Série 3

Exercice 1. Soit $N \geqslant 1$ et $M|N$ alors l'ensemble des multiples de M dans $\{0, \cdots, N-1\}$ forme un sous-groupe de $\mathbb{Z}/N\mathbb{Z}$ et reciproquement tout sous-groupe est de cette forme (raisonnr comme pour les sous-groupes de $\mathbb{Z}$.)

Exercice 2. Soit $N \in \mathbb{Z}$ et

$$[\times N] : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & Nn \end{array}.$$

Montrer que $[\times N]$ est un morphisme de groupes. Reciproquement montrer que tout endomorphisme $\phi : \mathbb{Z} \to \mathbb{Z}$ est de la forme $\phi = [\times N]$ (considerer $\phi(1)$.)

Exercice 3. (preuve de l'Identite de Bezout) On rappelle que les sous-groupes de $\mathbb{Z}$ (muni de l'addition) sont exactement les ensembles de la forme

$$N\mathbb{Z}$$

avec $N \in \mathbb{Z}$.

— Montrer que $M\mathbb{Z} \subset N\mathbb{Z}$ si et seulement si N divise M.

— Soient m, n des entiers. On considere le sous-ensemble

$$\langle m, n\rangle = \{am + bn,\ a, b \in \mathbb{Z}\}$$

Montrer que $\langle m, n\rangle$ est un sous-groupe de $\mathbb{Z}$.

— Montrer que $1 \in \langle 2, 3\rangle$ et que $\langle 2, 3\rangle = \mathbb{Z}$.

— Montrer que en general $\langle m, n\rangle = (m, n)\mathbb{Z}$ ou (m, n) est le pgdc de m et n (utiliser la definition du pgdc). ATTENTION : ne pas utiliser l'identite de Bezout pour la demonstration car c'est le but de l'exercice !

— En deduire (Identite de Bezout) que etant donne $m, n \in \mathbb{Z}$, il existe $a, b \in \mathbb{Z}$ tel que

$$am + bn = (m, n).$$

Exercice 4. En considerant les formule pour le cosinus et le sinus d'une somme montrer que l'application

$$\exp(2\pi i.) : \begin{array}{ccc} \mathbb{R} & \mapsto & \mathbb{C}^1 \\ x & \mapsto & \exp(2\pi i x) = \cos(2\pi x) + i\sin(2\pi x) \end{array}$$

est un morphisme du groupe $(\mathbb{R}, +)$ vers le groupe $(\mathbb{C}^1, \times)$ ou

$$\mathbb{C}^1 = \{z \in \mathbb{C},\ |z| = 1\} \subset \mathbb{C}^\times$$

est le groupe multiplicatif des nombres complexes de module 1. Ce morphisme est-t-il injectif ?

Exercice 5. (Sera fait en cours le semaine prochaine mais interessant pour s'entrainer) Soit $\phi : (G, \times) \to (H, \star)$ un morphisme de groupes. Montrer que les ensembles suivants (appeles "noyau" et "image" de ϕ) sont des sous-groupes de G et H respectivement

$$\ker(\phi) := \phi^{-1}(\{e_H\}) = \{g \in G,\ \phi(g) = e_H\} \subset G,$$

$$\mathrm{Im}(\phi) := \phi(G) = \{h \text{ de la forme } h = \phi(g),\ g \in G\} \subset H.$$

Exercice 6 ($\star$)**.** On rappelle (voir le cours) que etant donne un groupe $(G, .)$ et un element $g \in G$, l'application de translation a gauche

$$t_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & t_g(g') = g.g' \end{array}$$

est une application bijective et sa reciproque est $t_{g^{-1}}$. En d'autres termes $t_g \in \mathrm{Bij}(G)$.

1. Montrer que t_g n'est un morphisme de groupes que si $g = e_G$.
2. Montrer que l'application
$$t_. : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & t_g \end{array}$$
est un morphisme de groupes de $(G, .)$ vers le groupe des bijections sur G, $(\mathrm{Bij}(G), \circ)$.
3. Montrer que t est injectif : ($t_g = t_{g'} \Longrightarrow g = g'$).
4. On a vu en cours qu'une source importante de groupes est le groupe $(\mathrm{Bij}(E), \circ)$ des bijections d'un ensemble sur lui-meme (les permutations d'un ensemble) et les sous-groupes de ce groupe. Montrer que reciproquement tout groupe $(G, .)$ est isomorphe a un sous-groupe d'un groupe $\mathrm{Bij}(E)$ pour E un ensemble bien choisi.
5. Montrer que si G est un groupe fini de cardinal $|G| = n \geqslant 1$ alors G est isomorphe a un sous-groupe du groupe $\mathfrak{S}_n = \mathrm{Bij}(\{1, \cdots, n\})$ des permutations de l'ensemble $\{1, \cdots, n\}$. (on montrera que si E et F sont des ensembles en bijection l'un avec l'autre alors -en utilisant cette bijection- les groupes $\mathrm{Bij}(E)$ et $\mathrm{Bij}(F)$ sont isomorphes).

Exercice 7 ($\star$)**.** Soit un groupe $(G, .)$ et un element $g \in G$, l'application de "conjugaison par g" est l'application de G vers G definies par

$$\mathrm{Ad}_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & \mathrm{Ad}_g(g') = g.g'.g^{-1} \end{array}.$$

1. Montrer que pour tout g, Ad_g est un automorphisme (de groupe) dont le morphisme reciproque est $\mathrm{Ad}_{g^{-1}}$. Ainsi $\mathrm{Ad}_g \in \mathrm{Aut}(G)$.

2. Montrer que l'application qui en resulte

$$\mathrm{Ad}_{\cdot} : \begin{array}{ccc} G & \mapsto & \mathrm{Aut}(G) \\ g & \mapsto & \mathrm{Ad}_g \end{array}$$

est un morphisme de groupes de $(G, .)$ vers le groupe des automorphismes (de groupe) de G, $(\mathrm{Aut}(G), \circ)$.

3. Montrer que le noyau de cette application est le sous-ensemble de G donne par

$$\ker(\mathrm{Ad}_{\cdot}) = \{g \in G,\ \forall g' \in G,\ g.g' = g'.g\} =: Z_G.$$

C'est a dire l'ensemble des elements de G qui commutent avec tous les elements de g. On appelle ce sous-groupe le centre de G.

4. Montrer que Z_G est un sous-groupe commutatif de G.