EPFL Automne 2016
Geometrie, MATH-120

Solutions série 3

Exercice 2. On considere

$$\mathbb{Z}^2 = \{(m,n),\ m,n \in \mathbb{Z}\}.$$

Montrer que $\mathbb{Z}^2$ est un sous-groupe de $(\mathbb{R}^2,+)$.

1. Soient $a,b,c,d \in \mathbb{Z}$, montrer que l'application

   $$\phi : (m,n) \in \mathbb{Z}^2 \to (am+bn, cm+dn)$$

   est un endomorphisme de $(\mathbb{Z}^2,+)$.
2. Montrer que tout endomorphisme de $(\mathbb{Z}^2,+)$ est de la forme ci-dessus.
3. Montrer que si $ad-bc \neq 0$ alors ϕ est injectif (on pourra considerer l'application similaire dans $\mathbb{R}^2$).
4. Montrer que si $ad-bc = \pm 1$ alors ϕ est un isomorphisme de groupes et donner la reciproque .
5. Montrer que si $ad-bc \neq \pm 1$ alors ϕ n'est pas un isomorphisme.

Solution 2. Let $(m_1,n_1),(m_2,n_2) \in \mathbb{Z}^2$. Then $(m_1,n_1)-(m_2,n_2) = (m_1-m_2, n_1-n_2) \in \mathbb{Z}^2$, since m_1-m_2 and n_1-n_2 are both integers if m_1,n_1,m_2,n_2 are integers. Thus $\mathbb{Z}^2$ is a subgroup of $\mathbb{R}^2$.

1. Let $(m_1,n_1),(m_2,n_2) \in \mathbb{Z}^2$. Then :

$$\begin{aligned}
&\phi((m_1,n_1)+(m_2,n_2)) \\
&\qquad = \phi(m_1+m_2,\ n_1+n_2) && (1.1)\\
&\qquad = (a(m_1+m_2)+b(n_1+n_2),\ c(m_1+m_2)+d(n_1+n_2)) && (1.2)\\
&\qquad = ((am_1+bn_1)+(am_2+n_2),\ (cm_1+dn_1)+(cm_2+dn_2)) \\
&\qquad = (am_1+bn_1, cm_1+dn_1)+(am_2+n_2, cm_2+dn_2) && (1.3)\\
&\qquad = \phi(m_1,n_1)+\phi(m_2,n_2). && (1.4)
\end{aligned}$$

Thus ϕ is a morphism. We used rules of addition in $\mathbb{Z}^2$ in order to obtain (1.1), (1.3), and the definition of ϕ in order to obtain (1.2), (1.4).

2. Let $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$ be any endomorphism. Denote $\phi(1,0) =: (A, C)$ and $\phi(0,1) =: (B, D)$. For every $(m, n) \in \mathbb{Z}^2$ such that $m, n > 0$ we have :

$$\begin{aligned}
\phi(m,n) &= \phi(\underbrace{(1,0)+(1,0)+\ldots+(1,0)}_{m}+\underbrace{(0,1)+(0,1)+\ldots+(0,1)}_{n}) \\
&= \underbrace{\phi(1,0)+\phi(1,0)+\ldots+\phi(1,0)}_{m}+\underbrace{\phi(0,1)+\phi(0,1)+\ldots+\phi(0,1)}_{n} \\
&= \underbrace{(A,C)+(A,C)+\ldots+(A,C)}_{m}+\underbrace{(B,D)+(B,D)+\ldots+(B,D)}_{n} \\
&= (\underbrace{A+A+\ldots+A}_{m},\underbrace{C+C+\ldots+C}_{m})+(\underbrace{B+B+\ldots+B}_{n},\underbrace{D+D+\ldots+D}_{n}) \\
&= (Am, Cm) + (Bn, Dn) \\
&= (Am + Bn, Cm + Dn).
\end{aligned}$$

Note that $\phi(0,0) = (0,0) = (A0 + B0, C0 + D0)$ since every morphism maps the neutral element to the neutral element. We also have

$$\begin{aligned}
&\phi(-1,0) + \phi(1,0) = \phi(0,0) \\
\Rightarrow\ &\phi(-1,0) + (A,C) = (0,0) \\
\Rightarrow\ &\phi(-1,0) = (0,0) - (A,C) \\
\Rightarrow\ &\phi(-1,0) = (-A,-C),
\end{aligned}$$

and similarly $\phi(0,-1) = (-B,-D)$. Now we can use the same technique as for $m > 0, n > 0$ to verify that $\phi(m,n) = (Am + Bn, Cm + Dn)$ holds for all the remaining combination of signs of m and n.

3. Let $ad - bc \neq 0$. In order to prove that ϕ is an injection, it suffices to show $\ker(\phi) = \{(0,0)\}$, since $(0,0)$ is the neutral element in $(\mathbb{Z}^2, +)$. Suppose that $(m,n) \in \mathbb{Z}^2$ is such that $\phi(m,n) = (0,0)$, i.e. $(am+bn, cm+dn) = (0,0)$. Then the numbers m and n make a solution of the 2×2 linear system of equations

$$\left\{ \begin{array}{rcl} am + bn &=& 0, \\ cm + dn &=& 0. \end{array} \right.$$

This system has a unique solution if and only if $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$, and this is precisely iff $ad - bc \neq 0$. In that case, the unique solution is $(m,n) = (0,0)$, which implies $\ker(\phi) = \{(0,0)\}$.

4. Suppose that $ad - bc = 1$, and let $\psi(m,n) := (dm - bn, -cm + an)$. The function $\psi : \mathbb{Z}^2 \to \mathbb{Z}^2$ is a morphism and

$$\begin{aligned}
(\psi \circ \phi)(m,n) &= \psi(am + bn, cm + dn) \\
&= (d(am+bn) - b(cm+dn), -c(am+bn) + a(cm+dn)) \\
&= ((ad-bc)m, (ad-bc)n) \\
&= (m,n),
\end{aligned}$$

for all $(m,n) \in \mathbb{Z}^2$. Similarly, $\phi \circ \psi = id$, and thus ϕ is invertible with $\phi^{-1} = \psi$. If $ad - bc = -1$, the same holds for $\psi(m,n) := (-dm + bn, cm - an)$.

How did we come up with the formulae for ψ ? Let us rewrite $\phi(m,n)$ in a slightly different form, where we replace an ordered pair (m,n) with a 2d-vector :

$$\phi\left(\begin{bmatrix} m \\ n \end{bmatrix}\right) = \begin{bmatrix} am + bn \\ cm + dn \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix}.$$

Composition of two morphisms then amounts to matrix multiplication, and the inverse of a morphism can be computed via the matrix inverse :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

5. Let $M = ad - bc$ be such that $M \neq \pm 1$. If $M = 0$, by using the solution of subtask 3., we can see that ϕ is not injective, and thus not an isomorphism. Suppose that $|M| > 1$, and that ϕ is an isomorphism. Since ϕ is a surjection, there exists $(m_1, n_1) \in \mathbb{Z}^2$ such that $\phi(m_1, n_1) = (am_1 + bn_1, cm_1 + dn_1) = (0, 1)$. Thus $cm_1 + dn_1 = 1$, and Bezout's theorem implies $GCD(c,d) = 1$. On the other hand, there also exists $(m_2, n_2) \in \mathbb{Z}^2$ such that $\phi(m_2, n_2) = (am_2 + bn_2, cm_2 + dn_2) = (1, 0)$, i.e.

$$am_2 + bn_2 = 1, \tag{1.5}$$
$$cm_2 + dn_2 = 0. \tag{1.6}$$

Multiply (1.6) with a, and subtract (1.5) multiplied with c to get

$$(ad - bc)n_2 = -c,$$

from which we conclude that c is divisible by M. Similarly, multiply (1.6) with b, and subtract (1.5) multiplied with d to get

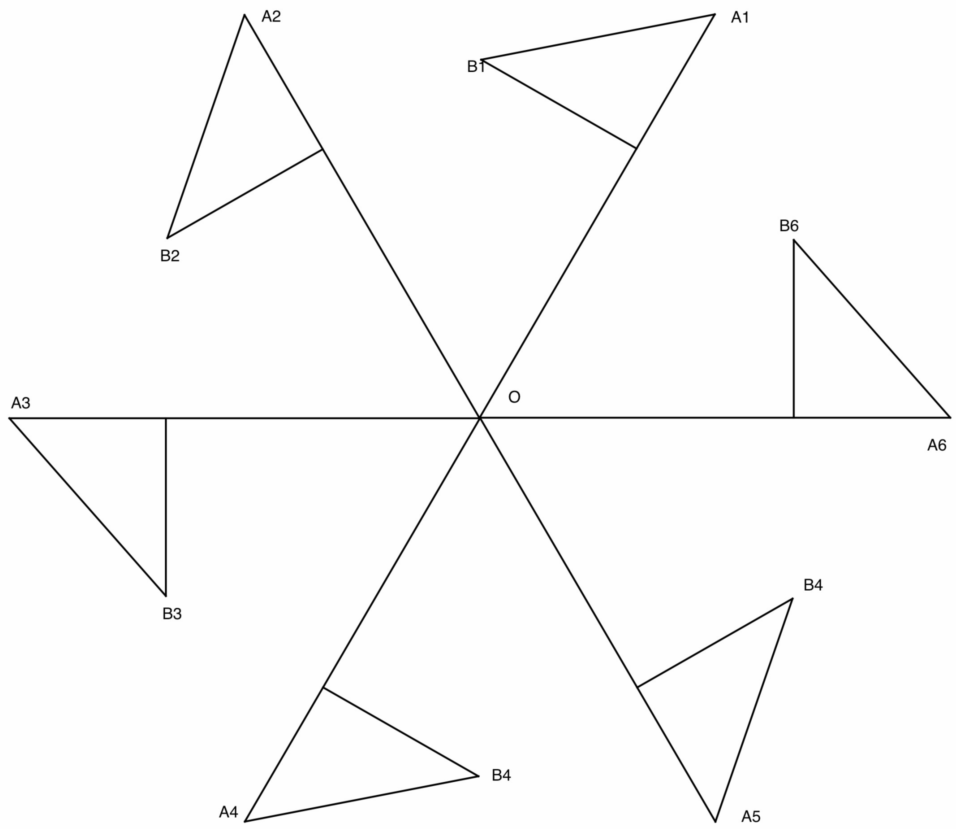
$$(ad - bc)m_2 = d,$$

from which we conclude that d is also divisible by M. This is a contradiction since $GCD(c,d) = 1$. Thus ϕ cannot be an isomorphism if $ad - bc \neq 1$.

Exercice 3. Une isometrie du plan $\mathbb{R}^2$est une application $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ telle que

$$\forall P, Q \in \mathbb{R}^2,\ d(\phi(P), \phi(Q)) = d(P, Q)$$

ou $d(.,.)$ est la distance euclidienne usuelle dans $\mathbb{R}^2$. On admet que l'ensemble $\mathrm{Isom}(\mathbb{R}^2)$ des isometries du plan forme un groupe pour la composition des applications.



En utilisant le fait (admis) qu'une isometrie $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ qui laisse trois points non-alignes P_1, P_2, P_3 invariants ($\phi(P_i) = P_i,\ i = 1, 2, 3$) est l'identité $\mathrm{Id}_{\mathbb{R}^2}$, montrer que l'ensemble des isometries $\mathrm{Isom}_F(\mathbb{R}^2) = \{\phi \in \mathrm{Isom}(\mathbb{R}^2),\ \phi(F) = F\}$ qui preservent la figure ci-dessous est le groupe des rotations de centre $(0, 0)$ et d'angle un multiple de 60^o.

Pour cela on pourra considerer une telle isometrie, ϕ, considerer les valeurs possibles des points $A_6, 0, A_3, B_6$ et montrer qu'il existe une rotation comme ci-dessus qui envoie ces points sur les meme images.

Solution 3. We make several observations in order to prove the statement of the exercise.

Observation 1 : An isometry maps line segments to line segments of the same length. Let $\overline{AB}$ be a given line segment. Then $P \in \overline{AB}$ if and only if $d(A, P) + d(P, B) = d(A, B)$ (the triangle inequality). By using this and the fact that ϕ is an isometry, we have $d(\phi(A), \phi(P)) + d(\phi(P), \phi(B)) = d(A, P) + d(P, B) = d(A, B) = d(\phi(A), \phi(B))$. Thus, $\phi(P) \in \overline{\phi(A)\phi(B)}$. Conversely, if $Q \in \overline{\phi(A)\phi(B)}$, then $\phi^{-1}(Q) \in \overline{AB}$ since ϕ^{-1} is an isometry as well. Therefore, $\phi(\overline{AB}) = \overline{\phi(A)\phi(B)}$.

Observation 2 : ϕ permutes the tuples $(\overline{A_1A_4}, \overline{A_2A_5}, \overline{A_3A_6})$ and $(A_1, A_2, A_3, A_4, A_5, A_6)$. Let F denote the entire figure. From Observation 1, $\phi(\overline{A_1A_4}) \subseteq F$ is a line segment of the same length. There exist only three line segments in F of this length, and these are $\overline{A_1A_4}, \overline{A_2A_5}, \overline{A_3A_6}$. Thus $\phi(\overline{A_1A_4}) \in \{\overline{A_1A_4}, \overline{A_2A_5}, \overline{A_3A_6}\}$, and the endpoints $\phi(A_1), \phi(A_4)$ lie in the set $\{A_1, A_2, A_3, A_4, A_5, A_6\}$. The same holds for $\phi(\overline{A_2A_5})$ and $\phi(\overline{A_3A_6})$ and the endpoints A_2, A_5, A_3, A_6. Finally, note that $\phi(A_i) \neq \phi(A_j)$ for all $i \neq j$ since $d(\phi(A_i), \phi(A_j)) = d(A_i, A_j) > 0$. Thus, $(\phi(A_1), \phi(A_2), \phi(A_3), \phi(A_4), \phi(A_5), \phi(A_6))$ is a permutation of $(A_1, A_2, A_3, A_4, A_5, A_6)$, and $(\phi(\overline{A_1A_4}), \phi(\overline{A_2A_5}), \phi(\overline{A_3A_6}))$ is a permutation of $(\overline{A_1A_4}, \overline{A_2A_5}, \overline{A_3A_6})$.

Observation 3 : $\phi(O) = O$. Since $O \in \overline{A_1A_4} \cap \overline{A_2A_5} \cap \overline{A_3A_6}$, we have that $\phi(O) \in \phi(\overline{A_1A_4}) \cap \phi(\overline{A_2A_5}) \cap \phi(\overline{A_3A_6}) = \overline{A_1A_4} \cap \overline{A_2A_5} \cap \overline{A_3A_6}$, where we used Observation 2 for the last equality. The only point in $\overline{A_1A_4} \cap \overline{A_2A_5} \cap \overline{A_3A_6}$ is O, and thus $\phi(O) = O$.

Observation 4 : If $\phi(A_1) = A_i$, then $\phi(B_1) = B_i$. Let $\phi(A_1) = A_i$. Since $d(\phi(B_1), \phi(A_1)) = d(B_1, A_1)$, the point $\phi(B_1)$ lies on the circle k_1 of radius $d(B_1, A_1)$ with the center at $\phi(A_1) = A_i$. Similarly, since $d(\phi(B_1), \phi(O)) = d(B_1, O)$, the point $\phi(B_1)$ lies on the circle k_2 of radius $d(B_1, 0)$ with the center at $\phi(O) = O$. The circles k_1 and k_2 intersect at two points : B_i and B_{i-1}. If $\phi(B_1) = B_{i-1}$ then $\phi(\overline{A_1B_1}) = \overline{A_iB_{i-1}}$, which cannot hold true since $\overline{A_1B_1} \subseteq F$ and $\overline{A_iB_{i-1}} \nsubseteq F$. Thus $\phi(B_1) = B_i$.

Observation 5 : ϕ is a rotation by a multiple of 60^o. Assume that $\phi(A_1) = A_i$. Then $\phi(B_1) = B_i$ and $\phi(O) = O$. Denote with r the rotation by $60^o \cdot (i-1)$ degrees around O, and let $\psi = r^{-1} \circ \phi$. Then $r(A_1) = A_i$, $r(B_1) = B_i$, $r(O) = O$, from which we have $\psi(A_1) = A_1$, $\psi(B_1) = B_1$, $\psi(O) = O$. Since ψ is an isometry (a composition of two isometries) with three fixed ("invariant") points, it has to be equal to identity. Therefore, $\phi = r$.

Exercice 5 ($\star\star$)**.** On rappelle (voir le cours) que etant donne un groupe $(G, .)$ et un element $g \in G$, l'application de conjugaison

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

est un morphisme de groupe bijectif (ie. un isomorphisme) et sa reciproque est $\mathrm{Ad}_{g^{-1}}$.

En d'autres termes $\mathrm{Ad}_g \in \mathrm{Isom}_{Gr}(G)$.

Montrer que l'application qui en resulte

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

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

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

$$Z_G = \{g \in G,\ \forall g' \in G,\ g.g' = g'.g\}.$$

   C'est a dire l'ensemble des elements de G qui commutent avec tous les elements de g.
2. Montrer que c'est un sous-groupe : on l'appelle le centre de G.

Solution 5. In order to make more clear what we need to show, let us introduce notation $\mathrm{Ad}(g) = Ad_g$. The task is to demonstrate that $\mathrm{Ad} : G \to \mathrm{Isom}(G)$ is a morphism, i.e. $\mathrm{Ad}(g.h) = \mathrm{Ad}(g) \circ \mathrm{Ad}(h)$, for all $g, h \in G$. Take any two elements $g, h \in G$. To show that *functions* $\mathrm{Ad}(g.h)$ and $\mathrm{Ad}(g) \circ \mathrm{Ad}(h)$ coincide, we need to show that they coincide at each element of their domain, which is G. For every $x \in G$ we have :

$$\begin{aligned}(\mathrm{Ad}(g.h))\,(x) &= \mathrm{Ad}_{g.h}(x) = (g.h).x.(g.h)^{-1} = g.h.x.h^{-1}.g^{-1} \\ &= g.(h.x.h^{-1}).g^{-1} = g.\mathrm{Ad}_h(x).g^{-1} = \mathrm{Ad}_g(\mathrm{Ad}_h(x)) = (\mathrm{Ad}_g \circ \mathrm{Ad}_h)(x) \\ &= (\mathrm{Ad}(g) \circ \mathrm{Ad}(h))(x).\end{aligned}$$

1. The neutral element in $\mathrm{Isom}(G)$ is the identity mapping. Let $g \in \ker(\mathrm{Ad})$. Then $\mathrm{Ad}_g = id$, and for each $x \in G$ it holds that $\mathrm{Ad}_g(x) = id(x)$, i.e. $g.x.g^{-1} = x$. Multiplying by g from the right, we have $g.x = x.g$, and thus $g \in Z_G$.
   Conversely, let $g \in Z_G$. Then it holds that $g.x = x.g$ for all $x \in G$, from which we have $g.x.g^{-1} = x$, i.e. $\mathrm{Ad}_g(x) = id(x)$, so $\mathrm{Ad}_g = id$ and $g \in \ker(\mathrm{Ad})$.
2. Take any $g, h \in Z_G$. Then $g.h^{-1} \in Z_G$ since for all $x \in G$ we have

$$\begin{aligned}(g.h^{-1}).x &= g.(h^{-1}.x) \\ &= (h^{-1}.x).g \qquad (1.7) \\ &= (x^{-1}.h)^{-1}.g \\ &= (h.x^{-1})^{-1}.g \qquad (1.8) \\ &= x.h^{-1}.g \\ &= x.(g.h^{-1}). \qquad (1.9)\end{aligned}$$

   To get (1.7) and (1.9), respectively, we used $g \in Z_G$, so it commutes with any element of G including $h^{-1}.x$ and h^{-1}, respectively. To get (1.8), we used $h \in Z_G$, so it commutes with any element of G including x^{-1}.