Devoir maison

(à rendre le lundi 5 octobre 2015)

Solution proposée.

Exercice 1. (7 pts)

1. **(2 pts)** Appelons f l'application donnée (elle est bien définie car, à $g \in G$ fixé, les éléments g^{-1} et $i(g)$ font sens et tombent dans G – *a fortiori* leur produit). On a alors pour tous $a, b \in G$ les implications

$$f(a) = f(b) \Longrightarrow a^{-1} i(a) = b^{-1} i(b) \underset{\text{morphisme}}{\overset{i \text{ est un}}{\Longrightarrow}} i\left(ab^{-1}\right) = ab^{-1} \Longrightarrow ab^{-1} \in \operatorname{Fix} i \Longrightarrow ab^{-1} = 1 \Longrightarrow a = b.$$

   Puisque les ensembles source et but de f sont de même cardinal fini, l'injectivité de f implique sa surjectivité.

2. **(1 pt)** Soit $g \in G$. Soit a un antécédent de g par f. On a alors les égalités

$$i(g) = i(f(a)) = i\left(a^{-1} i(a)\right) = i(a)^{-1} \underbrace{i^2(a)}_{=\mathrm{Id}(a)=a} = \left(a^{-1} i(a)\right)^{-1} = f(a)^{-1} = g^{-1}.$$

3. **(1 pt)** On a à $a, b \in G$ fixés les égalités

$$ab = \left(a^{-1}\right)^{-1} \left(b^{-1}\right)^{-1} = i\left(a^{-1}\right) i\left(b^{-1}\right) \underset{\text{morphisme}}{\overset{i \text{ est un}}{=}} i\left(a^{-1} b^{-1}\right) = i\left((ba)^{-1}\right) = \left((ba)^{-1}\right)^{-1} = ba.$$

   L'involution i partitionne G en paires de la forme $\{g, i(g)\}$, lesquelles sont de cardinal 1 ou 2, le cas du singleton ayant lieu ssi $g = i(g)$, *i. e.* ssi $g = \operatorname{Fix} i$ ou encore ssi $g = 1$. Il y a donc une seule paire réduite à un singleton, les autres étant toutes de cardinal 2. Additionner ces cardinaux donne un ordre impair pour G.

4. **(2 pts)** Les questions précédentes montrent qu'un tel automorphisme vaut nécessairement l'inversion. Montrons que cette dernière, notée I, répond à la question. C'est clairement une involution. Le calcul de la question 3 montre par ailleurs que I est un morphisme : pour tout $\alpha, \beta \in \Gamma$ on a les égalités

$$I(\alpha\beta) = (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} \underset{\text{abélien}}{\overset{\Gamma \text{ est}}{=}} \alpha^{-1}\beta^{-1} = I(\alpha) I(\beta).$$

   Soit enfin $\gamma \in \operatorname{Fix} I$. Puisque $\gamma^2 = 1$, l'ordre de γ vaut 1 ou 2 ; or cet ordre divise celui de Γ, qui est impair, donc ne saurait être 2. On a par conséquent l'inclusion $\operatorname{Fix} I \subset \{1\}$, l'inclusion $\supset$ étant immédiate.

Exercice 2. (8 pts)

1. **(1 pt)** Le groupe additif $\mathbf{Z}/2$ en est un, *a fortiori* toutes ses puissances entières $\left(\mathbf{Z}/2\right)^n$. Ces dernières sont deux à deux non isomorphes car leurs cardinaux sont (deux à deux) distincts.

2. **(1 pt)** Soient a et b deux entiers dans une même classe modulo 2. Leur différence est alors un certain multiple de 2, mettons $2m$. On a alors les égalités $g^b = g^{a+2m} = g^a \left(g^2\right)^m = g^a$.

   Autre démonstration (qui donne une information plus précise) : si z est pair, on a $g^z = \left(g^2\right)^{\frac{z}{2}} = 1^{\frac{z}{2}} = 1$; si z est impair, on a $g^z = g^{1+2\frac{z-1}{2}} = g\left(g^2\right)^{\frac{z-1}{2}} = g1 = g$.

3. **(1 pt)** On a pour tous $a, b \in G$ les égalités

$$ab = a1b = a(ab)^2 b = a(abab)b = a^2(ba)b^2 = ba.$$

4. **(2 pts)** Notons $\mathcal{E}$ l'ensemble des parties génératrices finies de G. Puisque $G = \langle G \rangle$ est fini, on a l'appartenance $G \in \mathcal{E}$. La partie $\{|E| \ ; \ E \in \mathcal{E}\}$ de $\mathbf{N}$ est par conséquent non vide (elle contient $|G|$), donc admet un minimum n. Soit $E \in \mathcal{G}$ tel que $|E| = n$. Alors E convient.

5. **(3 pts)** Notons φ l'application donnée. Elle est bien définie d'après la question 2. Sa surjectivité équivaut au caractère générateur de la partie $\{g_1, g_2, ..., g_n\}$. Elle est un morphisme vu à (a_i) et (b_i) fixés dans $\left(\mathbf{Z}/2\right)^n$ les égalités

$$\begin{aligned}\varphi\left(\left(\overline{a_i}\right)+\left(\overline{b_i}\right)\right) &= \varphi\left(\overline{a_i}+\overline{b_i}\right)=\varphi\left(\overline{a_i+b_i}\right)=\sum_{i=1}^{n}\left(a_i+b_i\right)g_i=\sum_{i=1}^{n}\left(a_ig_i+b_ig_i\right)\\ &= \sum_{i=1}^{n}a_ig_i+\sum_{i=1}^{n}b_ig_i=\varphi\left(\overline{a_i}\right)+\varphi\left(\overline{b_i}\right).\end{aligned}$$

Montrons enfin son injectivité. Soit $(\overline{a_i}) \in \left(\mathbf{Z}/2\right)^n$ tel que $\sum_{i=1}^n a_ig_i = 0$. Supposons par l'absurde les a_i non tous nuls (cela implique $n \geq 1$). Soit i_0 tel que $a_{i_0} \neq 0$. Alors $g_{i_0} = \sum_{i\neq i_0} -a_ig_i$ est engendré par les $g_{i\neq i_0}$, ce qui montre que la partie $\{g_i\}_{i\neq i_0}$ engendre G ; étant par ailleurs finie, elle tombe dans $\mathcal{E}$, donc son cardinal $n-1$ doit donc majorer $\min_{E\in\mathcal{E}}|E| = n$: contradiction.

Remarque. On a un peu l'impression de faire une théorie de la dimension des "**Z**-espaces vectoriels". C'est normal. On aurait pu munir G d'une structure de $\mathbf{Z}/2$-espace vectoriel (une seule action scalaire est alors envisageable : laquelle ?) : étant fini, G est de dimension finie sur $\mathbf{Z}/2$, donc isomorphe en tant qu'espace vectoriel à $\left(\mathbf{Z}/2\right)^{\dim G}$, *a fortiori* en tant que *groupe*.

Exercice 3. (7 pts)

Soient $\begin{pmatrix}s\\t\end{pmatrix}$ et $\begin{pmatrix}\sigma\\\tau\end{pmatrix}$ dans $S\times T$.

Les préservations du neutre et de la loi par φ s'écrivent[1]

$$^1s = s \qquad \text{et} \qquad {}^t\left({}^\tau s\right) = {}^{t\tau}s.$$

De même, les préservations par le morphisme $\varphi(t)$ du neutre, de la loi et de l'inverse se réécrivent

$${}^t1 = 1, \qquad {}^t(s\sigma) = {}^ts\,{}^t\sigma \qquad \text{et} \qquad {}^t\left(s^{-1}\right) = \left({}^ts\right)^{-1} \text{ (abrégé } {}^ts^{-1}).$$

1. **(1 pt)** On a les équivalences

$$\begin{pmatrix}s\\t\end{pmatrix}*\begin{pmatrix}\sigma\\\tau\end{pmatrix}=\begin{pmatrix}s\\t\end{pmatrix}\begin{pmatrix}\sigma\\\tau\end{pmatrix}\iff\begin{pmatrix}s\,{}^t\sigma\\t\tau\end{pmatrix}=\begin{pmatrix}s\sigma\\t\tau\end{pmatrix}\iff\begin{cases}s\,{}^t\sigma=s\sigma\\t\tau=t\tau\end{cases}\iff{}^t\sigma=\sigma\,;$$

quantifier universellement sur σ donne $\varphi(t) = \mathrm{Id}$, puis quantifier universellement sur t donne « φ constant égal à $1_{\mathrm{Aut}\,S} = \mathrm{Id}_S$ ». La condition cherchée est donc la trivialité du morphisme φ.

La loi produit est par conséquent un cas particulier de loi $*$.

2. **(3,5 pts)** Tout d'abord, l'application $*$ est bien définie car le ${}^t\sigma$ de l'abscisse de $\begin{pmatrix}s\\t\end{pmatrix}*\begin{pmatrix}\sigma\\\tau\end{pmatrix}$ reste dans S.

Montrons que $\begin{pmatrix}1\\1\end{pmatrix}$ est neutre : cela vient des égalités

$$\begin{aligned}\begin{pmatrix}1\\1\end{pmatrix}*\begin{pmatrix}s\\t\end{pmatrix} &= \begin{pmatrix}1\,{}^1s\\1\,t\end{pmatrix}=\begin{pmatrix}1\,s\\t\end{pmatrix}=\begin{pmatrix}s\\t\end{pmatrix}\\ \text{et }\begin{pmatrix}s\\t\end{pmatrix}*\begin{pmatrix}1\\1\end{pmatrix} &= \begin{pmatrix}s\,{}^t1\\t\,1\end{pmatrix}=\begin{pmatrix}s\,1\\t\end{pmatrix}=\begin{pmatrix}s\\t\end{pmatrix}.\end{aligned}$$

Montrons que $\begin{pmatrix}s\\t\end{pmatrix}$ et $\begin{pmatrix}{}^{t^{-1}}s^{-1}\\t^{-1}\end{pmatrix}$ (intuité par une petite analyse) sont inverses l'un de l'autre : on a

$$\begin{aligned}\begin{pmatrix}s\\t\end{pmatrix}*\begin{pmatrix}{}^{t^{-1}}s^{-1}\\t^{-1}\end{pmatrix} &= \begin{pmatrix}s\;{}^t\left({}^{t^{-1}}s^{-1}\right)\\t\;t^{-1}\end{pmatrix}=\begin{pmatrix}s\;{}^{t\,t^{-1}}s^{-1}\\1\end{pmatrix}=\begin{pmatrix}s\;{}^1s^{-1}\\1\end{pmatrix}=\begin{pmatrix}s\;s^{-1}\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}\\ \text{et }\begin{pmatrix}{}^{t^{-1}}s^{-1}\\t^{-1}\end{pmatrix}*\begin{pmatrix}s\\t\end{pmatrix} &= \begin{pmatrix}{}^{t^{-1}}s^{-1}\;{}^{t^{-1}}s\\t^{-1}\;t\end{pmatrix}=\begin{pmatrix}{}^{t^{-1}}\left(s^{-1}\;s\right)\\1\end{pmatrix}=\begin{pmatrix}{}^{t^{-1}}1\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}.\end{aligned}$$

[1] attention à ne pas écrire ${}^ts\,{}^\tau s = {}^{t\tau}s$: lorsque $t = 1 = \tau$, on obtiendrait alors $s^2 = s$, forçant $s = 1$

Montrons enfin l'associativité : pour chaque $\begin{pmatrix}\mathfrak{s}\\ \mathfrak{t}\end{pmatrix} \in S \times T$, on a

$$\begin{array}{rcl}\begin{pmatrix}s\\ t\end{pmatrix} * \left(\begin{pmatrix}\sigma\\ \tau\end{pmatrix} * \begin{pmatrix}\mathfrak{s}\\ \mathfrak{t}\end{pmatrix}\right) & = & \begin{pmatrix}s\\ t\end{pmatrix} * \begin{pmatrix}\sigma\ {}^{\tau}\mathfrak{s}\\ \tau\mathfrak{t}\end{pmatrix} = \begin{pmatrix}s\ {}^{t}(\sigma\ {}^{\tau}\mathfrak{s})\\ t(\tau\mathfrak{t})\end{pmatrix} = \begin{pmatrix}s\ {}^{t}\sigma\ {}^{t}({}^{\tau}\mathfrak{s})\\ t\tau\mathfrak{t}\end{pmatrix}\\ \text{et } \left(\begin{pmatrix}s\\ t\end{pmatrix} * \begin{pmatrix}\sigma\\ \tau\end{pmatrix}\right) * \begin{pmatrix}\mathfrak{s}\\ \mathfrak{t}\end{pmatrix} & = & \begin{pmatrix}s\ {}^{t}\sigma\\ t\tau\end{pmatrix} * \begin{pmatrix}\mathfrak{s}\\ \mathfrak{t}\end{pmatrix} = \begin{pmatrix}s\ {}^{t}\sigma\ {}^{t\tau}\mathfrak{s}\\ (t\tau)\,\mathfrak{t}\end{pmatrix} = \begin{pmatrix}s\ {}^{t}\sigma\ {}^{t\tau}\mathfrak{s}\\ t\tau\mathfrak{t}\end{pmatrix} = \begin{pmatrix}\|\\ \|\end{pmatrix}.\end{array}$$

3. **(2,5 pts)** L'hypothèse « S stable par conjugaison » permet de donner sens à l'application $\begin{cases} T & \longrightarrow & \operatorname{Aut} S\\ t & \longmapsto & s \mapsto tst^{-1}\end{cases}$. Cette dernière est par ailleurs un morphisme d'après un exercice du cours. On peut donc utiliser ce qui précède.

   Pour tout n, notons E_n l'égalité $\begin{pmatrix}s\\ t\end{pmatrix}^{*n} = \begin{pmatrix}(st)^n t^{-n}\\ t^n\end{pmatrix}$. Montrons $\forall n \in \mathbf{N},\ E_n$ par récurrence.

   On a $\begin{pmatrix}(st)^0 t^{-0}\\ t^0\end{pmatrix} = \begin{pmatrix}1\cdot 1\\ 1\end{pmatrix} = \begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}s\\ t\end{pmatrix}^{*0}$, d'où E_0.

   Soit $n \in \mathbf{N}$ tel que E_n. On a alors

$$\begin{array}{rcl}\begin{pmatrix}s\\ t\end{pmatrix}^{*(n+1)} & = & \begin{pmatrix}s\\ t\end{pmatrix} * \begin{pmatrix}s\\ t\end{pmatrix}^{*n} = \begin{pmatrix}s\\ t\end{pmatrix} * \begin{pmatrix}(st)^n t^{-n}\\ t^n\end{pmatrix} = \begin{pmatrix}s\ {}^{t}[(st)^n t^{-n}]\\ t\ t^n\end{pmatrix}\\ & = & \begin{pmatrix}st\,(st)^n t^{-n} t^{-1}\\ t^{n+1}\end{pmatrix} = \begin{pmatrix}(st)^{n+1} t^{-(n+1)}\\ t^{n+1}\end{pmatrix}, \text{ d'où } E_{n+1}.\end{array}$$

Exercice 4. **(10,5 pts)**

1. **(2 pts)** Les entiers p et q étant premiers, ils sont supérieurs à 2, d'où $|G| = pq \geq 2\cdot 2 > 1$ et G n'est pas trivial. Soit $g \in G$ autre que le neutre. L'ordre de g divise alors $|G| = pq$, donc par primalité de p et q appartient à $\{1, p, q, pq\}$. L'ordre 1 est exclu, l'ordre p ou q conclut. Il reste l'ordre pq (alors G est cyclique) : dans ce cas, l'élément g^p est d'ordre q vu à $n \in \mathbf{N}^*$ fixé les équivalences[2]

$$(g^p)^n = 1 \iff g^{pn} = 1 \iff \omega(g) \mid pn \iff pq \mid pn \iff q \mid n$$

   (le plus petit tel n, à savoir $\omega(g^p)$, vaut donc q).

2. **(2,5 pts)** Le cours sur les groupes cycliques donne un isomorphisme $\begin{cases} \langle a\rangle & \xrightarrow{\sim} & \mathbf{Z}/p\\ a^k & \longmapsto & \overline{k}\end{cases}$ et un isomorphisme $\begin{cases} \mathbf{Z}/p & \xrightarrow{\sim} & \mathbf{U}_p\\ \overline{k} & \longmapsto & e^{2i\pi\frac{k}{p}}\end{cases}$, ce qui par composition donne un isomorphisme $\begin{cases} \langle a\rangle & \xrightarrow{\sim} & \mathbf{U}_p\\ a^k & \longmapsto & e^{2i\pi\frac{k}{p}}\end{cases}$ (*idem* pour b). On en déduit un isomorphisme "produit" $\begin{cases} \langle a\rangle \times \langle b\rangle & \xrightarrow{\sim} & \mathbf{U}_p \times \mathbf{U}_q\\ (a^k, b^\ell) & \longmapsto & \left(e^{2i\pi\frac{k}{p}}, e^{2i\pi\frac{\ell}{q}}\right)\end{cases}$. Montrons par ailleurs que la multiplication complexe induit un isomorphisme $\mathbf{U}_p \times \mathbf{U}_q \simeq \mathbf{U}_{pq}$: il en résultera par composition et comme demandé un isomorphisme $\langle a\rangle \times \langle b\rangle \simeq \mathbf{U}_{pq}$.

   Le groupe des complexes unitaires étant abélien, sa multiplication induit bien un morphisme $\mathbf{U}_p \times \mathbf{U}_q \longrightarrow \mathbf{U}$. Son image est incluse dans $\mathbf{U}_{pq}$ vu pour chaque (u, v) source les égalités $(uv)^{pq} = (u^p)^q (v^q)^p = 1^q 1^p = 1$. Vu par ailleurs l'égalité des cardinaux $|\mathbf{U}_p \times \mathbf{U}_q| = |\mathbf{U}_p| \times |\mathbf{U}_q| = pq = |\mathbf{U}_{pq}|$, il suffit de montrer l'injectivité.

   Soit donc $(u, v) \in \mathbf{U}_p \times \mathbf{U}_q$ tel que $1 = uv$. Élever à la puissance p donne $1 = u^p v^p = v^p$, ce qui montre que l'ordre de v divise p, *i. e.* appartient à $\{1, p\}$. Cet ordre divisant par ailleurs celui q du groupe $\mathbf{U}_q$ (où tombe v), il appartient également à $\{1, q\}$. L'intersection de ces deux paires se réduisant à $\{1\}$, l'ordre de v vaut 1 et v est le neutre. (*Idem* pour u.)

3. **(1 pt)** Le fait que a et b commutent de G traduit précisément le fait que la multiplication de G induit un morphisme de groupes $\langle a\rangle \times \langle b\rangle \longrightarrow G$. Ce morphisme est par ailleurs bijectif (la démonstration du cas $\mathbf{U}_p \times \mathbf{U}_q \simeq \mathbf{U}_{pq}$ s'adapte sans modification). Par conséquent, G est isomorphe à $\langle a\rangle \times \langle b\rangle \simeq \mathbf{U}_p \times \mathbf{U}_q \simeq \mathbf{U}_{pq}$ et ce dernier est cyclique.

[2] on aurait de même $\omega(g^q) = p$

4. **(1 pt)** $\mathfrak{S}_3$ est de cardinal $6 = 2 \cdot 3$ avec 2 et 3 premiers distincts. Toute transposition est d'ordre 2, tout cycle est d'ordre 3. En rajoutant Id (d'ordre 1), on vient de lister tous les éléments de $\mathfrak{S}_3$: aucun d'eux n'est d'ordre 6, d'où la non-cyclicité de $\mathfrak{S}_3$ (autre argument : un groupe monogène est abélien, ce qui n'est pas le cas de $\mathfrak{S}_3$).

5. **(1 pt)** La classe des sous-groupes de G étant stable par conjugaison, celle des sous-groupes d'ordre p est stable par conjugaison. Or par hypothèse cette classe est réduite à $\langle a \rangle$, ce qui conclut.

6. **(2 pts)** La question 3 de l'exercice 3 et la stabilité de $\langle a \rangle$ par conjugaison donne sens à la loi considérée. Montrons que (a, b) engendre $\langle a \rangle \times \langle b \rangle$. Pour cela, montrons que son ordre ω vaut pq.

   La même question 3 nous livre l'égalité $\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} (ab)^\omega \, b^{-\omega} \\ b^\omega \end{pmatrix}$, *i. e.* $b^\omega = 1 = (ab)^\omega$. La première égalité $b^\omega = 1$ montre que ω est multiple de l'ordre q de b, donc vaut q ou pq. Supposons par l'absurde qu'il vaille q : la deuxième égalité $(ab)^\omega = 1$ montre alors que le sous-groupe $\langle ab \rangle$ est d'ordre 1 ou q. S'il valait 1, alors a et b seraient inverses l'un de l'autre, donc auraient même ordre, d'où l'absurde égalité $p = q$. Par conséquent, $\langle ab \rangle$ est d'ordre q ; or par hypothèse le seul sous-groupe d'ordre q est $\langle b \rangle$. Ce dernier contient donc ab ; contenant par ailleurs b, il contient a, dont l'ordre p doit par conséquent diviser celui q de $\langle b \rangle$: contradiction.

7. **(1 pt)** Notons μ la multiplication $\begin{cases} \langle a \rangle \times \langle b \rangle & \longrightarrow & G \\ (s, t) & \longmapsto & st \end{cases}$. On a alors pour tous $\begin{cases} s, \sigma \in \langle a \rangle \\ t, \tau \in \langle b \rangle \end{cases}$ les égalités

$$\mu\left(\begin{pmatrix} s \\ t \end{pmatrix}\begin{pmatrix} \sigma \\ \tau \end{pmatrix}\right) = \mu\begin{pmatrix} s \; {}^t\sigma \\ t\tau \end{pmatrix} = \mu\begin{pmatrix} s \; t\sigma t^{-1} \\ t\tau \end{pmatrix} = s \; t\sigma t^{-1} \; t\tau = st \; \sigma\tau = \mu\begin{pmatrix} s \\ t \end{pmatrix}\mu\begin{pmatrix} \sigma \\ \tau \end{pmatrix}.$$

   On a déjà vu que μ est bijective : il résulte que G est, *via* μ, isomorphe à $\langle a \rangle \times \langle b \rangle$, lequel est cyclique par la question précédente.

   (bonus) Regardons l'ordre de l'élément ab (image de (a, b) par l'isomorphisme μ). Reprendre la fin de la question précédente élimine les cas où cet ordre vaudrait 1, p ou q, d'où la cyclicité de G en court-circuitant les questions 5 à 7. Cependant, nous n'aurions alors pas vu cette application de la loi $*$ qui permet de transformer la multiplication en un morphisme, ce qui eût été fort dommage.