Devoir surveillé

samedi 11 octobre 2014

Mise en bouche.

1. **(2 pts)** Soit $m \in M^\times$. L'image m^{-1} fait sens par définition de $M^\times$; vu par ailleurs les égalités $mm^{-1} = 1 = m^{-1}m$ définissant l'inverse m^{-1}, l'image m^{-1} est inversible d'inverse m, d'où l'appartenance $m^{-1} \in M^\times$ et l'involutivité demandé. Enfin, étant donné un $n \in M^\times$, on a les égalités

$$(mn)\left(n^{-1}m^{-1}\right) \overset{\substack{\text{associativité}\\ \text{de la loi de } M}}{=} m\left(nn^{-1}\right)m^{-1} \overset{\substack{\text{définition}\\ \text{d'un inverse}}}{=} m1m^{-1} \overset{\substack{\text{définition}\\ \text{du neutre}}}{=} mm^{-1} \overset{\substack{\text{définition}\\ \text{d'un inverse}}}{=} 1$$
$$\text{et} \qquad \left(n^{-1}m^{-1}\right)(mn) = n^{-1}\left(m^{-1}m\right)n = n^{-1}1n = n^{-1}n = 1,$$

ce qui montre que mn et $n^{-1}m^{-1}$ sont inverses l'un de l'autre, d'où l'on tire l'égalité $(mn)^{-1} = n^{-1}m^{-1}$ signifiant bien que l'inversion "inverse" la loi de M.

2. **(1 pt)** L'application i est (d'après la question précédente) une involution, donc une bijection de G sur G. On demande donc de montrer qu'elle est un morphisme (de groupes) ssi G est abélien. Or, se rappelant (*cf.* question précédente) les égalités $i(ab) = i(b)\,i(a)$ (valides pour tous $a, b \in G$), on a les équivalences

$$\begin{aligned} G \text{ est abélien} &\iff \forall a,b \in G,\ ab = ba \\ &\overset{i \text{ injectif}}{\iff} \forall a,b \in G,\ i(ab) = i(ba) \\ &\iff \forall a,b \in G,\ i(b)\,i(a) = i(ba) \\ &\iff i \text{ est un morphisme, } c.\ q.\ f.\ d.. \end{aligned}$$

(1 pt) Notons m l'application $\left\{ \begin{array}{ccc} G^2 & \longrightarrow & G \\ (a,b) & \longmapsto & ab \end{array} \right.$. On a alors les équivalences

$$\begin{aligned} m \text{ est un morphsime} &\iff \forall a,b,\alpha,\beta \in G^4,\ m\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}\right) = m\begin{pmatrix} a \\ b \end{pmatrix} m\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &\iff \forall a,b,\alpha,\beta \in G^4,\ m\begin{pmatrix} a\alpha \\ b\beta \end{pmatrix} = ab\ \alpha\beta \\ &\iff \forall a,b,\alpha,\beta \in G^4,\ a\alpha b\beta = ab\alpha\beta \\ &\overset{\substack{\text{simplification}\\ \text{par } a \text{ et par } \beta}}{\iff} \forall a,b,\alpha,\beta \in G^4,\ \alpha b = b\alpha \\ &\iff \forall b,\alpha \in G^2,\ \alpha b = b\alpha \\ &\iff G \text{ est abélien, } c.\ q.\ f.\ d.. \end{aligned}$$

3. **(1 pt)** Les égalités (à $x \in G$ fixé)

$$\begin{aligned} \left[\delta_a \circ \delta_{a^{-1}}\right](x) &= \delta_a\left(\delta_{a^{-1}}(x)\right) = a\left(a^{-1}x\right) = \left(aa^{-1}\right)x = 1x = x \text{ et} \\ \left[\delta_{a^{-1}} \circ \delta_a\right](x) &= \delta_{a^{-1}}\left(\delta_a(x)\right) = a^{-1}(ax) = \left(a^{-1}a\right)x = 1x = x \end{aligned}$$

montrent que δ_a et $\delta_{a^{-1}}$ sont réciproques l'une de l'autres. On montrerait de même que γ_a et $\gamma_{a^{-1}}$ sont réciproques l'une de l'autre.

(1 pt) Puisque δ_a et γ_a sont des bijections de G sur G, elles seront des automorphismes de G ssi elles en sont des endomorphismes, *i. e.* ssi elles sont des morphismes de groupes. Soit donc $g \in G$ tel que δ_g soit un morphisme de groupes. Alors δ_g doit préserver le neutre, d'où les égalités $1 = \delta_g(1) = g1 = g$. Réciproquement, il est clair que δ_1 et γ_1 (valant Id_G) sont des automorphismes de G.

Finalement, δ_a et γ_a ne sont (presque) jamais des automorphismes de G, sauf si $a = 1$ (cas trivial où les deux translations agissent comme l'identité).

Sous-groupes cycliques. Soient a et b dans $\mathbf{N}^*$.

1. **(2 pts)** Puisque $\mathbf{U}_a$ est un sous-groupe de $\mathbf{C}^*$, il contient le même neutre que $\mathbf{U}_b$ (le 1 complexe) et est stable par produit et par inversion. On en déduit les équivalences

$$\begin{aligned}\mathbf{U}_a \text{ est un sous-groupe de } \mathbf{U}_b &\overset{\mathbf{U}_a \text{ est un sous-groupe de } \mathbf{C}^*}{\iff} \mathbf{U}_a \subset \mathbf{U}_b \overset{\mathbf{U}_a \text{ est monogène}}{\iff} \left\langle e^{\frac{2\pi i}{a}} \right\rangle \subset \mathbf{U}_b \overset{\mathbf{U}_b \text{ est un sous-groupe}}{\iff} e^{\frac{2\pi i}{a}} \in \mathbf{U}_b \\ &\iff \left(e^{\frac{2\pi i}{a}}\right)^b = 1 \iff e^{2\pi i \frac{b}{a}} = 1 \overset{\text{définition de } \pi}{\iff} 2\pi i \frac{b}{a} \in 2\pi i \mathbf{Z} \\ &\iff \frac{b}{a} \in \mathbf{Z} \iff a \mid b.\end{aligned}$$

2. **(2 pts)** Soit φ un tel morphisme. Soit $\alpha \in \mathbf{U}_a$. On a alors, en suivant le triangle gauche du diagramme commutatif, l'égalité $\varphi\binom{\alpha}{1} = \alpha$. De même, pour tout $\beta \in \mathbf{U}_b$, on aura $\varphi\binom{1}{\beta} = \beta$, d'où l'on déduit

$$\varphi\binom{\alpha}{\beta} = \varphi\left(\binom{\alpha}{1}\binom{1}{\beta}\right) = \varphi\binom{\alpha}{1}\varphi\binom{1}{\beta} = \alpha\beta.$$

Ainsi φ doit-il agir tout simpement comme la multiplication (complexe). Réciproquement, puisque $\mathbf{C}^*$ est abélien, la multiplication induite sur le produit de deux quelconques de ses sous-groupes (en particulier sur $\mathbf{U}_a \times \mathbf{U}_b$) sera un morphisme de groupes.

3. Vu les cardinaux, le morphisme φ est bijectif ssi il est injectif, donc sera un isomorphime de groupes ssi il est injectif.

(1 pt) Supposons a et b étrangers. Soit $(x, y) \in \operatorname{Ker}\varphi$. Puisque $\operatorname{Ker}\varphi \subset \mathbf{U}_a \times ?$, le complexe x appartient à $\mathbf{U}_a$, donc son ordre divise $|\mathbf{U}_a| = a$; or ce complexe vaut aussi y^{-1} (puique $xy = 1$), lequel tombe dans $\mathbf{U}_b$, donc son ordre doit aussi diviser $|\mathbf{U}_b| = b$. Finalement l'ordre de x doit diviser $a \wedge b = 1$, d'où les égalités $x = 1$ et $y = x^{-1} = 1$.

(1 pt) Supposons φ injectif. Soit $d \mid a \wedge b$. Alors $\mathbf{U}_d$ est inclus dans $\mathbf{U}_a$ et dans $\mathbf{U}_b$, donc on peut parler (à $x \in \mathbf{U}_d$ fixé) des images par φ de $\binom{1}{x}$ et de $\binom{x}{1}$; or ces images sont égales (à x), d'où par injectivité les égalités $\binom{1}{x} = \binom{x}{1}$ et $x = 1$, forçant l'inclusion $\mathbf{U}_d \subset \{1\}$ et la comparaison $d = |\mathbf{U}_d| \leq 1$

Isomorphismes.

1. **(1 pt)** Le monoïde $(\mathbf{N}, +)$ est monogène, au contraire de $(\mathbf{N}^*, \times)$, donx ces monoïdes se sauraient être isomorphes. (Si $\varphi : \mathbf{N} \longrightarrow \mathbf{N}^*$ désignait un tel isomorphisme, en notant $a := \varphi(1)$, on aurait les égalités

$$\mathbf{N}^* = \operatorname{Im}\varphi = \varphi(\mathbf{N}) = \varphi(\langle 1 \rangle) = \langle \varphi(1) \rangle = \langle a \rangle = \{a^n \ ; \ n \in \mathbf{N}\}, \text{ ce qui serait absurde.)}$$

(1 pt) Le groupe $\mathbf{C}^*$ contient un élément d'ordre 3 (par exemple $e^{\frac{2\pi i}{3}}$), au contraire de $\mathbf{R}^*$ (le binôme $X^3 - 1$ n'a qu'un seule racine réelle, 1, qui n'est pas d'ordre 3), donc ces groupes ne sauraient être isomorphes.

2. **(2 pts)** Regardons les cardinaux :

G	$\mathbf{U}_3 \times \mathbf{U}_2$	$\mathbf{U}_3$	$\mathbf{Z}/6$	$\mathfrak{S}_3$	$\mathfrak{S}_6$
$\lvert G\rvert$	$3 \times 2 = 6$	3	6	$3! = 6$	$6! = 720$

. Cela permet d'isoler $\mathbf{U}_3$ et $\mathfrak{S}_6$ dans leurs classes d'isomorphie respectives. Parmi les trois groupes restants, deux sont isomorphes ($\mathbf{U}_3 \times \mathbf{U}_2$ et $\mathbf{Z}/6$, tous deux à $\mathbf{U}_6$ d'après l'exercice précédent) et abéliens, tandis que le troisième ($\mathfrak{S}_3$) n'est pas abélien.

3. **(2 pts)** Abrégeons $n := 42$. L'ensemble $GL_n(\mathbf{Q})$ s'injecte dans $\mathbf{Q}^{n \times n}$ qui est dénombrable, tandis que $GL_n(\mathbf{R})$ et $GL_n(\mathbf{C})$ contiennent (dans leur centre) une partie indénombrable $\mathbf{R}^*$. Par ailleurs, les groupes $\mathbf{R}^*$ et $\mathbf{C}^*$ n'étant pas isomorphes, les centres de $GL_n(\mathbf{R})$ et $GL_n(\mathbf{C})$ ne peuvent l'être, *a fortiori* $GL_n(\mathbf{R})$ et $GL_n(\mathbf{C})$.

4. **(1 pt)** On utilise l'injection $(\lambda_1, \lambda_2, ..., \lambda_n) \mapsto \operatorname{Diag}(\lambda_1, \lambda_2, ..., \lambda_n)$, bien définie d'après le critère connu d'inversibilité des matrices diagonales. C'est un morphisme de groupes d'après le calcul connu des produits de matrices diagonales.

(1 pt) L'image par le plongement ci-dessus de la puissance $\{\pm 1\}^n$ est un sous-groupe (formé de symétries linéaires) répondant à la question.

Bonus : montrons le point admis avec des outils provenant de la réduction des matrices. Soit G un tel sous-groupe. Il est abélien car pour tous $a, b \in G$ on a

$$ab = a1b = a(ab)^2 b = aababb = a^2bab^2 = 1ba1 = ba.$$

Tous les éléments de G sont annulés par le polynôme X^2-1, dont sont diagonalisables à spectre dans $\{\pm 1\}$; puisqu'ils commutent, ils sont *co*diagonalisables à spectre dans $\{\pm 1\}$, ce qui montre que G est conjugué à un ensemble de matrices diagonales à valeurs dans $\{\pm 1\}$. Or il n'y a qu'au plus $\#\{\pm 1\} \leq 2$ choix par coordonnée et n coordonées en tout, d'où la comparaison $|G| \leq 2 \cdot 2 \cdot \cdots \cdot 2 = 2^n$.

(2 pts) Soient a et b dans $\mathbf{N}^*$ tels que $GL_a(K)$ est isomorphe à $GL_b(K)$. Observer que l'hypothèse $2 \neq 0$ implique l'égalité cardinale $\#\{\pm 1\} = 2$. L'image du sous-groupe $\{\pm 1\}^a$ (qui est d'ordre 2^a par injectivité) est alors un sous-groupe de $GL_b(K)$ dont tous les éléments sont involutifs (car images d'involutions par un morphisme), donc est de cardinal $\leq 2^b$ (d'après le point ci-dessus), d'où les comparaisons $2^a \leq 2^b$ et $a \leq b$. Le même raisonnement tient dans l'autre sens et livre l'égalité $a = b$.

Entremets. **(4 pts)** Le radical $\sqrt{1+a^2}$ doit faire penser à du sinus hyperbolique. En se souvenant de l'égalité $\operatorname{ch}\operatorname{ash} a = \sqrt{1+a^2}$ valide pour tout réel a, il apparaît (à a, b réels fixés) les égalités

$$a@b = a\sqrt{1+b^2} + b\sqrt{1+a^2} = (\operatorname{sh}\operatorname{ash} a)(\operatorname{ch}\operatorname{ash} b) + (\operatorname{sh}\operatorname{ash} b)(\operatorname{ch}\operatorname{ash} a) = \operatorname{sh}(\operatorname{ash} a + \operatorname{ash} b).$$

Ainsi la loi @ est-elle la conjuguée de l'addition du groupe $\mathbf{R}$ par la bijection sh. Toutes les propriétés de l'addition se transportent automatiquement, en particulier le fait que tout élément admette des racines à tout ordre (un réel a est pour tout naturel $n > 0$ le n-ième itéré de $\frac{a}{n}$).

Commutants.

1. **(2 pts)** La mesure de probabilité étant uniforme, la probabilité p vaut $\frac{\#\{(a,b)\in G^2\ ;\ ab=ba\}}{\#G^2}$. À $a \in G$ fixé, l'ensemble $\{(a,b) \in G^2\ ;\ ab = ba\}$ est équipotent à $\{b \in G\ ;\ ab = ba\}$ *via* la bijection $(a,b) \leftrightarrow b$; par conséquent, sommer à abscisse fixée fournit les égalités

$$p = \frac{1}{\#G^2}\sum_{a\in G} \#\{(a,b) \in G^2\ ;\ ab = ba\} = \frac{1}{\#G^2}\sum_{a\in G} \#\{b \in G\ ;\ ab = ba\} = \frac{1}{|G|^2}\sum_{a\in G} \#\operatorname{Comm}\{a\}.$$

Lorsque $a \in Z$, son commutant est tout G, sinon $\operatorname{Comm}\{a\}$ est un sous-groupe strict et est donc (par Lagrange) d'ordre $\leq \frac{|G|}{2}$. En séparant la somme selon ces deux cas, on obtient

$$p|G|^2 = \sum_{a\in Z} \#\underbrace{\operatorname{Comm}\{a\}}_{=G} + \sum_{a\in G\setminus Z} \underbrace{\#\operatorname{Comm}\{a\}}_{\leq \frac{|G|}{2}} \leq \sum_{a\in Z} |G| + \sum_{a\in G\setminus Z} \frac{|G|}{2} = |Z|\,|G| + (|G| - |Z|)\,\frac{|G|}{2}.$$

2. **(1 pt)** Pour tous $a, b \in G$ on a les égalités

$$(aZ)(bZ) = a(Zb)Z \overset{Z \text{ est}}{\underset{\text{abélien}}{=}} a(bZ)Z = abZZ \overset{Z \text{ est un}}{\underset{\text{groupe}}{=}} abZ,$$

ce qui montre que la multiplication des parties de G induit une loi sur ${}^{G}\!/_{Z}$ telle que $\forall a, b \in G,\ \overline{a}\,\overline{b} = \overline{ab}$. Ces égalités permettent de transporter la structure du groupe G sur ${}^{G}\!/_{Z}$ en passant tout "sous la barre" (tout se passe exactement comme on l'a fait en cours pour le groupe ${}^{\mathbf{Z}}\!/_{n}$).

(1 pt) Supposons ${}^{G}\!/_{Z}$ cyclique. Montrons alors que G est abélien, ce qui contredira l'hypothèse $p < 1$. Soit a un élément de G dont la classe $\overline{a}$ modulo Z engendre ${}^{G}\!/_{Z}$. Soient g et g' dans G. Leurs classes modulo Z sont des puissances de $\overline{a}$, mettons $\overline{g} = \overline{a}^n = \overline{a^n}$. Il y a donc un $z \in Z$ tel que $g = za^n$. De même, on peut écrire $g' = z'a^{n'}$ avec $z' \in Z$. Il est alors clair que g et g' commutent, au vu des égalités $gg' = zz'a^{n+n'} = g'g$.

(1 pt) Tout groupe d'ordre 1, 2 ou 3 est cyclique (le premier trivialement, les deux autres car 2 et 3 sont premiers), donc ${}^{G}\!/_{Z}$ doit être d'ordre au moins 4, *i. e.* $\left|{}^{G}\!/_{Z}\right| \geq 4$, ce qui se réécrit $\frac{|G|}{|Z|} \geq 4$, d'où la comparaison voulue.

3. **(1 pt)** La comparaison de la première question se réécrit $p \leq \frac{|Z|}{2|G|} + \frac{1}{2}$. La deuxième question permet de conclure à $p \leq \frac{1}{2}\frac{1}{4} + \frac{1}{2} = \frac{5}{8} = 62,5\%$.

(2 pts) Suivons l'indication et montrons que le groupe $\mathbf{H}_8$ réalise l'égalité[1]. Le centre de $\mathbf{H}_8$ vaut $\{\pm 1\}$, qui est bien d'indice 4. Par ailleurs, le commutant de $\pm i$ vaut $\{\pm 1, \pm i\}$, donc est bien d'indice 2 (de même pour $\pm j$ et $\pm k$).

[1] Cela ne tombe pas du ciel : on essaie un groupe d'ordre 8 pour faire apparaître le dénominateur de p.