Université de Bourgogne Mardi 26 mars 2019
Licence 3 Mathématiques 8h-10h

Examen Partiel d'Algèbre 2

Exercice 1 (Questions de cours)

1. Soit G un groupe fini et H un sous-groupe de G. Énoncer et démontrer le théorème de Lagrange.
2. On note G/H l'ensemble des classes à gauche modulo H. Donner une condition nécessaire et suffisante sur H pour que la structure de groupe de G induise une structure de groupe sur le quotient G/H. Démontrer votre affirmation.
3. Démontrer que le centre $Z(G)$ d'un groupe G est un sous-groupe distingué de G.

Réponse.

1. Le théorème de Lagrange nous dit que pour un groupe fini G, l'ordre $|H|$ de H divise l'ordre $|G|$ de G.
Plus précisément, la relation « modulo H à gauche » définie par :
$$(x \mathcal{R} y) \iff (x^{-1}y \in H) \iff (y \in xH)$$
est une relation d'équivalence et le cardinal $\mathrm{card}(G/H)$ de l'ensemble G/H des classes d'équivalence (dites classes à gauche modulo H) satisfait :
$$|G| = \mathrm{card}(G/H) \times |H|.$$
On note alors $[G : H]$ le nombre entier $\mathrm{card}(G/H) = \frac{|G|}{|H|}$ et on l'appelle l'indice de H dans G.
Démonstration.
La relation $\mathcal{R}$ est une relation d'équivalence :
— l'élément neutre 1_G de G est dans H, donc la relation est réflexive ;
— H est stable par passage à l'inverse : $\forall x, y \in G \quad (x^{-1}y \in H) \implies (y^{-1}x \in H)$ donc $\mathcal{R}$ est symétrique ;
— H est stable par produit : $\forall x, y, z \in G \quad (x^{-1}y \in H \text{ et } y^{-1}z \in H) \implies (x^{-1}z \in H)$ donc $\mathcal{R}$ est transitive.
Les classes d'équivalence forment une partition de G, sont de la forme $xH = \{xy : y \in H\}$ pour $x \in G$, et sont toutes en bijection avec H : les applications de multiplication à gauche par x et x^{-1}
$$g_x : \begin{array}{ccc} G & \longrightarrow & G \\ y & \longmapsto & g_x(y) = xy \end{array} \quad \text{et} \quad g_{x^{-1}} : \begin{array}{ccc} G & \longrightarrow & G \\ y & \longmapsto & g_{x^{-1}}(y) = x^{-1}y \end{array}$$
sont inverses l'une de l'autre donc bijectives et g_x envoie H sur xH. Par conséquent, toutes les classes à gauche ont le cardinal $|H|$ de H et ainsi, si G est fini, $|G| = \mathrm{card}(G/H) \times |H|$.
Remarque : on peut remplacer la la relation « modulo H à gauche » par la relation « modulo H à droite ». On a alors une bijection entre les classes à gauches et les classes à droite.
2. Pour que la structure de groupe de G induise une structure de groupe sur le quotient G/H, il faut et il suffit que H soit un sous-groupe distingué de G.
Démonstration.
Remarquons au préalable que pour tout $h \in H$, $hH = H$ et que $HH = \{hh' : h, h' \in H\} = H$.
— Supposons que G induise une structure de groupe sur le quotient G/H. Soient $x, y \in G$. Alors $xHyH = zH$ pour un $z \in G$. On doit donc avoir $xyh = z$ pour un certain $h \in H$ et donc $xHyH = xyhH = xyH$. Mais ceci implique en particulier, pour tout $x \in G$, que $xHx^{-1}H = xx^{-1}H = H$, c'est à dire $xHx^{-1} = H$. Donc H doit-être un sous-groupe distingué de G.
— Réciproquement, si H est un sous-groupe distingué de G, pour tous $x, y \in G$, $xHyH = xy(y^{-1}Hy)H = xyH$ donc le produit de deux classes à gauche est une classe à gauche. Il est immédiat de voir que ce produit est associatif en raison de l'associativité du produit dans G, que H est élément neutre et que l'inverse de xH est $x^{-1}H$. Donc G induit une structure de groupe sur le quotient G/H.
3. Le centre $Z(G) = \{z \in G : \forall x \in G \; zx = xz\}$ est bien un sous-groupe de G :
— $1_G \in Z(G)$, car 1_G commute avec tous les éléments de G ;
— si $z_1, z_2 \in Z(G)$ alors pour tout $x \in G \quad (z_1z_2)x = z_1xz_2 = x(z_1z_2)$ donc $z_1z_2 \in Z(G)$;
— si $z \in Z(G)$ alors pour tout $x \in G \quad z^{-1}x = (x^{-1}z)^{-1} = (zx^{-1})^{-1} = xz^{-1}$ donc $z^{-1} \in Z(G)$.
Soit $z \in Z(G)$. Pour tout $x \in G$, $xz = zx$ donc $xzx^{-1} = z \in Z(G)$. Ainsi $Z(G)$ est un sous-groupe distingué de G.

Exercice 2 (Petites questions indépendantes vue en TD)

1. Montrer que tout groupe d'ordre p premier est un groupe cyclique.
2. Soit G un groupe tel que tout élément différent de 1_G est d'ordre 2. Démontrer que G est abélien.
3. Soient G un groupe et H un sous groupe de G d'indice 2. Démontrer que H est distingué dans G.
4. Soit G un groupe d'ordre $2n$. Montrer qu'il a un élément d'ordre 2.

Réponse.

1. Soit G un groupe d'ordre p premier et $a \in G \setminus \{1_G\}$. D'après le théorème de Lagrange, l'ordre du sous-groupe $< a >= \{a^n : n \in \mathbb{Z}\}$ engendré par a divise p (et est différent de 1), donc est égal à p. Donc $< a >= G$: il est donc cyclique.
2. Soient $a, b \in G$. Alors $(ab)^2 = 1_G = abab$, et $a^2 = b^2 = 1_G$. D'où $ab = a(abab)b = ba$. Ainsi tous les éléments commutent deux à deux, autrement dit G est abélien.
3. Rappelons qu'un sous-groupe H de G est distingué dans G si et seulement si les classes à gauche modulo H sont aussi les classes à droite. Si H est d'indice 2, alors il y a deux classes à gauche modulo H dont l'une est H, et donc l'autre classe est nécessairement $G \setminus H$. Mais il en est de même pour les classes à droite. Donc H est un sous-groupe distingué de G.
4. Soit G un groupe d'ordre $2n$. Supposons que G ne possède pas d'élément d'ordre 2. Alors pour tout $x \in G \setminus \{1_G\}$ $x \neq x^{-1}$. On peut donc partitionner $G \setminus \{1_G\}$ en paires $\{x, x^{-1}\}$ ce qui implique que $|G| - 1 = 2n - 1$ est pair, d'où une contradiction. Donc G possède au moins un élément d'ordre 2 (et même un nombre impair d'éléments d'ordre 2).

Exercice 3 (Normalisateur)
Soit G un groupe et H un sous-groupe de G. On appelle normalisateur de H dans G et on le note $\mathcal{N}(H)$ l'ensemble

$$\mathcal{N}(H) = \{x \in G : xHx^{-1} = H\}.$$

1. Montrer que $\mathcal{N}(H)$ est un sous-groupe de G contenant H.
2. Montrer que H est un sous-groupe distingué de $\mathcal{N}(H)$. Que peut-on dire de H si $\mathcal{N}(H) = G$?
3. Montrer que $Z(G) \subset \mathcal{N}(H)$.
4. Soit K un sous-groupe de G qui contient H et tel que H est distingué dans K. Montrer que $K \subset \mathcal{N}(H)$ et en déduire que $\mathcal{N}(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.

Réponse.

1. $1_G \in \mathcal{N}(H)$, et si $x, y \in \mathcal{N}(H)$,

$$\left(xHx^{-1} = H \text{ et } yHy^{-1} = H\right) \implies \left(xyH(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1}\right)$$

$$\left(xHx^{-1} = H\right) \implies \left(x^{-1}Hx = H\right)$$

   donc xy et x^{-1} sont dans H donc $\mathcal{N}(H)$ est un sous-groupe de G. De plus, si $h \in H$, $hHh^{-1} = H$ donc $H \subset \mathcal{N}(H)$.
2. Par définition, pour tout $x \in \mathcal{N}(H)$, on a $xHx^{-1} = H$ donc H est distingué dans $\mathcal{N}(H)$. Évidemment, $N(H) = G$ si et seulement si H est distingué dans G.
3. Si $x \in Z(G)$ alors pour tout $h \in H$, $xhx^{-1} = h$ donc $xHx^{-1} = H$ et donc $x \in Z(G)$. Ainsi $Z(G) \subset \mathcal{N}(H)$.
4. Si H est un sous-groupe distingué de K, alors pour tout $x \in K$, $xHx^{-1} = H$, donc $x \in \mathcal{N}(H)$. Par conséquent, $K \subset \mathcal{N}(H)$. Ainsi $\mathcal{N}(H)$ contient tous les sous-groupes de G qui contiennent H et dans lesquels H est distingué, et $\mathcal{N}(H)$ vérifie lui même cette propriété. Donc c'est le plus grand sous-groupe de G dans lequel H est distingué.

Exercice 4 (Un drôle d'automorphisme)
Soit G un groupe. On suppose qu'il existe un entier $n \geq 2$ tel que l'application $f : G \to G$ définie pour $x \in G$ par $f(x) = x^n$ est un automorphisme de G.

1. Montrer que pour tous x, y dans G, il existe un unique $z \in G$ tel que $y = xz^n$.
2. Montrer alors que $x^{n-1}y = x(zx)^n x^{-1}$.
3. En déduire que pour tout $x \in G$ on a $x^{n-1} \in Z(G)$.

Réponse.

1. f est un automorphisme donc est surjectif. Soient x, y dans G. Alors il existe $z \in G$ tel que $\varphi(z) = z^n = x^{-1}y$, c'est à dire $y = xz^n$.
2. Comme φ est un homomorphisme
$$x^{n-1}y = x^n z^n = \varphi(x)\varphi(z) = \varphi(xz) = (xz)^n = xz(xz)^{n-2}xz = x(zx)^{n-1}z = x(zx)^{n-1}zxx^{-1} = x(zx)^n x^{-1}.$$
3. On a $x^{n-1}y = x(zx)^n x^{-1} = x\varphi(zx)x^{-1} = x\varphi(z)\varphi(x)x^{-1} = xz^n x^{n-1} = yx^{n-1}$. Or x et y sont choisis arbitrairement donc pour tout $x \in G$, $x^{n-1} \in Z(G)$.

Exercice 5 (Groupe de matrices)
On considère $\mathcal{G}$ le sous-ensemble de $\mathrm{GL}_3(\mathbb{R})$ donné par
$$\mathcal{G} = \left\{ \begin{pmatrix} a & b & c \\ 0 & a^{-1} & d \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbb{R}^*,\ b, c, d \in \mathbb{R} \right\}$$
et $\mathcal{H}$ et $\mathcal{K}$ les sous-ensembles de $\mathcal{G}$ définis par
$$\mathcal{H} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbb{R}^* \right\} \qquad \mathcal{K} = \left\{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix} : b, c, d \in \mathbb{R} \right\}.$$
1. Montrer que $\mathcal{G}$ est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$;
2. Montrer que $\mathcal{H}$ et $\mathcal{K}$ sont deux sous-groupes de $\mathcal{G}$ et que $\mathcal{HK} = \mathcal{G}$.
3. Calculer ABA^{-1} et $ABA^{-1}B^{-1}$ pour $A \in \mathcal{H}$ et $B \in \mathcal{K}$.
4. En déduire que
   (a) $\mathcal{K}$ est distingué dans $\mathcal{G}$;
   (b) $\mathcal{K}$ est un sous-groupe du groupe dérivé $D(\mathcal{G})$ de $\mathcal{G}$.
5. Montrer que le groupe quotient $\mathcal{G}/\mathcal{K}$ est abélien, isomorphe à $(\mathbb{R}^*, \times)$.
6. En déduire que $\mathcal{K} = D(\mathcal{G})$.
7. Déterminer le centre de $Z(\mathcal{G})$ de $\mathcal{G}$.

Réponse.
1. Méthode douce. La matrice identité est dans $\mathcal{G}$. Le produit A_1A_2 de deux matrices triangulaires supérieures A_1 et A_2 est une matrice triangulaire supérieure, dont les termes diagonaux sont les produits des termes diagonaux correspondants de A_1 et A_2. Il s'ensuit que que $\mathcal{G}$ est stable par produit. L'inverse A_1^{-1} d'une matrice triangulaire supérieure A_1 est une matrice triangulaire supérieure, dont les termes diagonaux sont les inverses des termes diagonaux de A_1. Il s'ensuit que que $\mathcal{G}$ est stable par inverse, et donc c'est un sous groupe de $\mathcal{G}$.

   Méthode calculatoire. La matrice identité est dans $\mathcal{G}$ et pour (a_1, b_1, c_1, d_1) et (a_2, b_2, c_2, d_2) dans $\mathbb{R}^* \times \mathbb{R}^3$ on a :
$$\begin{pmatrix} a_1 & b_1 & c_1 \\ 0 & a_1^{-1} & d_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 & c_2 \\ 0 & a_2^{-1} & d_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2^{-1} & b_1d_2 + a_1c_2 + c_1 \\ 0 & (a_1a_2)^{-1} & d_2a_1^{-1} + d_1 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{G}$$
   et
$$\begin{pmatrix} a_1 & b_1 & c_1 \\ 0 & a_1^{-1} & d_1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a_1^{-1} & -b_1 & b_1d_1 - c_1a_1^{-1} \\ 0 & a_1 & -a_1d_1 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{G}$$
   Ce qui prouve que $\mathcal{G}$ est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$.
2. L'identité est dans $\mathcal{H}$ et $\mathcal{K}$ et dans les calculs de la question précédente,
   (a) en prenant $b_1 = c_1 = d_1 = b_2 = c_2 = d_2 = 0$, on prouve que $\mathcal{H}$ est un sous groupe de $\mathcal{G}$;
   (b) en prenant $a_1 = a_2 = 1$, on prouve que $\mathcal{K}$ est un sous groupe de $\mathcal{G}$;
   (c) en prenant $a_1 = a \neq 0$, $b_1 = c_1 = d_1 = 0$, $a_2 = 1$, $b_2 = \frac{b}{a}$,$c_2 = \frac{c-bd}{a}$ et $d_2 = ad$, on obtient la matrice
$$\begin{pmatrix} a & b & c \\ 0 & a^{-1} & d \\ 0 & 0 & 1 \end{pmatrix}$$
   ce qui prouve que $\mathcal{HK} = \mathcal{G}$. Autrement dit, $\mathcal{H} \cup \mathcal{K}$ est un système de générateurs de $\mathcal{G}$.

3. Soient $A \in \mathcal{H}$ et $B \in \mathcal{K}$:

$$A = \begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & b & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix}.$$

Alors

$$ABA^{-1} = \begin{pmatrix} 1 & a^2 b & ac \\ 0 & 1 & da^{-1} \\ 0 & 0 & 1 \end{pmatrix} \qquad ABA^{-1}B^{-1} = \begin{pmatrix} 1 & a^2 b - b & -a^2 bd + bd + ac - c \\ 0 & 1 & da^{-1} - d \\ 0 & 0 & 1 \end{pmatrix}$$

4. (a) Comme $\mathcal{H}$ et $\mathcal{K}$ sont des sous-groupes et que $G = HK$, pour montrer que $\mathcal{K} \triangleleft \mathcal{G}$ il suffit de montrer que toute conjuguée d'une matrice de $B \in \mathcal{K}$ par une matrice de $A \in H$ est encore dans $\mathcal{K}$: c'est bien le cas puisque $ABA^{-1} \in \mathcal{H}$.

   (b) Soit $(x, y, z) \in \mathbb{R}^3$. On choisit $a = 2, \quad b = \frac{x}{3}, \quad c = y - 2xz, \quad d = -2z$. Alors

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = ABA^{-1}B^{-1} \in D(\mathcal{G})$$

   Donc $\mathcal{K} \subset D(\mathcal{G})$.

5. Le quotient $\mathcal{G}/\mathcal{K}$ est formé des classes d'équivalence de matrices $A \in \mathcal{H}$: en effet, comme $\mathcal{G} = \mathcal{H}\mathcal{K}$, toute matrice de $\mathcal{G}$ est dans $[A] = A\mathcal{K}$ pour un certain $A \in \mathcal{H}$. On en déduit l'isomorphisme (évidemment bijectif) :

$$\begin{array}{rccc} \Phi : & \mathbb{R}^* & \longrightarrow & \mathcal{G}/\mathcal{K} \\ & a & \longmapsto & \left[\begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \end{array} \qquad \Phi(a_1 \times a_2) = \Phi(a_1)\Phi(a_2)$$

car

$$\left[\begin{pmatrix} a_1 a_2 & 0 & 0 \\ 0 & (a_1 a_2)^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] = \left[\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_1^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & 0 & 0 \\ 0 & a_2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] = \left[\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_1^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \left[\begin{pmatrix} a_2 & 0 & 0 \\ 0 & a_2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right].$$

Donc $\mathcal{G}/\mathcal{K}$ est isomorphe à $(\mathbb{R}^*, \times)$ donc est abélien.

6. Comme $\mathcal{G}/\mathcal{K}$ est abélien, $D(\mathcal{G}) \subset \mathcal{K}$ et donc, avec 4.(b), $D(\mathcal{G}) = \mathcal{K}$.

7. Une matrice du centre $Z(\mathcal{G})$ doit commuter avec toute matrice de $\mathcal{H}$. Fixons $X = \begin{pmatrix} x & y & z \\ 0 & x^{-1} & t \\ 0 & 0 & 1 \end{pmatrix} \in Z(\mathcal{G})$.

Pour tout $a \in \mathbb{R}^*$, X satisfait :

$$\begin{pmatrix} x & y & z \\ 0 & x^{-1} & t \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x & y & z \\ 0 & x^{-1} & t \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} x & a^2 y & az \\ 0 & x^{-1} & ta^{-1} \\ 0 & 0 & 1 \end{pmatrix}$$

Si $a \neq 1$ on a nécessairement $y = z = t = 0$ donc $X \in \mathcal{H}$. Or le calcul de ABA^{-1} de la question 3 nous dit que la seule matrice de $\mathcal{H}$ qui commute avec toutes les matrices de $\mathcal{K}$ est l'identité. Donc $Z(\mathcal{G})$ est réduit à l'identité.