Partie 1 : structures quotients et applications

Lire le premier théorème d'isomorphisme pour les groupes sur la page wikipedia intitulées "Théorèmes d'isomorphisme" (ou les pages 402 à 406 du livre "Toute l'algèbre de la licence" de J.-P. Escoffier). Ce théorème d'isomorphisme se généralise aux structures d'anneaux et d'espaces vectoriels.

Exercice 1 *Groupes quotients et isomorphismes.*

1. Montrer que le groupe alterné A_n (formé des permutations paires) est un sous-groupe distingué du groupe des permutations S_n et décrire le groupe quotient S_n/A_n.

2. Montrer que le groupe spécial linéaire $SL_n(\mathbb{K})$ (formé des matrices $n \times n$ à coefficient dans un corps $\mathbb{K}$ et de déterminant 1) est un sous-groupe distingué du groupe linéaire $\mathrm{GL}_n(\mathbb{K})$ et décrire le groupe quotient $\mathrm{GL}_n(\mathbb{K})/SL_n(\mathbb{K})$.

3. Montrer que $\mathbb{Z}$ est un sous-goupe distingué de $\mathbb{R}$ et que le quotient $\mathbb{R}/\mathbb{Z}$ est isomorphe au groupe $\mathbb{U}$ des nombres complexes de module 1.

Exercice 2 *Anneaux quotients et isomorphismes.*

1. Montrer que les anneaux suivants sont isomorphes :
a. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[X]/(X^2-2)$. **b.** $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2+1)$.

2. Décrire les anneaux $\mathbb{Z}[j]$, $\mathbb{Z}[1+i]$ comme des quotients de l'anneau $\mathbb{Z}[X]$.

3. Décrire l'anneau $\mathbb{Z}[X]/(10X-1)$ comme un sous-anneau de $\mathbb{C}$.

4. Que peut-on dire de $\mathbb{R}[X]/(X-a)$, $a \in \mathbb{R}$? de $\mathbb{R}[X]/(X^2+1)$?

5. Montrer que $\mathbb{R}[X]/(X^2-1)$ est isomorphe à $\mathbb{R}\times\mathbb{R}$ muni de la loi $+$ habituelle et de la loi $\times$ définie par $(a,b)\times(a',b') = (aa'+bb', ab'+a'b)$. Est-ce un corps ?

6. Décrire les quotients $\mathbb{Q}[X]/(X^2+1)$, $\mathbb{Q}[X]/(X^2-2)$. Sont-ils isomorphes ?

7. Montrer les isomorphismes suivants pour p premier et d entier, $d \geq 1$:

$$\mathbb{Z}[i\sqrt{d}]/(p) \simeq \mathbb{Z}[X]/(X^2+d,p) \simeq \mathbb{F}_p[X]/(X^2+d).$$

Exercice 3 *Espaces vectoriels quotients et isomorphismes.*
Soit E un espace vectoriel, F un sous-espace vectoriel de E, G un supplémentaire de F dans E. Montrer de deux manières que les espaces vectoriels G et E/F sont isomorphes :

a. par les définitions

b. en utilisant le premier théorème d'isomorphisme.

Exercice 4 *Avec ou sans quotient ? Intersection de sous-espaces vectoriels*
Soit E un espace vectoriel de dimension finie n. Soient $F_1, ..., F_k$ des sous-espaces vectoriels de E. Montrer de deux manières différentes que si $\sum_{i=1}^k \dim F_i > n(k-1)$, alors $\cap_{i=1}^k F_i \neq \{0\}$:

1. en utilisant une application $\phi : F_1 \times \cdots \times F_k \to E^{k-1}$ dont le noyau est isomorphe à $\cap_{i=1}^k F_i$,

2. en utilisant une application $\psi : E \to E/F_1 \times \cdots \times E/F_k$ dont le noyau est $\cap_{i=1}^k F_i$.

Partie 2 : arithmétique et quotients.

Exercice 5

1. Quels sont les polynômes irréductibles de $\mathbb{C}[X]$? de $\mathbb{R}[X]$?

2. Montrer qu'un polynôme de degré 3 de $\mathbb{Q}[X]$ sans racine (dans $\mathbb{Q}$) est irréductible.

3. Donner un polynôme de degré 4 de $\mathbb{Q}[X]$ sans racine (dans $\mathbb{Q}$) mais pas irréductible.

Remarque : on montre dans l'exercice suivant qu'il y a des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

Exercice 6 *Application du critère d'Eisenstein*

Le résultat suivant s'appelle le critère d'Eisenstein : Soit $P = a_nX^n + ... + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que p divise $a_0, \dots a_{n-1}$, p ne divise pas a_n et p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{Q}[X]$.

1. Donner des polynômes irréductibles de tout degré dans $\mathbb{Z}[X]$ vérifiant le critère d'Eisenstein.

2. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$ (indication : pour tout $a \in \mathbb{Q}$, $P(X)$ est irréductible si et seulement si $P(X+a)$ est irréductible) :

a. $X^4 + 6X^3 - 12X^2 + 3X + 15$, **b.** $X^4 + 1$, **c.** $X^{p-1} + X^{p-2} + \cdots + 1$ pour tout p premier.

Exercice 7 *(irréductibilité par réduction modulo 2)*

[Gourdon, Algèbre, ex.11 p.69]

Soit $P = a_nX^n + ... + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ et $\overline{P} = \overline{a_n}X^n + ... + \overline{a_0} \in \mathbb{F}_p[X]$ l'image du polynôme P dans $\mathbb{F}_p[X]$. On dit qu'un polynôme P est irréductible modulo p si son image dans $\mathbb{F}_p[X]$ est irréductible.

1. Montrer que si $\overline{P}$ est irréductible, alors P l'est aussi. La réciproque est-elle vraie ?

2. Montrer que le polynôme $X^4 + X + 1$ de $\mathbb{Z}[X]$ est irréductible (indication : le réduire modulo 2).

Exercice 8 *(irréductibilité et réduction modulo p)*

Le critère d'Eisenstein montre que le polynôme $P = X^4 + 1$ est irréductible sur $\mathbb{Z}$ (et sur $\mathbb{Q}$). Nous allons montrer qu'il est réductible modulo p pour tout nombre premier p.

1. Montrer que P est réductible modulo 2.

2. Soit p un nombre premier tel que -1 est un carré modulo p (c'est-à-dire $p \equiv 1[4]$ d'après l'exercice 1). Montrer que P est réductible modulo p.

3. Soit p un nombre premier tel que 2 est un carré modulo p. Montrer que P est réductible modulo p. Indication : utiliser le fait que $X^4 + 1 = (X^2+1)^2 - 2X^2$).

4. Soit p un nombre premier tel que -2 est un carré modulo p. Montrer que P est réductible modulo p.

5. Montrer que si -1 et 2 ne sont pas des carrés modulo p, alors -2 est un carré modulo 2 (indication : caractériser les carrés de $\mathbb{F}_p$ comme dans l'exercice 1).

6. Conclure.

Partie 3 : algèbre bilinéaire et espaces euclidiens

Lire les pages 96, 97 du polycopié de G. Skandalis "Algèbre générale et algèbre linéaire" (ou les pages 352 à 354 du livre "Toute l'algèbre de la licence" de J.-P. Escoffier)

Exercice 9 *Matrices de formes bilinéaires et d'endomorphismes dans un espace euclidien*

Soit $(E, <,>)$ un espace euclidien. Soient $\mathcal{B}$ une base quelconque de E, $\mathcal{B}_0$ une base orthonormée de E.

1. Que peut-on dire de la matrice $\mathrm{mat}_{\mathcal{B}_0} <,>$ dans la base $\mathcal{B}_0$ du produit scalaire $<,>$?

2. Montrer que la matrice $M = \mathrm{mat}_{\mathcal{B}} <,>$ du produit scalaire $<,>$ dans la base $\mathcal{B}$ est diagonalisable (sur $\mathbb{R}$). Montrer qu'il existe une matrice inversible P telle que $M = P.\,{}^tP$. Montrer que les valeurs propres de M sont toutes strictement positives.

3. **a.** Donner la définition d'un endormorphisme orthogonal (ou isométrie) de E.

b. Caractériser les matrices dans $\mathcal{B}_0$ des endomorphismes orthogonaux de E.

c. Caractériser les matrices dans $\mathcal{B}$ des endomorphismes orthogonaux de E.

4. **a.** Donner la définition d'un endormorphisme symétrique (ou autoadjoint) de E.

b. Caractériser les matrices dans $\mathcal{B}_0$ des endomorphismes symétriques de E.

c. Caractériser les matrices dans $\mathcal{B}$ des endomorphismes symétriques de E.

Exercice 10

Pour chacun des deux endomorphismes de $\mathbb{R}^2$ dont les matrices dans la base canonique $\mathcal{B}$ de $\mathbb{R}^2$ sont les suivantes, dire s'il existe un produit scalaire sur $\mathbb{R}^2$ rendant l'endomorphisme autoadjoint :

a. $\mathrm{mat}_{\mathcal{B}}\, u = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$. **b.** $\mathrm{mat}_{\mathcal{B}}\, v = \begin{pmatrix} 1 & 4 \\ 1 & 1 \end{pmatrix}$.

Exercice 11

Soit $u : E \to E$ un endomorphisme d'un espace euclidien E. Soit $k \geq 1$ un entier. Montrer de deux manières que si $u^* = u$ et $u^k = 0$, alors $u = 0$:

a. en traitant d'abord le cas $k = 2$ par la définition de l'adjoint, puis le cas où k est une puissance de 2.

b. en utilisant le théorème spectral.

Exercice 12

Soit $u : E \to E$ un endomorphisme d'un espace euclidien E. Soit $k \geq 1$ un entier. Montrer que si $u^* = u$ et $u^k = id$, alors $u^2 = \mathrm{id}$.

Exercice 13 *(orthogonalisation simultanée de deux formes quadratiques)*

On considère la forme bilinéaire b sur $\mathbb{R}^2$ de matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dans la base canonique.

1. Donner la signature de la forme b.

On rappelle que l'orthogonal d'une partie A de $\mathbb{R}^2$ pour la forme b est l'ensemble :

$$A^{\perp} = \{u \in \mathbb{R}^2 \mid \forall v \in A,\ b(u,v) = 0\}.$$

2. Décrire l'orthogonal pour b du vecteur $(1, a) \in \mathbb{R}^2$ pour $a \in \mathbb{R}$. Quel est l'orthogonal du vecteur $(0, 1)$?

3. Décrire toutes les bases orthogonales pour b qui sont orthonormées pour la structure euclidienne usuelle de $\mathbb{R}^2$.

Exercice 14 *(diagonalisation d'un endomorphisme autoadjoint en base orthonormée)*

On se place dans l'espace vectoriel $\mathbb{R}^2$ muni de sa structure euclidienne canonique. On considère l'endomorphisme u de $\mathbb{R}^2$ dont la matrice dans la base canonique $\mathcal{B}$ de $\mathbb{R}^2$ est :

$$\operatorname{mat}_{\mathcal{B}} u = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}.$$

1. Justifier que u est un endomorphisme auto-adjoint de $\mathbb{R}^2$.

2. Diagonaliser u en base orthonormée et écrire matriciellement la formule de changement base.

3. En déduire la signature de la forme quadratique b dont la matrice dans la base canonique de $\mathbb{R}^2$ est :

$$\operatorname{mat}_{\mathcal{B}} b = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}.$$

4. Mêmes questions pour $\operatorname{mat}(u, \underline{e}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et faire le lien avec l'exercice précédent.

Exercice 15

La matrice $\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$ est-elle symétrique ? diagonalisable ?

Exercice 16

On se place dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne canonique. On considère l'endomorphisme u de $\mathbb{R}^3$ dont la matrice dans la base canonique $\underline{e}$ de $\mathbb{R}^3$ est :

$$\operatorname{mat}(u, \underline{e}) = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

Montrer que u est un endomorphisme symétrique et diagonaliser u en base orthonormée.

Exercice 17

1. Soit $A \in M_n(\mathbb{R})$ une matrice symétrique. On suppose que A est définie positive, au sens où la forme quadratique de $\mathbb{R}^n$ dont la matrice dans la base canonique est A est une forme définie positive. Montrer qu'il existe une unique matrice symétrique définie positive B telle que $A = B^2$.

2. Montrer qu'il n'existe pas de matrice symétrique B de $M_3(\mathbb{R})$ telle que $B^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

3. Montrer qu'il n'existe pas de matrice B de $M_3(\mathbb{R})$ telle que $B^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Exercice 18

Soit E un espace vectoriel de dimension 2 et $\underline{e} = (e_1, e_2)$ une base de E. On munit E du produit scalaire rendant $\underline{e}$ orthonormée et de l'orientation rendant $\underline{e}$ directe (on pourra traiter l'exercice avec $E = \mathbb{R}^2$ et $\underline{e}$ la base canonique).

1. Soit $u : E \to E$ l'endomorphisme de E dont la matrice dans la base $\underline{e}$ est :

$$\operatorname{mat}(u, \underline{e}) = \frac{1}{5}\begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix}.$$

Montrer que u est une rotation et donner son angle de rotation. Donner sa matrice dans la base $\underline{e'} = (e_2, e_1)$. Que constate-t-on ?

2. Soit $v : E \to E$ l'endomorphisme de E dont la matrice dans la base $\underline{e}$ est :

$$\mathrm{mat}(v, \underline{e}) = \frac{1}{5}\begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}.$$

Montrer que v est une symétrie orthogonale et déterminer son axe. Donner une base orthonormée $\underline{f} = (f_1, f_2)$ telle que $\mathrm{mat}(v, \underline{f}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Exercice 19

Soit E un espace vectoriel de dimension 3 et $\underline{e} = (e_1, e_2, e_3)$ une base de E. On munit E du produit scalaire rendant $\underline{e}$ orthonormée et de l'orientation rendant $\underline{e}$ directe (on pourra traiter l'exercice avec $E = \mathbb{R}^3$ et $\underline{e}$ la base canonique).

Soit $u : E \to E$ l'endomorphisme de E dont la matrice dans la base $\underline{e}$ est :

$$\mathrm{mat}(u, \underline{e}) = \frac{1}{3}\begin{pmatrix} 2 & 2 & -1 \\ -1 & 2 & 2 \\ 2 & -1 & 2 \end{pmatrix}.$$

1. Montrer que u est une rotation.

2. Déterminer $v_1 \in E$ et $\theta \in [0, 2\pi[$ tels que u est la rotation $r_{v_1,\theta}$ d'axe la droite dirigée et orientée par v_1 et d'angle θ. (Si H est un hyperplan d'un espace vectoriel orienté E de dimension n et si $v \in E \setminus H$, alors, par convention, on oriente H par toute base b_H de H telle que (b_H, v) soit une base directe de E.)

Exercice 20

Soit E un espace vectoriel de dimension 3 et $\underline{e} = (e_1, e_2, e_3)$ une base de E. On munit E du produit scalaire rendant $\underline{e}$ orthonormée et de l'orientation rendant E directe (on pourra traiter l'exercice avec $E = \mathbb{R}^3$ et $\underline{e}$ la base canonique).

Soit $u : E \to E$ l'endomorphisme de E dont la matrice dans la base $\underline{e}$ est :

$$\mathrm{mat}(u, \underline{e}) = \frac{1}{3}\begin{pmatrix} 2 & 2 & 1 \\ -1 & 2 & -2 \\ 2 & -1 & -2 \end{pmatrix}.$$

Montrer que u est un endomorphisme orthogonal (isométrie) et trouver ses caractéristiques.

Exercice 21

Compléter la matrice $\frac{1}{7}\begin{pmatrix} 6 & 3 & -2 \\ -2 & 6 & \cdot \\ 3 & \cdot & \cdot \end{pmatrix}$ en une matrice orthogonale.

Quelle isométrie de $\mathbb{R}^3$ définit-elle ? (c'est-à-dire si $\mathbb{R}^3$ est muni du produit scalaire et de son orientation canoniques et si u est l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique est la matrice précédente, décrire les caractéristiques de l'isométrie u.)