Devoir surveillé $n°01$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

• • • • • • • • • • •

Exercice I

1. Considérons une relation $\lambda_1 P_1 + \cdots + \lambda_p P_p = 0$. Si $\lambda_p \neq 0$, le membre de gauche de l'inégalité est un polynôme de degré $\deg(P_p) \neq -\infty$ puisque tous les polynômes sont supposés non nuls. Ce ne peut donc pas être le polynôme nul et on trouve que $\lambda_p = 0$. En itérant le raisonnement (en faisant une récurrence), on trouve successivement $\lambda_{p-1} = \cdots = \lambda_1 = 0$, c'est-à-dire que la famille $(P_1, \ldots, P_p)$ est une famille libre.

2. (a) f est clairement une application linéaire. D'autre part, puisque

$$\deg(abP(X) + (1-a-b)XP'(X) + X^2P(X)) \leq \deg(P(X)),$$

l'application f est bien à image dans E.
Pour $k \in [\![0, n]\!]$, on a $f(X^k) = (ab + k(1-a-b) + k(k-1))X^k = (k-a)(k-b)X^k$.

(b) • Premier cas cas : $n < a < b$. L'image d'une base est une base, donc f est une bijection.
• Deuxième cas : $a < b < n$. Dans ce cas $f(X^a) = f(X^b) = 0$ et $f(X^k) \neq 0$ pour $k \neq a$ et b. Donc $\ker(f) = \mathrm{Vect}(X^a, X^b)$ et $\mathrm{Im}(f) = \mathrm{Vect}(X^k, k \neq a, b)$.
• Troisième cas : $a < n < b$. Dans ce cas $f(X^a) = 0$ et $f(X^k) \neq 0$ pour $k \neq a$. Donc $\ker(f) = \mathrm{Vect}(X^a)$ et $\mathrm{Im}(f) = \mathrm{Vect}(X^k, k \neq a)$.

(c) Ici $a = 1$ et $b = 2$. P est solution si et seulement si $\deg P \leq 3$. Posons donc $P = a + bX + cX^2 + dX^3$, l'équation s'écrit donc

$$af(1) + bf(X) + cf(X^2) + df(X^3) = \delta + \gamma X + \beta X^2 + \alpha X^3$$

ou encore

$$2a + 2dX^3 = \delta + \gamma X + \beta X^2 + \alpha X^3.$$

Si $\beta \neq 0$ ou $\gamma \neq 0$, alors pas de solutions. Si $\beta = \gamma = 0$, alors les solutions sont de la forme $\frac{\delta}{2} + bX + cX^2 + \frac{\alpha}{2}X^3$ où b et c sont des réels.

3. (a) Il est clair que l'application φ est linéaire. On voit bien que $\forall P \in \mathbb{R}_n[X],\ \varphi^2(P) = P$. Donc φ est un automorphisme de $\mathbb{R}_n[X]$ et $\varphi^{-1} = \varphi$. On a d'une manière évidente $\varphi(X^k) = X^{n-k}$ pour tout $k \in [\![0, n]\!]$.

(b) On a $E = \ker(\varphi - id_{\mathbb{R}_n[X]})$ et $F = \ker(\varphi + id_{\mathbb{R}_n[X]})$. Donc E et F sont bien des sous-espaces vectoriels de $\mathbb{R}_n[X]$.
Si $P \in E \cap F$, alors $P(X) = -P(X) = 0$, donc $P = 0$.
Les polynomes $X - 1$ et $X + 1$ sont premiers entre eux, donc il existe U est V des polynomes tels que

$$1 = (X-1)U + (X+1)V$$

et donc

$$id_{\mathbb{R}_n[X]} = (\varphi - id_{\mathbb{R}_n[X]})U(\varphi) + (\varphi + id_{\mathbb{R}_n[X]})V(\varphi)$$

puis, pour tout $P \in \mathbb{R}_n[X]$, on a :

$$P = \underbrace{(\varphi(P) - P)U(\varphi)(P)}_{=P_1} + \underbrace{(\varphi(P) + P)V(\varphi)(P)}_{=P_2} = P_1 + P_2$$

On a $\varphi(P_1) + P_1 = \varphi(P_2) - P_2 = 0$ et $\varphi(P_2) - P_2 = \varphi(P_1) + P_1 = 0$. D'où $P_1 \in E$ et $P_2 \in F$ et par conséquent $\mathbb{R}_n[X] = E \oplus F$.

4. • Premier cas : $n = 2p$. Si $P = a_{2p}X^{2p} + ... + a_1X + a_0$, alors la conditions $\varphi(P) = P$ s'écrit :

$$\begin{cases} a_0 &= a_{2p} \\ a_1 &= a_{2p-1} \\ & \vdots \\ a_{p-1} &= a_{p+1} \end{cases}$$

Donc $P = a_0(1 + X^{2p}) + a_1(X + X^{2p-1}) + ... + a_{p-1}(X^{p-1} + X^{p+1}) + a_pX^p$. D'où,

$$E = \mathrm{Vect}(1 + X^{2p}, X + X^{2p-1}, ..., X^{p-1} + X^{p+1} + X^p)$$

et $\dim E = p + 1$.

• Deuxième cas : $n = 2p + 1$. Si $P = a_{2p+1}X^{2p+1} + ... + a_1X + a_0$, alors la conditions $\varphi(P) = P$ s'écrit :

$$\begin{cases} a_0 &= a_{2p+1} \\ a_1 &= a_{2p} \\ & \vdots \\ a_p &= a_{p+1} \end{cases}$$

Donc $P = a_0(1 + X^{2p+1}) + a_1(X + X^{2p}) + ... + a_p(X^p + X^{p+1})$. D'où,

$$E = \mathrm{Vect}(1 + X^{2p+1}, X + X^{2p}, ..., X^{p-1} + X^p + X^{p+1})$$

et $\dim E = p + 1$.

Exercice II

1. Changement de base

(a) On a

$$\begin{aligned}
\det(A - \lambda I_3) &= \det\begin{pmatrix} \frac{7}{2} - \lambda & \frac{-3}{2} & \frac{-1}{2} \\ \frac{3}{2} & \frac{1}{2} - \lambda & \frac{-1}{2} \\ 1 & -1 & 1 - \lambda \end{pmatrix} \\
&= \det\begin{pmatrix} 2 - \lambda & \frac{-3}{2} & \frac{-1}{2} \\ 2 - \lambda & \frac{1}{2} - \lambda & \frac{-1}{2} \\ 0 & -1 & 1 - \lambda \end{pmatrix}_{C_1 \leftarrow C_1 + C_2} \\
&= (2 - \lambda)\det\begin{pmatrix} 1 & \frac{-3}{2} & \frac{-1}{2} \\ 1 & \frac{1}{2} - \lambda & \frac{-1}{2} \\ 0 & -1 & 1 - \lambda \end{pmatrix} \\
&= (2 - \lambda)\det\begin{pmatrix} 1 & \frac{-3}{2} & \frac{-1}{2} \\ 0 & 2 - \lambda & 0 \\ 0 & -1 & 1 - \lambda \end{pmatrix}_{L_2 \leftarrow L_2 - L_1} \\
&= (2 - \lambda)^2(1 - \lambda).
\end{aligned}$$

(b) Déterminons $\ker(f - id_{\mathbb{R}^3})$. Un vecteur $X = {}^t(x, y, z) \in \mathbb{R}^3$ est dans $\ker(f - id_{\mathbb{R}^3})$ si et seulement si $(A - I_3)X = 0$, donc $\begin{cases} x - y = 0 \\ 2y - z = 0 \end{cases}$. D'où $\ker(f - id_{\mathbb{R}^3}) = \mathrm{Vect}(1, 1, 2)$, c'est une droite vectorielle.

Déterminons $\ker(f - 2id_{\mathbb{R}^3})$. Pour $X = {}^t(x, y, z) \in \mathbb{R}^3$,

$$(A - 2I_3)X = 0 \iff \left\{ \begin{array}{rcl} x - y & = & 0 \\ z & = & 0 \end{array} \right. ,$$

donc $\ker(f - 2id_E) = \mathrm{Vect}(1, 1, 0)$ c'est une droite vectorielle.

(c) D'après la question précdente $e_1 = (1, 1, 2)$ et $e_2 = (1, 1, 0)$.

2. (a) Un vecteur $u = (x, y, z)$ appartient à $\mathrm{Vect}(e_1, e_2)$ si et seulement si il existe $(\alpha, \beta) \in \mathbb{R}^2$ tel que $u = \alpha e_1 + \beta e_2$. Ceci équivaut à

$$(1) \left\{ \begin{array}{rcl} x & = & \alpha + \beta \\ y & = & \alpha + \beta \\ z & = & 2\alpha \end{array} \right.$$

et ceci implique que $x = y$.

Réciproquement, si $x = y$, alors en posant $\alpha = \dfrac{z}{2}$ puis $\beta = x - \alpha = x - \dfrac{z}{2}$ alors le système (1) est vérifié, et donc on a bien $u = \alpha e_1 + \beta e_2$. Nous avons donc démontré que $u = (x, y, z)$ appartient à $\mathrm{Vect}(e_1, e_2)$ si et seulement si $x = y$.

(b) On calcule le déterminant de la famille $\mathscr{B}$. On a

$$\det(e_1, e_2, e_3) = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{vmatrix}.$$

L'opération élémentaire $(L_1 \leftarrow L_1 - L_2)$ donne

$$\det(e_1, e_2, e_3) = \begin{vmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{vmatrix}.$$

En développant par rapport à la première ligne, ou en utilisant la règle de Sarrus, on obtient

$$\det(e_1, e_2, e_3) = -2.$$

Ce déterminant est non-nul, donc par théorème du cours la famille $\mathscr{B}$ est une base de $\mathbb{R}^3$.

3. (a) D'après la question précédente le déterminant de P est égal à -2, il est non nul donc P est inversible. On a $PP^{-1} = I_3$, donc

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Les opérations $(L_2 \leftarrow L_2 - L_1)$ et $(L_3 \leftarrow L_3 - 2L_1)$ donnent

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -2 & -1 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}.$$

L'opération $(L_2 \leftrightarrow L_3)$ donne

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & -1 \\ 0 & 0 & -1 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$

Les opérations $(L_2 \leftarrow L_2 - L_3)$ puis $(L_1 \leftarrow L_1 + L_3)$ donnent

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix} P^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$

Les opérations $(L_3 \leftarrow -L_3)$ puis $(L_2 \leftarrow -\frac{1}{2}L_2)$ donnent

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} P^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{-1}{2} \\ 1 & -1 & 0 \end{pmatrix}.$$

Enfin l'opération $(L_1 \leftarrow L_1 - L_2)$ donne

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} P^{-1} = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix}.$$

On a donc obtenu la matrice inverse de P :

$$P^{-1} = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix}.$$

(b) Soit $T = P^{-1}AP$. On calcule T :

$$\begin{aligned} T &= \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 7 & -3 & -1 \\ 3 & 1 & -1 \\ 2 & -2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}. \\ &= \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 2 & 4 & 6 \\ 2 & 4 & 2 \\ 4 & 0 & 4 \end{pmatrix}. \\ &= \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 0 & 2 \end{pmatrix}. \\ &= \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 0 & 4 \end{pmatrix} \end{aligned}$$

Et donc finalement

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

4. Commutant de A.

(a) i. D'après ce qui précède,

$$TN = (P^{-1}AP)(P^{-1}MP) = P^{-1}APP^{-1}MP.$$

Comme $PP^{-1} = I_3$ et $AM = MA$, alors

$$TN = P^{-1}AMP = P^{-1}MAP.$$

De même,

$$NT = (P^{-1}MP)(P^{-1}AP) = P^{-1}MAP.$$

On a donc bien $TN = NT$.

ii. On obtient

$$TN = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} = \begin{pmatrix} a & d & g \\ 2b+c & 2e+f & 2h+i \\ 2c & 2f & 2i \end{pmatrix}$$

et

$$NT = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} a & 2d & d+2g \\ b+2c & 2e & e+2h+ \\ c & 2f & f+2i \end{pmatrix}.$$

L'égalité $TN = NT$ donne les neuf équations suivantes :

$$a = a, d = 2d, g = d + 2g, 2b + c = b, 2e + f = 2e, 2h + i = e + 2h, 2c = c, 2f = 2f, 2i = f + 2i.$$

Ceci donne exactement $b = c = d = f = g = 0$ et $e = i$.

iii. D'après la question précédente, on a $TN = NT$ si et seulement si N s'écrit sous la forme

$$N = \begin{pmatrix} a & 0 & 0 \\ 0 & e & h \\ 0 & 0 & e \end{pmatrix}.$$

Or on a $N = P^{-1}MP$, donc en multipliant cette égalité par P à gauche et par P^{-1} à droite, on obtient $M = PNP^{-1}$, donc

$$\begin{aligned} M &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & e & h \\ 0 & 0 & e \end{pmatrix} \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} -a+3e+2h & a-e-2h & a-e \\ -a+e+2h & a+e-2h & a-e \\ -2a+2e & 2a-2e & 2a \end{pmatrix}. \end{aligned}$$

On peut écrire cette matrice sous la forme :

$$M = \frac{a}{2} \begin{pmatrix} -1 & 1 & 1 \\ -1 & 1 & 1 \\ -2 & 2 & 2 \end{pmatrix} + \frac{e}{2} \begin{pmatrix} 3 & -1 & -1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix} + h \begin{pmatrix} 1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (2)$$

(b) Si M est une matrice vérifiant $AM = MA$, alors d'après les questions précédentes on peut écrire M sous la forme (4). Réciproquement, si M s'écrit sous cette forme, alors on a $M = PNP^{-1}$ où N est de la forme

$$N = \begin{pmatrix} a & 0 & 0 \\ 0 & e & h \\ 0 & 0 & e \end{pmatrix}.$$

On a donc $TN = NT$, d'après ce qui précède, et ceci montre que $AM = MA$.
Ainsi, l'ensemble des matrices M de $\mathscr{M}_3(\mathbb{R})$ vérifiant $AM = MA$ est l'ensemble des matrices données par la formule (2) où a, e et h sont trois réels. C'est le sous-espace vectoriel engendré par les matrices $\begin{pmatrix} -1 & 1 & 1 \\ -1 & 1 & 1 \\ -2 & 2 & 2 \end{pmatrix}$, $\begin{pmatrix} 3 & -1 & -1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, il est de dimension 3.

Exercice III

1. e est élément de Z_G car $ex = xe$ pour tout $x \in G$. Soient $g, h \in Z_G$. Alors, pour tout $x \in G$, on a

$$ghx = g(hx) = (gx)h = xgh$$

et donc $gh \in Z_G$.
Enfin, si $g \in Z_G$, alors pour tout $x \in G$,

$$gx = xg \Rightarrow gxg^{-1} = xgg^{-1} = x \Rightarrow g^{-1}gxg^{-1} = g^{-1}x \Rightarrow xg^{-1} = g^{-1}x$$

où on a multiplié à droite puis à gauche par g^{-1}. On en déduit que $g^{-1} \in Z_G$ qui est donc un sous-groupe de G.

2. • Puisque $(\mathbb{Z}, +)$ est commutatif, alors $Z_{\mathbb{Z}} = \mathbb{Z}$.
• Remarquons d'abord que si $A = \lambda I_n$, $\lambda \in \mathbb{R}^*$, alors A commute avec toutes les matrices de $\mathbf{GL_n}(\mathbb{R})$ et donc A est dans le centre de $\mathbf{GL_n}(\mathbb{R})$.
Réciproquement, supposons que A commute avec toutes les matrices inversibles. Soit $i \neq j$, pour $M = I_n + E_{ij}$, $AM = MA$ donne $AE_{ij} = E_{ij}A$ où $(E_{ij})_{1 \leq i,j \leq n}$ désigne la base canonique de $\mathscr{M}_n(\mathbb{R})$.
Posons $A = \displaystyle\sum_{l=1}^{n}\sum_{k=1}^{n} a_{lk}E_{lk}$. Donc

$$AE_{ij} = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{lk}E_{lk}E_{ij} = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{lk}\delta_{ki}E_{lj} = \sum_{l=1}^{n} a_{li}E_{lj}$$

et

$$E_{ij}A = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{lk}E_{ij}E_{lk} = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{lk}\delta_{jl}E_{ik} = \sum_{k=1}^{n} a_{jk}E_{ik}.$$

Donc le seul terme que peuvent avoir en commun les deux matrices AE_{ij} et $E_{ij}A$ est situé sur la i-ème ligne et la j-ème colonne. Les coefficients correspondants doivent être égaux et donc on doit avoir $a_{ii} = a_{jj}$. Les autres coefficients doivent être nuls, ce qui signifie en particulier, pour $l \neq k$, que $a_{lk} = 0$. Ainsi, A est une matrice diagonale dont tous les coefficients diagonaux doivent être égaux et non nuls. On en déduit que $A = \lambda I_n$, $\lambda \in \mathbb{R}^*$. En conclusion,

$$Z_{\mathbf{GL_n}(\mathbb{R})} = \{\lambda I_n / \lambda \in \mathbb{R}^*\}.$$

• Soit σ une permutation qui commute avec toutes les permutations, en particulier $\sigma(1,2) = (1,2)\sigma$ ou encore $\sigma(1,2)\sigma^{-1} = (1,2)$. Mais $\sigma(1,2)\sigma^{-1} = (\sigma(1), \sigma(2))$, donc $\sigma(1) = 1$ et $\sigma(2) = 2$, puis $\sigma(3) = 3$. Ainsi

$$Z_{\mathscr{S}_n} = \{e\}$$

où e désigne l'élément neutre de $\mathscr{S}_3$.

3. e est élément de G_x car $ex = xe$. Soient $g, h \in G_x$. Alors on a $ghx = g(hx) = (gx)h = xgh$ et donc $gh \in G_x$.
Enfin, si $g \in G_x$, alors

$$gx = xg \Rightarrow gxg^{-1} = xgg^{-1} = x \Rightarrow g^{-1}gxg^{-1} = g^{-1}x \Rightarrow xg^{-1} = g^{-1}x$$

où on a multiplié à droite puis à gauche par g^{-1}. On en déduit que $g^{-1} \in G_x$ qui est donc un sous-groupe de G.

4. (a) • $\mathscr{R}$ est réflexive car $\forall x \in G$, $x\mathscr{R}x$ puisque $xe = ex$.
• $\mathscr{R}$ est symétrique, en effet, si $x\mathscr{R}y$, alors il existe $g \in G$ tel que $xg = gy$ ou encore $yg^{-1} = g^{-1}x$ et donc $y\mathscr{R}x$.
• $\mathscr{R}$ est transitive : si $x\mathscr{R}y$ et $y\mathscr{R}z$, alors il existe g et h dans G tels que $xg = gy$ et $yh = hz$, donc $xgh = gyh = ghz$ et par suite $x\mathscr{R}z$.
En conclusion, $\mathscr{R}$ est une relation d'équivalence sur G. De même, on peut vérifier facilement que $\mathscr{S}$ est une relation d'équivalence sur G.

(b) • Soient a et b de G tels que $\overline{a} = \overline{b}$, donc $ab^{-1} \in G_x$ ou encore $ab^{-1}x = xab^{-1}$ ce qui entraine $a^{-1}xa = b^{-1}xb$ et par conséquent $\varphi(\overline{a}) = \varphi(\overline{b})$. Ainsi φ est bien définie.
• φ est injective : on a :

$$\varphi(\overline{a}) = \varphi(\overline{b}) \Leftrightarrow a^{-1}xa = b^{-1}xb \Leftrightarrow ab^{-1} \in G_x \Leftrightarrow \overline{a} = \overline{b}.$$

Donc φ est injective.
• Soit $y \in \Theta_x$, donc $x\mathscr{R}y$ et alors il existe $g \in G$ tel que $y = g^{-1}xg = \varphi(\overline{g})$. D'où la surjectivité.

(c) Considérons l'application

$$\begin{array}{rccl} f: & \overline{a} & \longrightarrow & G_x \\ & b & \longmapsto & f(b) = ab^{-1} \end{array}$$

f est bien définie et est une bijection. En effet, si $f(b) = f(b')$ alors $ab^{-1} = ab'^{-1}$ et donc $b' = b$, de plus si $c \in G_x$, alors $c = a(a^{-1}c) = f(c^{-1}a)$. D'où l'égalité entre cardinaux :

$$\text{card}(\overline{a}) = \text{card}(G_x).$$

On a $\text{card}\,([G : G_x]) = \text{card}(\Theta_x)$. Or $G = \bigcup_{\overline{a} \in [G:G_x]} \overline{a}$, alors

$$\text{card}(G) = \sum_{\overline{a} \in [G:G_x]} \text{card}(\overline{a}) = \text{card}(\Theta_x) \times \text{card}(\overline{a}) = \text{card}(\Theta_x) \times \text{card}(G_x).$$

D'où

$$\text{card}(\Theta_x) = \frac{\text{card}(G)}{\text{card}(G_x)}.$$

(d) Si $x \in Z_G$, alors $xg = gx$ pour tout $g \in G$ et donc $O_x = \{x\}$ et par conséquent $\text{card}(O_x) = 1$.

(e) On a $G = \left(\bigcup_{i=1}^{r} \Theta_{x_i}\right) \cup \left(\bigcup_{x \in Z_G} \Theta_x\right)$, donc par passage au cardinal, on obtient l'égalité demandée :

$$\text{card}(G) = \sum_{i=1}^{r} \text{card}(\Theta_{x_i}) + \text{card}\left(\bigcup_{x \in Z_G} \Theta_x\right) = \sum_{i=1}^{r} \frac{\text{card}(G)}{\text{card}(G_{x_i})} + \text{card}(Z_G).$$

5. On a $\text{card}\, Z(G) = \text{card}(G) - \sum_{i=1}^{r} \frac{\text{card}(G)}{\text{card}(G_{x_i})}$. La somme indexée par i est une somme de puissances non nulles de p. Il en résulte que $\text{card}\,(Z_G)$ est divisible par p et ne peut donc être égal à 1.

• • • • • • • • • • •