TD n°11 : Modules

15 et 19/12/2023

Exercice 1. Autour de $\mathrm{SL}_n(A)$

Soit A un anneau commutatif euclidien et $n \geq 0$.

1. En reprenant la preuve de la structure des A-modules de type fini avec grand soin, démontrer que $\mathrm{SL}_n(A)$ est engendré par les transvections.
2. Démontrer que pour tout entier $N \geq 2$, l'anneau $\mathbb{Z}/N\mathbb{Z}$ est euclidien.
3. En déduire que pour tout entier $N \geq 2$, l'application de réduction modulo N suivante est surjective :

$$\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}).$$

Correction de l'exercice 1 :

1. Effectuons une récurrence sur n puisque le cas $n = 0$ est immédiat. Soit M une matrice de $\mathrm{SL}_n(A)$. Nous considérons l'ensemble des matrices obtenues par multiplication à gauche et à droite par des transvections ; il nous suffit de prouver que cet ensemble de matrices contient l'identité. L'identité matricielle
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$
démontre que l'on peut échanger (au signe près) deux colonnes ou deux lignes de M en restant dans notre ensemble : il suffit pour cela de multiplier par cette identité matricielle vu comme un bloc sur les indices concernés.

   Ceci implique qu'il existe une matrice dans notre ensemble de premier coefficient non nul. Considérons une matrice N dont le premier coefficient est non nul de stathme minimal. Supposons qu'il existe un autre coefficient sur la première ligne ou colonne de N qui ne soit pas divisible par $n_{1,1}$. Disons qu'il est en position $(1, i)$. La division euclidienne $n_{1,i} = n_{1,1}q + r$ avec $r \neq 0$ de stathme $\nu(r) < \nu(n_{1,1})$ permet, en multipliant à gauche par la transvection $\mathrm{Id} - qE_{1,i}$ de trouver une matrice N' dans notre ensemble avec un coefficient r. Quitte à échanger les lignes, l'ensemble contient une matrice de premier coefficient r, ce qui est impossible par minimalité de $\nu(n_{1,1})$. Ainsi, le coefficient $n_{1,1}$ divise tous les coefficients des premières lignes et colonnes de N. En appliquant à gauche et à droite les transvections comme ci-dessus, nous pouvons nous ramener à une matrice
$$N_1 = \begin{pmatrix} n_{1,1} & 0 \\ 0 & N_1' \end{pmatrix}.$$
   En examinant le déterminant, le coefficient $n_{1,1}$ est donc inversible. Quitte à ajouter la première colonne à la deuxième, puis $n_{1,1}^{-1}(1 - n_{1,1})$ fois la deuxième à la première, on obtient un 1 comme premier coefficient, puis on fait de nouveau des transvections de la première ligne pour obtenir une matirce
$$N_2 = \begin{pmatrix} 1 & 0 \\ 0 & N_2' \end{pmatrix}.$$
   L'hypothèse de récurrence conclut.
2. Considérons l'application $\nu : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}$ qui à $\overline{n}$ associe l'unique représentant dans $[\![0, N-1]\!]$. Pour prouver que c'est un stathme, prenons $\overline{a}$ et $\overline{b}$. La division euclidienne classique de $\nu(a)$ par $\nu(b)$ fournit une écriture $\nu(a) = q\nu(b) + r$ avec $0 \leq r < \nu(b) < N$. Ainsi, $r = \nu(\overline{r})$ et l'écriture $a = \overline{q}b + \overline{r}$ fournit une divison euclidienne pour ν.

3. Puisque $\mathbb{Z}/N\mathbb{Z}$ est euclidien, la question 1) affirme que son groupe spécial linéaire est engendré par les transvections. Une transvection $\mathrm{Id}_n + \overline{k}E_{i,j}$ dans $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ étant l'image de $\mathrm{Id}_n + kE_{i,j}$, la surjectivité en découle.

Exercice 2. Sous-espaces stables

Soit k un corps infini et $n \geq 0$. Soit V un k-espace vectoriel de dimension n et $u \in \mathcal{L}(V)$. Démontrer que V ne possède qu'un nombre fini de sous-k-espaces vectoriels stables par V si et seulement si le polynôme minimal de u est de degré n.

Indication : on pourra s'intéresser au lien entre le polynôme minimal de u et les facteurs invariants de V pour sa structure de $k[X]$-module donnée par u.

Correction de l'exerice 2 :

Considérons le k-espace vectoriel V comme un $k[X]$-module en décrétant [1] que la multiplication par X revient à appliquer u. L'anneau $k[X]$ étant principal et le $k[X]$-module V de type fini car engendré par une base de V, la structure des modules de type fini sur des anneaux principaux affirme qu'il existe une famille de polynômes non constants $(P_i)_{1\leq i\leq r}$ tels que

$$V \cong \bigoplus_{i=1}^{r} k[X]/(\prod_{j\leq i} P_j)$$

comme $k[X]$-module. La multiplication par $\prod P_i$ annule ce module, ce qui signifie que $(\prod P_i)(u) = 0$, i.e. que $\mu_u | (\prod P_i)$. Réciproquement, prenons le vecteur v correspondant au 1 du r-ième terme de la somme directe. La relation $P(u)(v) = 0$ implique que P est nul dans le r-ième terme de la somme directe, i.e. que $P \in (\prod P_i)$. Par conséquent $\mu_u \in (\prod P_i)$.

Comme k-espace vectoriel, le quotient $k[X]/(\mu_u)$ est de dimension $\deg(\mu_u)$. Si le polynôme minimal de u est de degré n, alors V est isomorphe pour des arguments de dimension, et au vu de ce qui précède, à $k[X]/(\mu_u)$ comme $k[X]$-module. Un sous-espace stable par u correspond exactement à un sous-$k[X]$-module de V. Avec l'isomorphisme que nous venons de donner, cela correspond à un idéal de $k[X]$ contenant (μ_u). Ces derniers sont paramétrés par les diviseurs de μ_u unitaires, donc en nombre fini.

Dans le cas contraire, le $k[X]$-module V contient un sous-module isomorphe à

$$k[X]/(P) \oplus k[X]/(PQ)$$

pour certains polynômes non constants P et Q. Pour chaque $x \in k$, considérons le sous-$k[X]$-module M_x engendré par $(\overline{1}, \overline{xQ})$. Si un élément $(\overline{1}, \overline{R})$ appartient à M_x, il doit s'écrire $(\overline{A}, \overline{xQA})$ pour un certain polynôme A avec $A \in 1 + Pk[X]$. A fortiori, le polynôme xQA appartient à $xQ + PQk[X]$. Puisque $xQ \equiv yQ \mod PQ$ implique que $x = y$, les sous-modules M_x sont distincts. Ceci fournit dans V une infinité [2] de sous-k-espaces vectoriels stables par u.

Exercice 3. Idéaux équivalents

Soit A un anneau commutatif intègre. Deux idéaux I et J de A sont dits équivalents s'il existe $(a, b) \in (A\backslash\{0\})^2$ tels que $aI = bJ$.

1. Démontrer que la relation "être équivalents" est une relation d'équivalence. Démontrer que A est principal si et seulement si tous ses idéaux non nuls sont équivalents.

1. Cette construction est encore plus limpide si l'on voit une structure de $k[X]$-module comme un morphisme d'anneaux $k[X]$: $\mathrm{End}_{\mathbb{Z}}(V)$ car alors l'image de k est ici donnée par la multiplication venant de la structure de k-espace vectoriel et il manque simplement l'image de X qui commute aux éléments de k, i.e. un endomorphisme de groupe, qui doit être k-linéaire au vu de la relation de commutation.
2. C'est ici que l'on utilise que k est infini.

2. Démontrer que deux idéaux sont équivalents si et seulement s'ils sont isomorphes comme A-modules.
3. Soit K le corps des fractions de A et V un K-espace vectoriel de dimension 1. Démontrer que tout sous-A-module de type fini de V est isomorphe à un idéal de A.

Correction de l'exercice 3 :

1. Vérifions simplement la transitivité. Si I_1, I_2 et I_3 sont trois idéaux avec $(a,b,c,d) \in (A\backslash\{0\})^4$ tels que $aI_1 = bI_2$ et $cI_2 = dI_3$ alors
$$acI_1 = bdI_3.$$
Nous utilisons l'intégrité de A pour conclure que ac et bd sont non nuls.

   Un anneau est principal si et seulement si tout idéal non nul s'écrit aA pour un certain $a \in A\backslash\{0\}$, si et seulement si tout idéal non nul est équivalent à A.
2. Soit I un idéal et $a \in A\backslash\{0\}$. La multiplication par a est un morphisme de A-module de I sur aI. De plus, il est injectif puisque A est intègre. Ainsi, les A-modules I et aI sont isomorphes. Il en découle immédiatement que deux idéaux équivalents sont isomorphes comme A-modules.

   Réciproquement, si I et J sont isomorphes comme A-modules, fixons $f : I \to J$ un tel isomorphisme. Soit $i \in I$. En pré-composant par l'inverse de $f(i)I \cong I$, en post-composant par $J \cong iJ$ nous obtenons un isomorphisme $\tilde{f}$ de A-modules de $f(i)I$ dans iJ qui envoie $if(i)$ sur lui-même. Pour tout élément $i' \in f(i)I$, nous écrivons alors que
$$f(i)i\tilde{f}(i') = \tilde{f}(f(i)ii') = i'\tilde{f}(f(i)i) = i'f(i)i,$$
où les deux premières égalités sont obtenues car $\tilde{f}$ est un morphisme de A-modules. Par intégrité de A, il en découle que $\tilde{f}(i') = i'$, i.e. que $\tilde{f}$ est l'identité et donc que $f(i)I = iJ$.
3. Soit $(x_i)_{i\leq n}$ une famille engendrant notre sous-A-module M de type fini. En multipliant par exemple par le produit a des dénominateurs, il se trouve que $(ax_i)_{i\leq n}$ est une famille d'éléments de A. L'image de M par la multiplication par a est donc un sous-A-module de A (i.e. un idéal de A), isomorphe à M.

Exercice 4. Matrices de carré $d\mathrm{Id}_2$

Soit $d \in \mathbb{Z}$ qui n'est pas un carré. Notons $\mathrm{S}_2(d)$ l'ensemble des matrices $S \in \mathrm{M}_2(\mathbb{Z})$ telles que $S^2 = d\mathrm{Id}_2$.

1. Donner un exemple d'une telle matrice.
2. Démontrer qu'un idéal non nul de $\mathbb{Z}[\sqrt{d}]$ contient un entier et en déduire que c'est un $\mathbb{Z}$-module libre de rang 2.
3. Soit M un $\mathbb{Z}[\sqrt{d}]$-module de groupe sous-jacent libre de rang 2. Démontrer que M est un sous-$\mathbb{Z}[\sqrt{d}]$-module d'un $\mathbb{Q}(\sqrt{d})$-espace vectoriel de dimension 1.
4. À partir des questions précédentes, exhiber des bijections entre :
   — Les classes de conjugaisons d'éléments de $\mathrm{S}_2(d)$ dans $\mathrm{GL}_2(\mathbb{Z})$.
   — Les classes d'isomorphismes de $\mathbb{Z}[\sqrt{d}]$-modules, de groupe abélien sous-jacent libre de rang 2.
   — Les classes d'équivalence [3] d'idéaux de l'anneau $\mathbb{Z}[\sqrt{d}]$.
5. Soit $n \in \mathbb{Z}$ tel que d est un carré modulo n et que $\mathbb{Z}[\sqrt{d}]$ est principal. Démontrer que n et $-n$ s'écrivent $a^2 - db^2$ avec $(a,b) \in \mathbb{Z}^2$.

3. Voir l'exercice précédent.

Correction de l'exercice 4 :

1. La matrice $\left(\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right)$ est à coefficients entiers de de carré $d\mathrm{Id}_2$.
2. Soit $a+b\sqrt{d}$ non nul dans un idéal I. L'idéal contient $n=(a+b\sqrt{d})(a-b\sqrt{d})$ qui est un entier non nul. Ainsi, nous avons la suite d'inclusions de groupes abéliens
$$n\mathbb{Z}[\sqrt{d}] \subseteq I \subseteq \mathbb{Z}[\sqrt{d}].$$
Les deux termes extrêmaux sont des groupes abéliens libres de rang 2. Puisque $\mathbb{Z}$ est principal, la deuxième inclusion implique que I est libre de rang fini inférieur à 2. La première inclusion implique que ce rang est exactement 2.
3. Écrivons $M=\mathbb{Z}e_1\oplus\mathbb{Z}e_2$ comme groupe abélien. Le $\mathbb{Q}$-espace vectoriel $V=\mathbb{Q}e_1\oplus\mathbb{Q}e_2$ muni de l'unique application $\mathbb{Q}$-linéaire qui étend la multiplication par $\sqrt{d}$ sur M est un $\mathbb{Q}(\sqrt{d})$-espace vectoriel [4]. En examinant les dimension, il est de dimension 2 sur $\mathbb{Q}$ donc de dimension 1 sur $\mathbb{Q}(\sqrt{d})$ et M en est un sous-$\mathbb{Z}[\sqrt{d}]$-module.
4. Soit S une matrice de $\mathrm{S}_2(d)$. Elle vérifie $S^2=d\mathrm{Id}_2$ et est à coefficients entiers ; elle correspond donc à un morphisme d'anneaux
$$\mathbb{Z}[\sqrt{d}]=\mathbb{Z}[X]/X^2-d \to \mathrm{End}_{\mathbb{Z}}\left(\mathbb{Z}^2\right), \quad X\mapsto S.$$
Elle fournit ainsi une structure de $\mathbb{Z}[\sqrt{d}]$-module sur $\mathbb{Z}^2$. Si $S_1=PS_2P^{-1}$, on vérifie que l'isomorphisme de groupe abéliens $P:\mathbb{Z}^2\to\mathbb{Z}^2$ envoie la multiplication par $\sqrt{d}$ donnée par S_1 sur le premier $\mathbb{Z}[\sqrt{d}]$-module sur la multiplication par $\sqrt{d}$ donnée par S_2 sur le second. Ainsi, P est un isomorphisme de $\mathbb{Z}[\sqrt{d}]$-modules.

   Soit M un $\mathbb{Z}[\sqrt{d}]$-module libre de rang 2. Grâce à la question 3, nous pouvons écrire M comme sous-$\mathbb{Z}[\sqrt{d}]$-module d'un $\mathbb{Q}(\sqrt{d})$-espace vectoriel de dimension 1. Puisque M est de type fini comme $\mathbb{Z}$-module, il l'est comme $\mathbb{Z}[\sqrt{d}]$-module. La dernier question de l'exercice précédent permet alors d'affirmer que M est isomorphe à un idéal de $\mathbb{Z}[\sqrt{d}]$ comme $\mathbb{Z}[\sqrt{d}]$. La deuxième question de l'exercice précédent affirme également que cet idéal est bien défini à équivalence près. Si M_1 et M_2 sont isomorphes, les idéaux associés le sont également et ils sont équivalents pour les mêmes raisons.

   Soit I un idéal de $\mathbb{Z}[\sqrt{d}]$. Grâce à la question 2), il est isomorphe à $\mathbb{Z}^2$ comme groupe abélien et la multiplication par $\sqrt{d}$ sur I induit un endomorphisme de $\mathbb{Z}^2$, ce carré d, autrement dit un élément de $\mathrm{S}_2(d)$. Le choix de l'isomorphisme de I avec $\mathbb{Z}^2$ revient à faire un changement de base, autrement dit à conjuguer la matrice obtenue. La classe de conjugaison de cette dernière est donc correctement définie à partir de I. Si I et J sont équivalents, ils sont isomorphes comme $\mathbb{Z}[\sqrt{d}]$-modules. Soit ι un tel isomorphisme. En choisissant une base $\mathcal{B}$ de I comme groupe abélien, la matrice de la multiplication par $\sqrt{d}$ dans cette base est exactement celle de la multiplication par $\sqrt{d}$ dans base $\iota(\mathcal{B})$ de J.

   Nous avons construit des applications circulairement et nous vérifions sans soucis que leur triple composée est l'identité.
5. Écrivons par hypothèse $d=a^2+nb$. Les matrices $\left(\begin{smallmatrix} a & \pm n \\ \pm b & -a \end{smallmatrix}\right)$ appartiennent à $\mathrm{S}_2(d)$ puisqu'elle sont de trace nulle et de déterminant $-d$. Or, toutes les matrices de $\mathrm{S}_2(d)$ sont conjuguées puisque tous les idéaux des $\mathbb{Z}[\sqrt{d}]$ sont équivalents. En choissant des signes positifs par exemple, il existe une matrice à coefficients entiers telle que
$$\begin{pmatrix} a & n \\ b & -a \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$
En observant le coefficient supérieur droit, nous obtenons $n=-\beta^2+d\alpha^2$, i.e. que $-n=\beta^2-d\alpha^2$. Nous concluons en appliquant le même raisonnement avec des signes négatifs.

4. Le voir en considérant que $\mathbb{Q}(\sqrt{d})=\mathbb{Q}[X]/X^2-d$ et qu'une structure d'espace vectoriel équivaut à un morphimse d'anneaux $\mathbb{Q}(\sqrt{d})\to\mathrm{End}_{\mathbb{Z}}(V)$.