Algèbre et géométrie 2e année

Chapitres concernés :

1. Structures algébriques
2. Valeurs propres, vecteurs propres
3. Réduction d'une matrice
4. Espaces vectoriels normés
5. Convexité
6. Topologie des espaces vectoriels normés
7. Espaces préhilbertiens réels
8. Endomorphismes des espaces euclidiens
9. Fonctions vectorielles, arcs paramétrés

Un groupe forcément abélien

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

Qu'un groupe dont tous les éléments x vérifie $x^2 = e$ est nécessairement abélien (commutatif).

- **L'énoncé**

Soit $(G,\times)$ un groupe vérifiant $x^2 = e$ pour tout $x \in G$. On veut montrer que G est commutatif, c'est-à-dire que $xy = yx$ (pour tous $x,y \in G$).

1) Montrer que pour tous $x,y \in G$: $(xy)^{-1} = xy$.

2) En déduire que $xy = yx$ et donc que G est commutatif.

- **Corrigé**

1) Comme pour tout $x \in G$ $x^2 = e$, on a $x^{-1} = x$ pour tout $x \in G$.

Comme pour $x,y \in G$, $xy \in G$ on a donc $(xy)^{-1} = xy$ (car la propriété précédente est vérifiée par tous les éléments de G, y compris xy !).

2) On a $(xy)^{-1} = xy$. Or $(xy)^{-1} = y^{-1}x^{-1}$. On a donc $xy = y^{-1}x^{-1}$.

La propriété $x^{-1} = x$ valable pour tout $x \in G$ donne $y^{-1} = y$ et $x^{-1} = x$. L'égalité $xy = y^{-1}x^{-1}$ devient alors $xy = yx$, ce qui prouve que G est commutatif (c'est-à-dire abélien).

☐ **Ce qu'il faut retenir du cours**

1) Si $x,y \in (G,\times)$ alors $xy \in G$.

2) $(xy)^{-1} = y^{-1}x^{-1}$.

3) G abélien (commutatif) si $xy = yx$ pour tous $x,y \in G$, $xy = yx$.

Réunion de deux sous-groupes

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

Que la réunion de deux sous-groupes n'est en général jamais un sous-groupe sauf si l'un est inclus dans l'autre.

- **L'énoncé**

Soient G_1 et G_2 deux sous-groupes d'un groupe $(G,\times)$.

1) Montrer l'implication : Si $G_1 \subset G_2$ ou $G_2 \subset G_1$ alors $G_1 \cup G_2$ est un sous-groupe.

2) Montrer l'implication : Si $G_1 \not\subset G_2$ et $G_2 \not\subset G_1$ alors $G_1 \cup G_2$ n'est pas un sous-groupe.

3) Que peut-on en déduire ?

- **Corrigé**

1) Si $G_1 \subset G_2$ alors $G_1 \cup G_2 = G_2$ est un sous-groupe.

Si $G_2 \subset G_1$ alors $G_1 \cup G_2 = G_1$ est un sous-groupe. D'où l'implication.

2) Supposons $G_1 \not\subset G_2$ et $G_2 \not\subset G_1$ et soit $\begin{cases} g_1 \in G_1 \text{ tel que } g_1 \notin G_2 \\ g_2 \in G_2 \text{ tel que } g_2 \notin G_1 \end{cases}$. Alors $g_1, g_2 \in G_1 \cup G_2$.

Montrons par un raisonnement par l'absurde que $G_1 \cup G_2$ n'est pas un sous-groupe.

Si $G_1 \cup G_2$ était un groupe alors $g_1 g_2 \in G_1 \cup G_2$ soit : $g_1 g_2 \in G_1$ ou $g_1 g_2 \in G_2$.

Donc $\begin{cases} g_2 = g_1^{-1} g_1 g_2 \in G_1 \text{ CONTRADICTION} \\ \text{ou} \\ g_1 = g_1 g_2 g_2^{-1} \in G_2 \text{ CONTRADICTION} \end{cases}$. Ainsi : $G_1 \cup G_2$ n'est pas un sous-groupe.

3) On obtient l'équivalence : $G_1 \cup G_2$ est un sous-groupe $\Leftrightarrow$ $G_1 \subset G_2$ ou $G_2 \subset G_1$.

☐ **Ce qu'il faut retenir du cours**

1) Pour montrer l'équivalence $P \Leftrightarrow Q$, on peut montrer que $P \Rightarrow Q$ et que $\text{non}P \Rightarrow \text{non}Q$.

2) Si $G_1 \not\subset G_2$ et $G_2 \not\subset G_1$, alors il existe des éléments qui sont dans G_1 sans être dans G_2 et réciproquement.

3) Le principe du raisonnement par l'absurde.

A quoi est isomorphe un groupe monogène ?

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

Que tout groupe monogène est soit isomorphe à $(\mathbb{Z},+)$ (s'il est infini), soit isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$ (s'il est fini d'ordre n).

- **L'énoncé**

Soit $G=\langle x\rangle=\{x^k : k\in\mathbb{Z}\}$ un groupe monogène (de générateur x et de loi $\times$)

1) Supposons x d'ordre infini, montrer à l'aide du morphisme $\phi:\mathbb{Z}\to G$ défini par $\phi(k)=x^k$, que G est isomorphe à $\mathbb{Z}$.

2) Supposons x d'ordre fini n, montrer à l'aide du morphisme $\theta:\mathbb{Z}/n\mathbb{Z}\to G$ défini par $\theta(\bar{k})=x^k$, que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

- **Corrigé**

1) ϕ est bien un homomorphisme de groupes car $\phi(k_1+k_2)=x^{k_1+k_2}=x^{k_1}x^{k_2}=\phi(k_1)\times\phi(k_2)$.

ϕ est surjectif car $G=\{x^k : k\in\mathbb{Z}\}$ donc pour tout $y\in G$, il existe $k\in\mathbb{Z}$ tel que $y=x^k$.

ϕ est injectif car $\phi(k_1)=\phi(k_2)\Leftrightarrow x^{k_1}=x^{k_2}\Leftrightarrow x^{k_1-k_2}=e$. Or x étant d'ordre infini, cela n'est possible que si $k_1-k_2=0$ soit $k_1=k_2$.

$\phi:\mathbb{Z}\to G$ étant bijectif, G est isomorphe à $\mathbb{Z}$.

2) θ est bien un homomorphisme de groupes car $\theta(\bar{k_1}+\bar{k_2})=x^{\bar{k_1}+\bar{k_2}}=x^{\bar{k_1}}x^{\bar{k_2}}=\theta(\bar{k_1})\times\theta(\bar{k_2})$.

θ est surjectif car $G=\{x^k : k\in\mathbb{Z}\}$ donc pour tout $y\in G$, il existe $k\in\mathbb{Z}$ tel que $y=x^k$ donc tel que $y=x^{\bar{k}}$ (car $x^{\bar{k}}=x^k$).

θ est injectif car $\theta(k_1)=\theta(k_2)\Leftrightarrow x^{k_1}=x^{k_2}\Leftrightarrow x^{k_1-k_2}=e\Leftrightarrow k_1-k_2$ est divisible par n (car x est d'ordre n) $\Leftrightarrow \bar{k_1}-\bar{k_2}=0[n]\Leftrightarrow\bar{k_1}=\bar{k_2}[n]$.

$\theta:\mathbb{Z}/n\mathbb{Z}\to G$ étant bijectif, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

☐ **Ce qu'il faut retenir du cours**

1) L'ordre d'un élément x d'un groupe : si pour tout entier $n\geq 1, x^n\neq e$ alors x est d'ordre infini, sinon on appelle ordre de x le plus petit entier $n\geq 1$ tel que $x^n=e$.

2) Qu'un morphisme de groupes bijectif permet de montrer que deux groupes sont isomorphes.

Le théorème chinois

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

Que si $\text{pgcd}(m,n)=1$ alors les groupes $\mathbb{Z}/mn\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ sont isomorphes.

- **L'énoncé**

Soit $\varphi:(\mathbb{Z},+)\to(\mathbb{Z}/m\mathbb{Z},+)\times(\mathbb{Z}/n\mathbb{Z},+)$ définie par $\varphi(x)=([x]_m,[x]_n)$ avec $\text{pgcd}(m,n)=1$.

1) Montrer que φ est un morphisme surjectif de groupes. Qu'en déduire pour $\text{Im}(\varphi)$?

2) Montrer que $\text{Ker}(\varphi)=m\mathbb{Z}\cap n\mathbb{Z}$. En déduire que $\text{Ker}(\varphi)=mn\mathbb{Z}$.

3) En utilisant le théorème suivant : « soit $\varphi:E\to F$ un morphisme de groupes, alors : $\text{Im}(\varphi)$ est isomorphe à $E/\text{Ker}(\varphi)$ », en déduire que $\mathbb{Z}/mn\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ sont isomorphes.

- **Corrigé**

1) $\varphi(a+b)=([a+b]_m,[a+b]_n)=([a]_m+[b]_m,[a]_n+[b]_n)=([a]_m,[a]_n)+([b]_m,[b]_n)=\varphi(a)+\varphi(b)$.

Donc φ est bien un morphisme de groupes. Montrons que φ est surjectif.

Soit $([c]_m,[d]_n)\in(\mathbb{Z}/m\mathbb{Z},+)\times(\mathbb{Z}/n\mathbb{Z},+)$. Comme $\text{pgcd}(m,n)=1$, il existe $a,b\in\mathbb{Z}$ tels que $am+bn=1$ (Bézout). Donc $\begin{cases}amc+bnc=c\\amd+bnd=d\end{cases}$ soit $\begin{cases}[bnc]_m=[c]_m\\[amd]_n=[d]_n\end{cases}$. Donc $\begin{cases}[bnc+amd]_m=[c]_m\\[bnc+amd]_n=[d]_n\end{cases}$.

Ainsi $\exists\, z\in\mathbb{Z}$ (à savoir $z=bnc+amd$) tel que $\varphi(z)=([c]_m,[d]_n)$, donc φ est surjectif.

Conclusion : $\text{Im}(\varphi)=(\mathbb{Z}/m\mathbb{Z},+)\times(\mathbb{Z}/n\mathbb{Z},+)$ (espace d'arrivée du morphisme φ).

2) On a $m\mathbb{Z}\cap n\mathbb{Z}=\text{Ker}(\varphi)$. En effet : $x\in m\mathbb{Z}\cap n\mathbb{Z}$ équivaut à « $\exists$ k, k' tels que $x=km=k'n$ ».

$\Leftrightarrow [x]_m=[0]_m$ et $[x]_n=[0]_n \Leftrightarrow \varphi(x)=([0]_m,[0]_n)=0_{(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})} \Leftrightarrow x\in\text{Ker}(\varphi)$.

Comme $\text{pgcd}(m,n)=1$, $m\mathbb{Z}\cap n\mathbb{Z}=mn\mathbb{Z}$. En effet, $mn\mathbb{Z}\subset m\mathbb{Z}\cap n\mathbb{Z}$ (car tout multiple de mn est multiple de m et de n). $m\mathbb{Z}\cap n\mathbb{Z}\subset mn\mathbb{Z}$ car si $x\in m\mathbb{Z}\cap n\mathbb{Z}$, il existe k et k' tels que $x=km=k'n$, donc m divise $k'n$ mais comme $\text{pgcd}(m,n)=1$, d'après Gauss, m divise k', donc il existe j tel que $k'=jm$, ce qui donne $x=jmn$ donc $x\in mn\mathbb{Z}$, ce qui prouve que $m\mathbb{Z}\cap n\mathbb{Z}\subset mn\mathbb{Z}$.

3) Comme $\text{Im}(\varphi)$ est isomorphe à $E/\text{Ker}(\varphi)$ où $E=\mathbb{Z}$ est l'ensemble de départ du morphisme φ et que $\text{Ker}(\varphi)=mn\mathbb{Z}$, on en déduit que $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$.

☐ **Ce qu'il faut retenir du cours**

1) $\varphi:(E,*)\to(F,\circ)$ est un morphisme de groupes équivaut à $\varphi(a*b)=\varphi(a)\circ\varphi(b)$.

2) Théorème de Bézout : $\text{pgcd}(m,n)=1 \Leftrightarrow \exists a,b\in\mathbb{Z} : am+bn=1$.

3) Théorème de Gauss : Si n divise ab et que n et a sont premiers entre eux alors n divise b.

Caractérisation des groupes finis

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

Qu'un groupe est fini si et seulement s'il a un nombre fini de sous-groupes.

- **L'énoncé**

1) Soit G un groupe fini, montrer qu'il a un nombre fini de sous-groupes.
2) Soit G un groupe qui admet un nombre fini de sous-groupes, montrer que G est fini.
3) Que peut-on en déduire ?

- **Corrigé**

1) Si G est fini alors l'ensemble de ses sous-groupes est inclus dans l'ensemble des parties de G. Comme G est de cardinal fini, l'ensemble de ses sous-parties également et donc l'ensemble de ses sous-groupes également.

2) Soit G un groupe qui admet un nombre fini de sous-groupes, alors les sous-groupes monogènes $\langle x \rangle$, pour $x \in G$ sont eux aussi en nombre fini.

Comme $G = \bigcup_{x \in G} \langle x \rangle$, on a aussi $G = \bigcup_{i=1}^{n} \langle x_i \rangle$ (où n est un nombre fini).

Supposons que l'un des sous-groupes monogènes $\langle x_i \rangle$ soit infini. Comme il est monogène, il serait isomorphe à $\mathbb{Z}$ (voir exercice « à quoi est isomorphe un groupe monogène ?»).
Or $\mathbb{Z}$ possède une infinité de sous-groupes (tous de la forme $n\mathbb{Z}$). CONTRADICTION !

Donc $G = \bigcup_{i=1}^{n} \langle x_i \rangle$ est fini comme union finie de sous-groupes finis.

3) On en déduit l'équivalence : G est un groupe fini $\Leftrightarrow$ G possède un nombre fini de sous-groupes.

☐ **Ce qu'il faut retenir du cours**

1) Tout groupe monogène est soit isomorphe à $\mathbb{Z}$ (s'il est infini), soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (s'il est fini d'ordre n).
2) $\mathbb{Z}$ possède une infinité de sous-groupes (tous de la forme $n\mathbb{Z}$).

Groupe $GL_2(\mathbb{Z})$

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**

L'équivalence : $M \in GL_2(\mathbb{Z}) \Leftrightarrow \det(M) = \pm 1$.

- **L'énoncé**

Soit $GL_2(\mathbb{Z})$ le groupe des matrices à coefficients dans $\mathbb{Z}$ inversibles dans l'ensemble des matrices à coefficients dans $\mathbb{Z}$. Montrer que pour toute matrice M à coefficients dans $\mathbb{Z}$, on a l'équivalence : $M \in GL_2(\mathbb{Z}) \Leftrightarrow \det(M) = \pm 1$.

- **Corrigé**

Montrons $M \in GL_2(\mathbb{Z}) \Rightarrow \det(M) = \pm 1$.

Soit $M \in GL_2(\mathbb{Z})$ alors $1 = \det(Id) = \det\left(MM^{-1}\right) = \det(M)\det\left(M^{-1}\right)$.

Or $M \in GL_2(\mathbb{Z})$ donc $\det(M) \in \mathbb{Z}$ et $M^{-1} \in GL_2(\mathbb{Z})$ donc $\det\left(M^{-1}\right) \in \mathbb{Z}$.

Ainsi $\det(M)\det\left(M^{-1}\right) = 1$ équivaut à $\begin{cases} \det(M) = 1 \\ \det\left(M^{-1}\right) = 1 \end{cases}$ ou $\begin{cases} \det(M) = -1 \\ \det\left(M^{-1}\right) = -1 \end{cases}$. D'où $\det(M) = \pm 1$.

Montrons $\det(M) = \pm 1 \Rightarrow M \in GL_2(\mathbb{Z})$.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $\det(M) = \pm 1$, a, b, c et d dans $\mathbb{Z}$. Comme $\det(M) \neq 0$, M est inversible.

Comme $M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, on a $M^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Comme a, b, c et d sont dans $\mathbb{Z}$, $M^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est à coefficient dans $\mathbb{Z}$. Donc $M \in GL_2(\mathbb{Z})$.

On a donc bien pour toute matrice M à coefficients dans $\mathbb{Z}$, l'équivalence :
$M \in GL_2(\mathbb{Z}) \Leftrightarrow \det(M) = \pm 1$.

☐ **Ce qu'il faut retenir du cours**

1) Si $M \in M_2(\mathbb{Z})$ alors $\det(M) \in \mathbb{Z}$ (car si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{Z}$ on a $\det(M) = ad - bc \in \mathbb{Z}$).

2) Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alors $M^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Le théorème de Lagrange

Chapitre concerné : 1. Structures algébriques

☐ **Ce que montre cet exo**
Que si G est un groupe fini et H un sous-groupe de G alors l'ordre de H divise l'ordre de G.

- **L'énoncé**

Soit $(G,\cdot)$ un groupe fini et soit H un sous-groupe de G.

1) On considère la relation binaire sur G définie par : $aRb \Leftrightarrow b^{-1}a \in H$. Montrer que R est une relation d'équivalence.

2) Soit $[a]_R = \{x \in G : xRa\}$ une classe d'équivalence. En considérant $\varphi : H \to [a]_R$ définie par $\varphi(x) = ax$, montrer que $[a]_R$ a pour cardinal ordre(H).

3) On rappelle qu'une relation d'équivalence sur G détermine une partition de G. En déduire le théorème de Lagrange (1736-1813), à savoir que l'ordre de H divise l'ordre de G.

- **Corrigé**

1) R est réflexive car $a^{-1}a = e \in H$ (donc on a aRa).

R est symétrique car si aRb alors $b^{-1}a \in H$ et donc $(b^{-1}a)^{-1} \in H$ soit $a^{-1}b \in H$ soit bRa.

R est transitive car si aRb et bRc alors $b^{-1}a, c^{-1}b \in H$ donc $c^{-1}bb^{-1}a = c^{-1}a \in H$ soit aRc.
Ainsi, R est bien une relation d'équivalence.

2) Considérons $\varphi : H \to [a]_R$ définie par $\varphi(x) = ax$. φ est bien à valeurs dans $[a]_R$ car pour tout $x \in H$, $\varphi(x) \in [a]_R$. En effet on a $\varphi(x)Ra$ car $a^{-1}\varphi(x) = a^{-1}ax = x$ et que $x \in H$.

φ est surjective par définition de $[a]_R$. En effet, soit $y \in [a]_R$ alors on a yRa donc $a^{-1}y \in H$ donc il existe $h \in H$ tel que $a^{-1}y = h$ ce qui donne $y = ah$ c'est-à-dire $y = \varphi(h)$.

φ est injective car $\varphi(x_1) = \varphi(x_2) \Leftrightarrow ax_1 = ax_2 \Leftrightarrow a^{-1}ax_1 = a^{-1}ax_2 \Leftrightarrow x_1 = x_2$.

φ étant bijective, $[a]_R$ et H sont isomorphes et donc $[a]_R$ a pour cardinal ordre(H).

3) Les classes $[a]_R$ forment une partition de G et sont toutes de cardinal ordre(H). Cela signifie que l'ordre de G est un multiple de ordre(H). Ainsi l'ordre de H divise l'ordre de G.

☐ **Ce qu'il faut retenir du cours**
1) L'ordre d'un sous-groupe est égal à son nombre d'éléments.
2) Une relation d'équivalence sur G détermine, grâce à ses classes d'équivalence, une partition de G.