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

---

1 Description des sous-groupes de $\mathbb{Z}^n$

Soit G un groupe abélien, dont la loi est notée additivement, isomorphe à $\mathbb{Z}^n$. Si $\phi : \mathbb{Z}^n \to G$ est un isomorphisme, alors, en posant $e_i = \phi(0, \dots, 0, 1, 0, \dots, 0)$ (où le 1 est à la $i^{\text{ième}}$ place), ϕ est de la forme :

$$\begin{array}{rccc} \phi : & \mathbb{Z}^n & \to & G \\ & (x_1, x_2, \dots, x_n) & \mapsto & x_1e_1 + x_2e_2 + \dots + x_ne_n \end{array}$$

Une famille telle famille $(e_1, e_2, \dots, e_n)$ est appelée base G.
Deux bases éventuelles ont même longueur : si $(e_1, e_2, \dots, e_n)$ et $(f_1, f_2, \dots, f_m)$ sont deux bases de G, alors il existe $A = (a_{i,j})_{i,j} \in \mathrm{M}_{n,m}(\mathbb{Z})$ et $B = (b_{i,j})_{i,j} \in \mathrm{M}_{m,n}(\mathbb{Z})$ telles que :

$$\forall j \in [\![1, m]\!],\ f_j = \sum_{i=1}^{n} a_{i,j} e_i \quad \text{et} \quad \forall i \in [\![1, n]\!],\ e_i = \sum_{k=1}^{m} b_{k,i} f_k$$

Il vient, pour tout $j \in [\![1, m]\!]$, $f_j = \displaystyle\sum_{i=1}^{n} a_{i,j} \sum_{k=1}^{m} b_{k,i} f_k = \sum_{k=1}^{m} \left(\sum_{i=1}^{n} b_{k,i} a_{i,j} \right) f_k$, d'où $BA = I_m$. De la même façon, $AB = I_n$ et l'on a $m = \mathrm{Tr}(BA) = \mathrm{Tr}(AB) = n$.

Si un groupe abélien G admet une base de longueur n, c'est-à-dire est isomorphe à $\mathbb{Z}^n$, l'entier n est donc déterminé de manière unique. On dit que G est un *groupe abélien libre de rang n*.

Proposition 1 *Si H est un sous-groupe de $\mathbb{Z}^n$, alors H est un groupe abélien libre de rang $r \leqslant n$.*

Preuve : par récurrence sur n.
$n = 1$: Un sous-groupe de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$, donc isomorphe à $\{0\}$ ou $\mathbb{Z}$. Il est donc libre de rang $r = 0$ ou 1.
Supposons $n > 1$ et le résultat vrai au rang $n - 1$. Soit H un sous-groupe de $\mathbb{Z}^n$. Notons $p : \mathbb{Z}^n \to \mathbb{Z}$ l'application définie par $p(x_1, x_2, \dots, x_n) = x_1$. L'ensemble $p(H)$ est un sous-groupe de $\mathbb{Z}$. Si $p(H) = \{0\}$ alors $H \subset \{0\} \times Z^{n-1}$ et l'hypothèse de récurrence permet de conclure. Sinon, $p(H)$ est de la forme $a\mathbb{Z}$, où $a \in \mathbb{N}^*$. Soit $f_1 \in H$ tel que $p(f_1) = a$. On a, pour tout $x \in H$, l'existence de $k \in \mathbb{Z}$ tel que $p(x) = k.a = k.p(f_1)$ d'où $p(x - k.f_1) = 0$ et $x - k.f_1 \in (\{0\} \times \mathbb{Z}^{n-1}) \cap H$. Ceci montre $H = \mathbb{Z}f_1 \oplus \big((\{0\} \times \mathbb{Z}^{n-1}) \cap H\big)$ (la somme est clairement directe puisque $\mathbb{Z}f_1 \oplus (\{0\} \cap \mathbb{Z}^{n-1}) = \{0\}$) et l'hypothèse de récurrence permet de conclure.

Théorème 1 *Soient G un groupe abélien libre de rang n et H un sous-groupe de G, de rang $r \leqslant n$. Il existe une base $(e_1, e_2, \dots, e_n)$ de G et $a_1, a_2, \dots, a_r \in \mathbb{N} \setminus \{0\}$ vérifiant $a_i | a_{i+1}$ pour tout $i \in [\![1, r-1]\!]$ et tels que $(a_1e_1, a_2e_2, \dots, a_re_r)$ soit une base de H.*

Preuve : Commençons par faire le constat suivant. Si $(e_1, e_2, \dots, e_n)$ est une base d'un groupe abélien G, on conserve une base en considérant la famille obtenue en procédant à l'une des opérations élémentaires suivantes :

- Remplacement de e_i par $-e_i$, opération codée $e_i \leftarrow -e_i$.
- Échange des deux vecteurs de la base, opération codée $e_i \leftrightarrow e_j$.
- Remplacement de e_i par $e_i + be_j$, où $b \in \mathbb{Z}$ (et $j \neq i$), opération codée $e_i \leftarrow e_i + be_j$.

Soient maintenant H un sous-groupe de G, une base $(e_1, e_2, \dots, e_n)$ et une base $(f_1, f_2, \dots, f_r)$ de H. Notons $A \in \mathrm{M}_{n,r}(\mathbb{Z})$ la matrice des coordonnées des f_j relativement à la base $(e_i)_i$. La modification de $(e_i)_i$ par l'une des transformations élémentaires mentionnées ci-dessus se traduit sur la matrice A par une opération élémentaire sur ses lignes. Plus précisément,

- $e_i \leftarrow -e_i$ correspond à $L_i \leftarrow -L_i$
- $e_i \leftrightarrow e_j$ correspond à $L_i \leftrightarrow L_j$
- $e_i \leftarrow e_i + be_j$ correspond à $L_j \leftarrow L_j - bL_i$

De la même façon, une opération élémentaire sur les vecteurs de la base $(f_1, f_2, \dots, f_r)$ se traduit par une opération élémentaire sur les colonnes de A :

- $f_i \leftarrow -f_i$ correspond à $C_i \leftarrow -C_i$
- $f_i \leftrightarrow f_j$ correspond à $C_i \leftrightarrow C_j$.
- $f_i \leftarrow f_i + bf_j$ correspond à $C_i \leftarrow C_i + bC_j$

Le théorème sera donc prouvé dès lors qu'on aura montré que par une succession d'opération élémentaires sur les lignes et colonnes de A, on peut aboutir à une matrice de la forme

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_r \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

où les a_i sont comme dans l'énoncé. L'algorithme suivant permet d'aboutir à une matrice de ce type :

Étape 1 : Choisir un couple (i, j) tel que $A_{i,j}$ soit non nul. Le placer en position $(1, 1)$ (à l'aide des opérations $C_j \leftrightarrow C_1$ puis $L_i \leftrightarrow L_1$).

Étape 2 : Pour chaque $j \in [\![2, r]\!]$, effectuer l'opération $C_j \leftarrow C_j - qC_1$, où q est le quotient dans la division euclidienne de $A_{1,j}$ par $A_{1,1}$.
S'il existe $j \in [\![2, r]\!]$ tel que $A_{1,j} \neq 0$, opérer $C_j \leftrightarrow C_1$ et recommencer l'étape 2.
Noter qu'à chaque itération de cette boucle à l'exception de la dernière, $|A_{1,1}|$ diminue strictement. Lorsque cette boucle s'achève, la première ligne est nulle à l'exception de $A_{1,1}$.

Étape 3 : Pour chaque $i \in [\![2, n]\!]$, effectuer l'opération $L_i \leftarrow L_i - qL_1$, où q est le quotient dans la division euclidienne de $A_{i,1}$ par $A_{1,1}$.
S'il existe $i \in [\![2, n]\!]$ tel que $A_{i,1} \neq 0$, opérer $L_i \leftrightarrow L_1$ et recommencer l'étape 3.
Noter qu'à chaque itération de cette boucle à l'exception de la dernière, $|A_{1,1}|$ diminue strictement. Lorsque cette boucle s'achève, la première ligne et la première colonne sont nulles à l'exception de $A_{1,1}$.

Étape 4 : S'il existe un couple $(i,j) \in [\![2,n]\!] \times [\![2,r]\!]$ tel que $A_{i,j}$ ne soit pas multiple de $A_{1,1}$, alors faire $L_i \leftrightarrow L_j$ et retourner à l'étape 2. Sinon, fin de l'algorithme.

On voit aisément que cet algorithme s'achève. Lorsque tel est le cas, la matrice A est de la forme $\begin{pmatrix} a_1 & 0_{1,r-1} \\ 0_{n-1,1} & A' \end{pmatrix}$, où $A' \in \mathrm{M}_{n-1,r-1}(\mathbb{Z})$ et tous les coefficients de A' sont des multiples de a_1. Il suffit ensuite d'appliquer de manière récursive de cet algorithme à la matrice A' pour achever la preuve.

Remarque : on peut prouver l'unicité de la suite $a_1, a_2, \ldots, a_r$, qui sont appelés les facteurs invariants de H.

2 Applications

• Soit G un groupe abélien libre de rang n. Soit H un sous-groupe de G et r son rang. Alors H est d'indice fini dans G si et seulement si $r = n$. Lorsque tel est le cas on a, en notant B une base de G et C une base de H :

$$[G : H] = \det_B(C)$$

• Soit G un groupe abélien fini. Soit $e_1, \ldots, e_n$ une famille génératrice finie de G. L'application

$$\begin{array}{ccc} \mathbb{Z}^n & \to & G \\ (x_1, x_2, \ldots, x_n) & \mapsto & x_1e_1 + x_2e_2 + \ldots + x_ne_n \end{array}$$

est un morphisme surjectif. Son noyau est un sous-groupe H de $\mathbb{Z}^n$ et l'on a $G \simeq \mathbb{Z}^n/H$. Puisque G est fini, H est d'indice fini dans $\mathbb{Z}^n$ et son rang vaut n. Il existe donc une base $(e_1, e_2, \ldots, e_n)$ de $\mathbb{Z}^n$ et $a_1, \ldots, a_n \in \mathbb{N}^*$, $a_i | a_{i+1}$, tels que $(a_1e_1, a_2e_2, \ldots, a_ne_n)$ soit une base de H. Il vient

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$$

(quitte à éliminer les premiers facteurs, on peut supposer $a_i \geqslant 2$).

• Soit $z \in \mathbb{Z}[i] \setminus \{0\}$ (anneau des entiers de Gauss). L'idéal $(z) = z\mathbb{Z}[i]$ est en particulier un sous-groupe de $\mathbb{Z}[i]$. On voit aisément que (z, iz) en est une base. L'indice de (z) dans $\mathbb{Z}[i]$ vaut donc $\det_{(1,i)}(z, iz) = N(z)$ (où l'on note $N(z) = |z|^2$, qu'on appelle classiquement la norme de z). En particulier, si z est un élément premier de $\mathbb{Z}[i]$, alors $\mathbb{Z}[i]/(z)$ est un corps et le théorème de Lagrange dans le groupe multiplicatif des inversibles conduit à l'énoncé suivant, équivalent dans $\mathbb{Z}[i]$ du petit théorème de Fermat :

$$\forall w \in \mathbb{Z}[i],\ \mathrm{pgcd}(w, z) = 1 \implies w^{N(z)-1} \equiv 1\ [z]$$

En particulier, si $p \in \mathbb{N}^*$ est un entier premier (dans $\mathbb{Z}$) vérifiant $p \equiv 3\ [4]$ alors p est premier dans $\mathbb{Z}[i]$ et

$$\forall w \in \mathbb{Z}[i],\ p \not| w \implies w^{p^2-1} \equiv 1\ [p]$$

3 Généralisation

Tout ceci reste vrai en remplaçant $\mathbb{Z}$ par un anneau euclidien A, modulo l'introduction de la structure de A-module. La structure de A-module est une structure similaire à celle d'espace vectoriel, les

scalaires étant pris dans A. C'est donc un ensemble M muni de deux lois $+ : M \times M \to M$ et $. : A \times M \to M$ vérifiant (avec les quantificateurs adéquats) :

$(A, +)$ est un groupe abélien,
$a.(x + y) = a.x + a.y$
$(a + b).x = a.x + b.x$
$a.(b.x) = (ab).x$
$1_A.x = x$

Un instant de réflexion convainc qu'un groupe abélien n'est pas autre chose qu'un $\mathbb{Z}$-module. On passe de la structure de groupe abélien (dont on note additivement la loi) à la structure de $\mathbb{Z}$-module en posant $\forall k \in \mathbb{Z},\ k.x = (x + x + \ldots + x)$ (k fois) ou $k.x = -(-x - x - \ldots - x)$ ($-k$ fois) selon le signe de k et on passe de la structure de $\mathbb{Z}$-module à la structure de groupe abélien en « oubliant » la loi $.$.
Les théorèmes concernant les sous-groupes de $\mathbb{Z}^n$ peuvent être regardés comme des théorèmes concernant les sous-$\mathbb{Z}$-modules de $\mathbb{Z}^n$ et sont transposables ainsi que leur démonstration, en théorèmes décrivant les sous-modules de A^n, A euclidien (et même A principal mais la preuve doit alors être revisitée).
Dans ce qui suit A est donc un anneau euclidien.

Un A-module sera dit libre de rang n s'il est isomorphe à A^n, c'est-à-dire s'il admet une base de longueur n (deux bases ont nécessairement même longueur – preuve identique au cas $A = \mathbb{Z}$ si A est de caractéristique nulle).

Proposition 2 *Si M est un sous-module de A^n, alors M est un module libre de rang $r \leqslant n$.*

Théorème 2 *Soient M un A-module libre de rang n et N un sous-module de M, de rang $r \leqslant n$. Il existe une base $(e_1, e_2, \ldots, e_n)$ de M et $a_1, a_2, \ldots, a_r \in A \setminus \{0\}$ vérifiant $a_i | a_{i+1}$ pour tout $i \in [\![1, r-1]\!]$ et tels que $(a_1 e_1, a_2 e_2, \ldots, a_r e_r)$ soit une base de H.*

Et comme pour les groupes fini, on déduit que tout A-module admettant une famille génératrice finie (on dit de type fini) est isomorphe à un module de la forme

$$A/(a_1) \times \ldots, A/(a_r) \times A^s$$

où $a_1, a_2, \ldots, a_r \in A \setminus \{0\}$ et vérifient $a_i | a_{i+1}$ pour tout $i \in [\![1, r-1]\!]$.

Une application très classique de ce résultat est la suivante. On considère un K-espace vectoriel E de dimension finie et $u \in L(E)$. On munit E d'une structure de $K[X]$-module en posant

$$\forall P \in K[X],\ \forall x \in E,\ P.x = P(u)(x)$$

Si on se rappelle qu'un endomorphisme u est dit cyclique s'il existe $a \in E$ tel que $a, u(a), \ldots, u^{n-1}(a)$ soit une base de E, on vérifie que dire que u est cyclique équivaut à dire que le $K[X]$-module associé E est monogène (les endomorphismes cycliques et les groupes cycliques sont donc des concepts très voisins).

N'importe quelle famille génératrice de l'espace vectoriel E est aussi une famille génératrice du $K[X]$-module E. Comme l'espace vectoriel E est de dimension finie, E est isomorphe en tant que $K[X]$-module à

$$K[X]/(P_1) \times \ldots, K[X]/(P_r)$$

où $P_1, P_2, \ldots, P_r \in K[X] \setminus \{0\}$ et vérifient $P_i | P_{i+1}$ pour tout $i \in [\![1, r-1]\!]$. Les P_i sont appelés les invariants de similitude de u. Notons $\phi : K[X]/(P_1) \times \ldots, K[X]/(P_r) \to E$ un isomorphisme et posons

$F_i = \phi(\{0\} \times \ldots \times \{0\} \times K[X]/(P_i) \times \{0\} \times \ldots \times \{0\})$, alors $E = \bigoplus_{i=1}^{r} F_i$, F_i est stable par u. De plus, u opère sur F_i exactement comme la multiplication par X dans $K[X]$ modulo P_i :

$$\begin{aligned} u(\phi(0,\ldots,0,[Q]_{P_i},0,\ldots,0)) &= X.(\phi(0,\ldots,0,[Q]_{P_i},0,\ldots,0)) \\ &= \phi(X.(0,\ldots,0,[Q]_{P_i},0,\ldots,0)) \\ &= \phi(0,\ldots,0,[XQ]_{P_i},0,\ldots,0) \end{aligned}$$

Or l'application $[Q]_{P_i} \mapsto [XQ]_{P_i}$ est un endomorphisme cyclique de $K[X]/(P_i)$. On a donc prouvé que E se décompose en somme directe de sous-espaces stables par F_i sur lesquels u induit des endomorphismes cycliques (théorème de Frobenius).

Remarque : pour plus de détails sur les invariants de similitude, on pourra lire le document de Gregory Vial à l'adresse http ://www.bretagne.ens-cachan.fr/math/people/gregory.vial/files/cplts/ivs.pdf.