École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD n° 11 : Modules sur les anneaux principaux

`À faire en priorité : 1 - (2) - 3 - 4 - 5`

Exercice 1.

Soit $n \geqslant 1$ un entier et k un corps. Décrire en terme d'algèbre linéaire ce qu'est un $k[X_1, \dots, X_n]$-module de dimension finie sur k.

Exercice 2.

1. Soient A un anneau principal, $n \geq 2$ et $a = (a_1, \dots, a_n) \in A^n$ premiers entre eux dans leur ensemble. Montrer qu'il existe une base de A^n contenant le vecteur $a = (a_1, \dots, a_n)$. En déduire qu'il existe un élément de $\mathrm{SL}_n(A)$ dont la première ligne est a.
2. Soit A un anneau euclidien. Montrer que $\mathrm{SL}_n(A)$ est engendré par les transvections élémentaires.
3. Supposons que A est euclidien. Soit $I \subset A$ un idéal, montrer qu'alors la réduction canonique $\mathrm{SL}_n(A) \to \mathrm{SL}_n(A/I)$ est surjectif. On commencera par montrer que $\mathrm{SL}_n(A/I)$ est engendré par des transvections élémentaires.

Exercice 3.

Soit $N > 1$ un entier. Posons $\Gamma(N) \coloneqq \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv \mathrm{id}_2 \pmod N\}$ comme sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$. On appelle $\Gamma(N)$ le *sous-groupe de congruence principal de niveau N*.

1. Montrer que $\Gamma(N)$ est distingué et d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$.
2. Montrer que $\Gamma(2)$ est engendré par $-\mathrm{I}_2$ et
$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$
3. Montrer que la réduction $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ est surjective.
4. Soit $N = p_1^{a_1} \cdots p_n^{a_n}$ la décomposition de N en facteurs premiers. Montrer qu'on a un isomorphisme naturel
$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{i=1}^{n} \mathrm{GL}_2(\mathbb{Z}/p^{a_i}\mathbb{Z}).$$
5. Montrer que $\det \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ est surjectif et en déduire
$$[\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma(N)] = N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right).$$
6. Montrer que $\Gamma(N)/\Gamma(N^2) \cong \mathbb{Z}/N^3\mathbb{Z}$. En déduire que $\Gamma(N)$ n'est pas engendré par deux transvections et $-\mathrm{I}_2$.

Exercice 4.

Soit k un corps fini. Le but est de comprendre la structure de k.

1. Montrer qu'il existe un entier premier p et un entier $n \geqslant 1$ tel que, en tant que $\mathbb{Z}$-module, $k \cong (\mathbb{Z}/p\mathbb{Z})^n$. Justifier de plus que $k^\times \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$.
2. Soit $\sigma \colon k \to k$ donné par $x \mapsto x^p$. Montrer que σ est un automorphisme d'anneau[1]. Montrer que σ est d'ordre n sur k.
3. D'une factorisation du polynôme $X^{p^n} - X$ sur k, en déduire que pour tout entier d tel que $d \mid n$, le corps k contient un unique sous-corps de cardinal p^d que l'on notera k_d. Montrer qu'il existe $\alpha \in k$ tel que $\{\sigma^i(\alpha)\}_{0 \leqslant i \leqslant n}$ est une $\mathbb{F}_p$-base de k.

[1] Il est tel que $\sigma(x+y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$, $\sigma(1) = 1$ et $\sigma(0) = 0$.

4. Montrer que le sous-groupe de $\mathrm{GL}(k)$ engendré par $k^\times$ et σ est isomorphe à $\mathbb{Z}/(p^n-1)\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$ non-trivial, observer que ce produit semi-direct est unique.

5. En déduire qu'(à unique isomorphisme près) il existe un unique corps fini de cardinal donné de la forme p^n et que $\mathrm{Aut}_{\mathbb{F}_p}(k) = \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Exercice 5. [Idéaux équivalents]

Soit A un anneau commutatif intègre de corps de fractions K. Soient I, J deux idéaux de A, on dit qu'ils sont *équivalents* s'il existe $a, b \in A \setminus \{0\}$ avec $aI = bJ$.

1. Montrer que A est principal si, et seulement si, tous ses idéaux sont équivalents.

2. Soit M un *idéal fractionnaire* de K i.e. un sous-A-module de type fini de K. Montrer que M est isomorphe à un idéal de A.

.

Exercice 6.

Soit $d \in \mathbb{Z}$ non carré. Pour $a, b, c \in \mathbb{Z}$ on pose

$$[a, b, c] \coloneqq \begin{pmatrix} b & c \\ a & -b \end{pmatrix}, \in \mathrm{M}_2(\mathbb{Z}).$$

On a donc $[a, b, c] \in \mathrm{S}_d \iff b^2 + ac = d$ (auquel cas a et c sont non nuls).

1. Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à

$$[-a, b, -c], \ \ [c, -b, a], \ \ [a, b + a, c - a - 2b] \ \text{ et } \ [a, b - a, c - a + 2b].$$

2. Soit $[a, b, c] \in \mathrm{S}_2(\mathbb{Z})$. Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à $[a', b', c']$ avec $2|b| \leq a \leq |c|$, puis l'inégalité $1 \leq a \leq 2\sqrt{|d|/3}$.

3. Redémontrer la principalité de $\mathbb{Z}[\sqrt{d}]$ pour $d = -2, -1, 2$.

4. Montrer les égalités

$$\mathrm{Cl}(3) = \{\overline{[1, 0, 3]}\}, \ \mathrm{Cl}(-3) = \{\overline{[1, 0, -3]}, \overline{[2, 1, -2]}\} \text{ et } \ \mathrm{Cl}(5) = \{\overline{[1, 0, 5]}, \overline{[2, 1, 2]}\}.$$

5. En déduire que $\mathbb{Z}[\sqrt{3}]$ est principal, mais pas $\mathbb{Z}[\sqrt{5}]$.

Exercice 7.

Soit $d \in \mathbb{Z}$ non carré. Notons $\mathrm{S}_2(d)$ l'ensemble des matrices $S \in \mathrm{M}_2(\mathbb{Z})$ avec $S^2 = d \in \mathbb{Z}$. Le groupe $\mathrm{GL}_2(\mathbb{Z})$ agit par conjugaison sur $\mathrm{S}_2(d)$ et on notera $\mathrm{Cl}(d)$ l'ensemble des orbites (*classes de conjugaisons*).

1. Montrer $\mathrm{S}_2(d) \neq \emptyset$.

2. Soit $S \in \mathrm{M}_2(\mathbb{Z})$. Vérifier $S \in \mathrm{S}_2(d) \iff \mathrm{tr}S = 0, \text{ et } \det S = -d$.

3. Montrer qu'il existe des bijections entre:

   - $\mathrm{Cl}(d)$,
   - classes d'isomorphisme de structures de $\mathbb{Z}[\sqrt{d}]$-modules sur $\mathbb{Z}^2$,
   - classes d'équivalence d'idéaux non nuls de $\mathbb{Z}[\sqrt{d}]$.

4. En déduire des représentants de $\mathrm{Cl}(d)$ pour $d = -2, -1, 2$.

5. On suppose que l'entier d est un carré modulo $n \in \mathbb{Z}$, et $\mathrm{Cl}(|d|)| = 1$. Montrer que $\pm n$ est de la forme $a^2 + db^2$ avec $a, b \in \mathbb{Z}$.

6. En considérant l'idéal $(2, \sqrt{-3} + 1)$ de $\mathbb{Z}[\sqrt{-3}]$, exhiber deux éléments de $\mathrm{S}_2(-3)$ non conjugués.