément une base (cf la description des $\mathbb{Z}$-bases de $(\mathbb{Z}^n, +)$ ci-dessous) ; $\mathbb{Z}^n$ contient beaucoup de sous-groupes de rang n ; un sous-groupe de $(\mathbb{Z}^n, +)$ n'est pas forcément facteur direct.
2. Autre preuve du lemme 8. Soient $(A, +)$ un g.a.l.t.f possédant une $\mathbb{Z}$-base de cardinal n et p un nombre premier. Le quotient A/pA, isomorphe à $((\mathbb{Z}/p\mathbb{Z})^n, +)$, est donc naturellement un $\mathbb{F}_p$-espace vectoriel de dimension n. Cet argument s'étend aux modules libres de type fini sur un anneau commutatif en remplaçant le nombre premier p par un idéal maximal.

Le premier résultat concernant les sous-groupes de $\mathbb{Z}^n$ est le :

Théorème 2. *Soit n dans $\mathbb{N}^*$. Tout sous-groupe de $(\mathbb{Z}^n, +)$ est un g.a.l.t.f de rang $\leq n$.*

Preuve. Si $n = 1$, la division euclidienne montre classiquement que les sous-groupes de $(\mathbb{Z}, +)$ sont les $a\mathbb{Z}$ avec $a \in \mathbb{N}$, d'où le résultat.

Supposons $n \geq 2$ et le résultat acquis à l'ordre n. Soient A un sous-groupe de $(\mathbb{Z}^n, +)$ et $\Gamma = \mathbb{Z}^{n-1} \times \{0\}$. Si $A \subset \Gamma$, l'hypothèse de récurrence permet de conclure. Sinon, soit π le morphisme de $(\mathbb{Z}^n, +)$ dans $(\mathbb{Z}, +)$ qui à $x = (x_1, \ldots, x_n)$ associe x_n. L'image $\pi(A)$ est un sous-groupe non nul de $(\mathbb{Z}, +)$, ce qui fournit a dans A tel que $\pi(A) = \pi(a)\mathbb{Z}$. On vérifie aisément que $(\Gamma \cap A) \oplus \mathbb{Z}a = A$. On applique l'hypothèse de récurrence au sous-groupe $\Gamma \cap A$ de Γ, obtenant un entier m de $\{0, \ldots, n-1\}$ et une $\mathbb{Z}$-base $(a_1, \ldots a_m)$ de $\Gamma \cap A$. La famille $(a_1, \ldots, a_m, a)$ est alors une $\mathbb{Z}$-base de A.

Le théorème précédent ne s'étend pas aux groupes non abéliens. Soit L_2 le groupe libre à deux générateurs x et y. Pour $n \in \mathbb{N}^*$, soit $a_n = x^n y x^{-n}$. Il n'est pas difficile de prouver que $a_1, \ldots, a_n$ ne vérifient aucune relation non triviale ; le sous-groupe de L_2 engendré par tous les a_i est donc le groupe libre sur un alphabet dénombrable.

3 Equivalence de matrices entières et théorème de structure

Voici le résultat central de ce texte.

Théorème 3. *Soit $(G, +)$ un g.a.t.f. Il existe deux entiers naturels m et n, une suite $d_1, \ldots, d_m$ d'entiers ≥ 2 tels que :*
- $d_1 \mid d_2 \mid \cdots \mid d_m$,
- $(G, +)$ est isomorphe à : $(\mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z},\ +)$.
De plus, n, m, $d_1, \ldots, d_m$ sont entièrement déterminés par G.

Ce résultat contient évidemment le théorème de structure des g.a.f. La preuve de l'existence repose sur le « théorème de la base adaptée » ci-après.

Théorème 4. *Soient n dans $\mathbb{N}^*$ et A un sous-groupe de $(\mathbb{Z}^n, +)$. Il existe m dans $\{0, \ldots, n\}$, $d_1, \ldots, d_m$ dans $\mathbb{N}^*$ et une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$ tels que :*
- $d_1 \mid d_2 \mid \cdots \mid d_m$,
- $(d_1 e_1, \ldots, d_m e_m)$ est une $\mathbb{Z}$-base de A.

Preuve de l'existence dans le théorème de struture des g.a.t.f à partir du théorème de la base adaptée. Soit $(G, +)$ un g.a.t.f admettant une famille génératrice de cardinal $n \in \mathbb{N}^*$. On a vu au début du paragraphe **2** que G est (isomorphe à) un quotient de $\mathbb{Z}^n$ par un sous-groupe A. Soient $m, d_1, \ldots, d_m, e_1, \ldots, e_n$ comme dans le théorème de la base adaptée. Alors $\mathbb{Z}^n/A$ est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \times \mathbb{Z}^{n-m}$, ce qui établit le résultat désiré.

Reste à prouver le théorème de la base adaptée. Dans ce but, décrivons toutes les $\mathbb{Z}$-bases d'un g.a.l.t.f ; on sait déjà que toutes ont même cardinal.

Lemme 9. *Soient n dans $\mathbb{N}^*$, $e = (e_1, \ldots, e_n)$ une $\mathbb{Z}$-base d'un g.a.l.t.f A, $f_1, \ldots, f_n$ des éléments de A, P_e^f la matrice de présentation de $(f_1, \ldots, f_n)$ dans e. Il y a équivalence entre :*
i) $(f_1, \ldots, f_n)$ est une $\mathbb{Z}$-base de A,
ii) $P_e^f \in GL_n(\mathbb{Z})$.

Preuve. Si on a *i)*, la matrice P_e^f est dans $\mathcal{M}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$ et son inverse P_f^e appartient à $\mathcal{M}_n(\mathbb{Z})$ d'où *ii)*. Si on a *ii)*, $(f_1, \ldots, f_n)$ est $\mathbb{Z}$-libre, $\mathbb{Z}f_1 \oplus \cdots \oplus \mathbb{Z}f_n$ contient $e_1, \ldots, e_n$ donc est égal à A.

Ce lemme permet de déduire le théorème de la base adaptée d'un énoncé matriciel. Disons, si $(m, n) \in (\mathbb{N}^*)^2$, que deux matrices A et B de $\mathcal{M}_{n,m}(\mathbb{Z})$ sont équivalentes (sous-entendu : sur $\mathbb{Z}$) si et seulement s'il existe P dans $\mathrm{GL}_n(\mathbb{Z})$ et Q dans $\mathrm{GL}_m(\mathbb{Z})$ telles que $B = PAQ$.

Théorème 5. *Soit M dans $\mathcal{M}_{n,m}(\mathbb{Z})$. Il existe $r \in \{0, \ldots, \min(n, m)\}$ et $d_1, \ldots, d_r$ dans $\mathbb{N}^*$ tels que :*
- $d_1 \mid d_2 \mid \cdots \mid d_r$,
- M est équivalente à :

$$\left(\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & d_r & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{array}\right) \in \mathcal{M}_{n,m}(\mathbb{Z}).$$

Preuve du théorème de la base adaptée à partir du théorème d'équivalence. Soient n dans $\mathbb{N}^*$, A un sous-groupe de $(\mathbb{Z}^n, +)$, $e = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{Z}^n$, m le rang de A que l'on suppose ≥ 1, $\alpha = (\alpha_1, \ldots, \alpha_m)$ une $\mathbb{Z}$-base de A. Soient $f = (f_1, \ldots, f_n)$ une $\mathbb{Z}$-base de $\mathbb{Z}^n$, $\beta = (\beta_1, \ldots, \beta_m)$ une $\mathbb{Z}$-base de A. On a :

$$\mathrm{Mat}_e(\alpha) = \mathrm{Mat}_e(f)\ \mathrm{Mat}_f(\beta)\ \mathrm{Mat}_\beta(\alpha).$$

Les matrices $Mat_e(\alpha)$ et $Mat_f(\beta)$ sont de rang m. Il reste à choisir f et β pour que $\mathrm{Mat}_f(\beta)$ soit de la forme :

$$\left(\begin{array}{cccc} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \vdots & & \ddots & d_m \\ \vdots & & & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{array}\right) \in \mathcal{M}_{n,m}(\mathbb{Z}).$$

Nous donnerons une démonstration algorithmique du théorème 5. Le point de départ en est l'interprétation de certaines opérations élémentaires comme multiplication (à gauche ou à droite selon qu'on agit sur les lignes ou les colonnes) par des matrices de $\mathrm{GL}_n(\mathbb{Z})$ ou $\mathrm{GL}_m(\mathbb{Z})$. Tel est le cas de :
- $L_i \leftarrow -L_i$,
- $C_j \leftarrow -C_j$,
- $L_i \leftarrow L_i + \lambda L_j$ avec $\lambda \in \mathbb{Z}$ et $i \neq j$,

- $C_i \leftarrow C_i + \lambda C_j$ avec $\lambda \in \mathbb{Z}$ et $i \neq j$,
- $L_i \leftrightarrow L_j$,
- $C_i \leftrightarrow C_j$.

Preuve du théorème 5. Par récurrence, on se ramène à établir le :

Lemme 10. *Soient $(m,n) \in (\mathbb{N}^*)^2$ et M dans $\mathcal{M}_{n,m}(\mathbb{Z}) \setminus \{0\}$. Il existe d dans $\mathbb{N}^*$ et une matrice A de $\mathcal{M}_{n-1,m-1}(\mathbb{Z})$ à coefficients divisibles par d tels que M soit équivalente à :*

$$\left(\begin{array}{c|ccc} d & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A & \\ 0 & & & \end{array}\right).$$

Preuve du lemme. Il s'agit en fait d'un code.

Si $M = (\alpha_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$, posons :

$$\alpha(M) = \min\{\,|\alpha_{i,j}| \mid 1 \leq i \leq n,\ 1 \leq j \leq m,\ \alpha_{i,j} \neq 0\}\,.$$

On vérifie le lemme par récurrence sur $\alpha(M)$. Si $\alpha(M) = 1$, on échange, si besoin est, des lignes et des colonnes pour transformer M en une matrice dont le terme d'indice $(1,1)$ est ± 1 ; quitte à changer L_1 en $-L_1$, on peut supposer que ce terme est 1. Par des opérations de la forme : $L_i \leftarrow L_i + \lambda L_1$ avec $\lambda \in \mathbb{Z}$ et $2 \leq i \leq n$ ou $C_i \leftarrow C_i + \lambda C_1$ avec $\lambda \in \mathbb{Z}$ et $2 \leq j \leq n$, on obtient une matrice de la forme désirée avec $d = 1$.

Supposons $p \geq 2$, et le lemme acquis si $\alpha(M) \leq p-1$. Soit M dans $\mathcal{M}_{n,m}(\mathbb{Z})$ telle que $\alpha(M) = p$. Comme précédemment, on obtient une matrice M' équivalente à M dont le terme d'indice $(1,1)$ est p.

Supposons alors que l'un des termes de la première ligne ou de la première colonne de M' soit non divisible par p ; notons a ce terme, et effectuons la division euclidienne de a par p : $a = qp + r$ avec $q \in \mathbb{Z}$ et $0 < r < p$. Par une opération élémentaire de l'un des types : $L_i \leftarrow L_i - qL_1$ ou $C_j \leftarrow C_j - qC_1$, on obtient une matrice M'' équivalente à M telle que $0 < \alpha(M'') \leq r < p$, à laquelle on applique l'hypothèse de récurrence.

On peut donc supposer que tous les termes de la première ligne et de la première colonne de M' sont divisibles par p. Par des opérations élémentaires de la forme : $L_i \leftarrow L_i + \lambda L_1$ et $C_i \leftarrow C_i + \lambda C_1$, on obtient une matrice N de la forme :

$$\left(\begin{array}{c|ccc} p & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right).$$

Si tous les termes de B sont divisibles par p, on a gagné. Sinon, une opération élémentaire du type : $L_1 \leftarrow L_1 - L_i$ avec i bien choisi, permet de se retrouver dans le cas où l'un des termes de la première ligne n'est pas divisible par p, ce qui achève la démonstration.

Pour établir l'assertion d'unicité dans le théorème de structure, il suffit de voir que, si G est le groupe : $\mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$, que n, m et les d_i sont

déterminés par G. Mais n est le rang de G et, d'autre part, notant Tor G le sous-groupe des éléments d'ordre fini de G (« sous-groupe de torsion de G ») ; on a :

$$\text{Tor } G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}.$$

L'unicité dans le théorème de structure des g.a.f montre que m et les d_i sont déterminés par G.

Remarques

1. Dans le théorème 4 (resp. 5), m et $d_1, \ldots, d_m$ (resp. r et $d_1, \ldots, d_r$) sont déterminés par le sous-groupe A (resp. par la matrice M). Il suffit en effet d'appliquer la partie unicité du théorème de structure au groupe quotient $\mathbb{Z}^n/A$ (resp. $\mathbb{Z}^n/\text{Im}M$). Des preuves directes sont possibles : ainsi dans le théorème 5, on peut interpréter r comme le rang de M et $d_1 \ldots d_s$ comme le pgcd des déterminants d'ordre s extraits de M si $1 \leq s \leq r$.
2. Pour $n = 1$, le théorème d'équivalence montre que si $v =^t (v_1, \ldots, v_n)$ est un vecteur colonne de $\mathbb{Z}^n$, l'orbite $\{Pv\ , P \in \text{GL}_n(\mathbb{Z})\}$ contient un vecteur ${}^t(d, 0, \ldots, 0)$ avec d dans $\mathbb{N}$. La remarque précédente montre que d est le p.g.c.d des v_i. On a ainsi montré que les orbites de l'action naturelle de $\text{GL}_n(\mathbb{Z})$ dans $\mathbb{Z}^n$ sont les ensembles de vecteurs dont les coordonnées ont un p.g.c.d fixé. On en déduit en particulier le :

   Lemme 11. *Soit $v =^t (v_1, \ldots, v_n)$ dans $\mathbb{Z}^n$. Le sous-groupe $\mathbb{Z}v$ est facteur direct dans $\mathbb{Z}^n$ si et seulement si les v_i sont premiers entre eux dans leur ensemble.*

   Un vecteur v vérifiant la condition du lemme est dit *primitif*.

Terminons par quelques exercices.

Exercice 6. *Soient G_1, G_2, H trois g.a.t.f. On suppose que $G_1 \times H$ et $G_2 \times H$ sont isomorphes. Montrer que G_1 et G_2 sont isomorphes.*

Exercice 7. *a) Soit A un sous-groupe de $\mathbb{Z}^n$ de rang p. Montrer que A est facteur direct dans $\mathbb{Z}^n$ si et seulement s'il existe une forme p-linéaire alternée f sur $\mathbb{Z}^n$ et $(e_1, \ldots, e_p)$ dans A^p tels que : $f(e_1, \ldots, e_p) = 1$.*

b) Soient $x_1, \ldots, x_p$ des éléments de $\mathbb{Z}^n$. À quelle condition peut-on compléter $(x_1, \ldots, x_p)$ en une $\mathbb{Z}$-base de $\mathbb{Z}^n$?

Exercice 8. *Quels sont les g.a.t.f dont le groupe d'automorphismes est fini ?*

Exercice 9. *Montrer que si G est un g.a.l.t.f et m un élément de $\mathbb{N}^*$, l'ensemble des sous-groupes d'indice m de G est fini.*

Exercice 10. *a) Si A est dans $\mathcal{M}_n(\mathbb{Z})$, on note Γ_A le sous-groupe de $\mathbb{Z}^n$ engendré par les colonnes de A. Montrer que Γ_A est de rang n si et seulement si A est dans $GL_n(\mathbb{Q})$ et, dans ce cas exprimer l'indice de A dans $\mathbb{Z}^n$ (c'est-à-dire le cardinal du quotient $\mathbb{Z}^n/A$) à l'aide du déterminant de A.*

On note $\sim$ la relation d'équivalence définie sur $\mathcal{M}_n(\mathbb{Z}) \cap GL_n(\mathbb{Q})$ par : $A \sim B$ si et seulement s'il existe P dans $GL_n(\mathbb{Z})$ telle que $B = AP$.

b) Soient A et B dans $\mathcal{M}_n(\mathbb{Z}) \cap GL_n(\mathbb{Q})$. Montrer que $\Gamma_A = \Gamma_B$ équivaut à : $A \sim B$.

Exercice 11. *Une matrice $M = (m_{i,j})_{1 \leq i,j \leq n}$ de $\mathcal{M}_n(\mathbb{Z})$ est dite sous forme d'Hermite si et seulement si M est triangulaire supérieure à termes diagonaux strictement positifs et si, pour tout (i,j) tel que $1 \leq i < j \leq n$, on a : $0 \leq m_{i,j} < m_{i,i}$.*

a) Montrer que toute classe de la relation $\sim$ de l'exercice précédent contient exactement une matrice sous forme d'Hermite.

b) Si m est dans $\mathbb{N}^*$, montrer que le nombre de sous-groupes d'indice m de $\mathbb{Z}^n$ est égal au nombre de matrices de déterminant m de $\mathcal{M}_n(\mathbb{Z})$ sous forme d'Hermite.

Exercice 12. *Si $n \geq 2$, le groupe $SL_n(\mathbb{Z})$ est engendré par les matrices $T_{i,j}(1)$ pour i et j distincts dans $\{1, \ldots, n\}$.*