TD n° 3 - Solutions

Exercice 4.

1. • Il est clair que l'élément neutre $e_G \in Z(G)$ car $e_G h = h e_G \quad \forall h \in G$.
   • Si $g_1, g_2 \in Z(G)$ sont deux éléments de $Z(G)$, alors

   $$(g_1 g_2)h = g_1(g_2 h) = g_1(h g_2) = (g_1 h)g_2 = (h g_1)g_2 = h(g_1 g_2) \quad \forall h \in G,$$

   donc $g_1 g_2 \in Z(G)$.
   • Si $g \in Z(G)$, alors $gh = hg \quad \forall h \in G$ et en multipliant cette idéntité par l'inverse g^{-1} à gauche et à droite on a que

   $$g^{-1} g h g^{-1} = g^{-1} h g g^{-1} \quad \forall h \in G \;\Leftrightarrow\; h g^{-1} = g^{-1} h \quad \forall h \in G$$

   ce qui equivaut à $g^{-1} \in Z(G)$.

   Cela montre que $Z(G)$ est un sous-groupe de G.

2. Pour tout $h \in G$ on a que

   $$(hxh^{-1})^2 = (hxh^{-1})(hxh^{-1}) = hx(h^{-1}h)xh^{-1} = hx^2h^{-1} = hh^{-1} = e_G.$$

   D'après l'hypothèse, les seuls éléments de G avec cette propriété sont e_G et x, donc on a deux cas :

   • Soit $hxh^{-1} = e_G$, ce qui équivaut à $hx = h \Leftrightarrow h^{-1}hx = h^{-1}h \Leftrightarrow x = e_G$, faux car cela contredit l'énoncé.
   • Soit $hxh^{-1} = x$, donc on a $hxh^{-1}h = xh \Leftrightarrow hx = xh \quad \forall h \in G$ ce qui équivaut à $x \in Z(G)$.

Exercice 5.

1. • Implication directe $\Rightarrow$: Si H est un sous-groupe de G, par définition on a que pour tous $h_1, h_2 \in H, \quad h_1 h_2 \in H$.
   • Implication réciproque $\Leftarrow$: Il faut supposer en plus que H est un ensemble non-vide.
   On a G un groupe fini, donc soit $n \in \mathbb{N}^*$ l'ordre de G. Tout élément g de G est donc d'ordre fini inférieur à n et on a aussi $g^n = e_G$.
   – Si $h \in H$ alors tout puissance de h est dans H, y inclus $h^n = e_G$. L'élément neutre e_G est dans H.
   – D'après l'hypothèse, pour tous $h_1, h_2 \in H, \quad h_1 h_2 \in H$.
   – Soit $h \in H$. Comme $h^n = e_G$, on a que $h^{-1} = h^{n-1} \in H$. L'inverse h^{-1} est dans H.

   Cela montre que H est un sous-groupe de G.

2. Un contre-exemple dans le cas infini sera le sous-ensemble $\mathbb{N} \subset \mathbb{Z}$ qui n'est pas un sous-groupe du groupe additif $(\mathbb{Z}, +)$.

Exercice 9.

1. Les morphismes de groupes φ de $\mathbb{Z}$ dans $\mathbb{Z}$ sont donnés par $\varphi(1)$. En effet, on montre par récurrence que
$$\varphi(n) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = n \cdot \varphi(1)$$
lorsque $n \geq 0$. Et puis $\varphi(n) = \varphi(-(-n)) = -\varphi(-n) = -(-n) \cdot \varphi(1) = n \cdot \varphi(1)$ lorsque n est négatif. La multiplication par $d = \varphi(1)$ est toujours injective sauf quand d est nul. Par contre elle n'est surjective que quand $d = 1$.

2. Les morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Q}$ sont de la forme $\varphi : r = \frac{p}{q} \mapsto \frac{p}{q} \cdot \varphi(1)$. Pour montrer cela on procède par étapes comme on l'a fait en TD. D'abord on on le montre quand $q = 1$ et $p \geq 0$, puis on le montre pour p entier quelconque (positif ou négatif). Après on déduit du cas précédent le cas où $p = 1$ et q est quelconque, enfin on prouve la formule générale.

   φ est injectif lorsque $\varphi(1)$ est non nul. Par contre, contrairement au cas précédent avec $\mathbb{Z}$, φ est toujours surjectif, à moins que $\varphi(1)$ soit nul. φ est donc toujours un isomorphisme excepté quand c'est le morphisme nul.

Exercice 10. Les groupes suivants sont-ils isomorphes ?

1. Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes *via* le morphisme exponentiel.

2. $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ne sont pas isomorphes. Supposons en effet l'existence d'un isomorphisme
$$\varphi : \mathbb{R}^* \to \mathbb{R}.$$
On aurait alors
$$2\varphi(-1) = \varphi(-1) + \varphi(-1) = \varphi((-1)^2) = \varphi(1) = 0.$$
Et donc $\varphi(-1) = 0 = \varphi(1)$ ce qui contredit l'injectivité de φ.

   Remarque : C'est donc essentiellement le fait que 2 soit inversible dans $\mathbb{R}$ qui empêche que $\mathbb{R}$ et $\mathbb{R}^*$ soient isomorphes ...

3. $\mathbb{C}$ et $\mathbb{C}^*$ sont isomorphes toujours grâce à l'application exponentielle.

4. $\mathbb{Q}$ et $\mathbb{Q}_+^*$ ne sont pas isomorphes. En effet, un morphisme $\varphi : \mathbb{Q} \to \mathbb{Q}_+^*$ est de la forme $\frac{p}{q} \mapsto \varphi(1)^{\frac{p}{q}}$ (montrer cette formule par étapes : d'abord quand $q = 1$ et $p \geq 0$, puis pour p entier quelconque, puis quand $p = 1$ et q quelconque, puis la formule générale).
   Mais $\varphi(1)$ est un rationnel $\frac{a}{b}$.
   Il est bien connu qu'un rationnel positif $\neq 1$ n'a toutes ses racines dans $\mathbb{Q}$.

Exercice 11.

1. Le groupe ayant le plus petit cardinal possible est le groupe à un élément c'est-à-dire réduit à son élément neutre.

2. Le groupe de Klein $F = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique : $(1,0)$, $(1,1)$ et $(0,1)$ sont tous les trois d'ordre 2. C'est bien le groupe non cyclique de cardinal possible le plus petite possible car tout groupe de cardinal premier est cyclique et 2 et 3 sont premiers.

3. F est isomorphe au sous-groupe de S_4 engendré par (1 2) et (3 4) *via* le morphisme :
$$\varphi : \left\{ \begin{array}{lcl} F = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & S_4 \\ (0,0),\ (1,0),\ (0,1),\ (1,1) & \mapsto & Id,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4) \end{array} \right.$$

   En réalité F est également un sous-groupe de A_4 mais cette fois celui engendré par (1 2)(3 4), (1 3)(2 4) et (1 4)(2 3). Il est en effet facile de voir que chacun de ces élément est d'ordre 2 et que le produit de deux de ceux-ci donne le troisième. D'autre part, tous ces éléments sont dans A_4 car il sont produit d'un nombre pair de transpositions.

4. Tout groupe G de cardinal n se plonge dans S_n *via*

$$\begin{array}{rcl} \varphi : G & \to & Bij(G) \cong S_n \\ g & \mapsto & \{\varphi_g : x \mapsto gx\} \end{array}$$

(vérifier que c'est un morphisme injectif.)

Ainsi un groupe de cardinal 2 se plonge dans S_2 qui est abélien ($S_2 \cong \mathbb{Z}/2\mathbb{Z}$) donc ne peut être abélien.

Les groupes de cardinal 3 sont donc à chercher comme sous-groupes de S_3. Or les sous-groupes de S_3 sont ceux de cardinal 2 engendré par une transposition et ceux de cardinal 3 engendré par un 3-cycle. Dans le premier cas il sont isomorphes à S_2 donc abélien, dans le second cas il sont isomorphes à $\mathbb{Z}/3\mathbb{Z}$ aussi abélien.

Les seuls groupes de cardinal 4 sont le groupe de Klein F et $\mathbb{Z}/4\mathbb{Z}$ (pour s'en convaincre écrire toutes les tables possibles avec 4 éléments) et les deux sont abéliens.

Tout groupe monogène (=cyclique) est abélien puisque toutes les puissances d'un même élément commutent les unes avec les autres. Ainsi en particulier tout groupe de cardinal premier est abélien. En particulier, il n'existe pas de groupe non abélien de cardinal 5.

On cherche donc un groupe abélien de cardinal ≥ 6. En réalité, le groupe S_3 n'est pas commutatif et est de cardinal 6. Il possède une interprétation géométrique puisque c'est le groupe des symétries du triangle équilatéral (ou groupe diédral d'ordre 6), que l'on note D_6 (ou parfois D_3). Il est engendré par une rotation d'ordre 3 et une symétrie orthogonale.

5. Pour tout $n \in \mathbb{N}$, S_n se plonge dans S_{n+1}. Ainsi, S_3 se plonge dans tous les S_n pour $n > 4$.

Exercice 12. Soit G un groupe et soit $g \in G$. On définit $f : \mathbb{Z} \to G, n \mapsto g^n$.

1. C'est clair : $f(0) = g^0 = e_G$; pour tout $n \in \mathbb{Z}$, $f(-n) = g^{-n} = (g^n)^{-1} = f(n)^{-1}$; pour tous $n, m \in \mathbb{Z}$, $f(n+m) = g^{n+m} = g^n g^m = f(n)f(m)$.

2. f est surjectif ssi G est (monogène) engendré par g.

3. f est injectif si pour tous $n \in \mathbb{Z}$, $g^n \neq e_G$, c'est-à-dire si g est d'ordre infini.

4. Soit $N \in \mathbb{N}$ est l'ordre de g (avec la convention que $N = 0$ si g n'est pas d'ordre fini).

$N \cdot \mathbb{Z}$ est alors le noyau de f. En effet, il est immédiat que $N \cdot \mathbb{Z} \subset \ker f$. Inversément, si $f(n) = e_G$ c'est que $g^n = e_G$ donc que n divise l'ordre de g c'est-à-dire N (voir le cours).

Ainsi, f induit un morphisme injectif $Z/N \cdot \mathbb{Z} = Z/\ker f \to G$ donc un isomorphisme avec son image, c'est-à-dire ici avec $< g >$.

5. Il suffit d'appliquer la question précédente avec $G = \mathbb{C}$ et $g = e^{2i\pi/N}$. On a alors un isomorphisme entre $\mu_N =< g >$ et $\mathbb{Z}/N \cdot \mathbb{Z}$ car g est bien d'ordre exactement N.

6. Il y a autant de tels isomorphismes que de générateurs de $\mu_N =< g >$. Or

$$\begin{array}{rll} < g^k >=< g > & \textit{si et seulement si} & g^k \text{ est un générateur de } < g >, \\ & \textit{si et seulement si} & \exists s \in \mathbb{Z} \text{ tel que } e^{2i\pi/N} = g = (g^k)^s = e^{2iks\pi/N}, \\ & \textit{si et seulement si} & \exists s \in \mathbb{Z} \text{ tel que } \dfrac{ks-1}{N} \in \mathbb{Z}, \\ & \textit{si et seulement si} & \exists s, t \in \mathbb{Z} \text{ tels que } ks - 1 = tN, \\ & \textit{si et seulement si} & pgcd(k, N) = 1. \end{array}$$

Il y a une fonction qui compte le nombre de tels $0 < k < N$ premiers avec N qui s'appelle la fonction indicatrice d'Euler.