EPFL Automne 2017
Geometrie, MATH-120

Solutions série 3

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 $\phi(1)$).

Solution 2. On a, pour tout $n_1, n_2 \in \mathbb{Z}$,

$$[\times N](n_1 + n_2) = N(n_1 + n_2) = Nn_1 + Nn_2 = [\times N](n_1) + [\times N](n_2).$$

La loi de composition interne consideree dans $\mathbb{Z}$ (qui est l'ensemble de depart et d'arrivee de l'application $[\times N]$) etant l'addition usuelle, l'egalite ci-dessus montre que $[\times N]$ verifie le critere de morphisme et est donc un morphisme de groupes.

Reciproquement, soit $\phi : \mathbb{Z} \to \mathbb{Z}$ un morphisme de groupes. Montrons par recurrence que, pour tout $n \in \mathbb{N}$, $\phi(n) = n\phi(1)$. Considerons tout d'abord le cas $n = 0$. Par definition d'un morphisme de groupes, $\phi(0) = 0$ etant donne que 0 est l'element neutre dans $\mathbb{Z}$. On a donc bien $\phi(0) = 0\phi(1)$. Maintenant, supposons que $\phi(n) = n\phi(1)$ pour un $n \in \mathbb{N}$ et montrons que $\phi(n+1) = (n+1)\phi(1)$. On a, en utilisant la definition d'un morphisme de groupes, $\phi(n + 1) = \phi(n) + \phi(1) = n\phi(1) + \phi(1) = (n + 1)\phi(1)$. Ainsi, nous avons montre que, pour tout $n \in \mathbb{N}$, $\phi(n) = n\phi(1)$. Maintenant, soit $n \in \mathbb{Z}$ et tel que $n < 0$. En utilisant la definition d'un morphisme de groupes ainsi que le fait que l'inverse dans $\mathbb{Z}$ est l'oppose, on a $\phi(n) = \phi(-(-n)) = -\phi(-n)$. Comme $-n \in \mathbb{N}$, on sait d'apres la preuve dans le cas des entiers naturels que $\phi(-n) = (-n)\phi(1)$, ce qui donne $\phi(n) = n\phi(1)$. Finalement, on a donc, pour tout $n \in \mathbb{Z}$, $\phi(n) = Nn$ en posant $N = \phi(1) \in \mathbb{Z}$ (puisque le domaine d'arrivee de ϕ est $\mathbb{Z}$). L'endomorphisme ϕ est donc bien de la forme $[\times N]$.

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 $a, b \in \mathbb{Z}$ tels que

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

Solution 3. — Supposons que $M\mathbb{Z} \subset N\mathbb{Z}$. Puisque $M \in M\mathbb{Z}$, on a $M \in N\mathbb{Z}$, ce qui signifie qu'il existe $k \in \mathbb{Z}$ tel que $M = kN$. Ainsi, N divise M. Inversement, supposons que N divise M. Il existe donc $l \in \mathbb{Z}$ tel que $M = lN$. Soit $t \in M\mathbb{Z}$. On sait alors qu'il existe $q \in \mathbb{Z}$ tel que $t = qM$, ce qui donne $t = qlN$, ce qui montre que $t \in N\mathbb{Z}$ puisque $ql \in \mathbb{Z}$. Ainsi, $M\mathbb{Z} \subset N\mathbb{Z}$.

— Soient $m, n \in \mathbb{Z}$ et $h \in \langle m, n\rangle$. Par definition de $\langle m, n\rangle$, il existe $a, b \in \mathbb{Z}$ tels que $h = am + bn$. Comme $m, n, a, b \in \mathbb{Z}$, on a $am + bn \in \mathbb{Z}$ et donc $h \in \mathbb{Z}$. Ainsi, $\langle m, n\rangle \subset \mathbb{Z}$. Maintenant, soient $h_1, h_2 \in \langle m, n\rangle$. Il existe donc $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tels que $h_1 = a_1m + b_1n$ et $h_2 = a_2m + b_2n$. Ainsi, $h_1 - h_2 = (a_1 - a_2)m + (b_1 - b_2)n$. Comme $a_1 - a_2 \in \mathbb{Z}$ et que $b_1 - b_2 \in \mathbb{Z}$, cela montre que $h_1 - h_2 \in \langle m, n\rangle$. Comme la loi de composition interne consideree dans $\mathbb{Z}$ est l'addition usuelle et que l'inverse et l'oppose, cela montre que le critere de sous-groupe est verifie. Finalement $\langle m, n\rangle$ est bien un sous-groupe de $\mathbb{Z}$.

— Il est clair que $2 \in \langle 2, 3\rangle$ (il suffit de prendre $a = 1$ et $b = 0$ qui appartiennent bien a $\mathbb{Z}$). De meme, $3 \in \langle 2, 3\rangle$ (il suffit de prendre $a = 0$ et $b = 1$). Ainsi, comme $\langle 2, 3\rangle$ est un sous-groupe, $-2 \in \langle 2, 3\rangle$ et $1 = 3 + (-2) \in \langle 2, 3\rangle$. On a vu a la question precedente que $\langle 2, 3\rangle \in \mathbb{Z}$. Maintenant, soit $n \in \mathbb{Z}$. On a $n = 2(-n) + 3n$ et donc $n \in \langle 2, 3\rangle$ puisque $n \in \mathbb{Z}$ et $-n \in \mathbb{Z}$. Ainsi, $\mathbb{Z} \subset \langle 2, 3\rangle$. Finalement, on obtient que $\langle 2, 3\rangle = \mathbb{Z}$.

— Il est rappele dans l'enonce que tout sous-groupe de $\mathbb{Z}$ est de la forme $N\mathbb{Z}$ avec $N \in \mathbb{Z}$. Ainsi, comme $\langle m, n\rangle$ est un sous-groupe de $\mathbb{Z}$, on peut l'ecrire $\langle m, n\rangle = d\mathbb{Z}$ pour $d \in \mathbb{Z}$. On a donc que $m \in d\mathbb{Z}$ et $n \in d\mathbb{Z}$ et donc que d est un diviseur commun de m et n. Soit maintenant e un diviseur commun quelconque de m et n. Il existe alors $k_1, k_2 \in \mathbb{Z}$ tels que $m = k_1e$ et $n = k_2e$. Soit $h \in \langle m, n\rangle$. Par definition de $\langle m, n\rangle$, il existe $a, b \in \mathbb{Z}$ tels que $h = am + bn$. Ainsi, $h = (ak_1 + bk_2)e$, ce qui montre que $h \in e\mathbb{Z}$ etant donne que $ak_1 + bk_2 \in \mathbb{Z}$. Ainsi, $\langle m, n\rangle \subset e\mathbb{Z}$ et donc $d\mathbb{Z} \subset e\mathbb{Z}$. La premiere question nous donne alors que e divise d. Donc d est un diviseur commun de m et n et est un multiple de n'importe quel diviseur commun de m et n. On en conclut que $d = (m, n)$.

— Nous avons vu a la question precedente que $\langle m, n\rangle = (m, n)\mathbb{Z}$. Ainsi, en particulier, $(m, n) \in \langle m, n\rangle$. Par definition de $\langle m, n\rangle$, il existe donc $a, b \in \mathbb{Z}$ tels que

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

Exercice 6. 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).

Solution 6. 1. Prenons tout d'abord $g = e_G$. On a, par les proprietes d'associativite et de neutralite que, pour tout $g_1, g_2 \in G$, $t_g(g_1.g_2) = e_G.g_1.g_2 = (e_G.g_1).g_2 = (e_G.g_1).(e_G.g_2) = t_g(g_1).t_g(g_2)$. Donc, si $g = e_G$, le critere de morphisme est verifie et t_g est bien un morphisme de groupes. Maintenant, soit $g \neq e_G$. On a alors $t_g(e_G) = g.e_G = g$ par la propriete de neutralite. Ainsi, $t_g(e_G) \neq e_G$ et donc t_g n'est pas un morphisme de groupes. Finalement, on obtient le resultat voulu.

2. Soient $g_1, g_2 \in G$. Par definition de t, $t(g_1.g_2) = t_{g_1.g_2}$. Ainsi, en utilisant l'associativite, pour $h \in G$, $t(g_1.g_2)(h) = t_{g_1.g_2}(h) = (g_1.g_2).h = g_1.g_2.h$. Par ailleurs, $(t_{g_1} \circ t_{g_2})(h) = t_{g_1}(t_{g_2}(h)) = t_{g_1}(g_2.h) = g_1.(g_2.h) = g_1.g_2.h$. Ainsi, pour tout

$h \in G$, $t(g_1.g_2)(h) = (t_{g_1} \circ t_{g_2})(h)$ et donc $t_{g_1.g_2} = t_{g_1} \circ t_{g_2}$. Cela montre que t verifie le critere de morphisme et est donc un morphisme de groupes de $(G, .)$ vers $(\text{Bij}(G), \circ)$.

3. Soient $g, g' \in G$ tels que $t_g = t_{g'}$. On sait alors que, pour tout $h \in G$, $t_g(h) = t_{g'}(h)$, i.e., $g.h = g'.h$. Comme G est un groupe, $h \in G$ possede un element inverse note h^{-1}. On a donc $g.h.h^{-1} = g'.h.h^{-1}$, et ainsi, par la propriete d'associativite, $g.(h.h^{-1}) = g'.(h.h^{-1})$. Cela donne, en utilisant la propriete de simplification, $g.e_G = g'.e_G$ et donc, par la propriete de neutralite, $g = g'$. Ainsi, $t_g = t_{g'} \Longrightarrow g = g'$, ce qui montre que t est injectif.

4. Soit $(G, .)$ un groupe. Nous allons tout d'abord montrer que l'ensemble $A = \{t_g : g \in G\}$ est un sous-goupe de $\text{Bij}(G)$. Nous avons vu en cours que, pour tout $g \in G$, $t_g \in \text{Bij}(G)$ et t_g admet $t_{g^{-1}}$ comme application reciproque. Ainsi, $A \subset \text{Bij}(G)$. Maintenant, soient $a_1, a_2 \in A$. Nous savons par definition de A qu'il existe $g_1, g_2 \in G$ tels que $a_1 = t_{g_1}$ et $a_2 = t_{g_2}$. Soit $h \in G$. On a, en utilisant l'associativite,

$$(a_1 \circ a_2^{-1})(h) = (t_{g_1} \circ t_{g_2^{-1}})(h) = t_{g_1}(t_{g_2^{-1}}(h)) = t_{g_1}(g_2^{-1}.h) = g_1.(g_2^{-1}.h) = g_1.g_2^{-1}.h.$$

   Ainsi, $a_1 \circ a_2^{-1} = t_{g_1.g_2^{-1}}$. Comme G est un groupe, $g_1.g_2^{-1} \in G$ et donc $a_1 \circ a_2^{-1} \in A$. Le critere de sous-groupe est donc verifie et ainsi A est un sous-groupe de $\text{Bij}(G)$. Nous montrons maintenant que G est isomorphe a A. Pour cela, considerons l'application

$$t_A : \begin{array}{ccc} G & \mapsto & A \\ g & \mapsto & t_g \end{array}.$$

   La question 2 nous donne que t_A est un morphisme de groupes de $(G, .)$ vers $(A, \circ)$. Par ailleurs, grace a la question 3, nous savons que t_A est injective. De plus, par definition de A, t_A est clairement surjective et donc bijective. Finalement t_A est un isomorphisme (i.e. un morphisme de groupes bijectif) de G vers A et donc G est bien isomorphe a A qui est un sous-groupe de $\text{Bij}(G)$.

5. Considerons des ensembles E et F en bijection. Notons h une bijection de E vers F. Nous avons

$$h : \begin{array}{ccc} E & \mapsto & F \\ e & \mapsto & h(e) \end{array}.$$

   Comme h est bijective, nous pouvons considerer son application reciproque h^{-1} qui est egalement bijective. Ainsi, comme la composee d'applications bijectives est bijective, pour tout $k \in \text{Bij}(E)$, l'application $h \circ k \circ h^{-1}$ est bijective. Par ailleurs, pour tout $f \in F$, $(h \circ k \circ h^{-1})(f) \in F$. Ainsi, $h \circ k \circ h^{-1} \in \text{Bij}(F)$. Considerons maintenant l'application

$$I : \begin{array}{ccc} \text{Bij}(E) & \mapsto & \text{Bij}(F) \\ k & \mapsto & h \circ k \circ h^{-1} \end{array}$$

et montrons qu'il s'agit d'un isomorphisme de $(\mathrm{Bij}(E), \circ)$ vers $(\mathrm{Bij}(F), \circ)$. Soient $k_1, k_2 \in \mathrm{Bij}(E)$. Nous avons $I(k_1 \circ k_2) = h \circ (k_1 \circ k_2) \circ h^{-1}$. Par ailleurs, en utilisant les proprietes d'associativite, de simplification et de neutralite, on obtient

$$\begin{aligned} I(k_1) \circ I(k_2) = (h \circ k_1 \circ h^{-1}) \circ (h \circ k_2 \circ h^{-1}) &= h \circ k_1 \circ (h^{-1} \circ h) \circ k_2 \circ h^{-1} \\ &= h \circ k_1 \circ Id_E \circ k_2 \circ h^{-1} \\ &= h \circ (k_1 \circ Id_E) \circ k_2 \circ h^{-1} \\ &= h \circ k_1 \circ k_2 \circ h^{-1} \\ &= h \circ (k_1 \circ k_2) \circ h^{-1}. \end{aligned}$$

On a donc $I(k_1 \circ k_2) = I(k_1) \circ I(k_2)$. Ainsi le critere de morphisme est verifie et I est bien un morphisme de groupes de $(\mathrm{Bij}(E), \circ)$ vers $(\mathrm{Bij}(F), \circ)$. Il nous reste a montrer que I est une application bijective. Soient $k_1, k_2 \in \mathrm{Bij}(E)$. On a que $I(k_1) = I(k_2)$ implique $h \circ k_1 \circ h^{-1} = h \circ k_2 \circ h^{-1}$, ce qui implique $h^{-1} \circ h \circ k_1 \circ h^{-1} \circ h = h^{-1} \circ h \circ k_2 \circ h^{-1} \circ h$ et donc, par associativite, simplification et neutralite, $k_1 = k_2$. Donc I est injective. Maintenant, soit $l \in \mathrm{Bij}(F)$. En choisissant $k = h^{-1} \circ l \circ h$ qui appartient a $\mathrm{Bij}(E)$, il est clair que $l = h \circ k \circ h^{-1} = I(k)$. Ainsi, I est surjective et donc bijective. Finalement, I est bien un isomorphisme de $(\mathrm{Bij}(E), \circ)$ vers $(\mathrm{Bij}(F), \circ)$.
Considerons maintenant un groupe fini de cardinal $|G| = n \geqslant 1$. Ainsi, nous pouvons ecrire G sous la forme $\{g_1, \ldots, g_n\}$ et nous introduisons l'application

$$B : \begin{array}{ccc} \{1, \ldots, n\} & \mapsto & G \\ i & \mapsto & g_i \end{array}.$$

Il est clair que B est bijective. Ainsi, G et $\{1, \ldots, n\}$ sont en bijection et on sait donc d'apres le resultat precedent que $(\mathrm{Bij}(G), \circ)$ est isomorphe a $(\mathrm{Bij}(\{1, \ldots, n\}), \circ)$. Ainsi, il est facile de voir que tout sous-groupe H de $\mathrm{Bij}(G)$ est isomorphe a un sous-groupe de $\mathrm{Bij}(\{1, \ldots, n\})$, plus precisement l'image de H par l'isomorphisme considere. Comme G est isomorphe a un sous-groupe de $\mathrm{Bij}(G)$ (voir question 4) et que la composee de deux isomorphismes est un isomorphisme, G est isomorphe a un sous-groupe de $\mathfrak{S}_n = \mathrm{Bij}(\{1, \ldots, n\})$.