

Exercice 1 *Théorème de Lagrange et conséquences*

1. Démontrer le théorème de Lagrange :

Soient G un groupe d'ordre fini et H un sous-groupe de G . L'ordre de H divise l'ordre de G .

2. En déduire les corollaires suivants :

a) Dans tout groupe G d'ordre fini, l'ordre d'un élément a divise l'ordre de G .

b) Si G est un groupe d'ordre n , alors, pour tout a dans G , on a : $a^n = 1$.

c) Tout groupe d'ordre un nombre premier est cyclique.

3. Applications :

a) Théorème d'Euler :

On note $\varphi(n) = \text{Card}\{m \in [1, n] \text{ tel que } (m, n) = 1\}$

Soit n un entier supérieur ou égal à 2. Soit $a \in \mathbb{Z}^*$ que $(a, n) = 1$. Alors : $a^{\varphi(n)} = 1 [n]$

b) Petit théorème de Fermat :

Soit p un nombre premier.

i) Pour tout $a \in \mathbb{Z}^*$ tel que $(a, p) = 1$: $a^{p-1} = 1 [p]$

ii) Pour tout $a \in \mathbb{Z}$, on a : $a^p = a [p]$

Exercice 2 *Groupes cycliques*

Soit G un groupe cyclique fini.

1. Démontrer que G est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ avec $m \in \mathbb{N}^*$.

2. Démontrer que tout sous-groupe de G est encore cyclique.

3. Démontrer que pour tout diviseur d de l'ordre de G , il existe un unique sous-groupe H de G d'ordre d .

Exercice 3 *Théorème de Cayley*

Le but de cet exercice est de démontrer que tout groupe fini G d'ordre n est isomorphe à un sous-groupe de $\text{Bij}(G)$ (groupe des bijections de G dans lui même)

1. Soit $g \in G$. On considère l'application suivante :

$$\begin{aligned} \varphi_g : G &\rightarrow G \\ x &\mapsto gx \end{aligned}$$

Démontrer que φ_g est bijective.

2. On considère maintenant l'application θ suivante :

$$\begin{aligned} \theta : G &\rightarrow \text{Bij}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

Démontrer que θ est un morphisme de groupes.

Démontrer que θ est injectif et conclure.

Exercice 4 Groupe Diédral

Soit n un entier supérieur ou égal à 3.

On se propose de déterminer l'ensemble G des isométries (du plan) préservant les sommets d'un n -gone.

Soient O le centre du n -gone, A_0 l'un de ses sommets et g un élément de G .

On note A_0, A_1, \dots, A_{n-1} les sommets du n -gone, dans cet ordre.

On note s la symétrie d'axe (OA_0) et r_i la rotation de centre O qui envoie A_0 en A_i . ($0 \leq i \leq n-1$)

1. Démontrer que G est un groupe dont l'ordre divise $n!$.
2. a) On suppose dans cette question de $g(A_0) = A_0$. Que peut-on dire de g ?
b) On suppose dans cette question de $g(A_0) = A_i$. ($1 \leq i \leq n-1$)

Démontrer que : $g = r_i$ ou $g = r_i \circ s$

- c) En déduire que : $G = \langle r, s \rangle$ où $r = r_1$

Préciser l'ordre de G .

3. Compositions d'éléments de G :

a) Démontrer que : $s \circ r \circ s \circ r = Id$

b) Démontrer que : $\forall i, j \in [0, n-1]^2, (r^i \circ s) \circ (r^j \circ s) = r^{i-j}$

Exercice 5 Formule des classes - Applications aux p -groupes

Soit G un groupe fini.

On appelle centre de G l'ensemble : $Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$

1. Démontrer que $Z(G)$ est un sous-groupe distingué de G .
2. On fait opérer G sur lui-même par conjugaison :

$$G \times G \rightarrow G \\ (g, x) \mapsto g \cdot x = gxg^{-1}$$

On note pour tout x de G : $S_x = \{g \in G \mid g \cdot x = x\}$ (stabilisateur de x)

Démontrer la formule des classes suivante :

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_{x \in I'} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

Où I' est une partie de G contenant exactement un représentant non central de chaque classe de conjugaison.

3. Applications aux p -groupes. (Groupes d'ordre p^α , où p premier et $\alpha \in \mathbb{N}^*$)
 - a) Démontrer que le centre d'un p -groupe est non trivial. (C'est-à-dire non réduit à l'élément neutre)
 - b) Démontrer que pour $\alpha = 2$ les p -groupes sont abéliens.

Exercice 1

1. Notons multiplicativement la loi de G .

Définissons, sur G , une relation \mathcal{R} par :

$$\forall (x, y) \in G^2, (x \mathcal{R} y \Leftrightarrow x^{-1}y \in H)$$

a. Montrons que \mathcal{R} est une relation d'équivalence :

- $x^{-1}x = 1 \in H$ donc $x \mathcal{R} x$, **\mathcal{R} est réflexive.**
- $x \mathcal{R} y \Leftrightarrow x^{-1}y \in H \stackrel{H \text{ sous groupe}}{\Leftrightarrow} (x^{-1}y)^{-1} \in H \Leftrightarrow y^{-1}x \in H \Leftrightarrow y \mathcal{R} x$, donc **\mathcal{R} est symétrique.**
- $(x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow (x^{-1}y \in H \text{ et } y^{-1}z \in H) \Rightarrow (x^{-1}y y^{-1}z = x^{-1}z \in H) \Rightarrow (x \mathcal{R} z)$, **\mathcal{R} est transitif.**

Donc \mathcal{R} est bien une **relation d'équivalence**.

La classe d'équivalence d'un élément a de G est, par définition :

$$\{y \in G \mid a \mathcal{R} y\} = \{y \in G \mid a^{-1}y \in H\} = \{y \in G \mid \exists h \in H, a^{-1}y = h\} = \{y \in G \mid \exists h \in H, y = ah\} = aH$$

Cet ensemble est appelé **classe à gauche (de a) modulo H** .

b. Montrons que toutes les classes à gauche ont $|H|$ éléments :

Pour cela, on considère, pour tout $a \in G$, l'application

$$\begin{aligned} \varphi_a : H &\rightarrow aH \\ h &\mapsto ah \end{aligned}$$

- $\varphi_a(h_1) = \varphi_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$, donc φ_a est **injective**.
- $\forall y \in aH, \exists h \in H$ tel que $y = ah$ donc φ_a est **surjective**.

φ_a étant **bijective**, on déduit :

$$\forall a \in G, |aH| = |H|$$

c. Montrons que toutes les classes à gauche sont disjointes :

Considérons deux classes aH et bH (a et b dans G) et supposons $aH \cap bH \neq \emptyset$.

Soit $g \in aH \cap bH$. Alors :

$$\exists h \in H \text{ tel que } g = ah \text{ et } \exists h' \in H \text{ tel que } g = bh'$$

On a alors : $ah = bh'$

$$a = bh'h^{-1}$$

Tout élément ah'' de aH s'écrit donc : $bh'h^{-1}h''$

Or, $h'h^{-1}h'' \in H$, donc tout élément ah'' de aH est aussi élément de bH , d'où :

$$aH \subset bH$$

On montre, de même : $bH \subset aH$

On a donc : $aH = bH$

Ceci prouve que **les classes à gauches sont disjointes**.

Remarque : on pouvait affirmer ce résultat directement car les classes d'équivalences forment une partition de G .

d. Concluons :

En notant m le nombre de classes à gauches, on a donc :

$$G = \coprod_{n=1}^m a_n H$$

D'où :

$$|G| = \sum_{n=1}^m |a_n H| = \sum_{n=1}^m |H| = m|H|$$

L'ordre du sous-groupe H divise donc l'ordre du groupe G .

Notons que cette démonstration peut se faire aussi en raisonnant sur les classes à droite Ha et, qu'en cas de groupe commutatif, les classes à gauche et à droite coïncident ($aH = Ha$).

2. Preuve des corollaires :

- Comme G est fini d'ordre n , le sous-groupe $\langle a \rangle$ est aussi fini d'ordre m . On applique alors le théorème de Lagrange au sous groupe $\langle a \rangle$ pour obtenir : $m \mid n$.
- Soit m l'ordre a . (On a donc : $a^m = 1$). On sait que m divise n : $n = km$. Donc $a^n = (a^m)^k = 1$.
- Soit G un groupe d'ordre un nombre premier p . Soit $a \neq 1$ dans G . Notons m son ordre ($m > 1$ car $a \neq 1$). Comme m divise p , on a nécessairement $m = p$ donc $G = \langle a \rangle$.

3. a) Puisque a est premier avec n , on a : $\bar{a} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ (groupe multiplicatif d'ordre $\varphi(n)$)

Notons d l'ordre de \bar{a} . D'après le corollaire 2.a) du théorème de Lagrange : d divise $\varphi(n)$.

Donc il existe $k \in \mathbb{N}^*$ tel que : $\varphi(n) = kd$

D'où : $\bar{a}^{\varphi(n)} = (\bar{a}^d)^k = \bar{1}$ (Égalité dans $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$)

Donc $a^{\varphi(n)} = 1 [n]$

b) Comme $(a, p) = 1$, le théorème d'Euler permet d'affirmer : $a^{\varphi(p)} = 1 [p]$

Et comme p est premier, $\varphi(p) = p - 1$, d'où : $a^{p-1} = 1 [p]$

Ce qui prouve le premier point. Pour le second :

- si $(a, p) = 1$, alors il suffit de multiplier l'égalité ci-dessus par a pour obtenir : $a^p = a [p]$
- si $(a, p) \neq 1$, alors p divise a . Donc a et a^p sont des multiples de p , donc : $a^p = a = 0 [p]$

On a donc bien : $\forall a \in \mathbb{Z}, a^p = a [p]$

Exercice 2

1. Comme G est cyclique, il est de la forme :

$$G = \{a^n, n \in \mathbb{Z}\} \quad \text{où } a \in G \text{ (} a \text{ s'appelle un générateur de } G \text{)}$$

Montrons que si G est fini, alors G est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ pour $m \in \mathbb{N}^*$.

Pour cela, on considère l'application :

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow G \\ n &\mapsto a^n \end{aligned}$$

- $\text{Im}(\varphi_a) = G$ donc φ_a est **surjectif**. (Car G est cyclique engendré par a)
- $\varphi_a(n + n') = a^{n+n'} = a^n \times a^{n'} = \varphi_a(n) \times \varphi_a(n')$ donc φ_a est un **morphisme de groupes**.

On sait que le noyau d'un morphisme de groupe est un sous-groupe, donc :

$$\text{Ker}(\varphi_a) = \{n \in \mathbb{Z} \mid a^n = 1\} \text{ est un } \mathbf{\text{sous-groupe de } \mathbb{Z}}$$

Par conséquent, il existe $m \in \mathbb{N}$ tel que : $\text{Ker}(\varphi_a) = m\mathbb{Z}$

Deux cas se présentent alors :

$m = 0$: et alors $\text{Ker}(\varphi_a) = \{0\}$, φ_a est injective et donc bijective. Donc G est infini et isomorphe à $(\mathbb{Z}, +)$. Ce qui n'est pas le cas, par hypothèse.

$m \in \mathbb{N}^*$: dans ce cas, φ_a n'est pas injective. Mais :

$$\varphi_a(n) = \varphi_a(n') \Rightarrow a^n = a^{n'} \Rightarrow a^{n-n'} = 1 \Rightarrow n - n' \in \text{Ker}(\varphi_a) \Rightarrow n - n' \in m\mathbb{Z} \Rightarrow n = n' [m]$$

$\varphi_a(n)$ ne dépend donc que de la classe \bar{n} de n modulo m .

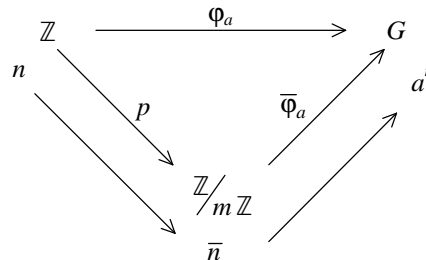
Définissons alors :

$$\begin{aligned} \bar{\varphi}_a : \mathbb{Z}/\text{ker}(\varphi_a) = \mathbb{Z}/m\mathbb{Z} &\rightarrow G \\ \bar{n} &\mapsto a^n \end{aligned}$$

Ainsi, ce nouveau morphisme $\bar{\varphi}_a$ est injectif (puisque $\bar{\varphi}_a(\bar{n}) = \bar{\varphi}_a(\bar{n}') \Rightarrow \bar{n} = \bar{n}'$) et surjectif.

Donc G est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

On dit que l'on a factorisé le morphisme φ_a :



L'entier $m \in \mathbb{N}^*$ vérifie donc $a^m = 1$ et c'est le plus petit. (En effet : $a^k = 1 \Rightarrow k \in \text{Ker}(\varphi_a) \Rightarrow k \in m\mathbb{Z}$)

Cet entier m s'appelle **l'ordre de l'élément a** .

2. Soit H un sous-groupe de G . Soit a un générateur de G .

Posons $d = \min\{n \in \mathbb{N}^* \mid a^n \in H\}$

(Cet entier d existe bien car $G = \langle a^n \rangle$ et tout ensemble non vide de \mathbb{N} admet un plus petit élément)

On a évidemment $a^d \in H$ et par conséquent $\langle a^d \rangle \subset H$.

Réciproquement, montrons que $H \subset \langle a^d \rangle$:

Soit $h \in H$. Alors, il existe $n \in \mathbb{N}^*$, $n \geq d$, tel que : $h = a^n$

Effectuons la division euclidienne de n par d :

$$\exists(q, r) \in \mathbb{N}^* \times \llbracket 0, d-1 \rrbracket, n = qd + r$$

Alors :

$$h = a^n = a^{qd+r} = (a^d)^q a^r$$

Or, comme $h \in H$ et $a^d \in H$ (et donc $(a^d)^q \in H$) on a :

$$a^r \in H$$

Et comme $r \in \llbracket 0, d-1 \rrbracket$, la définition de d implique : $r = 0$.

Donc $h = (a^d)^q$. Autrement dit, $h \in \langle a^d \rangle$. On en déduit : $H \subset \langle a^d \rangle$. Donc H est cyclique.

3. Soit a un générateur de G .

Soit d un diviseur de m : $\exists q \in \mathbb{N}, m = dq$.

Notons $H = \langle a^q \rangle$ et montrons que H est d'ordre d :

Il est clair que : $(a^q)^d = a^{qd} = a^m = 1$. Ce qui prouve déjà que d divise l'ordre de a^q .

S'il existe $d' < d$ tel que $(a^q)^{d'} = 1$ alors, qd' serait multiple de $m = dq$ (puisque a est d'ordre m car générateur de G). Donc d' serait multiple de d . Absurde car $d' < d$.

Ceci prouve que l'ordre de a^q est bien d .

Donc H est bien d'ordre d .

Montrons l'unicité :

Soit H' un sous-groupe cyclique de G d'ordre d .

Donc H' est engendré par un certain élément qui sera lui-même une certaine puissance du générateur a de G .

On peut donc écrire : $H' = \langle a^{q'} \rangle$ avec $q' \in \mathbb{N}$

Et comme H' est d'ordre d : dq' multiple de $m = dq$

Donc : q' multiple de q

Ce qui prouve : $H' \subset H$

Et comme les ordres sont égaux : $H' = H$

Exercice 3 Théorème de Cayley

1. Comme G est fini, il suffit de prouver l'injectivité.

Soient x et y dans G tels que :

$$\varphi_g(x) = \varphi_g(y)$$

$$gx = gy$$

Comme G est un groupe, g^{-1} existe. En multipliant à gauche par g^{-1} , on obtient bien :

$$x = y$$

Donc φ_g est injective et, par suite, bijective.

2. Soient g et g' deux éléments de G . On a :

$$\forall x \in G, \theta(gg')(x) = \varphi_{gg'}(x) = gg'x = \varphi_g(g'x) = \varphi_g \circ \varphi_{g'}(x) = \theta(g) \circ \theta(g')(x)$$

D'où : $\theta(gg') = \theta(g) \circ \theta(g')$

Ce qui prouve que θ est un morphisme de groupes.

Montrons que θ est injectif :

Soient g et g' dans G tels que : $\theta(g) = \theta(g')$

Alors : $\forall x \in G, \theta(g)(x) = \theta(g')(x)$

C'est-à-dire : $\varphi_g(x) = \varphi_{g'}(x)$

$$gx = g'x$$

Et en multipliant à droite par x^{-1} : $g = g'$

Ce qui prouve l'injectivité du morphisme θ .

On sait que l'image $\text{Im}(\theta)$ du morphisme θ est un sous-groupe de $\text{Bij}(G)$.

On a donc un isomorphisme entre G et un sous-groupe de $\text{Bij}(G)$.

Exercice 4 *Groupe Diédral*

1) Il est clair que G est un sous-groupe du groupe symétrique S_n . D'après le théorème de Lagrange, on peut affirmer que l'ordre de G divise n !

2) a) g possède déjà deux points fixes. Il y a évidemment A_0 . Mais également O . En effet, comme g est affine, elle conserve le barycentre d'une famille de points. Donc $g(O) = O$.

(Car O est l'isobarycentre de A_0, A_1, \dots, A_{n-1})

En conséquence, g fixe la droite (A_0O) . (Puisque cette droite est l'ensemble des barycentres de A_0 et O)

On en déduit : $g = s$ ou $g = Id$

b) On a : $r_i^{-1} \circ g(A_0) = r_i^{-1}(A_i) = A_0$.

Et d'après a) : $r_i^{-1} \circ g = s$ ou $r_i^{-1} \circ g = Id$

D'où : $g = r_i \circ s$ ou $g = r_i$

De plus, ces deux isométries sont bien distinctes puisque l'on a, par exemple :

$$r_i \circ s(A_1) = r_i(A_{n-1}) = A_{i-1 [n]} \text{ et } r_i(A_1) = A_{i+1 [n]}$$

Or, $i-1 = i+1 [n]$ entraîne, $2 = 0 [n]$ ce qui est exclu car $n \geq 3$. Donc $r_i \circ s(A_1) \neq r_i(A_1)$.

c) D'après les questions a) et b), on a examiné toutes les possibilités de transformation du point A_0 .

(À chaque image possible de A_0 correspond deux isométries distinctes).

On a la liste des isométries suivantes :

$$Id, r_1, r_2, \dots, r_{n-1}, r_1 \circ s, r_2 \circ s, \dots, r_{n-1} \circ s$$

En notant $r = r_1$, on a bien : $G = \langle r, s \rangle$

L'ordre de G est $2n$. (Et : $|\langle r \rangle| = n, |\langle s \rangle| = 2$)

3) a) $r \circ s \circ r(A_0) = r \circ s(A_1) = r(A_{n-1}) = A_0$.

Donc, d'après 2)a) : $r \circ s \circ r = Id$ ou $r \circ s \circ r = s$

Or : $r \circ s \circ r(A_1) = r \circ s(A_2) = r(A_{n-2}) = A_{n-1}$. Donc $r \circ s \circ r \neq Id$.

D'où : $r \circ s \circ r = s$

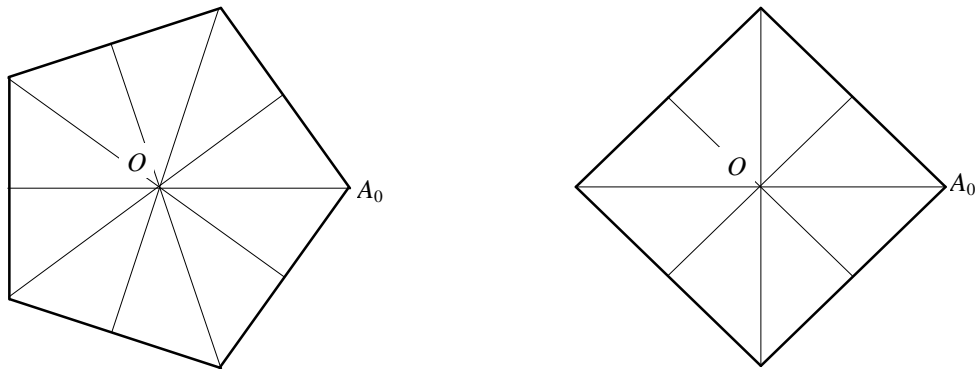
$$s \circ r \circ s \circ r = Id$$

(On a aussi : $r \circ s \circ r \circ s = Id$)

b) Utilisons $r \circ s = s \circ r^{-1}$. (D'après 3)a))

$$(r^j \circ s) \circ (r^j \circ s) = r^j \circ s \circ \underbrace{r \circ \dots \circ r}_{j \text{ fois}} \circ s = r^j \circ s \circ s \circ r^{-j} = r^{j-j}$$

Illustration des axes de symétries dans les cas impairs et pairs :



Exercice 5 Formule des classes - Applications

1. On peut le prouver "à la main" ou de la manière savante suivante :

Soit

$$\begin{aligned} i : G &\rightarrow \text{Aut}(G) \\ g &\mapsto i_g : G \rightarrow G \\ x &\mapsto gxg^{-1} \end{aligned}$$

On vérifie que i est un morphisme de groupe dont le noyau est $Z(G)$, ce qui prouve le résultat.

2. Puisque les orbites sous G forment une partition de X , on a :

$$\text{Card}(X) = \sum_{x \in I} \text{Card}(G \cdot x)$$

Où I est une partie de G contenant exactement un représentant de chaque orbite.

En outre, on sait que : G/S_x et $\text{Orb}_G(x)$ sont **isomorphes**

(Il suffit pour prouver cela de factoriser l'application d'orbite $g \mapsto g \cdot x$ via son noyau qui est S_x)

Donc :

$$\text{Card}(G \cdot x) = \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

D'où :

$$\text{Card}(X) = \sum_{x \in I} \frac{\text{Card}(G)}{\text{Card}(S_x)} \quad (\text{Formule des classes})$$

Dans le cas où G opère sur lui-même par conjugaison, chaque élément x du centre $Z(G)$ définit une orbite réduite à lui-même :

En effet, rappelons que : $\text{Orb}_G(x) = G \cdot x = \{g \cdot x \text{ où } g \in G\} = \{gxg^{-1} \text{ où } g \in G\}$

On a donc : $x \in Z(G) \Leftrightarrow \text{Orb}_G(x) = \{x\}$

La formule des classes devient, en posant $I = I' \cup Z(G)$:

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_{x \in I'} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

Où I' est une partie de G contenant exactement un représentant non central de chaque classe de conjugaison.

3. D'après le théorème de Lagrange, pour tout $x \in G$, $\text{Card}(S_x)$ divise $\text{Card}(G) = p^\alpha$.

Or, si x est non central (et donc $x \neq 1$), alors $\text{Card}(S_x) > 1$ donc $\text{Card}(S_x) = p^\beta$ avec $1 \leq \beta \leq \alpha$.

Par ailleurs :

$$x \in Z(G) \Leftrightarrow \forall y \in G, xy = yx \Leftrightarrow \forall y \in G, x = yxy^{-1} \Leftrightarrow \forall y \in G, x = y \cdot x \Leftrightarrow \forall y \in G, y \in S_x \Leftrightarrow S_x = G$$

Mais comme x est non central, S_x est un sous-groupe propre de G (contraposée de $x \in Z(G) \Leftrightarrow G = S_x$)

Donc :
$$1 \leq \beta < \alpha$$

D'où :
$$\frac{\text{Card}(G)}{\text{Card}(S_{x_i})} = 0 [p]$$

On a donc :
$$\text{Card}(Z(G)) = \text{Card}(G) [p] = 0 [p]$$

Or, $\text{Card}(Z(G)) \geq 1$, (car $Z(G)$ contient au moins le neutre), donc :

$$\text{Card}(Z(G)) = p^\gamma \text{ avec } \gamma \geq 1$$

Ce qui prouve a).

Lorsque $\alpha = 2$, le raisonnement ci-dessus montre que :

$$\text{Card}(Z(G)) = p \text{ ou } p^2$$

Supposons $\text{Card}(Z(G)) = p$. Il existe alors $x \in G \setminus Z(G)$.

Mais, on a facilement :
$$S_x = Z_G(x)$$

Or, $x \in S_x = Z_G(x)$ et $Z(G) \subset Z_G(x)$.

Donc $\text{Card}(Z_G(x)) \geq \text{Card}(Z(G))$.

Mais comme $x \in Z_G(x) \setminus Z(G)$.

On a : $\text{Card}(Z_G(x)) \geq p + 1$.

Donc, d'après le théorème de Lagrange : $\text{Card}(Z_G(x)) = p^2$.

Donc $Z_G(x) = G$ et par suite $x \in Z(G)$. Contradiction.

Donc $\text{Card}(Z(G)) = p^2$ et donc G est abélien d'où b).

Remarque : cela ne fonctionnerait pas avec un groupe d'ordre p^3 .

