4. Complément I : le groupe $\mathrm{SL}_n(A)$ et transvections

Quand l'anneau A est supposé euclidien, la démonstration du Théorème 2.4 peut-être rendue entièrement algorithmique, car c'est le cas des relations de Bézout :

THÉORÈME 4.1. *Si A est un euclidien, alors $\mathrm{SL}_n(A)$ est engendré par les transvections standards.*

Un corps étant trivialement euclidien, cet énoncé généralise la Proposition 3.5 Chap. 5. Dans le cas $A = \mathbb{Z}$, on a $\mathrm{T}_{i,j}(m) = \mathrm{T}_{i,j}(1)^m$ pour tout $m \in \mathbb{Z}$, de sorte que $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les $\mathrm{T}_{i,j}(1)$ avec $1 \leqslant i \neq j \leqslant n$, qui sont en nombre fini.

COROLLAIRE 4.2. *Le groupe $\mathrm{SL}_n(\mathbb{Z})$ est de type fini.*

Le groupe infini $\mathrm{SL}_n(\mathbb{Z})$ est très intéressant, et intervient dans de nombreux aspects de la géométrie et de la théorie des nombres. Le cas $n = 2$ est tout particulièrement important. On pose

$$\mathrm{T} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \mathrm{L} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{et} \quad \mathrm{S} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Ce sont des éléments de $\mathrm{SL}_2(A)$ pour tout anneau A.

COROLLAIRE 4.3. *$\mathrm{SL}_2(\mathbb{Z})$ est engendré par T et L, ou encore par S et T.*

En effet, la première assertion se déduit du Théorème 4.1 et de la discussion ci-dessus. Pour la seconde, un petit calcul montre que l'on a $\mathrm{T}\,\mathrm{S} = \mathrm{L}\,\mathrm{T}^{-1}$.

DÉMONSTRATION — (Démonstration du Théorème 4.1) C'est une variante de la démonstration du Théorème 2.4 dans laquelle on part d'une matrice $M \in \mathrm{SL}_n(A)$ (avec $n = p = q$, donc). On ne s'autorise qu'à multiplier à gauche et à droite par des produits finis de transvections standards (équivalences *élémentaires*), et on veut aboutir à l'identité. On remplace dans la récurrence la fonction ν par un stathme euclidien φ sur A donné par hypothèse. Pour échanger deux lignes ou deux colonnes, on remplace τ par la matrice $\pm S$ ci-dessus (ce qui force à changer le signe d'une des deux lignes ou colonnes, celle que l'on veut, mais c'est sans indicence), qui est un produit de transvections par la formule $\mathrm{S} = \mathrm{T}^{-1}\,\mathrm{L}\,\mathrm{T}^{-1}$. Dans le Cas 1, on écrit plutôt $m_{1,j} = qm_{1,1} + r$ avec $\varphi(r) < \varphi(m_{1,1})$, et on remplace Q par la transvection $\mathrm{T}_{j,1}(-q)$. Idem dans le Cas 2. Après le Cas 2, on a $m_{i,1} = m_{1,j} = 0$ pour $i, j \neq 1$, et donc $m_{1,1} \in A^\times$ car alors $m_{1,1}$ divise $\det M = 1$. À ce stade il est plus simple de rajouter à la deuxième colonne $m_{1,1}^{-1}$ fois la première, de sorte que M contient le coefficient 1, puis de placer ce 1 en position $(1, 1)$, et de recommencer l'argument en supposant $m_{1,1} = 1$. □

REMARQUE 4.4. (i) Une autre démonstration du Corollaire 4.3, plus géométrique, consiste à faire agir $\mathrm{SL}_2(\mathbb{Z})$ par homographie sur $\widehat{\mathbb{C}} \smallsetminus \widehat{\mathbb{R}} = \mathbb{C} \smallsetminus \mathbb{R}$. Cette action préserve le demi-plan supérieur $\{\tau \in \mathbb{C} \mid \Im\,\tau > 0\}$, aussi appelé *demi-plan de Poincaré*. C'est l'un des points de départs de la théorie des *formes modulaires*, pour laquelle nous renvoyons au Ch. VII du cours d'arithmétique de Serre [**SER70**] ou encore aux notes de votre serviteur [**CHE15**].

(ii) P. Cohn et K. Dennis ont montré que pour $d < 0$, $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ est engendré par les transvections si, et seulement si, $d = -1, -2, -3$. Noter que $\mathbb{Z}[\sqrt{-3}]$ n'est pas principal comme on l'a vu. Ils ont aussi montré que pour $d < 0$ et $d \equiv 1 \bmod 4$, alors $\mathrm{SL}_2(\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ est engendré par les transvections si, et seulement si, $d = -3, -7, -11$. En particulier, ce n'est pas le cas de $d = -19$, pour lesquels $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est pourtant principal. En revanche, dans tous ces cas, $\mathrm{SL}_n(A)$ est engendré par les transvections pour $n \geqslant 3$.

(ii) Nous renvoyons à l'Exercice 8.15 pour un autre exemple particulièrement intéressant d'anneau A dans lequel $\mathrm{SL}_2(A)$ n'est pas engendré par les transvections (*exemple de Bass-Milnor-Serre*).

Discutons un peu plus certains aspects de la structure du groupe infini $\mathrm{SL}_n(\mathbb{Z})$. On rappelle que pour tout morphisme d'anneaux $f : A \to B$, on a un morphisme de groupes $\mathrm{GL}_n(A) \to \mathrm{GL}_n(B), (m_{i,j}) \mapsto (f(m_{i,j}))$, induisant un morphisme $\mathrm{SL}_n(A) \to \mathrm{SL}_n(B)$ si en outre A et B sont commutatifs. Appliquant cette observation au morphisme canonique $f : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ de réduction modulo N, on en déduit un morphisme naturel $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$.

Corollaire 4.5. *Pour tout entier $n, N \geqslant 1$, le morphisme de groupes $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, induit par la réduction modulo N des coefficients, est surjectif.*

Démonstration — En effet, l'anneau $\mathbb{Z}/N\mathbb{Z}$ est euclidien par la Remarque 6.2, donc le groupe $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ est engendré par les $\mathrm{T}_{i,j}(\overline{m})$ avec $m \in \mathbb{Z}$, par le Théorème 4.1. Mais cette transvection est l'image de $\mathrm{T}_{i,j}(m) \in \mathrm{SL}_n(\mathbb{Z})$ par le morphisme de l'énoncé, qui est donc surjectif. □

Le noyau du morphisme ci-dessus est le sous-groupe $\Gamma_n(N)$ des matrices $M \in \mathrm{SL}_n(\mathbb{Z})$ avec $M \equiv 1_n \bmod N$. On l'appelle *sous-groupe de congruence principal de niveau N*. C'est un sous-groupe distingué et d'indice fini de $\mathrm{SL}_n(\mathbb{Z})$. D'après le corollaire on a même un isomorphisme

$$\mathrm{SL}_n(\mathbb{Z})/\Gamma_n(N) \simeq \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}). \tag{68}$$

Définition 4.6. *Un sous-groupe d'indice fini $\Gamma \subset \mathrm{SL}_n(\mathbb{Z})$ est dit de congruence s'il existe un entier $N \geqslant 1$ avec $\Gamma_n(N) \subset \Gamma$.*

Étant donné que l'on a $\cap_{N\geqslant 1} N\mathbb{Z} = \{0\}$, on a aussi $\cap_{N\geqslant 1}\Gamma_n(N) = \{1\}$. On dit que le groupe $\mathrm{SL}_n(\mathbb{Z})$ est *résiduellement fini*. Du coup, on peut se demander si tout sous-groupe d'indice fini de $\mathrm{SL}_n(\mathbb{Z})$ est de congruence. Un fait remarquable, démontré par Bass, Milnor et Serre[6], et indépendamment par Mennicke (1968), est que c'est le cas pour tout $n \geqslant 3$. On se propose dans ce qui suit de démontrer que cette propriété est fausse pour $\mathrm{SL}_2(\mathbb{Z})$, un énoncé plus ancien connu de Klein, Fricke et Pick, et dont la démonstration illustrera bien certaines notions du cours.

Théorème 4.7. (Klein, Fricke, Pick) *Il existe des sous-groupes d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ qui ne sont pas de congruence.*

6. H. Bass, J. Milnor & J.-P. Serre, *A solution of the congruence subgroup problem for SL_n ($n \geqslant 3$) and Sp_{2n} ($n \geqslant 2$)*, Publications Mathématiques de l'IHÉS 33 (1967).

Pour $N \geqslant 1$, on pose $\Gamma(N) = \Gamma_2(N)$. Pour démontrer le théorème, on commence par examiner la structure du sous-groupe $\Gamma(2)$. Il contient dans son centre la matrice -1_2, et il contient aussi les deux matrices

$$A = \mathrm{T}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ et } B = \mathrm{L}^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

LEMME 4.8. *On a* $\Gamma(2) = \langle -1_2, A, B \rangle$.

DÉMONSTRATION — Soit $H = \langle A, B \rangle$ le sous-groupe de $\Gamma(2)$ engendré par A et B. Pour $g \in \Gamma(2)$ on pose $\mathrm{m}(g) = \mathrm{Min}\{|g_{1,1}|, |g_{1,2}|, |g_{2,1}|, |g_{2,2}|\}$. Observons que si on a $\mathrm{m}(g) = 0$ alors on a $g_{1,2} = 0$ ou $g_{2,1} = 0$ car $g_{1,1}$ et $g_{2,2}$ sont impairs, et donc $g_{1,1} = g_{2,2} = \pm 1$ et $\pm g \in \langle A \rangle \cup \langle B \rangle \subset H$. Sinon, il suffit par récurrence de montrer qu'il existe $h \in H$ avec $\mathrm{m}(gh) < \mathrm{m}(g)$ ou $\mathrm{m}(hg) < \mathrm{m}(g)$.

Quitte à remplacer g par sa transposée (la transposition préserve H et m) on peut supposer que l'on a $\mathrm{m}(g) = |g_{1,1}|$ ou $|g_{1,2}|$. Dans le cas $\mathrm{m}(g) = |g_{1,1}| > 0$, on constate que pour m bien choisi, le coefficient $(gA^{-m})_{1,2} = g_{1,2} - 2mg_{1,1}$ est $\leqslant |g_{1,1}|$, et donc $< |g_{1,1}|$ pour des raisons de parité. De même, dans le cas $\mathrm{m}(g) = |g_{1,2}| > 0$, pour m bien choisi, le coefficient $(gB^{-m})_{1,1} = g_{1,1} - 2mg_{1,2}$ est $\leqslant |g_{1,2}|$, et donc $< |g_{1,2}|$ pour des raisons de parité. □

PROPOSITION 4.9. *Le sous-groupe* $\langle A, B \rangle$ *de* $\mathrm{SL}_2(\mathbb{Z})$ *est libre de rang* 2 *sur* $\{A, B\}$.

DÉMONSTRATION — Soit F_2 le groupe libre sur l'ensemble à deux éléments $\{a, b\}$ (voir le Complément § 8 Chap. 2). Soit $f : \mathrm{F}_2 \to \mathrm{SL}_2(\mathbb{Z})$ le morphisme de groupes envoyant a sur A et b sur B. Par définition, l'image de f est $\langle A, B \rangle$, et on veut montrer son injectivité.

On considère pour cela l'action par homographies de $\mathrm{SL}_2(\mathbb{Z})$ sur $\widehat{\mathbb{R}} = \mathbb{R} \coprod \{\infty\}$. On pose $X = \{t \in \mathbb{R},\ |t| < 1\}$ et $Y = \{t \in \mathbb{R},\ |t| > 1\}$. On a $X \coprod Y \subset \widehat{\mathbb{R}}$ et

$$A^m X \subset Y \text{ et } B^m Y \subset X \text{ pour tout } m \in \mathbb{Z} \text{ non nul.} \tag{69}$$

En effet, pour $|t| < 1$ on a $|t+2m| > 1$, et donc pour $|t| > 1$ on a aussi $|t/(2mt+1)| < 1$. Soit $w \in \mathrm{F}_2$ un mot réduit en a et b non trivial. Pour montrer $f(w) \neq 1$, on peut d'abord conjuguer w par une puissance convenable de b, puis de a, de sorte que l'on peut supposer que w est de la forme

$$w = a^{m_1} b^{m_2} a^{m_3} \cdots b^{m_{k-1}} a^{m_k}$$

avec $k \geqslant 3$ et les m_i, pour $i = 1, \ldots, k$, *tous non nuls*. Mais alors par (69) on constate que l'on a $f(w)(X) \subset Y$. Cela montre $f(w) \neq 1_2$ (cette méthode s'appelle *l'argument du ping pong* de J. Tits). □

COROLLAIRE 4.10. *On a* $\Gamma(2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{F}_2$.

DÉMONSTRATION — L'élément -1_2 est dans le centre de $\Gamma(2)$. Le Lemme 4.8 montre $\Gamma(2) = \{\pm 1_2\}H$ avec $H = \langle A, B \rangle$. Pour voir que c'est un produit direct interne de $\{\pm 1_2\}$ et H, il suffit de justifier $-1_2 \notin H$. Pour cela, il suffit d'observer que tout élément de H a ses coefficient diagonaux $\equiv 1 \bmod 4$, ce qui n'est pas le cas de -1_2. On conclut par la Proposition 4.9. □

COROLLAIRE 4.11. *Pour tout entier $n \geqslant 1$, il existe un morphisme de groupes surjectif $\Gamma(2) \to \mathrm{A}_n$.*

DÉMONSTRATION — Le groupe A_n est engendré par deux éléments. Par exemple, pour n impair, le 3-cycle $(1\,2\,3)$ et le n-cycle standard $(1\,2\,\cdots\,n)$ conviennent, car le groupe engendré contient tous les $(i\ i+1\ i+2)$ avec $1 \leqslant i \leqslant n-2$ et ces derniers engendrent A_n (voir l'Exercice 4.6). Pour n pair, le 3-cycle $(1\,2\,3)$ et le $n-1$-cycle $(2\,3\,\cdots\,n)$ conviennent, car les $(1\ i\ i{+}1)$ engendrent aussi A_n à cause par exemple de l'identité $(1\ i\ i+1)(1\ i+1\ i+2) = (i\ i+1\ i+2)$. Ainsi, par la propriété universelle du groupe libre, il existe un morphisme surjectif $\mathrm{F}_2 \to \mathrm{A}_n$, et on conclut en le composant avec le morphisme $\Gamma(2) \to \mathrm{F}_2$ donné par le Corollaire 4.10. □

Pour démontrer le Théorème 4.7, il suffit donc de démontrer la :

PROPOSITION 4.12. *Pour $n \geqslant 6$, le noyau d'un morphisme surjectif $\Gamma(2) \to \mathrm{A}_n$ n'est pas de congruence.*

DÉMONSTRATION — Soit $f : \Gamma(2) \to \mathrm{A}_n$ un morphisme surjectif et notons H son noyau. Supposons H de congruence, disons $H \supset \Gamma(N)$ pour un certain $N \geqslant 1$. L'inclusion $T^N \subset \Gamma(N) \subset H \subsetneq \Gamma(2)$ montre $N \equiv 0 \bmod 2$ et $N > 2$. Comme $\Gamma(N)$ est distingué dans $\Gamma(2)$, et que A_n est simple pour $n \geqslant 6$, le groupe $\Gamma(2)/\Gamma(N)$ a donc un facteur de Jordan-Hölder [7] isomorphe à A_n, ainsi donc que $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, car $\Gamma(2)$ est distingué dans $\mathrm{SL}_2(\mathbb{Z})$.

Or on connaît les facteurs de Jordan-Hölder de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ d'après le Lemme 4.13 suivant : oubliant les multiplicités, ce sont ceux des groupes $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ avec $p|N$, ainsi que $\mathbb{Z}/p\mathbb{Z}$ si p^2 divise N. D'après le Théorème 3.1 Chap. 5, les facteurs de Jordan-Hölder de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ sont $\mathbb{Z}/2\mathbb{Z}$ et le groupe simple $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ pour $p \geqslant 5$, et par les isomorphismes miraculeux, ce sont $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ pour $p = 2, 3$. Aucun d'entre eux n'est isomorphe à A_n pour $n \geqslant 6$ d'après la Proposition 4.8 Chap. 5. [8] □

Dans la démonstration ci-dessus, on a utilisé le dévissage suivant du groupe fini $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, dans lequel $n \geqslant 1$ est un entier arbitraire.

LEMME 4.13. *(i) Pour $M, N \geqslant 1$ premiers entre eux on a un isomorphisme*

$$\mathrm{SL}_n(\mathbb{Z}/MN\mathbb{Z}) \xrightarrow{\sim} \mathrm{SL}_n(\mathbb{Z}/M\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}).$$

(ii) Pour tout p premier et $m \geqslant 1$, on a une suite exacte courte

$$1 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{n^2-1} \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^{m+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z}) \longrightarrow 1.$$

DÉMONSTRATION — Pour le (i), on utilise l'isomorphisme chinois et le fait immédiat suivant. Si $f : A \times B \to C$ est un isomorphisme entre anneaux commutatifs, alors $((a_{i,j}), (b_{i,j})) \mapsto (f(a_{i,j}, b_{i,j})_{i,j})$ est un isomorphisme de groupes $\mathrm{SL}_n(A) \times \mathrm{SL}_n(B) \to \mathrm{SL}_n(C)$.

Pour le (ii), le morphisme d'anneaux $\mathbb{Z}/p^{m+1}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ de réduction modulo p^m induit un morphisme de groupes $f : \mathrm{SL}_n(\mathbb{Z}/p^{m+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$. Ce morphisme

7. Nous renvoyons au Complément §8 Chap. 2 pour la notion de facteur de Jordan-Hölder.

8. Notons que l'on a utilisé sans le dire le théorème de Jordan-Hölder (Théorème 8.3 Chap. 2), on aurait pu s'en passer mais c'est tout de même agréable et intuitif ici de l'utiliser.

est surjectif car son image contient les transvections standards de $\mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$, et ces dernières sont génératrices comme on l'a vu dans la démonstration du Corollaire 4.5. Il ne reste qu'à étudier son noyau $\ker f$.

Soit $M \in \mathrm{M}_n(\mathbb{Z}/p^{m+1}\mathbb{Z})$ dont la réduction modulo p^m est l'identité. On peut écrire $M \equiv 1_n + p^m X$ pour un certain $X \in \mathrm{M}_n(\mathbb{Z})$ dont la réduction modulo p est uniquement déterminée par M : on la note $r(M)$. En utilisant la congruence $p^{2m} \equiv 0 \bmod p^{m+1}$ dans $\mathbb{Z}$, on constate par multilinéarité alternée du déterminant

$$\det M \equiv \det(1_n + p^m X) \equiv 1 + p^m \mathrm{tr}\, X \bmod p^{m+1}.$$

On en déduit que l'on a $M \in \ker f \iff \mathrm{tr}\, r(M) = 0$. Ainsi, $r : M \mapsto r(M)$ définit une bijection entre $\ker f$ et le sous-groupe $V \subset \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ des matrices de trace nulel. Ce dernier est un sous $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de codimension 1, donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{n^2-1}$, et il ne reste qu'à vérifier que r est un morphisme de groupes $\ker f \to V$. Mais si on a $M = 1_n + p^m X$ et $N = 1_n + p^m Y$ avec $X, Y \in \mathrm{M}_n(\mathbb{Z})$, on a

$$MN = (1_n + p^m X)(1_n + p^m Y) \equiv 1_n + p^m(X + Y) \bmod p^{m+1}\mathrm{M}_n(\mathbb{Z})$$

toujours car $p^{2m} \equiv 0 \bmod p^{m+1}$, ce qui signifie exactement $r(MN) = r(M) + r(N)$. □

5. Complément II : deux démonstrations de l'assertion d'unicité

Dans ce complément nous détaillons deux démonstrations de l'assertion d'unicité du Théorème 3.3.

5.1. Méthode 1 : une variante du cas $A = \mathbb{Z}$. On explique d'abord comment montrer cette unicité en utilisant une variante de l'argument donné dans le cas $A = \mathbb{Z}$ au Chapitre 3.

Pour tout anneau intègre A, et tout A-module M, posons

$$M_{\mathrm{tor}} = \{m \in M \mid \exists a \in A \smallsetminus \{0\},\ am = 0\}.$$

C'est alors un sous-module de M appelé *sous-module de torsion* (et ses éléments sont les *éléments de torsion* de M). Tout isomorphisme A-linéaire $M \simeq N$ induit un isomorphisme A-linéaire $M_{\mathrm{tor}} \simeq N_{\mathrm{tor}}$. Si M est comme dans l'énoncé, la torsion du module de droite est $\{0\} \oplus A/a_1A \oplus A/a_2A \oplus \cdots \oplus A/a_nA$ et en particulier on a $M/M_{\mathrm{tor}} \simeq A^r$. Le Théorème 1.18 conclut alors l'unicité du r, et on peut donc supposer $r = 0$ et $M = M_{\mathrm{tor}}$.

On procède alors de manière similaire à l'argument d'unicité dans le théorème de structure des groupes abéliens finis (Théorème 3.1 Chap. 3, voir la fin de la Section 3). Pour une suite $a = (a_1 \mid a_2 \mid \cdots \mid a_n)$ d'éléments non nuls de A on pose

$$M_a := A/a_1A \oplus A/a_2A \oplus \cdots \oplus A/a_nA.$$

On suppose $M_a \simeq M_b$ avec $b = (b_1 \mid b_2 \mid \cdots \mid b_m)$ et on veut montrer $n = m$ et $a_i \sim b_i$ pour tout $i = 1, \ldots, n$. On raisonne par récurrence sur l'entier r somme de $n + m$ et du nombre miminal de diviseurs irréductibles de a_nb_m (comptés avec multiplicités). Le cas minimal $r = 2$ est trivial. De plus, si a_1 et b_1 sont des unités, on peut supprimer a_1 et b_1 et donc diminuer $n + m$ de 2 et conclure par récurrence.

Disons que a_1 est non inversible, et choisissons un facteur irréductible π de a_1, qui divise alors tous les a_i. Pour M un A-module quelconque, on pose

$$M[\pi] = \{x \in M \mid \pi x = 0\}.$$

C'est un $A/\pi A$-module de manière naturelle, via $(a + \pi A, x) \mapsto ax$, donc un espace vectoriel sur le corps $k = A/\pi A$ (Corollaire 9.16). On a un isomorphisme de $A/\pi A$-espaces vectoriels $M_a[\pi] \simeq M_b[\pi]$ car on a $M_a \simeq M_b$. Mais on constate que pour $f \in A$, on a $(A/fA)[\pi] = \{0\}$ si π est premier avec f (par Bézout), et $A/fA[\pi] = gA/fA \simeq A/\pi A$ (de dimension 1 sur k) si $f = \pi g$. On a donc

$$n = \dim_k M_a[\pi] = \dim_k M_b[\pi]$$

et n éléments b_i sont divisibles par π. Cela montre d'abord $n \leqslant m$, puis $m \leqslant n$ par symétrie, et donc $n = m$ et π divise tous les b_i. Posons maintenant

$$\pi M = \{\pi x \mid x \in M\},$$

encore un sous-A-module de M. Pour $f = \pi g \in A$ avec $g \in A$, on constate que le A-module $\pi A/fA$ est isomorphe à A/gA. Ainsi, on a $\pi M_a \simeq M_{a'}$ avec $a'_i = a_i/\pi$, $\pi M_b \simeq M_{b'}$ avec $b'_i = b_i/\pi$ et $M_{a'} \simeq M_{b'}$ car $M_a \simeq M_b$. On conclut donc par récurrence, car $b'_n b_n$ a deux diviseurs irréductibles de moins que $a_n b_m$.

5.2. Méthode 2 : une preuve par les idéaux de Fitting. Cette autre démonstration, à la fois plus générale et plus dans l'esprit des arguments de la Section 2, est basée sur la construction des *idéaux de Fitting*[9] d'un module de type fini. Soient A un anneau commutatif noethérien,[10] et M un A-module de type fini. Fixons $\underline{g} = (g_1, \dots, g_p)$ une famille génératrice de M, avec $p = |\underline{g}|$, et notons

$$\pi_{\underline{g}} : A^p \longrightarrow M, \quad (a_1, \dots, a_p) \mapsto \sum_{i=1}^{p} a_i g_i,$$

la surjection A-linéaire associée. Le noyau de $\pi_{\underline{g}}$ est un sous-A-module de A^p appelé *module des relations entre les éléments de* $\underline{g}$. Il est de type fini car A est noethérien. Soit $\underline{r} = (r_1, \dots, r_q)$ une famille génératrice du A-module $\ker \pi_{\underline{g}}$. On a une application linéaire $u_{\underline{g},\underline{r}} : A^q \longrightarrow A^p$, $(x_i) \mapsto \sum_{i=1}^{q} x_i r_i$, d'image $\ker \pi_{\underline{g}}$. Si on écrit $r_j = (a_{1,j}, a_{2,j}, \dots, a_{p,j})$, la matrice de $u_{\underline{g},\underline{r}}$ dans les bases canoniques respectives est

$$M_{\underline{g},\underline{r}} := \mathrm{Mat}_{\mathrm{can},\mathrm{can}}\, u_{\underline{g},\underline{r}} = (a_{i,j}) \in \mathrm{M}_{p,q}(A).$$

On rappelle que l'on a défini $\mathrm{c}_k(N)$ pour tout $N \in \mathrm{M}_{p,q}(A)$ et $k \in \mathbb{Z}$.

LEMME 5.1. *Dans les notations ci-dessus, et pour tout $i \in \mathbb{Z}$, l'idéal $\mathrm{c}_{p-i}(M_{\underline{g},\underline{r}})$ de A ne dépend que de la classe d'isomorphisme du A-module de type fini M.*

La présence du $-i$ (plutôt que $+i$) est faite pour coller avec la convention usuelle d'indexation des idéaux de Fitting dans la Définition 5.2 ci-dessous. Bien noter en revanche que p désigne ci-dessus le cardinal de $\underline{g}$.

DÉMONSTRATION — Supposons d'abord $\underline{g}$ fixée, et que $\underline{r'}$ est réunion de $\underline{r}$ et d'une autre relation. La matrice $M_{\underline{g},\underline{r'}}$ est dans $\mathrm{M}_{p,q+1}(A)$ et est obtenue à partir de $M_{\underline{g},\underline{r}}$ en ajoutant une colonne qui est combinaison A-linéaire des autres. On a donc clairement

9. H. Fitting, *Die Determinantenideale eines Moduls*, Jahresbericht der Deutschen Mathematiker-Vereinigung, p. 195–228 (1936).

10. L'hypothèse noethérienne est en fait inutile, mais nous la faisons pour simplifier l'argument.

$\mathrm{c}_k(M_{\underline{g},\underline{r}'}) = \mathrm{c}_k(M_{\underline{g},\underline{r}})$ pour tout $k \in \mathbb{Z}$. On en déduit que cette égalité vaut plus généralement pour tout $\underline{r}$ et $\underline{r}'$, en ajoutant un à un les éléments de $\underline{r}'$ à $\underline{r}$, puis en supprimant un à un ceux de $\underline{r}$.

Supposons maintenant que la famille génératrice $\underline{g}'$ est obtenue à partir de $\underline{g}$ en rajoutant un seul élément, disons l'élément $g_{p+1} \in M$. Écrivons $g_{p+1} = \sum_{i=1}^{p} a_i g_i$. On constate que le noyau de $\pi_{\underline{g}'}$ est le sous-module de A^{q+1} engendré par la famille $\underline{r}'$ constituée des $r_i \times 0$ avec $r_i \in \underline{r}$ et par l'élément $x = (-a_1, -a_2, \ldots, -a_p, 1)$. En effet, si $v = (b_1, \ldots, b_q)$ est dans $\ker \pi_{\underline{g}'}$ alors $v - b_q x$ est dans $(\ker \pi_{\underline{g}'}) \cap (A^q \times \{0\}) = (\ker \pi_{\underline{g}}) \times \{0\}$. On a donc l'égalité matricielle

$$M_{\underline{g}',\underline{r}'} = \begin{bmatrix} M_{\underline{g},\underline{r}'} & X \\ 0_{1\times q} & 1 \end{bmatrix} \in \mathrm{M}_{p+1,q+1}(A), \text{ avec } X = \begin{bmatrix} -a_1 & \vdots & -a_p \end{bmatrix} \in A^p.$$

On a alors $\mathrm{c}_{k+1}(M_{\underline{g}',\underline{r}'}) = \mathrm{c}_k(M_{\underline{g},\underline{r}})$. En effet, tout mineur de taille $1 \leqslant k \leqslant \min(p,q)$ de $M_{\underline{g},\underline{r}}$ est un mineur de taille $k+1$ de $M_{\underline{g}',\underline{r}'}$ (ajouter la dernière ligne et la dernière colonne). De même, tout mineur de taille $k+1$ de $M_{\underline{g}',\underline{r}'}$ est soit nul, soit un mineur de taille k ou $k+1$ de $M_{\underline{g},\underline{r}}$, et donc dans $\mathrm{c}_k(M_{\underline{g},\underline{r}})$ dans tous les cas, ce qui conclut. Au final, on en déduit que l'idéal $\mathrm{c}_{|\underline{g}|+k}(M_{\underline{g},\underline{r}})$, dont on sait déjà qu'il ne dépend pas de $\underline{r}$, ne dépend pas non plus du choix de $\underline{g}$: pour deux familles génératrices $\underline{g}$ et $\underline{g}'$ on passe de $\underline{g}$ à $\underline{g} \cup \underline{g}'$ en ajoutant un par un les éléments de $\underline{g}'$, puis à $\underline{g}'$ en enlevant un par un les éléments de $\underline{g}$.

On a montré que M étant donné, l'idéal de l'énoncé ne dépend pas des choix de $\underline{g}$ et $\underline{r}$. Enfin, si $f : M' \xrightarrow{\sim} M$ est un isomorphisme de A-modules, et si on pose $\underline{g}' = f^{-1}(\underline{g})$, on a clairement $M_{\underline{g},\underline{r}} = M'_{\underline{g}',\underline{r}}$, d'où la dernière assertion. □

Définition 5.2. *Pour tout $i \in \mathbb{Z}$ l'idéal du Lemme 5.1 est appelé i-ème idéal de Fitting du A-module de type fini M, et noté* $\mathrm{Fitt}_i(M)$. *Il ne dépend que de la classe d'isomorphisme de M.*

Pour conclure l'unicité, il ne reste qu'à déterminer les $\mathrm{Fitt}_k(M)$ avec $M = A^r \oplus A/a_1A \oplus \cdots \oplus A/a_nA$ et $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$ et les $a_i \in A$ non nuls. En utilisant les générateurs et relations évidents définissant M on a pour tout $k \in \mathbb{Z}$

$$\mathrm{Fitt}_k(M) = \mathrm{c}_{n+r-k}(D) \text{ avec } D = \begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_n & \end{bmatrix}.$$

On a déjà vu $\mathrm{c}_i(D) = a_1 \cdots a_i A$ pour $1 \leqslant i \leqslant n$ en fin de Section 2, et on a $\mathrm{c}_i(D) = 0$ pour $i > n$. Autrement dit, on a $\mathrm{Fitt}_k(M) = \{0\}$ pour $k < r$, et pour $r \leqslant k < r+n$ on a $\mathrm{Fitt}_r(M) = a_1 a_2 \cdots a_{n+r-k} A$ (non nul). Cela montre l'unicité du r et des a_i modulo association. ▫

Remarque 5.3. Par définition on a $\mathrm{Fitt}_i(M) = \{0\}$ pour $i < 0$ et $\mathrm{Fitt}_i(M) \subset \mathrm{Fitt}_{i+1}(M)$ pour tout $i \in \mathbb{Z}$ (un mineur de taille $k+1$ est toujours combinaison A-linéaire de mineurs de taille k, en développant une colonne). D'une certaine manière, $\mathrm{Fitt}_i(M)$ mesure l'aptitude de M à être engendré par i éléments.