Problème 4

Groupes finis

Ce problème a pour objet l'étude de quelques propriétés des groupes finis avec une attention particulière pour les groupes finis de matrices. La première partie est l'occasion de revoir quelques résultats classiques sur les groupes finis.

Les notions qu'il peut être utile de revoir sont les suivantes :

- ordre d'un élément dans un groupe ;
- classes à gauche suivant un sous-groupe et groupe quotient ;
- groupes cycliques ;
- opération d'un groupe sur un ensemble ;
- groupe symétrique et groupe alterné ;
- réduction des matrices réelles orthogonales ;
- matrices de transvections et de dilatation.

Rappelons quelques unes de ces notions de cours.

Si G est un groupe, pour tout a dans G, on note $\langle a\rangle = \left\{a^k \mid k \in \mathbb{Z}\right\}$ le sous groupe de G engendré par a. Le groupe $\langle a\rangle$ est dit monogène.

Si $\langle a\rangle$ est infini, on dit alors que a est d'ordre infini dans G, sinon on dit que le groupe $\langle a\rangle$ est cyclique, que a est d'ordre fini dans G et l'ordre de a est l'entier $\theta(a) = \operatorname{card}(\langle a\rangle)$.

On a aussi, pour a d'ordre fini dans G :

$$\begin{aligned} m = \theta(a) &= \min\left\{k \in \mathbb{N}^* \mid a^k = 1\right\} \\ \langle a\rangle &= \left\{1, a, \cdots, a^{m-1}\right\} \text{ isomorphe à } \frac{\mathbb{Z}}{m\mathbb{Z}} \\ a^k = 1 &\Leftrightarrow k \text{ multiple de } m \end{aligned}$$

Nous utiliserons quelques résultats de la partie **II** du problème 2, en particulier le théorème de Lagrange, le petit théorème de Fermat et les résultats suivants : tout sous groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K}\setminus\{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique, tout sous-groupe d'un groupe cyclique G d'ordre n est cyclique et pour tout diviseur q de n, il existe un unique sous groupe de G d'ordre q.

Si H est un sous-groupe d'un groupe G, on peut alors considerer l'ensemble quotient G/H des classes à gauche suivant H. Les éléments de G/H sont les classes d'équivalence $\overline{g} = gH$ pour la relation d'équivalence définie par $g \sim h$ si, et seulement si, $g^{-1}h \in H$.

Cet ensemble est muni d'une structure de groupe compatible avec celle de$G$ dans le cas où H est distingué dans G, c'est-à-dire tel que $gH = Hg$ (ou de manière équivalente $g^{-1}Hg = H$) pour tout $g \in G$. Cette loi de groupe est définie par :

$$\overline{g}\overline{h} = \overline{gh}$$

L'opération ainsi définie est valide puisque pour $g' \in \overline{g}$ et $h' \in \overline{h}$, on a $g^{-1}g' \in H$ et $h^{-1}h' \in H$, donc $(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h' = h^{-1}h'g^{-1}g' \in H$ et $g'h' \sim gh$, ce qui signifie que $\overline{gh} = \overline{g'h'}$.

Dans le cas où G est commutatif, tous ses sous-groupes sont distingués et G/H est un groupe.

Si G, G' sont deux groupes et φ un morphisme de groupes de G dans G', alors $\ker(\varphi)$ est distingué. En effet, pour $g \in G$ et $h \in H = \ker(\varphi)$, on a :

$$\varphi\left(g^{-1}hg\right) = \varphi\left(g^{-1}\right)\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1 \cdot \varphi(g) = 1$$

donc $g^{-1}Hg \subset H$ et en écrivant tout $h \in H$ sous la forme :

$$h = g^{-1}\left(ghg^{-1}\right)g$$

avec $ghg^{-1} \in \left(g^{-1}\right)^{-1} Hg^{-1} \subset H$, on déduit que $H \subset g^{-1}Hg$ et l'égalité.

Dans le cas où φ est de plus surjectif, un tel morphisme induit un isomorphisme de groupes de $G/\ker(\varphi)$ sur G' et pour G, G' finis, en en déduit que $\text{card}(G) = \text{card}(\ker(\varphi))\,\text{card}(G')$. Cet argument est parfois utile pour effectuer des raisonements par récurrence.

On rappelle que si G est un groupe et X un ensemble non vide, on dit que G opére à gauche sur X si on a une application :

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

telle que :

$$\begin{cases} \forall x \in X,\ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times X,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$$

Une telle application est aussi appelée action à gauche de G sur X.

Pour tout $x \in X$, on dit que le sous-ensemble de X :

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

est l'orbite de x sous l'action de G.

On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur X ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in X$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de X.

Pour tout $x \in X$, on dit que l'ensemble :

$$G_x = \{g \in G \mid g \cdot x = x\}$$

est le stabilisateur de x sous l'action de G. Ces stabilisateurs sont des sous-groupes de G (en général non distingués).

4.1 Énoncé

Les groupes sont notés multiplicativement et on note 1 l'élément neutre.

Pour ce problème, sauf précision contraire, tous les groupes considérés sont finis avec au moins deux éléments.

Si p, q sont deux entiers relatifs, on note $p \wedge q$ le pgcd de p et q et $p \vee q$ le ppcm de p et q.

– I – Généralités

1. Montrer qu'un groupe est fini si et seulement si l'ensemble de ses sous-groupes est fini.
2. Soit G un groupe commutatif, $p \geq 2$ un entier et $g_1, g_2, \cdots, g_p$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, m_2, \cdots, m_p$. Montrer qu'il existe dans G un élément d'ordre égal au ppcm de ces ordres.
3. Soit $G = \{g_1, g_2, \cdots, g_n\}$ un groupe commutatif fini d'ordre n et :
$$m = \text{ppcm}\left\{\theta\left(g_i\right) \mid 1 \leq i \leq n\right\}.$$
   (a) Montrer que $m = \max\left\{\theta\left(g_i\right) \mid 1 \leq i \leq n\right\}$.
   (b) Montrer que n divise le produit des ordres $\prod_{i=1}^{n} \theta\left(g_i\right)$.
   (c) Montrer que m a les mêmes facteurs premiers que n.
4. On désigne par φ la fonction indicatrice d'Euler. Montrer que si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique. Réciproquement, on peut montrer que la réciproque est vrai, c'est-à-dire qu'un entier $n \geq 2$ est premier avec $\varphi(n)$, si, et seulement si, tout groupe commutatif d'ordre n est cyclique.
5. Soit G un groupe tel que tout élément de G soit d'ordre au plus égal à 2.
   (a) Montrer que G est commutatif.
   (b) On suppose de plus que G est fini. Montrer que $\text{card}\,(G) = 2^n$.
6. Soit G est un groupe, non nécessairement fini, opérant sur un ensemble X. On note, pour tout $x \in X$:
$$G \cdot x = \{g \cdot x \mid g \in G\}$$
   l'orbite de x sous l'action de G et :
$$G_x = \{g \in G \mid g \cdot x = x\}$$
   le stabilisateur de x sous l'action de G.
   (a) Montrer que pour tout $x \in X$ l'application :
$$\begin{array}{rccc} \varphi_x : & \dfrac{G}{G_x} & \to & G \cdot x \\ & \overline{g} = g \cdot G_x & \mapsto & g \cdot x \end{array}$$
   est bien définie et bijective.
   (b) On suppose que G et X sont finis et on note $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes. Montrer que :
$$\text{card}\,(X) = \sum_{i=1}^{r} \text{card}\,(G \cdot x_i) = \sum_{i=1}^{r} \frac{\text{card}\,(G)}{\text{card}\,(G_{x_i})}$$
   (formule des classes).
   (c) On suppose que X est fini et G fini de cardinal p^α, où p est un nombre premier et α un entier naturel non nul (on dit que G est un p-groupe). On note X^G l'ensemble des éléments $x \in X$ tels que $G \cdot x = \{x\}$ (orbite réduite à un seul élément). Montrer que :
$$\text{card}\left(X^G\right) \equiv \text{card}\,(X) \pmod{p}.$$

7. On rappelle que le centre d'un groupe G, noté $Z(G)$, est l'ensemble des éléments de G qui commutent à tout élément de G.
   (a) Montrer que $Z(G)$ est un sous-groupe commutatif de G.
   (b) On fait opérer le groupe G sur lui même par conjugaison ($g \cdot x = gxg^{-1}$, pour $(g,x) \in G \times G$) et on note G_x le stabilisateur de $x \in G$. On note $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites non réduites à un élément et deux à deux distinctes. Montrer que :
$$\begin{aligned} \operatorname{card}(G) &= \operatorname{card}(Z(G)) + \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) \\ &= \operatorname{card}(Z(G)) + \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}. \end{aligned}$$
   (c) Montrer que le centre d'un p-groupe n'est pas réduit à $\{1\}$.
8. On se propose de montrer que si G est un groupe d'ordre p^2 avec p premier, alors il est commutatif.
   (a) On suppose que le centre $Z(G)$ du groupe G est de cardinal p et on se donne un élément $h \in G \setminus Z(G)$. Montrer que $Z(G) \cap \langle h \rangle = \{1\}$.
   (b) Avec l'hypothèse de la question précédente, montrer que tout élément de G s'écrit de manière unique $g^i h^j$ où i, j sont des entiers compris entre 0 et $p-1$ et conclure.

– II – Exemples et contre-exemples

1. Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.
2. Donner des exemples de groupes dans lequel on peut trouver deux éléments d'ordre fini dont le produit est d'ordre infini.
3. On désigne par A_4 le groupe des permutations paires de l'ensemble $\{1,2,3,4\}$. Pour $i \neq j$ compris entre 1 et 4, on note τ_{ij} la transposition qui envoie i sur j.
   (a) Donner la liste de tous les éléments de A_4.
   (b) Montrer que $H = \{I_d, \tau_{12} \circ \tau_{34}, \tau_{13} \circ \tau_{24}, \tau_{23} \circ \tau_{14}\}$ est un sous-groupe distingué de A_4.
   (c) On désigne par $D(A_4)$ le sous-groupe de A_4 engendré par les commutateurs $\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1}$, où σ, τ sont dans A_4 (le groupe dérivé de A_4). Montrer que $D(A_4) = H$.
   (d) Montrer que A_4 n'a pas de sous-groupe d'ordre 6.
4. Si p est un nombre premier, peut-on affirmer que tout groupe d'ordre p^3 est commutatif ?

– III – Le lemme de Cauchy

1. Soit G un groupe commutatif fini d'ordre n.
   (a) Soient H un sous-groupe de G et $\overline{g} = gH$ un élément du groupe quotient G/H. Comparer l'ordre de $\overline{g}$ dans G/H avec l'ordre de g dans H.
   (b) Montrer que pour tout diviseur premier p de n il existe dans G un élément d'ordre p (lemme de Cauchy dans le cas commutatif). On peut procéder par récurrence sur l'ordre $n \geq 2$ de G.

2. Déduire de la question **I.3c** une deuxième démonstration du lemme de Cauchy dans le cas commutatif.
3. En utilisant le résultat de la question **I.5**, montrer le cas particulier suivant du lemme de Cauchy : si G est un groupe fini d'ordre $2p$ avec p premier, il existe alors un élément d'ordre p dans G.
4. On se propose de montrer le lemme de Cauchy pour tout groupe fini.
   Soit G un groupe fini de cardinal n et p un diviseur premier de n. On note X l'ensemble des p-uplets $(x_1, \cdots, x_p) \in G^p$ tels que $x_1 \cdots x_p = 1$.
   (a) Calculer le cardinal de X.
   (b) On désigne par H le sous-groupe de $\mathfrak{S}_p$ (groupe des permutations de $\{1, 2, \cdots, p\}$) engendré par le p-cycle $\sigma = (1, 2, \cdots, p)$.
   Montrer que l'application :
   $$\left(\sigma^k, (x_1, \cdots, x_p)\right) \mapsto \left(x_{\sigma^k(1)}, \cdots, x_{\sigma^k(p)}\right)$$
   définit une action de H sur X.
   (c) En utilisant les notations de **I.6c**, montrer que, pour cette action, $X^H \neq \varnothing$ et $\operatorname{card}\left(X^H\right)$ est divisible par p.
   (d) Déduire de ce qui précède qu'il existe dans G un élément d'ordre p (lemme de Cauchy).
5. Donner une deuxième démonstration du lemme de Cauchy en utilisant le résultat dans le cas commutatif. On peut procéder par récurrence sur l'ordre du groupe et utiliser les résultats de **I.7**.

– IV – Groupes finis de matrices

1. Soit $\mathbb{K}$ un corps fini (et commutatif, d'après le théorème de Wedderburn qui est admis) et φ un morphisme de groupes de $GL_n(\mathbb{K})$ dans $\mathbb{K}^*$. On note $(E_{ij})_{1 \leq i,j \leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$. Pour $\lambda \in \mathbb{K}^*$ on note :
   $$D_\lambda = I_n + (\lambda - 1) E_{nn}$$
   une matrice de dilatation et pour $\lambda \in \mathbb{K}$, $i \neq j$ compris entre 1 et n :
   $$T_\lambda = I_n + \lambda E_{ij}$$
   une matrice de transvection (le couple (i, j) avec $i \neq j$ est fixé).
   (a) Montrer qu'il existe un entier naturel r tel que :
   $$\forall \lambda \in \mathbb{K}^*,\ \varphi(D_\lambda) = \lambda^r.$$
   (b) Montrer que, pour $i \neq j$ fixés entre 1 et n et λ, μ dans $\mathbb{K}$, on a $T_\lambda T_\mu = T_{\lambda+\mu}$.
   (c) Que dire d'un morphisme de groupes de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \cdot)$?
   (d) Montrer que, pour $i \neq j$ fixés entre 1 et n, on a :
   $$\forall \lambda \in \mathbb{K},\ \varphi(T_\lambda) = 1.$$

(e) Déduire de ce qui précède que :

$$\forall A \in GL_n(\mathbb{K}),\ \varphi(A) = (\det(A))^r.$$

2. On note $O_2^+(\mathbb{R})$ le groupe des matrices de rotations du plan vectoriel euclidien.

   (a) Montrer que tout sous-groupe fini de $O_2^+(\mathbb{R})$ est cyclique.

   (b) Soit $G = \{I_2, R_1, \cdots, R_{n-1}\}$ un sous-groupe d'ordre n de $O_2^+(\mathbb{R})$, où pour tout k compris entre 1 et $n-1$, on a noté :

   $$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$$

   la matrice, dans la base canonique de $\mathbb{R}^2$, de la rotation d'angle θ_k, avec :

   $$0 < \theta_1 < \cdots < \theta_{n-1} < 2\pi.$$

   Montrer que G est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$ (rotation d'angle $\frac{2\pi}{n}$).

   (c) Retrouver le résultat de la question **III.2a** en utilisant un isomorphisme entre $O_2^+(\mathbb{R})$ et $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$.

3. Soit G un sous-groupe du groupe $GL_n(\mathbb{R})$ des matrices inversibles d'ordre n tel que $A^2 = I_n$ pour toute matrice A dans G.

   (a) Montrer que G est fini de cardinal 2^p avec p compris entre 1 et n.

   (b) Montrer que si n est différent de m, alors les groupes $GL_n(\mathbb{R})$ et $GL_m(\mathbb{R})$ ne sont pas isomorphes.

4. Soit G un sous-groupe fini de $GL_n(\mathbb{R})$ de cardinal $p \geq 2$.

   (a) Montrer que $B = \frac{1}{p}\sum_{A\in G} A$ est la matrice dans la base canonique de $\mathbb{R}^n$ d'un projecteur.

   (b) Montrer que $\sum_{A\in G} \mathrm{tr}(A)$ est un entier divisible par p, où $\mathrm{tr}(A)$ désigne la trace de la matrice A.

   (c) Montrer que si $\sum_{A\in G} \mathrm{tr}(A) = 0$, alors $\sum_{A\in G} A = 0$.

5. Soit F un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ contenant I_n et stable par le produit matriciel. Montrer que $F \cap GL_n(\mathbb{R})$ est un sous-groupe infini de $GL_n(\mathbb{R})$.

6. Soit G un sous groupe fini de $GL(\mathbb{R}^n)$. Montrer que si F est un sous-espace vectoriel de $\mathbb{R}^n$ stable par tous les éléments de G, il admet alors un supplémentaire également stable par tous les éléments de G.

7. Soit G un sous groupe de $O_n(\mathbb{R})$. On suppose qu'il existe un entier naturel non nul m tel que $A^m = I_n$ pour tout $A \in G$. Montrer que l'ensemble :

   $$\mathrm{tr}(G) = \{\mathrm{tr}(A) \mid A \in G\}$$

   est fini.

8. Soit G un sous groupe de $O_n(\mathbb{R})$. On note F le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ engendré par G et $\mathcal{B} = (A_1, \cdots, A_p)$ une base de F extraite de G.
   (a) Montrer que la matrice $G = ((\mathrm{tr}(A_i\,{}^tA_j)))_{1\leq i,j\leq p}$ est inversible dans $\mathcal{M}_p(\mathbb{R})$.
   (b) Montrer que si $\mathrm{tr}(G)$ est fini, alors G est fini.
9. Le résultat de la question **IV.8b** est-il encore vrai pour un sous-groupe de $GL_n(\mathbb{R})$?
10. Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{R})$ est nilpotente si et seulement si $\mathrm{tr}\left(A^k\right) = 0$ pour tout entier naturel non nul k.
11. Soit G un sous-groupe de $GL_n(\mathbb{R})$ tel que toutes les matrices de G soient diagonalisables. On note F le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ engendré par G et $\mathcal{B} = (A_1, \cdots, A_p)$ une base de F extraite de G.
   (a) Montrer que l'application :
$$\begin{array}{rccc} \varphi : & G & \to & \mathbb{R}^p \\ & A & \mapsto & (\mathrm{tr}(AA_1), \cdots, \mathrm{tr}(AA_p)) \end{array}$$
   est injective.
   (b) Montrer que si on suppose de plus que $\mathrm{tr}(G)$ est fini, alors G est fini.

4.2 Corrigé

– I – Généralités

1. Si G est un groupe fini d'orde n alors l'ensemble $\mathcal{P}(G)$ des parties de G est fini de cardinal 2^n et il en est de même de l'ensemble des sous-groupes de G.
Pour la réciproque, il revient au même de montrer que si G est infini, alors l'ensemble de ses sous-groupes l'est aussi.
Soit donc G un groupe infini et $\mathcal{H} = \{\langle g\rangle \mid g \in G\}$ la famille de tous les sous groupes monogènes de G. Si cette famille est infinie il en est alors de même de l'ensemble des sous-groupes de G. Sinon, comme $G = \bigcup_{g\in G} \langle g\rangle$ est infini, il existe nécessairement un élément $g \in G$ d'ordre infini et les $\langle g^n\rangle$ où n décrit $\mathbb{N}$ constitue une famille infinie de sous-groupes de G. En effet l'égalité $\langle g^n\rangle = \langle g^m\rangle$ entraîne $g^n = g^{km}$, soit $g^{n-km} = 1$ et $n - km = 0$ (g est d'ordre infini), c'est-à-dire que m divise n. Comme n et m jouent des rôles symétriques, on a aussi n qui divise m et en définitive $n = m$.
On peut aussi dire que si $g \in G$ est d'ordre infini, alors $\langle g\rangle$ est isomorphe au groupe additif $\mathbb{Z}$ et on sait que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où n décrit $\mathbb{N}$, il y en adonc une infinité et $\langle g\rangle$ a une infinité de sous-groupes.
2. On procède par récurrence sur $p \geq 2$.
Pour $p = 2$, la démonstration est faite en **II.2f** du problème 2 en utilisant les décompositions en facteurs premiers de m_1 et m_2.
Supposant le résultat acquis pour $p \geq 2$, soit $g_1, g_2, \cdots, g_{p+1}$ deux à deux distincts dans G d'ordres respectifs $m_1, m_2, \cdots, m_{p+1}$. L'hypothèse de récuurence nous dit qu'il existe $g_0 \in G$ d'ordre $m_0 = \mathrm{ppcm}(m_1, m_2, \cdots, m_p)$ et le cas $p = 2$ qu'il existe g d'ordre :
$$\begin{aligned} \mathrm{ppcm}(m_0, m_{p+1}) &= \mathrm{ppcm}(\mathrm{ppcm}(m_1, m_2, \cdots, m_p), m_0) \\ &= \mathrm{ppcm}(m_1, m_2, \cdots, m_{p+1}) \end{aligned}$$

(associativité du ppcm).
On peut aussi procéder directement. Pour ce faire on écrit la décomposition en facteurs premiers du ppcm, noté m, des ordres respectifs de $g_1, g_2, \cdots, g_p$:

$$m = \prod_{k=1}^{r} p_k^{\alpha_k}$$

de telle sorte que, pour tout entier k compris entre 1 et r, l'ordre $\theta(g_k)$ de g_k soit un multiple de $p_k^{\alpha_k}$, soit $\theta(g_k) = p_k^{\alpha_k} m_k$ l'entier m_k étant premier avec p_k. L'élément $g_k^{m_k}$ est alors d'ordre $p_k^{\alpha_k}$ et $g = \prod_{k=1}^{r} g_k^{m_k}$ est alors d'ordre m. En effet, on a bien $g^m = \prod_{k=1}^{r} g_k^{m \cdot m_k} = \prod_{k=1}^{r} g_k^{m' \cdot \theta(g_k)} = 1$ ($m' = \dfrac{m \cdot m_k}{\theta(g_k)} = \dfrac{m}{p_k^{\alpha_k}}$), donc l'ordre de g divise m, soit $\theta(g) = \prod_{k=1}^{r} p_k^{\beta_k}$ avec $0 \leq \beta_k \leq \alpha_k$. Mais si pour l'un des indices k on a $\beta_k < \alpha_k$, par exemple pour $k = 1$ (pour simplifier), on aura en notant $m' = p_1^{\beta_1} \prod_{k=2}^{r} p_k^{\alpha_k} = q\theta(g)$:

$$1 = g^{m'} = (g_1^{m_1})^{m'} \prod_{k=2}^{r} (g_k^{m_k})^{m'} = (g_1^{m_1})^{m'}$$

puisque m' est multiple de $p_k^{\alpha_k}$ pour $k \neq 1$. Il en résulte que l'ordre de $g_1^{m_1}$ est un diviseur de m', ce qui contredit le fait que cet ordre contient $p_1^{\alpha_1}$ dans sa décomposition en facteurs premiers. On a donc $\beta_k = \alpha_k$ pour tout k et g est d'ordre m.

3.

(a) Comme G est commutatif fini, on peut trouver g_j et g_k dans G tels que :

$$\begin{cases} \theta(g_j) = \text{ppcm}\{\theta(g_i) \mid 1 \leq i \leq n\} \\ \theta(g_k) = \max\{\theta(g_i) \mid 1 \leq i \leq n\} \end{cases}$$

On a alors $\theta(g_j) \leq \theta(g_k)$ ($\theta(g_k)$ est le plus grand) et $\theta(g_k)$ divise $\theta(g_j)$ ($\theta(g_j)$ est multiple de tous les ordres) donc $\theta(g_k) \leq \theta(g_j)$ et $\theta(g_j) = \theta(g_k)$.

(b) En remarquant que $\prod_{i=1}^{n} \theta(g_i)$ est le cardinal de $\prod_{i=1}^{n} \langle g_i \rangle$, on est amené à considérer l'application φ du groupe produit $H = \prod_{i=1}^{n} \langle g_i \rangle$ dans G définie par :

$$\forall x = (x_1, \cdots, x_n) \in H,\ \varphi(x) = \prod_{i=1}^{n} x_i$$

Cette application est surjective et comme G est commutatif, c'est un morphisme de groupes. Ce morphisme φ induit alors un isomorphisme du groupe quotient $\dfrac{H}{\ker(\varphi)}$ sur G, ce qui entraîne $\text{card}(H) = \text{card}(\ker(\psi))\,\text{card}(G)$ et $n = \text{card}(G)$ divise $\text{card}(H) = \prod_{i=1}^{n} \theta(g_i)$.

(c) $m = \theta(g_j)$ divise l'ordre de G, donc les facteurs premiers de m sont aussi des facteurs premiers de n.
Le ppcm m des ordres des éléments de G étant multiple de chaque $\theta(g_i)$, m^n est multiple de $\prod_{i=1}^{n} \theta(g_i)$ donc de n, et les facteurs premiers de n sont aussi des facteurs premiers de m. En définitive m et n ont les mêmes facteurs premiers.

4. On désigne par m le ppcm de tous les ordres des éléments de G (groupe d'ordre n) et par g_0 un élément d'ordre m dans G. Comme m et n ont les mêmes facteurs premiers, $m = \theta(g_0)$ divisant n, on a les décompositions en facteurs premiers $m = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $n = \prod_{k=1}^{r} p_k^{\beta_k}$, où les p_k sont premiers deux à deux distincts et $1 \leq \alpha_k \leq \beta_k$ pour tout k compris entre 1 et n. Sachant que :
$$\varphi(n) = \prod_{k=1}^{r} p_k^{\beta_k - 1}(p_k - 1)$$
on déduit que si $\varphi(n)$ est premier avec n, alors tous les β_k valent 1 (sinon p_k divise $\varphi(n)$ et n) et les α_k valent aussi 1, ce qui donne $n = m$ et G est cyclique puisque g_0 est d'ordre $n = \text{card}(G)$.
Voir Francinou et Giannella pour la réciproque.

5.

   (a) Si tous les éléments de G sont d'ordre au plus égal à 2, alors pour tout $x \in G$, on a $x^2 = 1$ et $x = x^{-1}$. Pour x, y dans G, on a alors $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$, c'est-à-dire que G est commutatif.

   (b) On suppose de plus que G est fini. Si G est réduit à $\{1\}$ alors $\text{card}(G) = 1 = 2^0$. Si G n'est pas réduit à $\{1\}$, il existe $g \in G \setminus \{1\}$ tel que $\langle g \rangle = \{1, g\}$ et le groupe quotient $\dfrac{G}{\langle g \rangle}$ est de cardinal strictement inférieur à $\text{card}(G)$ avec tous ses éléments d'ordre au plus égal à 2. On conclut alors par récurrence sur l'ordre de G. En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à $\text{card}(G)$, on a $\text{card}\left(\dfrac{G}{\langle g \rangle}\right) = 2^p$ et $\text{card}(G) = 2^{p+1}$.
   Une autre solution consiste à dire que le ppcm des ordres des éléments de G est égal à 2, et comme ce ppcm a les mêmes facteurs premiers que n, on a nécessairement $n = 2^q$.
   On peut également dire que si p est un diviseur premier de n alors il existe un élément g dans G d'ordre p (voir la partie **III** sur le lemme de Cauchy), mais l'ordre de cet élément est 1 ou 2, on a donc $p = 2$. Ce qui prouve que 2 est le seul diviseur premier de n et $n = 2^q$.

6. (a) En remarquant que pour g, h dans G l'égalité $g \cdot x = h \cdot x$ équivaut à $h^{-1}g \cdot x = x$, soit à $h^{-1}g \in G_x$ ou encore à $\overline{g} = \overline{h}$ dans $\dfrac{G}{G_x}$, on déduit que l'application φ_x est bien définie et injective. Cette application étant clairement surjective, elle définie une bijection de $\dfrac{G}{G_x}$ sur $G \cdot x$.

   (b) Si X est fini, on a alors un nombre fini d'orbites $G \cdot x_1, \cdots, G \cdot x_r$ qui forment une partition de X et :
   $$\text{card}(X) = \sum_{i=1}^{r} \text{card}(G \cdot x_i).$$
   En utilisant la bijection de $\dfrac{G}{G_{x_i}}$ sur $G \cdot x_i$, on déduit que si G est aussi fini, alors :
   $$\text{card}(G \cdot x_i) = \text{card}\left(\frac{G}{G_{x_i}}\right) = \frac{\text{card}(G)}{\text{card}(G_{x_i})}.$$

(c) On suppose que $X^G \neq \emptyset$.
On range les orbites deux à deux distinctes, $G \cdot x_1, \cdots, G \cdot x_r$, de telle sorte les q premières sont celles réduites à un seul élément, l'entier q étant le cardinal de X^G.
Pour i compris entre 1 et q, on a $G_{x_i} = G$ et $[G : G_{x_i}] = \operatorname{card}\left(\dfrac{G}{G_{x_i}}\right) = 1$.
Pour i compris entre $q+1$ et r, G_{x_i} est un sous-groupe strict de G qui est d'ordre p^α, donc $\operatorname{card}(G_{x_i}) = p^\beta$ avec $0 \leq \beta < \alpha$ et $[G : G_{x_i}] = p^{\alpha-\beta}$ avec $1 \leq \alpha - \beta \leq \alpha$.
La formule des classes donne alors :

$$\operatorname{card}(X) = q + \sum_{i=q+1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})} \equiv q \pmod{p}$$

Si $X^G = \emptyset$, on a alors $q = 0$ et cette formule est encore valable.
Si $q = r$, on a alors $X^G = X$ et $q = r = \operatorname{card}(X)$.

7. (a) $Z(G)$ est non vide puisqu'il contient 1. Si g, h sont dans $Z(G)$, alors pour tout $k \in G$ on a :

$$gh^{-1}k = g\left(k^{-1}h\right)^{-1} = gkh^{-1} = kgh^{-1},$$

c'est-à-dire que gh^{-1} est dans $Z(G)$. On a donc ainsi montré que $Z(G)$ est un sous-groupe de G. Ce sous-groupe est clairement commutatif.

(b) L'orbite $G \cdot x$ est réduite à $\{x\}$ si et seulement si $gxg^{-1} = x$ pour tout $g \in G$, ce qui revient à dire que $gx = xg$, c'est-à-dire $x \in Z(G)$. Le résultat s'obtient donc en distinguant dans la formule des classes les orbites à un élément (il y en a autant que d'éléments de $Z(G)$) des orbites à plus de 2 éléments.

(c) Soit G un p-groupe à p^α éléments. Si $\alpha = 1$, alors G est cyclique donc commutatif et $Z(G) = G$.
On suppose $\alpha \geq 2$. Avec les notations de la question précédente, pour $1 \leq i \leq r$, on a :

$$\frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})} = \operatorname{card}(G \cdot x_i) \geq 2$$

et $\operatorname{card}(G_{x_i}) = p^\beta$ avec $0 \leq \beta \leq \alpha - 1$, ce qui donne $\operatorname{card}(G \cdot x_i) = p^{\alpha-\beta}$ avec $\alpha - \beta \geq 1$. Il en résulte que :

$$\operatorname{card}(Z(G)) = \operatorname{card}(G) - \sum_{i=q+1}^{r} \operatorname{card}(G \cdot x_i)$$

est divisible par p. Enfin avec $\operatorname{card}(Z(G)) \geq 1$, on déduit que $\operatorname{card}(Z(G)) \geq p$ et $Z(G)$ est non trivial.

8. On sait que $Z(G)$ est non trivial, il est donc de cardinal p ou p^2 et il s'agit de montrer qu'il est de cardinal p^2.

(a) Si $Z(G)$ est de cardinal p, il est alors cyclique, soit $Z(G) = \langle g \rangle$. Si $h \in G \setminus Z(G)$, alors h ne peut être d'ordre p^2. En effet si h est d'ordre p^2, alors $G = \langle h \rangle$ et G serait commutatif ce qui contredit l'hypothèse $G \neq Z(G)$. Cet élément h est donc d'ordre p et l'intersection $K = Z(G) \cap \langle h \rangle$ est un sous-groupe de G d'ordre 1 ou p. Mais K de cardinal p entraîne $K = Z(G)$ et $h \in Z(G)$ contraire à l'hypothèse. On a donc $Z(G) \cap \langle h \rangle = \{1\}$.

(b) En utilisant l'application :

$$\begin{array}{rccc} \varphi : & \{0,1,\cdots,p-1\}^2 & \to & G \\ & (i,j) & \mapsto & g^i h^j \end{array}$$

nous déduisons que tout élément de G s'écrit de manière unique $g^i h^j$. Pour ce faire il suffit de montrer que φ est injective. Si $g^i h^j = g^{i'} h^{j'}$, alors $g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h \rangle = \{1\}$ et $g^{i-i'} = h^{j'-j} = 1$ ce qui entraîne que p divise $i - i'$ et $j - j'$, ces entiers étant compris entre $-p+1$ et $p-1$, et nécessairement $i = i'$, $j = j'$. Avec les cardinaux il en résulte que φ est une bijection.
Si k, k' sont dans G, il s'écrivent $k = g^i h^j$ et $k' = g^{i'} h^{j'}$ et comme g commute à tout G, on en déduit que k et k' commutent. Le groupe G serait alors commutatif ce qui est contraire à l'hypothèse $G \neq Z(G)$.
En définitive $Z(G)$ ne peut être de cardinal p, il est donc de cardinal p^2 et G est commutatif.

– II – Exemples et contre-exemples

1. Le groupe des rotations vectorielles de $\mathbb{R}^2$ d'angle $2\pi r$ avec r rationnel (ou $G = \{e^{2i\pi r} \mid r \in \mathbb{Q}\}$) est infini avec tous ses éléments d'ordre fini ($R\left(2\pi\frac{p}{q}\right)^q = I_d$).
   Si p est un nombre premier supérieur ou égal à 2, alors le groupe additif $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ est infini et tous ses éléments non nuls sont d'ordre p.
   Si on définit sur le corps $\mathbb{Q}$ des rationnels la relation d'équivalence $r \backsim s$ si et seulement si $r - s \in \mathbb{Z}$, alors le groupe quotient $\frac{\mathbb{Q}}{\mathbb{Z}}$ pour cette relation d'équivalence est infini et tous ses éléments sont d'ordre fini ($q\frac{\overline{p}}{q} = \overline{0}$).
   Si X est un ensemble infini, alors l'ensemble $\mathcal{P}(X)$ munit de l'opération différence symétrique $(A, B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$ est un groupe infini et tous ses éléments différents de l'ensemble vide sont d'ordre 2.
2. Dans le groupe linéaire $GL(\mathbb{R}^2)$, le produit de deux réflexions vectorielles $\sigma_{\mathcal{D}}$ et $\sigma_{\mathcal{D}'}$ d'axes $\mathcal{D}$ et $\mathcal{D}'$ faisant un angle α est une rotation d'angle 2α. Chaque réflexion est d'ordre 2 et la composée $\sigma_{\mathcal{D}} \circ \sigma_{\mathcal{D}'}$ est d'ordre infini si $\frac{2\pi}{2\alpha} \notin \mathbb{Q}$.
   Dans le groupe affine $GA(\mathbb{R}^2)$, le produit de deux symétries centrales σ_O et $\sigma_{O'}$ (d'ordres 2) de centres distincts O et O' est la translation de vecteur $2\overrightarrow{OO'}$ qui est d'ordre infini.
   Dans le groupe des matrices réelles inversibles d'ordre 2, les matrices $A = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ sont d'ordre 2 alors que $AB = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ est d'ordre infini (pour tout $n \in \mathbb{N}$, on a $(AB)^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$).
3.
   (a) Le groupe A_4 est formé des 12 éléments suivants :
   - l'identité ;
   - 3 éléments d'ordre 2 : $\tau_{12} \circ \tau_{34}, \tau_{13} \circ \tau_{24}, \tau_{23} \circ \tau_{14}$;

– 8 éléments d'ordre 3 : $(1,2,3)$, $(1,2,4)$, $(1,3,2)$, $(1,3,4)$, $(1,4,2)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$.

(b) L'ensemble H est formé de Id et tous les éléments d'ordre 2 de A_4, il en résulte que c'est un sous-groupe distingué de A_4. En effet si σ, τ sont d'ordre 2, il en est de même de $\sigma \circ \tau^{-1} = \sigma \circ \tau$ puisque σ et τ commutent et pour $\sigma \in A_4$, $\tau \in H$, on a $(\sigma \circ \tau \circ \sigma^{-1})^2 = I_d$.

(c) Le groupe quotient $\dfrac{A_4}{H}$ est d'ordre 3, donc cyclique et en particulier commutatif. Il en résulte que pour tous σ, τ dans A_4, on a $[\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1}] = [I_d]$ et $\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} \in H$. On a donc $D(A_4) \subset H$ et $D(A_4)$ est de cardinal 1, 2 ou 4 d'après le théorème de Lagrange. Le groupe A_4 n'étant pas commutatif, le cardinal de $D(A_4)$ n'est pas égal à 1. S'il est égal à 2, alors $D(A_4) = \{I_d, \tau\}$ avec $\tau = \tau_{ij} \circ \tau_{k\ell}$ où $\{i,j,k,\ell\} = \{1,2,3,4\}$, et pour $\sigma = (i,j,k)$ on a :

$$\sigma \circ \tau \circ \sigma^{-1} = \tau_{\sigma(i),\sigma(j)} \circ \tau_{\sigma(k),\sigma(\ell)} = \tau_{jk} \circ \tau_{i\ell} \notin H.$$

En définitive, $D(A_4)$ a 4 éléments et on a l'égalité $D(A_4) = H$.

(d) Si K est un sous-groupe de A_4 d'ordre 6, il est d'indice 2 et nécessairement distingué dans A_4. Le groupe quotient $\dfrac{A_4}{K}$ est alors cyclique d'ordre 2, donc commutatif et K doit contenir $D(A_4)$, ce qui est en contradiction avec le théorème de Lagrange ($4 = \text{card}(D(A_4))$ doit diviser $6 = \text{card}(K)$, ce qui est faux). En définitive il n'est pas possible de trouver un sous-groupe d'ordre 6 dans A_4.

4. Le groupe des isométries du plan qui conservent les sommets d'un carré (le groupe du carré) est d'ordre 2^3 et non commutatif.

– III – Le lemme de Cauchy

1.

(a) Soit $g \in G$ d'ordre p et q l'ordre de $\overline{g}$ dans G/H. Avec $\overline{g}^p = \overline{g^p} = \overline{1}$, on déduit que q divise p.

(b) Pour $n = 2$, on a $G = \{1, g\}$ avec g d'orde 2 et 2 est le seul diviseur premier de n.
Supposons le résultat acquis pour tous les groupes commutatifs d'ordre $m < n$, où $n \geq 3$.
Soient G un groupe commutatif d'ordre n, p un diviseur premier de n et $g \in G \setminus \{1\}$.
Si $G = \langle g \rangle$, alors G est cyclique et g est d'ordre n. Pour tout diviseur premier p de n, l'élément $h = g^{\frac{n}{p}}$ est alors d'ordre p dans G ($\left\langle g^{\frac{n}{p}} \right\rangle$ est en fait l'unique sous-groupe d'ordre p du groupe cyclique G).
Si $H = \langle g \rangle \underset{\neq}{\subset} G$ et p divise $m = \text{card}(H) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément h dans H, donc dans G, qui est d'ordre p.
Supposons enfin que $H \underset{\neq}{\subset} G$ avec p ne divisant pas $m = \text{card}(H)$. Comme p premier ne divise pas m, il est premier avec m et le groupe quotient $\dfrac{G}{H}$ est commutatif d'ordre $r = \dfrac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m, le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $\overline{h}$ d'ordre p dans $\dfrac{G}{H}$ et l'ordre q de H dans G est un multiple de p. L'élément $k = h^{\frac{q}{p}}$ est alors d'ordre p dans G.

2. Si p est un diviseur premier de n, c'est également un diviseur premier de $\theta(g_0) = \text{ppcm}\{\theta(g) \mid g \in G\}$, soit $\theta(g_0) = pq$ et g_0^q est d'ordre p dans G.
3. Si G est d'ordre $2p$ avec p premier, le théorème de Lagrange nous dit que les éléments de $G \setminus \{1\}$ sont d'ordre 2, p ou $2p$. S'il n'y a aucun élément d'ordre p, il n'y en a pas d'ordre $2p$ (si g est d'ordre $2p$, alors g^2 est d'ordre p), donc tous les éléments de $G \setminus \{1\}$ sont d'ordre 2 et $p \neq 2$, donc G est commutatif d'ordre 2^n, ce qui impose $n = 2$ et $p = 2$, soit une contradiction. Il existe donc dans G des éléments d'ordre p.
4.
   (a) L'application $(x_1, \cdots, x_p) \mapsto (x_1, \cdots, x_{p-1})$ réalise une bijection de X sur G^{p-1} (de l'égalité $x_1 \cdots x_p = 1$, on déduit que la connaissance des x_i pour $1 \leq i \leq p-1$ détermine x_p de manière unique). On a donc :
   $$\text{card}(X) = n^{p-1}.$$
   (b) On note $H = \langle\sigma\rangle = \{I_d, \sigma, \cdots, \sigma^{p-1}\}$ le groupe engendré par le p-cycle σ.
   Pour $x = (x_1, \cdots, x_p) \in X$, on a $x_1(x_2 \cdots x_p) = 1$, donc x_1 est l'inverse de $x_2 \cdots x_p$ et on a aussi $(x_2 \cdots x_p)\, x_1 = 1$, ce qui signifie que $(x_2, \cdots, x_p, x_1) = \left(x_{\sigma(1)}, \cdots, x_{\sigma(p)}\right) \in X$. Il en résulte que pour tout entier k compris entre 0 et $p-1$, $\left(x_{\sigma^k(1)}, \cdots, x_{\sigma^k(p)}\right) \in X$. On peut donc définir l'application :
   $$\left(\sigma^k, (x_1, \cdots, x_p)\right) \mapsto \left(x_{\sigma^k(1)}, \cdots, x_{\sigma^k(p)}\right)$$
   de $H \times X$ dans X. Cette application définit bien une action.
   (c) On a :
   $$\text{card}\left(X^H\right) \equiv \text{card}(X) \pmod{p}$$
   avec $\text{card}(X) = n^{p-1}$ divisible par p, ce qui entraîne que $\text{card}\left(X^H\right)$ est également divisible par p. En remarquant que $x = (1, \cdots, 1)$ est dans X^H, on déduit que X^H est non vide.
   (d) De $\text{card}\left(X^H\right) \geq 1$ et $\text{card}\left(X^H\right)$ divisible par p, on déduit que $\text{card}\left(X^H\right) \geq p \geq 2$ et en remarquant que $x = (x_1, \cdots, x_p) \in X^H$ équivaut à dire que $x_1 = \cdots = x_p = g$ avec $g \in G$ tel que $g^p = 1$, on déduit qu'il existe $g \neq 1$ tel que $g^p = 1$, ce qui signifie que g est d'ordre p.
5. On procède par récurrence sur l'ordre n du groupe G.
   Pour $n = 2$, $G = \{1, g\}$ est cyclique avec g d'ordre 2.
   Supposons le résultat acquis pour les groupes d'ordre strictement inférieur à n et soit G un groupe d'ordre $n \geq 3$. On note p un diviseur premier de n.
   Si G admet un sous-groupe H d'ordre $n' < n$ divisible par p, alors H admet un élément d'ordre p par hypothèse de récurrence et cet élément est d'ordre p dans G.
   Dans le cas contraire, en écrivant $n = p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p, si H est un sous-groupe strict de G, son ordre qui divise $p^\alpha m$ et est premier avec p va diviser m et $[G : H] = \dfrac{\text{card}(G)}{\text{card}(G)} = p^\alpha m'$ avec $m' < m$. En faisant agir G sur lui même par conjugaison, on déduit que :
   $$\text{card}(Z(G)) = \text{card}(G) - \sum_{i=q+1}^{r} \frac{\text{card}(G)}{\text{card}(G_{x_i})}$$
   est divisible par p. En définitive, $Z(G)$ est un groupe commutatif de cardinal divisible par p, il admet donc un élément d'ordre p qui est d'ordre p dans G.

– IV– Groupes finis de matrices

1. On remarque que pour tout $\lambda \in \mathbb{K}$ on a $\det(E_\lambda) = 1$ et pour tout $\lambda \in \mathbb{K}^*$, $\det(D_\lambda) = \lambda$.
On rappelle que si $T_\lambda = T_\lambda^{(i,j)}$ est une matrice de transvection, alors la multiplication à gauche [resp. à droite] d'une matrice A par T_λ revient à effectuer l'opération élémentaire :

$$L_i \mapsto L_i + \lambda L_j \ (\text{rep. } C_j \mapsto C_j + \lambda C_i)$$

où L_i [resp. C_j] désigne la ligne numéro i [resp. la colonne numéro j] de A.
De plus $GL_n(\mathbb{K})$ est engendré par l'ensembles des matrices de transvection ou dilatation, c'est-à-dire que tout matrice $A \in GL_n(\mathbb{K})$ s'écrit $A = T_1 \cdots T_\alpha D_{\det(A)} T_{\alpha+1} \cdots T_\beta$, où les T_k sont des matrices de transvection (voir [6], chapitre 5, paragraphe 4).

   (a) On sait que $\mathbb{K}^*$ est cyclique, soit $\mathbb{K}^* = \{1, \mu, \cdots, \mu^{q-1}\}$. Tout élément λ de $\mathbb{K}^*$ s'écrit donc $\lambda = \mu^k$ où k est compris entre 0 et $q-1$ et avec :

$$D_\lambda = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & \lambda \end{pmatrix} = D_\mu^k$$

   on a $\varphi(D_\lambda) = \varphi(D_\mu)^k$. Puis en écrivant que $\varphi(D_\mu) = \mu^r$ dans $\mathbb{K}^*$, où r est un entier compris entre 0 et $q-1$, on déduit que $\varphi(D_\lambda) = \mu^{rk} = \left(\mu^k\right)^r = \lambda^r$.

   (b) Pour $1 \leq i \neq j \leq n$, on a $E_{ij}^2 = 0$, ce qui entraîne pour λ, μ dans $\mathbb{K}$:

$$T_\lambda T_\mu = I_n + (\lambda + \mu) E_{ij} + \lambda\mu E_{ij}^2 = T_{\lambda+\mu}.$$

   On peut aussi dire que $T_\lambda T_\mu$ est déduit de T_μ en ajoutant à sa ligne i sa ligne j multipliée par λ, ce qui donne la matrice $T_{\lambda+\mu}$.
   Prenant $\mu = -\lambda$, on a $T_\lambda T_{-\lambda} = T_0 = I_n$, ce qui signifie que T_λ est inversible d'inverse $T_{-\lambda}$ (pour les mêmes indices $i \neq j$).

   (c) Soit ψ un morphisme de groupes de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \cdot)$. Ces groupes étant finis, on a :

$$\text{card}(\mathbb{K}) = \text{card}(\ker(\psi))\,\text{card}(\text{Im}(\psi)),$$

   c'est-à-dire que $\text{card}(\text{Im}(\psi))$ divise $q+1 = \text{card}(\mathbb{K})$. Mais $\text{Im}(\psi)$ étant un sous groupe de $\mathbb{K}^*$ a un cardinal qui divise q et nécessairement $\text{card}(\text{Im}(\psi)) = 1$ du fait que $q+1$ et q sont premiers entre eux. On a donc $\text{Im}(\psi) = \{\psi(0)\} = \{1\}$, ce qui signifie que ψ est la fonction constante égale à 1.
   L'exemple de la fonction exponentielle réelle ou complexe nous montre que ce résultat est faux pour un corps infini.

   (d) Avec :

$$\forall (\lambda, \mu) \in \mathbb{K}^2,\ \varphi(T_{\lambda+\mu}) = \varphi(T_\lambda T_\mu) = \varphi(T_\lambda)\varphi(T_\mu),$$

   on déduit que l'application $\psi : \lambda \mapsto \varphi(T_\lambda)$ réalise un morphisme de groupes de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \cdot)$ et nécessairement $\varphi(T_\lambda) = 1$ pour toute matrice de transvection T_λ.

   (e) Sachant que toute matrice $A \in GL_n(\mathbb{K})$ s'écrit $A = T_1 \cdots T_\alpha D_{\det(A)} T_{\alpha+1} \cdots T_\beta$, où les T_k sont des matrices de transvection, on déduit de ce qui précède que $\varphi(A) = (\det(A))^r$.

2.

(a) Le groupe $O_2^+(\mathbb{R})$ est isomorphe au groupe multiplicatif Γ des nombres complexes de module égal à 1, un isomorphisme étant défini par l'application :

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mapsto e^{i\theta}.$$

Un sous-groupe fini de $O_2^+(\mathbb{R})$ est donc identifié à un sous-groupe fini de Γ, donc de $\mathbb{C}^*$, et en conséquence il est cyclique.

(b) Pour k compris entre 1 et $n-1$ l'ensemble :

$$I_k = \{j \in \mathbb{N} \mid \theta_k - j\theta_1 > 0\}$$

est non vide ($j = 0$ est dans I_k) et majoré ($0 \leq j < \dfrac{\theta_k}{\theta_1} \leq \dfrac{\theta_{n-1}}{\theta_1}$), il admet donc un plus grand élément j_k et on a :

$$j_k\theta_1 < \theta_k \leq (j_k + 1)\,\theta_1,$$

soit :

$$0 < \theta_k - j_k\theta_1 \leq \theta_1 < 2\pi$$

et :

$$R(\theta_k - j_k\theta_1) = R(\theta_k)\,R(\theta_1)^{-j_k} \in G$$

puisque G est un groupe. On a donc nécessairement $\theta_k - j_k\theta_1 = \theta_1$ et :

$$R(\theta_k) = R(\theta_1)^{j_k+1}.$$

On a donc ainsi montré que G est cyclique engendré par $R(\theta_1)$. D'autre part, comme G est d'ordre n, on a $R(\theta_1)^n = R(n\theta_1) = I_2$ et $n\theta_1 = 2p\pi$ avec p compris entre 1 et $n-1$, ce qui entraîne :

$$G = \left\langle R\left(p\frac{2\pi}{n}\right)\right\rangle \subset \left\langle R\left(\frac{2\pi}{n}\right)\right\rangle$$

et l'égalité avec les cardinaux.

(c) L'application :

$$\begin{array}{rccc} \varphi : & (\mathbb{R}, +) & \to & \left(O_2^+(\mathbb{R}), \cdot\right) \\ & \theta & \mapsto & R(\theta) \end{array}$$

est un morphisme de groupes surjectif de noyau $2\pi\mathbb{Z}$, d'où un isomorphisme de groupes de $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ sur $O_2^+(\mathbb{R})$. Il suffit alors de montrer que tout sous-groupe fini de $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ est cyclique. En considérant que l'ensemble des sous-groupes de $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ est en bijection avec l'ensemble des sous groupes additifs de $\mathbb{R}$ qui contiennent $2\pi\mathbb{Z}$ et qu'un sous-groupe additif de $\mathbb{R}$ est dense ou discret, on déduit, en notant p la surjection canonique de $\mathbb{R}$ sur $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$, que tout sous-groupe fini de $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ est de la forme $H = p(a\mathbb{Z})$, avec $a \in \mathbb{R}$ et $a\mathbb{Z} \supset 2\pi\mathbb{Z}$. On a donc $a = \dfrac{2\pi}{n}$ et $H = \left\langle p\left(\dfrac{2\pi}{n}\mathbb{Z}\right)\right\rangle$ où n est l'ordre de H.

3. (a) Des conditions $A^2 = I_n$ pour tout $A \in G$, on déduit que G est commutatif.
Toutes les matrices de G sont diagonalisables car annulées par le polynôme $X^2 - 1$ qui est scindé à racines simples dans $\mathbb{R}$ et avec la commutativité de G, on déduit que les matrices de G sont simultanément diagonalisables, c'est-à-dire qu'il existe une matrice P dans $GL_n(\mathbb{R})$ telle que pour tout $A \in G$, la matrice $\Delta = P^{-1}AP$ est diagonale. Avec $\Delta^2 = I_n$, on déduit que les termes diagonaux de Δ sont dans $\{-1, 1\}$. En notant $\lambda_k(A)$ les termes diagonaux de la matrice Δ, pour $k = 1, \cdots, n$, l'application $A \mapsto (\lambda_1(A), \cdots, \lambda_n(A))$ réalise alors un isomorphisme de groupes de G sur un sous groupe de $\{-1, 1\}^n$ et en conséquence G est fini de cardinal 2^p avec p compris entre 1 et n.

   (b) Supposons qu'il existe un isomorphisme de groupes φ de $GL_n(\mathbb{R})$ sur $GL_m(\mathbb{R})$. On désigne par G le sous groupe de G formé des matrices diagonales de la forme $g = \begin{pmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \varepsilon_n \end{pmatrix}$ où $\varepsilon_i = \pm 1$, pour $i = 1, \cdots, n$. Ce groupe est d'ordre 2^n avec tous ses éléments d'ordre inférieur ou égal à 2. Par l'isomorphisme φ il est transformé en un sous groupe H de $GL_m(\mathbb{R})$ ayant les mêmes propriétés. D'après ce qui précède, on a alors $n \leq m$. En raisonnant avec l'isomorphisme φ^{-1} on déduit qu'on a aussi $m \leq n$. Ce qui donne en définitive $m = n$.

4.

   (a) Pour tout $C \in G$ la translation $A \mapsto AC$ réalise une permutation de G, donc :

$$BC = \frac{1}{p} \sum_{A \in G} AC = B$$

   et :

$$B^2 = \frac{1}{p} \sum_{C \in G} BC = \frac{1}{p} \sum_{C \in G} B = \frac{1}{p} pB = B,$$

   ce qui signifie que B est un projecteur.

   (b) La matrice B étant celle d'un projecteur, on a $\operatorname{tr}(B) = \operatorname{rang}(B) \in \mathbb{N}$ et en conséquence $\sum_{A \in G} \operatorname{tr}(A) = p \operatorname{tr}(B)$ est un entier divisible par p.

   (c) Si B est non nulle, alors $\operatorname{tr}(B) = r \geq 1$ et $\sum_{A \in G} \operatorname{tr}(A) = pr \neq 0$, ce qui contredit l'hypothèse. On a donc $B = 0$ et $\sum_{A \in G} A = 0$.

5. Notons $G = F \cap GL_n(\mathbb{R})$. Cet ensemble est non vide puisqu'il contient I_n. Si A, B sont dans G, alors AB est également dans G puisque F est stable par le produit matriciel. Il reste à montrer que si $A \in G$, alors A^{-1} est dans F, ce qui résulte du fait que A^{-1} est un polynôme en A. En effet, le théorème de Cayley-Hamilton nous dit que si $P(X) = \sum_{k=0}^{n} \alpha_k X^k$ est le polynôme caractéristique de A, alors $P(A) = 0$ et avec $\alpha_0 = \det(A) \neq 0$, on déduit que $A^{-1} = -\frac{1}{\alpha_0} \sum_{k=1}^{n} \alpha_k A^{k-1} \in F$ puisque F contient I_n est stable par le produit et c'est un espace vectoriel. Enfin G est infini puisqu'il contient toutes les homothéties λI_n de rapport $\lambda \in \mathbb{R}^*$.

6. On note $\langle\cdot \mid \cdot\rangle$ le produit scalaire euclidien canonique de $\mathbb{R}^n$. Pour tout $g \in G$ l'application $(x,y) \mapsto \langle g(x) \mid g(y)\rangle$ définit un produit scalaire sur $\mathbb{R}^n$ et il en est de même de l'application ;
$$\varphi : (x,y) \mapsto \sum_{g\in G} \langle g(x) \mid g(y)\rangle$$
(une somme de produits scalaires est un produit scalaire). On désigne alors par H le supplémentaire orthogonal de F pour ce produit scalaire. Pour $g \in G$, $x \in H$ et $y \in F$, on a alors :
$$\begin{aligned}\varphi(g(x), y) = \sum_{u\in G} \langle u(g(x)) \mid u(y)\rangle &= \sum_{u\in G} \left\langle u\circ g(x) \mid u\circ g\left(g^{-1}(y)\right)\right\rangle \\ &= \sum_{v\in G} \left\langle v(x) \mid v\left(g^{-1}(y)\right)\right\rangle = \varphi\left(x, g^{-1}(y)\right)\end{aligned}$$
du fait que l'application $u \mapsto u\circ g$ est une permutation de G. Mais F est stable par g, donc $g(F) = F$ ($g(F) \subset F$ et l'égalité par les dimensions car g est un automorphisme) de sorte que $g^{-1}(y) = z \in F$ et $\varphi(x, g^{-1}(y)) = 0$. On a donc ainsi montré que $g(x) \in H$ pour tout $x \in H$, soit $g(H) \subset H$ et l'égalité par les dimensions. L'espace vectoriel H est donc un supplémentaire de F stable par G.

7. On sait qu'une matrice $A \in O_n(\mathbb{R})$ est semblable à une matrice diagonale par blocs de la forme :
$$D = \operatorname{diag}(I_p, -I_q, R(\theta_1), \cdots, R(\theta_s)),$$
où $R(\theta_k) = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k)\end{pmatrix}$ est la matrice de rotation d'angle $\theta_k \in]-\pi, \pi[\setminus\{0\}$.
La matrice A^m est alors semblable à la matrice :
$$D^m = \operatorname{diag}(I_p, (-1)^m I_q, R(m\theta_1), \cdots, R(m\theta_s))$$
et pour $A \in G$ la condition $A^m = I_n$ impose m pair et $m\theta_k \in]-m\pi, m\pi[\cap 2\pi\mathbb{Z}$, ce qui entraîne que les θ_k ne prennent qu'un nombre fini de valeurs. Avec :
$$\operatorname{tr}(A) = p - q + 2\sum_{k=1}^{s} \cos(\theta_k),$$
on déduit alors que les $\operatorname{tr}(A)$, pour A décrivant G, ne prennent qu'un nombre fini de valeurs, c'est-à-dire que $\operatorname{tr}(G)$ est fini.

8.

   (a) L'application $(A,B) \mapsto \operatorname{tr}(A\,{}^tB)$ définit un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$ (c'est le produit scalaire canonique de $\mathcal{M}_n(\mathbb{R})$ identifié à $\mathbb{R}^{n^2}$), donc sur F et la matrice B qui est la matrice de ce produit scalaire dans la base $\mathcal{B}$ est inversible (c'est une matrice de Gram).

   (b) Tout matrice $A \in G$ s'écrit, de manière unique :
$$A = \sum_{j=1}^{p} \lambda_j(A) A_j,$$
les $\lambda_j(A)$, pour j compris entre 1 et p, étant réels. On a alors pour tout i compris entre 1 et p :
$$\operatorname{tr}\left(A_i\,{}^tA\right) = \sum_{j=1}^{p} \lambda_j(A) \operatorname{tr}\left(A_i\,{}^tA_j\right)$$

et en notant :

$$\lambda(A) = \begin{pmatrix} \lambda_1(A) \\ \vdots \\ \lambda_p(A) \end{pmatrix}, \quad \tau(A) = \begin{pmatrix} \operatorname{tr}(A_1\,{}^tA) \\ \vdots \\ \operatorname{tr}(A_p\,{}^tA) \end{pmatrix},$$

cela s'écrit $\tau(A) = B\lambda(A)$, ce qui équivaut à $\lambda(A) = B^{-1}\tau(A)$, puisque B est inversible.
D'autre part, avec $A \in G \subset O_n(\mathbb{R})$, on a ${}^tA = A^{-1} \in G$ et $A_i\,{}^tA \in G$ pour tout i compris entre 1 et p. Avec l'hypothèse $\operatorname{tr}(G)$ fini, on déduit alors que $\tau(A)$ ne prend qu'un nombre fini de valeurs dans $\mathbb{R}^p$ quand A décrit G et il en est de même de $\lambda(A) = B^{-1}\tau(A)$. Il en résulte que le groupe G est fini.

9. L'ensemble G des matrices triangulaires supérieures réelles à diagonale unité forme un sous-groupe infini de $GL_n(\mathbb{R})$ avec $\operatorname{tr}(A) = n$ pour tout $A \in G$. Le résultat de la question **IV.7(b)** n'est donc pas vrai sur $GL_n(\mathbb{R})$.

10. Si A est nilpotente dans $\mathcal{M}_n(\mathbb{R})$, il en est de même de A^k pour tout entier naturel non nul k et 0 est la seule valeur propre complexe de A^k (le polynôme minimal d'une matrice nilpotente est de la forme X^p), donc $\operatorname{tr}\left(A^k\right) = 0$.
Pour la réciproque, on procède par récurrence sur $n \geq 1$. Pour $n = 1$, on a $\operatorname{tr}(A) = A$ et le résultat est trivial. Supposons le acquis pour les matrices réelles d'ordre au plus égal à n et soit $A \in \mathcal{M}_{n+1}(\mathbb{R})$ telle que $\operatorname{tr}\left(A^k\right) = 0$ pour tout $k \geq 1$. Si $P(X) = \sum_{k=0}^{n+1} \alpha_k X^k$ est le polynôme caractéristique de A, avec $P(A) = 0$ et $\operatorname{tr}\left(A^k\right) = 0$ pour $k = 1, \cdots, n+1$, on déduit que $\operatorname{tr}(P(A)) = n\alpha_0 = 0$ et $\alpha_0 = \det(A) = 0$, c'est-à-dire que 0 est valeur propre de A et il existe une matrice $P \in GL_{n+1}(\mathbb{R})$ telle que $P^{-1}AP = \begin{pmatrix} 0 & b \\ 0 & C \end{pmatrix}$ où $b \in \mathcal{M}_{1,n}(\mathbb{R})$ et $C \in \mathcal{M}_n(\mathbb{R})$. Avec $P^{-1}A^kP = \begin{pmatrix} 0 & bC^{k-1} \\ 0 & C^k \end{pmatrix}$, on déduit que $\operatorname{tr}\left(C^k\right) = \operatorname{tr}\left(A^k\right) = 0$ pour tout $k \geq 1$ et avec l'hypothèse de récurrence il en résulte que C est nilpotente. Enfin, en notant p l'indice de nilpotence de C, avec $A^{p+1} = P\begin{pmatrix} 0 & bC^p \\ 0 & C^{p+1} \end{pmatrix}P^{-1} = 0$, on déduit que A est nilpotente.

11.

(a) Si A, B dans G sont telles que $\varphi(A) = \varphi(B)$, on a alors $\operatorname{tr}((A-B)A_j) = 0$ pour tout j compris entre 1 et p et $\operatorname{tr}((A-B)X) = 0$ pour tout $X \in F$. On a alors $\operatorname{tr}((AB^{-1} - I_n)BX) = 0$ pour tout $X \in G$, ce qui équivaut à $\operatorname{tr}((AB^{-1} - I_n)Y) = 0$ pour tout $Y \in G$ puisque l'application $X \mapsto BX$ est une permutation de G. En posant $C = AB^{-1}$, on a $C \in G$ (c'est un groupe) et $\operatorname{tr}(CX) = \operatorname{tr}(X)$ pour tout $X \in G$, ce qui entraîne par récurrence $\operatorname{tr}\left(C^k\right) = \operatorname{tr}(I_n) = n$ pour tout $k \geq 1$. On a alors, pour tout $k \geq 1$:

$$\operatorname{tr}\left((C - I_n)^k\right) = \sum_{j=1}^{k} C_k^j (-1)^j \operatorname{tr}\left(C^{k-j}\right) = n\sum_{j=1}^{k} C_k^j (-1)^j = 0.$$

Il en résulte que la matrice $D = C - I_n$ est nilpotente. De plus la matrice C étant dans G est diagonalisable et il en est de même de D. En définitive la matrice D est diagonalisable et nilpotente, elle est donc nulle. On a donc $C = AB^{-1} = I_n$, c'est-à-dire que $A = B$. L'application φ est donc injective.

(b) Si $\operatorname{tr}(G)$ est fini alors $\varphi(G)$ est une partie finie de $\mathbb{R}^p$ en bijection avec G, il en résulte que G est fini.