Licence MPCI, 2e année
Algèbre Générale

Devoir Maison
A rendre pour le Jeudi 7 Mars

Les deux exercices sont indépendants. On apportera un soin particulier à la présentation et à la rédaction.

Exercice 1 (Un groupe de matrices)**.**

Soit l'ensemble suivant

$$\mathcal{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \text{ et } (a,b) \neq (0,0) \right\}$$

(1) Montrer que $\mathcal{C}$ est un sous-groupe abélien de $\mathrm{GL}_2(\mathbb{R})$. (Pour la multiplication des matrices)

> (a) Si $M \in \mathcal{C}$, alors $\det(M) = a^2 + b^2 \neq 0$ donc $M \in \mathrm{GL}_2(\mathbb{R})$.
>
> (b) $I_2 = \begin{pmatrix} 1 & 0 \\ -0 & 1 \end{pmatrix}$ est dans $\mathcal{C}$.
>
> (c) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ab' + ba') & aa' - bb' \end{pmatrix} \in \mathcal{C}$.
>
> (d) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ -(-b) & a \end{pmatrix} \in \mathcal{C}$
> Donc $\mathcal{C}$ est bien un groupe.
>
> (e) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ab' + ba') & aa' - bb' \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$
> Le groupe est bien abélien.

(2) Soit $\mathcal{U} = \{M \in \mathcal{C} \mid \det(M) = 1\}$. Justifier que $\mathcal{U}$ est un sous-groupe de $\mathcal{C}$.

> La restriction du déterminant est un morphisme de $\mathcal{C}$ dans $\mathbb{R}$. Et $\mathcal{U} = \mathrm{Ker}(\det)$. Donc $\mathcal{U}$ est un sous-groupe de $\mathcal{C}$.

(3) Soit $P : \mathcal{C} \to \mathcal{C}$ l'application définie par $P(M) = MM^\top$, où $M^\top$ désigne la transposée de M. Montrer que P est un morphisme et déterminer son noyau et son image.

> Soient $M, N \in \mathcal{C}$. On vérifie facilement que si $M \in \mathcal{C}$ alors $M^\top \in \mathcal{C}$ donc que P est bien à valeurs dans $\mathcal{C}$. On a
>
> $$P(MN) = (MN)(MN)^\top = MNN^\top M^\top = (MM^\top)(NN^\top) = P(M)P(N)$$
>
> (Rq : On a utilisé le fait que $\mathcal{C}$ est abélien dans l'avant-dernière étape). P est donc bien un morphisme.
> Soit $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alors $P(M) = (a^2 + b^2)I_2$. On en déduit que $M \in \mathrm{Ker}(P) \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow \det(M) = 1$. Donc $\mathrm{Ker}(P) = \mathcal{U}$.
> De même on en déduit que $\mathrm{Im(P)} \subset \{\lambda \mathrm{I}_2, \lambda \in \mathbb{R}^{+*}\}$. Et on montre l'égalité en notant que $\forall \lambda \in \mathbb{R}^{+*}, P(\sqrt{\lambda} I_2) = \lambda I^2$. Donc $\lambda I_2 \in \mathrm{Im(P)}$.

(4) Montrer que pour tout $x \in \mathcal{C}$, si x est d'ordre fini, alors $x \in \mathcal{U}$.

Soit $x \in \mathcal{C}$ d'ordre fini que l'on note n, avec $n \geq 1$. On a $x^n = I_2$. On en déduit que $\det(x^n) = 1 = (\det(x))^n$. Comme $\det(x) > 0$ on en déduit que $\det(x) = 1$.
Donc $x \in \mathcal{U}$.

(5) Pour tout $\theta \in \mathbb{R}$, on définit la matrice $R_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$. Montrer que l'application $\phi : \theta \mapsto R_\theta$ est un morphisme de $\mathbb{R}$ dans $\mathcal{C}$. Déterminer son noyau et son image.

On a

$$\begin{aligned}\phi(\theta+\theta') &= \begin{pmatrix} \cos(\theta+\theta') & \sin(\theta+\theta') \\ -\sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix} = \\ &= \begin{pmatrix} \cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta') & \sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta') \\ -(\sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta')) & \cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta') \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} \cos(\theta') & \sin(\theta') \\ -\sin(\theta') & \cos(\theta') \end{pmatrix} = \phi(\theta)\phi(\theta')\end{aligned}$$

$$\mathrm{Ker}\phi = \{\theta \in \mathbb{R} \mid \cos(\theta) = 1, \sin(\theta) = 0\} = 2\pi\mathbb{Z}$$

On montre maintenant que $\mathrm{Im}(\phi) = \mathcal{U}$. En effet, pour tout $\theta \in \mathbb{R}$, on a $\det(R_\theta) = \cos^2(\theta)+\sin^2(\theta) = 1$. Réciproquement, si $M \in \mathcal{U}$, alors $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $a^2+b^2 = 1$. Donc il existe $\theta \in \mathbb{R}$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$.

(6) Soit H un sous-groupe **d'ordre fini** de $\mathcal{C}$. Montrer que $H < \mathcal{U}$.

D'après le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe. Donc tous les éléments d'un groupe fini sont d'ordre fini. Donc tous les éléments de H sont d'ordre fini, et donc $H < \mathcal{U}$.

(7) Soit G la préimage de H par le morphisme ϕ, c'est à dire $G = \phi^{-1}(H)$. Montrer que $G \cap \mathbb{R}^{+*}$ est non-vide et admet un minimum.

En déduire que G est un groupe monogène, puis que H est un groupe cyclique.

C'était clairement la question la plus dure du DM.
Notons $E = G \cap \mathbb{R}^{+*}$.
Pour commencer, E est non-vide car il contient 2π. En effet, $\phi(2\pi) = I_2 \in H$. Donc E est une partie de $\mathbb{R}$ non-vide et minorée, donc E admet une borne inférieure notée θ_0.
Montrons maintenant que cette borne inférieure est atteinte, c'est à dire que $\theta_0 \in E$.
Supposons que cette borne inférieure n'est pas atteinte. Alors il existe une suite de réels distincts $\theta_n \in E$ qui converge vers θ_0. A partir d'un certain rang, tous les θ_n sont dans $]\theta_0, \theta_0+\pi[$ ce qui prouve que les éléments R_{θ_n} sont également distincts. Or les R_{θ_n} sont dans H donc on a donc trouvé une infinité d'élements distincts dans H, ce qui contredit le fait que H est fini. Donc la borne inférieure est atteinte, et donc E admet bien un minimum.
Pour la deuxième partie on montre que G est engendré par θ_0. Comme $\theta_0 \in E \subset G$, on en déduit que $\langle\theta_0\rangle$ est un sous-groupe de G.
Réciproquement, si $x \in G$. On peut écrire $x = \theta_0 q + r$ où $0 \leq r < \theta_0$. (c'est la "division euclidienne" de x par θ_0). Alors $r = x - \theta_0 q$ est un élément de G car x et θ_0 sont dans G qui est un sous-groupe. Et $0 \leq r < \theta_0$, donc par minimalité de θ_0 on en déduit que $r = 0$ et donc $x = \theta_0 q$, donc $x \in \theta_0\mathbb{Z}$.
Donc G est monogène. Si $M \in H$, alors il existe $\theta \in G$ tel que $M = R_\theta$. Or $\theta = n\theta_0$ pour un certain n. Donc $M = \phi(n\theta_0) = (\phi\theta_0)^n = R_{\theta_0}^n$. Cela prouve que tout élément de M est dans $\langle R_{\theta_0}\rangle$. Donc H est monogène et fini, donc H est cyclique.

(8) Le groupe $\mathcal{C}$ est isomorphe à un groupe bien connu. Déterminer ce groupe et exhibez un isomorphisme de $\mathcal{C}$ vers ce groupe. (Cette question est indépendente du reste de l'exercice)

Le groupe $\mathcal{C}$ est isomorphe à $\mathbb{C}^*$. On peut écrire une application

$$\begin{aligned} \Phi : \mathbb{C}^* &\longrightarrow \mathcal{C} \\ z = a + ib &\longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{aligned}$$

On vérifie facilement que c'est un morphisme car les formules du produit de deux matrices de $\mathcal{C}$ donnent la partie réelle et la partie imaginaire d'un produit de deux nombres complexes.

$$\mathrm{Ker}(\phi) = \{a + ib\, a = 1, b = 0\} = \{1\}$$

Et l'application est clairement surjective. donc Φ est un isomorphisme.
Remarque : Le déterminant correspond à $|z|^2$ l'application P correspond à $z \mapsto z\overline{z}$. Le sous-groupe $\mathcal{U}$ correspond au sous-groupe $\mathbb{U} < \mathbb{C}$.

Exercice 2 (Sous-groupes distingués)**.**

Soit G un groupe.

Définition. *Soit H un sous-ensemble de G. On dit que H est un* sous-groupe distingué *dans G (et on note cette propriété $H \triangleleft G$) si H est un sous-groupe de G, et que la condition suivante est vérifiée :*

$$\forall h \in H, \forall x \in G, xhx^{-1} \in H$$

Le but de l'exercice est de se familiariser avec ces sous-groupes et de voir pourquoi ils permettent de définir une loi de groupe sur G/H.

(1) On commence par un exemple. Dans le groupe $\mathrm{GL}(2, \mathbb{R})$, on considère les deux sous-ensembles :

$$\mathcal{E} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbb{R}^* \right\} \qquad \mathcal{D} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{R}^* \right\}$$

Montrer que $\mathcal{E}$ et $\mathcal{D}$ sont des sous-groupes. Puis montrer que $\mathcal{E}$ est distingué dans $\mathrm{GL}(2, \mathbb{R})$, mais que $\mathcal{D}$ n'est pas distingué dans $\mathrm{GL}(2, \mathbb{R})$.

— Soit $E = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathcal{E}$ alors $E = aI_2$. Donc pour tout $M \in \mathrm{GL}(2, \mathbb{R})$, on a

$$MEM^{-1} = M(aI_2)M^{-1} = aMI_2M^{-1} = aI_2 \in \mathcal{E}$$

Donc $\mathcal{E}$ est distingué.

— Il suffit de trouver un "contre-exemple" à la propriété. On choisit $D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors on a

$$MDM^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \notin \mathcal{D}$$

Donc $\mathcal{D}$ n'est pas distingué.

(2) Montrer que si G est commutatif et $H < G$, alors $H \triangleleft G$.

Soit $h \in H$ et $x \in G$. Alors $xhx^{-1} = xx^{-1}h = h \in H$ car G est commutatif. Donc $H \triangleleft G$.

(3) Montrer que le centre $Z(G)$ est un sous-groupe distingué de G.

$Z(G) = \{h \in G, \forall x \in G, xh = hx\}$. Soit $h \in Z(G)$ et $x \in G$. Alors $xhx^{-1} = hxx^{-1} = h \in Z(G)$. Donc $Z(G) \triangleleft G$.

(4) Soit G' un autre groupe, et $f \in \mathrm{Hom}(G, G')$. Montrer que $\mathrm{Ker} f$ est un sous-groupe distingué dans G.

Soit $h \in \mathrm{Ker}(f)$ et $x \in G$. On a

$$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)e'(f(x))^{-1} = f(x)(f(x))^{-1} = e_H$$

Donc $xhx^{-1} \in \mathrm{Ker}(f)$. On en déduit que $\mathrm{Ker}(f) \triangleleft G$.

(5) Est-ce que l'image Im(f) est un sous-groupe distingué de G' ? (Justifier votre réponse)

On utilise notre exemple de la question 1 et on trouve un morphisme tel que $\mathrm{Im(f)} = \mathcal{D}$. On définit

$$\begin{aligned} f : \mathbb{R}^* \times \mathbb{R}^* &\longrightarrow \mathrm{GL}(2, \mathbb{R}) \\ (a, b) &\longmapsto \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \end{aligned}$$

La loi de $\mathbb{R}^* \times \mathbb{R}^*$ étant la loi produit $(a, b)(a', b') = (aa', bb')$. On voit directement que f est un morphisme dont l'image est $\mathcal{D}$.

(6) Pour le reste de l'exercice, on suppose que H est un sous-groupe distingué de G. Soient $x, x', y, y' \in G$. Montrer que :

$$\text{Si } x \underset{H}{\sim} x' \ \text{ et } \ y \underset{H}{\sim} y', \ \text{ alors on a } \ (xy) \underset{H}{\sim} (x'y')$$

(La relation $\underset{H}{\sim}$ est la relation d'équivalence définie à partir de H)

On pose $h_x = x^{-1}x'$ et $h_y = y^{-1}y$. Comme $x \underset{H}{\sim} x'$ et $y \underset{H}{\sim} y'$, on en déduit que h_x et h_y sont dans H. Alors

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = y^{-1}h_x(yy^{-1})y'{-}1 = (y^{-1}h_xy)h_y$$

Comme H est distingué, on en déduit que $y^{-1}h_xy \in H$. Donc $(xy)^{-1}x'y' \in H$, et donc $(xy) \underset{H}{\sim} (x'y')$.

(7) Justifier que la loi de composition interne, :

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (xH, yH) &\longmapsto (xy)H \end{aligned}$$

est bien définie. (On dit qu'une application sur un ensemble quotient est bien définie si elle ne dépend pas du représentant choisi)

Si $xH = x'H$ alors $x \underset{H}{\sim} x'$. Donc d'après la question précédente, si $x'H = xH$ et $y'H = yH$ alors $xyH = x'y'H$. Donc le produit défini ne dépend pas de la façon de l'écrire, mais bien de la classe elle-même.

(8) Montrer que G/H, muni de cette loi, est un groupe. En déduire que l'application $\pi : G \longrightarrow G/H$ définie par $\pi(x) \longmapsto xH$ est un morphisme surjectif dont le noyau est H.

On définit une nouvelle loi, donc il faut montrer les trois axiomes.

— Associativité. Soient $xH, yH, zH \in G/H$.

$$((xH)(yH))zH = ((xy)H)zH = ((xy)z)H = (x(yz))H = (xH)((yz)H) = (xH)((yH)(zH))$$

— La classe eH est élément neutre

$$(eH)(xH) = (ex)H = xH = (xe)H = (xH)(eH)$$

— Tout élément xH a un inverse $(x^{-1})H$

$$(xH)(x^{-1}H) = (xx^{-1})H = eH = (x^{-1}x)H = (x^{-1}H)(xH)$$

Soient $x, y \in G$. On a $\pi(xy) = (xy)H = (xH)(yH) = \pi(x)\pi(y)$. Donc π est un morphisme. Ce morphisme est surjectif par définition de $G/H = \{xH, x \in G\}$. Enfin, si

$$x \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(x) = eH = xH \Leftrightarrow e^{-1}x \in H \Leftrightarrow x \in H$$

Donc $\mathrm{Ker}(\pi) = H$.