Ag 1 : exercices avec corrigés

Exercice 1. Il existe une bijection entre $\mathbf{Z}$ et $\mathbf{Q}$. Montrer qu'il n'y pas d'isomorphisme entre $(\mathbf{Z}, +)$ et $(\mathbf{Q}, +)$.

Si un tel isomorphisme ϕ de $(\mathbf{Z}, +)$ sur $(\mathbf{Q}, +)$ existe, notons $r = \phi(1)$. Alors par surjectivité de ϕ et propriété de morphisme, on a

$$\mathbf{Q} = \phi(\mathbf{Z}) = \{\phi(n) \ ; \ n \in \mathbf{Z}\} = \{n\phi(1) \ ; \ n \in \mathbf{Z}\}$$

En particulier, $r/2$, qui est un rationnel, serait de la forme nr avec $n \in \mathbf{Z}$, pas possible.

Exercice 2 (Commutant). Soit g un élément d'un groupe $(G, *)$. Montrer que l'ensemble des éléments de G qui commutent avec g est un sous-groupe de $(G, *)$.

On note $C(g)$ le commutant de g :

$$C(g) = \{h \in G \ ; \ h * g = g * h\}$$

Il est clair que $C(g)$ est une partie non vide de G ($e \in C(g)$, $g \in C(g)$ par exemple).
Soit $(h_1, h_2) \in C(g)^2$. Alors

$$\begin{aligned}(h_1 * h_2) * g &= h_1 * (h_2 * g) \\ &= h_1 * (g * h_2) \\ &= (h_1 * g) * h_2 \\ &= (g * h_1) * h_2 \\ &= g * (h_1 * h_2)\end{aligned}$$

donc $h_1 * h_2 \in C(g)$ (aux concours, la justification écrite ci-dessus serait jugée longue et un peu trop détaillée, en particulier parce qu'on pourrait sans dommage se débarrasser de toutes les parenthèses grâce à l'associativité de la loi $*$).
Soit $h \in C(g)$. Alors de $h*g = g*h$ on déduit $h^{-1}*h*g*h^{-1} = h^{-1}*g*h*h^{-1}$ qui s'écrit aussi $g * h^{-1} = h^{-1} * g$, donc $h^{-1} \in C(g)$. Par caractérisation des sous-groupes, on conclut.

Exercice 3 (Nombres décimaux). Montrer que l'ensemble des nombres décimaux est un anneau (on rappelle qu'un nombre décimal est un nombre dont le développement décimal « se termine »).

Notons D l'ensemble des nombres décimaux et montrons que c'est un sous-anneau de $(\mathbf{Q}, +, \times)$ ou de $(\mathbf{R}, +, \times)$. Il est commode pour cela de remarquer que, par définition, un nombre x est décimal si et seulement s'il existe $p \in \mathbf{N}$ tel que $10^p \times x \in \mathbf{Z}$.
Clairement, $1 \in D$.
Si $(x, y) \in D^2$, soit p, q dans $\mathbf{N}$ tels que $10^p x \in \mathbf{Z}$ et $10^q y \in \mathbf{Z}$. Si $r = \max(p, q)$, alors $r \in \mathbf{N}$, et $10^r(x - y) \in \mathbf{Z}$, d'où l'on déduit que $x - y \in D$.
Et aussi $10^{p+q}xy = 10^p x \times 10^q y \in \mathbf{Z}$, or $p + q \in \mathbf{N}$, donc $xy \in D$.
On a bien, par caractérisation, D sous-anneau de $(\mathbf{Q}, +, \times)$ ou de $(\mathbf{R}, +, \times)$.

Exercice 4 (Sous-groupes de groupes finis : problèmes de cardinaux)**.**

1. Soit $(G, \star)$ un groupe fini. Soit H un sous-groupe de G. Si $(a, b) \in G^2$, montrer que les ensembles $a \star H = \{a \star h \ ; \ h \in H\}$ et $b \star H$ sont égaux ou disjoints. En déduire que le cardinal de H divise celui de G (Oral Centrale).

   Ce résultat est le **théorème de Lagrange**. Il n'est pas au programme, mais est très classique. A l'oral X ou ens, il est souvent considéré comme acquis.

2. (Une version un peu plus sophistiquée) Soit $(G, \star)$ un groupe fini. Soit H un sous-groupe de G. On définit sur G la relation $\mathcal{R}$:

$$g \mathcal{R} g' \ \Leftrightarrow \ g^{-1} * g' \in H$$

   (a) Démontrer que $\mathcal{R}$ est une relation d'équivalence.

   (b) Démontrer que chaque classe d'équivalence a le même nombre d'éléments que H.

   (c) En déduire que le cardinal de H divise celui de G.

3. Soit G un groupe abélien fini d'ordre n, g_0 un élément de G, d'ordre m. Vérifier que l'application $g \mapsto g * g_0$ est une bijection de G sur lui-même. En déduire :

$$\prod_{g \in G} g = g_0^n \prod_{g \in G} g$$

   puis conclure que m divise n.

   On dit que **l'ordre d'un élément divise l'ordre du groupe**. C'est une méthode simple pour démontrer le théorème d'Euler ou le petit théorème de Fermat (probablement la plus rapide, dans le cadre du programme). Mais si G n'est pas abélien, (G fini), cette démonstration ne marche pas. Le résultat subsiste cependant : si g est un élément de G d'orde m, g engendre un sous-groupe H de cardinal m, donc m divise l'ordre de G d'après le théorème de Lagrange.

4. **Résumé :** Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe. L'ordre de tout élément divise l'ordre du groupe.

---

1. Supposons que $a \star H = \{a \star h \ ; \ h \in H\}$ et $b \star H$ ne soient pas disjoints. Il existe alors h_1 et h_2 dans H tels que $a \star h_1 = b \star h_2$. Montrons alors que $a \star H \subset b \star H$; soit $x \in a \star H$, et soit $h \in H$ tel que $x = a \star h$. Alors

$$x = b \star h_2 \star h_1^{-1} \star h \in b \star H$$

Donc on a bien $a \star H \subset b \star H$. De la même manière, on a $b \star H \subset a \star H$ (on peut aussi dire que $|a \star H| = |a \star H| = |H|$, car par exemple l'application $h \longmapsto a \star h$ est une bijection de H sur $a \star H$, la bijection réciproque étant $x \mapsto a^{-1} \star x$), on a donc bien, finalement, $b \star H$ et $a \star H$ égaux ou disjoints. Il existe alors $a_1, \ldots, a_m$ dans G tels que

$$G = \bigcup_{i=1}^{m} a_i \star H$$

(union disjointe). En effet, on prend $a_1 \in G$. Si $a_1 \star H \neq G$, on prend $a_2 \in G \setminus a_1 \star H$. Si l'existence affirmée ci-dessus est fausse, on peut définir une suite $(a_n)_{n \in \mathbf{N}_*} \in G^{\mathbf{N}_*}$ telle que

$$\forall n \in \mathbf{N}_* \qquad a_{n+1} \notin \bigcup_{i=1}^{m} a_i \star H$$

ce qui est contradictoire, on aurait en effet, pour tout $n \in \mathbf{N}_*$,

$$|G| \geq \left| \bigcup_{i=1}^{m} a_i \star H \right| = m|H|$$

(car la réunion est disjointe). On conclut donc.

2. (a) On montre sans grande difficulté, successivement, que $\mathcal{R}$ est réflexive, symétrique, transitive.

   (b) Si g et g' sont dans G,

$$\begin{aligned} g \mathcal{R} g' &\Leftrightarrow \ g^{-1} * g' \in H \\ &\Leftrightarrow \exists h \in G \qquad g^{-1} * g' = h \\ &\Leftrightarrow \exists h \in G \qquad g' = g * h \\ &\Leftrightarrow g' \in g * H \end{aligned}$$

   Donc la classe d'équivalence de g est $g * H$, qui a même cardinal que H (car $h \longmapsto a * h$ est une bijection de H sur $a * H$).

   (c) Les classes d'équivalence pour $\mathcal{R}$ forment une partition de G, s'il y en a m on a donc

$$m \times |H| = |G|$$

3. Voir cours.

Exercice 5. *Oral Centrale* On admet le théorème de Lagrange (voir ci-dessus). Soit G un groupe fini de cardinal supérieur à 2. On définit le centre de G :

$$Z = \{x \in G \ ; \ \forall y \in G \ xy = yx\}$$

Pour $x \in G$, on définit

$$C_x = \{y \in G \ ; \ xy = yx\}$$

1. Montrer que Z et C_x sont des sous-groupes de G.
2. On suppose que $\text{Card}(G)/\text{Card}(Z)$ est un nombre premier. Montrer que G est commutatif. On pourra supposer l'existence de $x \in G \setminus Z$ et considérer le sous-groupe engendré par x et Z.

---

1. Voir cours pour le centre et un exercice antérieur pour le commutant.
2. Suivons l'indication. Si $Z \neq G$ (si G non commutatif, donc), soit $x \in G \setminus Z$. Essayons de décrire le sous-groupe H engendré par x et Z. D'abord, x est d'ordre m dans G, où $m \geq 2$ (G est fini donc x est d'ordre fini, et il ne peut être d'ordre 1 sinon il serait égal à e). Donc H contient tous les $x^k z$ où $z \in Z$ et $0 \leq k \leq m-1$. Mais on constate facilement que $\{x^k z \ ; \ z \in Z \ , \ 0 \leq k \leq m-1\}$ est un sous-groupe de $(G, \ )$. En effet, il contient $e = x^0 e$, il est stable car

$$x^k z x^\ell z' = x^{k+\ell} z z'$$

(vu que z commute avec tout le monde), et $x^{k+\ell} = x^j$ où j est le reste de la division de $k+\ell$ par m, $zz' \in Z$. De même,

$$(x^k z)^{-1} = z^{-1} x^{-k} = x^{-k} z^{-1}$$

(car $z^{-1} \in Z$) et $x^{-k} = x^{m-k}$. Donc

$$H = \{x^k z \ ; \ z \in Z \ , \ 0 \leq k \leq m-1\}$$

Comme Z est un sous-groupe de H qui lui-même est un sous-groupe de G, on a (théorème de Lagrange) $|Z| \ | \ |H|$ et $|H| \ | \ |G|$. Comme $|G|/|Z|$ est premier, on a $H = G$ ou $H = Z$ (dans la factorisation $|G|/|Z| = |G|/|H| \times |H|/|Z|$, un des deux facteurs vaut 1). Mais $H = Z$ est impossible car $x \in H$ et $x \notin Z$. Donc $H = G$. Mais en montrant que H était stable, on a montré dans le même temps qu'il était commutatif...on conclut donc.

Exercice 6 (Sous-groupes de groupes finis : problèmes de cardinaux (suite))**.** Soit $(G, *)$ un groupe. On suppose que le cardinal de G s'écrit pq, avec q premier et $p < q$. Montrer que G contient au plus un sous-groupe de cardinal q. (Oral Centrale)

Soit H un sous-groupe de cardinal q. Tout élément de H est d'ordre divisant q, donc d'ordre 1 ou q. Donc tout élément de H qui n'est pas d'ordre 1 (donc qui

n'est pas l'élément neutre) est d'ordre q, donc engendre H. Supposons qu'il y ait deux sous-groupes H et H' d'ordre q, distincts. Alors $H \cap H' = \{e\}$ (car si $h \in H \cap H'$, si $h \neq e$, alors h engendre à la fois H et H', qui sont alors égaux). Montrons que l'application

$$(h, h') \longmapsto h * h'$$

est alors injective. En effet, si $h_1 * h'_1 = h_2 * h'_2$, on a $h_2^{-1} * h_1 = h'_2 * (h'_1)^{-1}$, cet élément de G étant à la fois dans H et H' est donc égal à e, d'où $h_1 = h_2$ et $h'_1 = h'_2$. Il y aurait donc au moins q^2 éléments dans G, ce qui est contraire à l'hypothèse.

Exercice 7. [*Oral PLSR*]
Soit $(G, .)$ un groupe, $\mathrm{Aut}(G)$ l'ensemble de ses automorphismes.

1. Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.
2. Déterminer les groupes finis tels que $\mathrm{Aut}(G)$ soit réduit à un élément.

Comme souvent, la deuxième question n'est pas facile à trouver. Elle est faite pour susciter un échange (indications/réactions aux indications) entre l'examinateur et le candidat. Des indications raisonnablement posables par l'examinateur sont à la fin de cette feuille d'exercices.

La première question est simple, c'est une entrée en matière dans laquelle il faut montrer clarté et précision.
Soit G un groupe fini tel que $\mathrm{Aut}(G)$ soit réduit à un élément. Alors, pour tout $g \in G$,

$$\phi_g \ : \ h \longmapsto ghg^{-1}$$

étant dans $\mathrm{Aut}(G)$, est égal à Id_G. On en déduit que G est commutatif.
Mais alors $x \longmapsto x^{-1}$ est aussi dans $\mathrm{Aut}(G)$, et donc est égal à Id_G. On en déduit que $(G, .)$ est un groupe fini tel que pour tout $g \in G$, $g^2 = e$.
Il existe alors des éléments $g_1, \ldots, g_m$ de G tels que, en notant $\langle g_1, \ldots, g_k \rangle$ le sous-groupe engendré par $\{g_1, \ldots, g_k\}$ (i.e. le plus petit sous-groupe contenant $g_1, \ldots, g_k$), on ait

$$\forall k \in [\![2, m \qquad g_k \notin \langle g_1, \ldots, g_{k-1} \rangle$$

et $G = \langle g_1, \ldots, g_m \rangle$ (sinon, on pourrait construire par récurrence une suite $(g_n)_{n \geq 1}$ d'éléments de G tels que

$$\forall k \leq 2 \qquad g_k \notin \langle g_1, \ldots, g_{k-1} \rangle$$

ce qui contredirait la finitude de G). On vérifie alors que

$$(h_1, \ldots, h_m) \longrightarrow h_1 \ldots h_m$$

est un isomorphisme de $C_{g_1} \times \cdots \times C_{g_m}$ sur $(G, .)$ où $C_g = \{e, g\}$ est le sous-groupe engendré par g. Ou encore, tout élément de G s'écrit de manière unique sous la forme

$$g_1^{\epsilon_1} \ldots g_m^{\epsilon_m}$$

où les ϵ_k sont dans $\{0,1\}$. L'application

$$g_1^{\epsilon_1}\dots g_m^{\epsilon_m} \longmapsto g_1^{\epsilon_2} g_2^{\epsilon_2}\dots g_m^{\epsilon_m}$$

définit alors un automorphisme de G autre que Id si $m \geq 2$. Les seuls groupes finis ayant un seul automorphisme sont donc $\{e\}$ et $\{e,g\}$ avec $g^2 = e$.

Exercice 8. [*Oral X*]
Soit G un groupe. Pour $(a,b) \in G^2$, on note $[a,b] = aba^{-1}b^{-1}$. On note D_G le sous-groupe de G engendré par les éléments de la forme $[a,b]$, i.e. le plus petit sous-groupe de G contenant les éléments de la forme $[a,b]$.

1. Montrer que $\forall g \in G \qquad gD_Gg^{-1} = D_G$.
2. Montrer que $\forall g \in G \quad g\ D_G = D_G\ g$.
3. On pose $\mathcal{Q}_G = \{xD_G\ ;\ x \in G\}$.
   (a) Montrer que $\mathcal{Q}_G$ est une partition de G.
   (b) Montrer que la fonction $(xD_G, yD_G) \longmapsto (xy)D_G$ est convenablement définie et munit $\mathcal{Q}_G$ d'une structure de groupe, puis montrer que $x \longmapsto xD_G$ est un morphisme de G dans $\mathcal{Q}_G$.
   (c) Montrer que $\mathcal{Q}_G$ est abélien.

---

1. Soit $(a,b) \in G^2$. Alors

   $$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}]$$

   L'application $h \longmapsto ghg^{-1}$ est un automorphisme du groupe G ; elle transforme les sous-groupes de G en sous-groupes de G. Elle laisse invariant $A = \{[a,b]\ ;\ (a,b) \in G^2\}$. Elle transforme donc les sous-groupes contenant A en les sous-groupes contenant A. Et comme elle préserve l'inclusion, elle transforme le plus petit d'entre eux, D_G, en lui-même. On a donc $gD_Gg^{-1} = D_G$, un peu mieux que la question posée (on voulait $gD_Gg^{-1} \subset D_G$.
2. Facile conséquence de ce qu'on a fait précédemment.
3. (a) Supposons $xD_G \cap yD_G \neq \emptyset$; il existe alors h_1, h_2 dans D_G tels que

   $$xh_1 = yh_2$$

   Mais alors, si $h \in D_G$,

   $$xh = y\underbrace{h_2h_1^{-1}h}_{\in D_G} \in yD_G$$

   d'où $xD_G \subset yD_G$ et, symétriquement, $yD_G \subset xD_G$, donc xD_G et yD_G sont, s'ils ne sont pas la même partie de G, deux parties disjointes de G.

(b) Pour la définition convenable, il s'agit de s'assurer que si $xD_G = x'D_G$ et $yD_G = y'D_G$ alors $xyD_G = x'y'D_G$. Ou encore, de manière équivalente, on doit montrer que si $x^{-1}x'$ et $y^{-1}y'$ sont dans D_G, alors $(xy)^{-1}x'y' \in D_G$. Mais...

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = \underbrace{y^{-1}y'}_{\in D_G}\ y'^{-1}\left(\underbrace{x^{-1}x'}_{\in D_G}\right)y'$$

et il suffit d'appliquer **1.** pour conclure.
Il est clair qu'on définit ainsi une loi interne sur $\mathcal{Q}_G$.
Cette loi est associative, la vérification en est très formelle : avec des notations évidentes,

$$xD_G(yD_G\ zD_G) = xD_G(yzD_G) = x(yz)D_G = (xy)zD_G = (xy)D_G\ zD_G = (xD_G\ yD_G)zD_G$$

L'élément $D_G = eD_G$ de $\mathcal{Q}_G$ est neutre. Et l'élément $x^{-1}D_G$ est symétrique de l'élément xD_G. La propriété de morphisme demandée est alors très simple à écrire, elle découle de la définition.

(c) Il s'agit de montrer que, pour tous x, y dans G,

$$(xy)D_G = (yx)D_G$$

ou encore que $(xy)^{-1}yx \in D_G$ ce qui est bien simple vu la définition de D_G.

Exercice 9. *Un classique par deux voies différentes*
Soit $(G, .)$ un groupe fini tel que

$$\forall x \in G \qquad x^2 = e$$

où e désigne l'élément neutre de G. Le but de l'exercice est de montrer que le cardinal de G (noté $|G|$) est une puissance de 2.

1. Montrer que $(G, .)$ est commutatif.
2. On suppose $G \neq \{e\}$. Montrer qu'il existe $m \in \mathbf{N}_*$ et $g_1, \ldots, g_m$ dans G tels que $\langle g_1, \ldots, g_m\rangle = G$ et, pour tout $k \in [\![2, m]\!]$,
$$g_k \notin \langle g_1, \ldots, g_{k-1}\rangle$$
où $\langle g_1, \ldots, g_m\rangle$ désigne le sous-groupe de $(G, .)$ engendré par $\{g_1, \ldots, g_m\}$.
3. Décrire G et conclure.
4. *[Pour les 5/2, autre méthode]* Définir une structure de $\mathbf{F}_2$-espace vectoriel sur G, où $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. Conclure.

Pour la commutativité, on part de

$$(x.y).(x.y) = e$$

et on compose à gauche par x, à droite par y. La suite de l'exercice est quasiment traitée dans l'exercice PLSR plus haut. Pour la structure d'espace vectoriel, la loi « d'addition » sera ici ., la loi externe sera

$$(\lambda, g) \longmapsto g^\lambda$$

Il suffit alors de dire que G est de dimension finie, et donc isomorphe à un certain $\mathbf{F}_2^m$.