Solution de l'exercice 1. 1. Montrons que l'application

$$f : G/K \to K\backslash G : gK \mapsto Kg^{-1}$$

est bien définie : si $aK = bK$ $(a, b \in G)$, alors $a = bk$ pour un $k \in K$, et en inversant $k^{-1}b^{-1} = a^{-1}$, où $k^{-1} \in K$, ce qui montre que a^{-1} et b^{-1} sont dans la même orbite pour l'action par translation à gauche, i.e., $f(aK) = Ka^{-1} = Kb^{-1} = f(bK)$.

En fait, cette application est une bijection. Elle est surjective car $im(f) = f(gK) : g \in G = Kg^{-1} : g \in G = Kg' : g' \in G$, où la dernière égalité vient du fait que l'inversion est une bijection de G. On montre qu'elle est injective en suivant le raisonnement du premier paragraphe dans l'autre sens.

Ainsi, on a bien une bijection comme demandé.

2. D'abord, supposons que G/K est fini. On remarque que les orbites de l'action de K sur H sont incluses dans les orbites de l'action de K sur G. Cela se traduit par une injection $H/K \to G/K : hK \mapsto hK$, où on note que les deux "hK" ne signifient pas la même chose (montrer que c'est bien une injection !). Dès lors, H/K est fini.

On a aussi une surjection $G/K \to G/H : gK \mapsto gH$ (montrer que c'est bien défini et que c'est une surjection !), ce qui montre que G/H est fini aussi.

Maintenant, supposons que G/H et H/K sont finis. Soient des ensembles de représentants $\{g_i : i \in I\}$ et $\{h_j : j \in J\}$ de G/H et H/K, respectivement. On montre que

$$G/K = \{g_i h_j K : (i, j) \in I \times J\}.$$

Soit gK un élément de G/K. Alors g appartient à une classe $g_i H$, pour un certain $i \in I$. Donc $g = g_i h$ pour un $h \in H$, et ce h appartient à une classe $h_j K$ pour un certain j. Donc $g = g_i h \in g_i h_j K$. On a ainsi montré que les $g_i h_j$, $(i, j) \in I \times J$, représentent toutes les classes de G/K (en fait, c'est même un ensemble de représentants, ce qu'on montre au point suivant). Cela implique que le cardinal de G/K est plus petit que $I \times J$, qui est fini. Donc G/K est fini.

3. Vu ce qu'on a montré ci-dessus, il suffit de montrer que les classes $g_i h_j K$ sont toutes distinctes, ou de manière équivalente, qu'elle sont 2 à 2 disjointes.

Soient $(i, j), (r, s) \in I \times J$ tels que $g_i h_j K \cap g_r h_s K \neq \emptyset$. Alors, en particulier, comme $\emptyset \neq g_i h_j K \cap g_r h_s K \subset g_i H \cap g_r H$, on doit avoir $i = r$ par définition d'un ensemble de représentants. Cela implique que $h_j K \cap h_s K \neq \emptyset$, et donc $j = s$.

Dès lors, $\{g_i h_j : (i, j) \in I \times J\}$ est un ensemble de représentants des classes de G/K. On a donc $[G : K] = |I \times J| = |I| \cdot |J| = [G : H] \cdot [H : K]$, car I, J sont finis.

Solution de l'exercice 2. 1. D'abord, montrons l'associativité. Soient $(h, k), (h', k'), (h'', k'') \in H \times K$. On a

$$\begin{aligned}((h, k) \star (h', k')) \star (h'', k'') &= (h \times h', k.h \odot k') \star (h'', k'') = ((h \times h') \times h'', (k.h \odot k').(h \times h') \odot k'') \\ &= ((h \times h') \times h'', k.h \odot k'.h \odot (h' \odot k''))\end{aligned}$$

et

$$\begin{aligned}(h, k) \star ((h', k') \star (h'', k'')) &= (h, k) \star (h' \times h'', k'.h' \odot k'') = (h \times (h' \times h''), k.h \odot (k'.h' \odot k'')) \\ &= (h \times (h' \times h''), k.h \odot k'.h \odot (h' \odot k'')),\end{aligned}$$

où la dernière égalité vient du fait que l'action de H sur K est "par automorphismes", ce qui nous permet de "distribuer" l'action. On conclut par associativité dans les groupes H et K.

Pour montrer que (e_H, e_K) est l'élément neutre, soit $(h,k) \in H \times K$. On a

$$(e_H, e_K) \star (h,k) = (e_H \times h, e_K.(e_H \odot k)) = (h,k)$$

car e_H agit trivialement sur K. Aussi,

$$(h,k) \star (e_H, e_K) = (h \times e_H, k.(h \odot e_K)) = (h, k.e_K) = (h,k)$$

où on a utilisé le fait que l'action est par automorphismes dans l'avant-dernière égalité, ce qui implique que tous les éléments de H fixent e_K.

Pour montrer que l'inversion est bien celle de l'énoncé, les calculs sont similaires.

2. Ce sont des morphismes car pour tous $h, h' \in H$, on a

$$i_1(h) \star i_1(h') = (h, e_K) \star (h', e_K) = (h \times h', e_K.(h \odot e_K)) = (h \times h', e_K) = i_1(h \times h')$$

et pour tous $k, k' \in K$, on a

$$i_2(k) \star i_2(k') = (e_H, k) \star (e_H, k') = (e_H \times e_H, k.(e_H \odot k')) = (e_H, k.k') = i_2(k.k').$$

Ils sont injectifs car leur noyau est trivial. En effet,

$$i_1(h) = (e_H, e_K) \Rightarrow (h, e_K) = (e_H, e_K) \Rightarrow h = e_H$$

et de même pour i_2.

3. Dès lors, on identifie H et K avec leurs images $i_1(H)$ et $i_2(K)$ (par exemple, $h \star k$ signifie maintenant $i_1(h) \star i_2(k) = (h, e_K) \star (e_H, k)$).

Montrons d'abord que K est distingué dans $H \ltimes_\odot K$. Pour tous $(h,k) \in H \ltimes_\odot K$, $h' \in K$, on a

$$(h,k) \star k' \star (h,k)^{-1} = (h, k.h \odot k') \star (h^{-1}, h^{-1} \odot k^{-1}),$$

qui est un élément de $i_2(K) \simeq K$ car sa première composante est e_H, ce qui conclut.

Montrons maintenant que $H \simeq i_1(H)$ agit sur K par conjugaison, i.e., l'action par conjugaison de H sur K dans $H \ltimes_\odot K$ correspond à l'action de H sur K donnée par $\odot$. Soient $h \in H$ et $k \in K$, on a

$$\begin{aligned} h \star k \star h^{-1} &= (h, e_K) \star (e_H, k) \star (h^{-1}, e_K) = (h \times e_H, e_K.h \odot k) \star (h^{-1}, e_K) = (e_H, (h \odot k).(e_H \odot e_K)) \\ &= (e_H, h \odot k) = h \odot k. \end{aligned}$$

Pour la dernière partie de l'énoncé, on va utiliser le théorème noyau-image (important de savoir l'utiliser !). Considérons le morphisme (vérifier que c'est bien un morphisme de groupes !)

$$f : H \ltimes_\odot K / rightarrow H : (h,k) \mapsto h,$$

qui est clairement surjectif. Son noyau est $i_2(K)$. Ainsi le théorème noyau-image nous donne l'isomorphisme attendu.

4. Lorsque l'action $\odot$ de H sur K est l'action triviale, la loi de groupe du produit semi-direct $H \ltimes_\odot K$ devient simplement

$$(h,k) \star (h', k') = (h \times h', k.h \odot k') = (h \times h', k.k'),$$

qui est la loi du produit direct $H \times K$. Donc on a $H \ltimes_\odot K = H \times K$ dans ce cas.

Solution de l'exercice 3. On appelle f l'application de l'énoncé. On montre d'abord que c'est un morphisme de groupes. Pour tous $(h,k),(h',k') \in H \ltimes K$, on a

$$f((h,k)\star(h',k')) = f(hh', k(h\odot k')) = f(hh', khk'h^{-1}) = khk'h^{-1}hh' = khk'h' = f(h,k)\cdot f(h',k'),$$

donc f est un morphisme de groupes.

Le morphisme f est injectif car son noyau est trivial. En effet, si $(h,k) \in \ker(f)$, alors $e_G = f(h,k) = kh$. Donc $k^-1 = h$ est un élément de $H \cap K = \{e_G\}$, donc $h = k = e_G$.

Le morphisme f est surjectif car $K.H = K^{-1}.H^{-1} = (H.K)^{-1} = G^{-1} = G$.

Ainsi, f est un isomorphisme.

Solution de l'exercice 4. 1. Montrons d'abord l'inclusion $G - G^+ \subset s \circ G^+$. Soit $s' \in G - G^+$, alors $s' = s \circ (s^{-1} \circ s')$, où $s^{-1} \circ s'$ appartient à G^+ (le produit de deux isométries non-spéciales est une isométrie spéciale). Donc $s' \in s \circ G^+$. Pour l'autre inclusion, il suffit de remarquer que, pour tout $r \in G^+$, $s \circ r$ est une isométrie non-spéciale dans G, donc appartient à $G - G^+$. Ainsi, on a $G - G^+ = s \circ G^+$. Pour l'autre égalité de l'énoncé, le raisonnement est exactement le même.

2. On a $s^1 = s \circ s = t_{2z}$ (résultat du cours), donc $2z \in \Gamma$.

3. On a (on ommet les $\circ$ pour la composition)

$$st_\gamma s^{-1} = t_z t_w (s_0 t_\gamma s_0^{-1}) t_{-w} t_{-z} = (s_0 t_\gamma s_0^{-1}) t_z t_w t_{-w} t_{-z} = s_0 t_\gamma s_0^{-1},$$

où le facteur entre parenthèse commute avec le reste car tous les facteurs sont des translations ($s_0 t_\gamma s_0^{-1}$ est une translation car les translations forment un sous-groupe distingué des isométries). Pour connaître le vecteur de la translation $s_0 t_\gamma s_0^{-1}$, on calcule l'image de 0, ce sera le vecteur recherché :

$$s_0 t_\gamma s_0^{-1}(0) = s_0 t_\gamma(0) = s_0(\gamma)$$

par linéarité de s_0. Ainsi, $st_\gamma s^{-1} = t_{s_0(\gamma)}$, et donc $s_0(\gamma) \in \Gamma$.

On a pris $\gamma \in \Gamma$ quelconque, donc $s_0(\Gamma) \in \Gamma$. En réappliquant s_0, on obtient $\Gamma = s_0 s_0(\Gamma) \in s_0(\Gamma)$. On obtient ainsi $s_0(\Gamma) = \Gamma$.

4. Soit Γ_1 l'ensemble des éléments de Γ de module 1. D'abord, $\mu_6 = \{\pm 1, \pm\omega_6, \pm(\omega_6 - 1)\}$ est bien inclus dans Γ_1. On montre que $\Gamma_1 = \mu_6$.

De l'hypothèse de minimalité de la norme de 1 parmi $\Gamma - \{0\}$, on déduit que Γ ne contient aucune paire de vecteurs distincts à distance de moins de 1 (si c'était le cas pour γ et γ', alors $\gamma - \gamma'$ serait un élément non-nul de norme < 1, ce qui contredit l'hypothèse).

Les éléments de μ_6 sont les sommets d'un hexagone régulier inscrit dans le cercle unité, et la distance entre deux sommets consécutifs est 1. Ces 6 sommets découpent le cercle en 6 arcs de cercle. Ainsi, si Γ_1 contenait un autre élément, il serait sur l'un de ses arcs de cercle, et il serait donc à distance < 1 des sommets délimitant cet arc. Dès lors, $\Gamma_1 = \mu_6$.

Comme s_0 est une isométrie linéaire, elle préserve la norme, donc préserve Γ_1, i.e., $s_0(\Gamma_1) \subset \Gamma_1$. Comme Γ_1 est fini et s_0 injectif, on a en fait $s_0(\mu_6) = s_0(\Gamma_1) = \Gamma_1 = \mu_6$.

5. On peut supposer $s_0(1) = \omega_6$. En effet, vu 4, on a $s_0(1) = \omega_6^k$ pour un $k \in \mathbb{Z}$, et on considère alors $r^{1-k} \circ s$ où $r \in G_0^+ \subset G^+ \subset G$, et on a bien $(r^{1-k} \circ s)_0(1) = r^{1-k} \circ s_0(1) = \omega_6$.

On a $2z \in \Gamma$ par le point 2. On sait aussi que z est parallèle à l'axe de la symétrie s_0, qui est $\mathbb{R}.(1+\omega_6)$. Ainsi, $2z \in \Gamma \cap \mathbb{R}.(1+\omega_6) = \mathbb{Z}.(1+\omega_6)$, donc $z = \frac{k}{2}(1+\omega_6)$ pour un entier k.

Si k est pair, alors $z \in \Gamma$ et on considère $t_{-z} \circ s \in G$, dont le "z" correspondant vaut 0.

Si k est impair, $k = 2l+1$ pour un $l \in \mathbb{Z}$, alors on considère $t_{-l(1+\omega_6)} \circ s$, dont le "z" correspondant vaut $(1+\omega_6)/2$.

6. Dans le cas $z = \frac{1}{2}(1+\omega_6)$,

$$t_{-\omega_6} \circ s = t_{-\omega_6} \circ t_{\frac{1}{2}(1+\omega_6)} \circ t_w \circ s_0 = t_{\frac{1}{2}(1-\omega_6)} \circ t_w \circ s_0$$

est une symétrie axiale car $\frac{1}{2}(1-\omega_6)$ est perpendiculaire à l'axe de $\circ t_w \circ s_0$ (calculer le produit scalaire par exemple).

Dès lors, dans les deux cas de 5, on peut trouver dans G une symétrie axiale s d'axe parallèle à la droite $\mathbb{R}(1+\omega_6)$.

7. Soit C l'ensemble des centres de rotation des rotations d'ordre 6 de G^+. On va montrer que $C = \Gamma$.

Montrons $C \subset \Gamma$. Soit $c \in C$. Soit $r \in G^+$ une rotation d'ordre 6 et de centre c. Alors r est d'angle (en paramètre complexe) $\pm\omega_6$. On suppose que c'est $+\omega_6$, quitte à prendre r^{-1} à la place, qui a le même centre que r. Alors on peut écrire r (en identifiant $\mathbb{R}^2 \simeq \mathbb{C}$) comme

$$r = t_z \circ r_0$$

où $z \in \mathbb{C}$. Vu que $G_0^+ \subset G$ par hypothèse, on a $r_0 \in G$ et donc $z \in \Gamma$. Le centre c de r est alors donné par

$$r(c) = c \Leftrightarrow z + \omega_6 c = c \Leftrightarrow c = \frac{z}{1-\omega_6} = \omega_6 z,$$

donc $c = \omega_6 z \in \omega_6 \Gamma \subset \Gamma$.

Montrons maintenant $\Gamma \subset C$. Soit $\gamma \in \Gamma$. Alors $\omega_6^{-1}\gamma$ appartient à Γ. La rotation $r = t_{\omega_6^{-1}\gamma} \circ r_0$ (où $r_0 \in G$ est la rotation linéaire envoyant 1 sur ω_6) appartient à G. Par le calcul ci-dessus, le centre de r est $\omega_6 \omega_6^{-1}\gamma = \gamma$, donc $\gamma \in C$.

Dès lors, $\Gamma = C$.

Montrons maintenant que $s(\Gamma) \subset \Gamma$, en montrons que $s(C) \subset C$. Soit $c \in C$ et $r \in G^+$ une rotation de centre c. Alors $s \circ c \circ s^{-1}$ est un élément de G^+ (car G^+ est distingué dans G), de centre $s(c)$ car

$$s \circ c \circ s^{-1}(s(c)) = s \circ r(c) = s(c).$$

Ainsi $s(c) \in C$. Dès lors, $s(\Gamma) \subset \Gamma$.

Vu 6, on sait que G contient une symétrie axiale s d'axe parallèle à $\mathbb{R}(1+\omega_6)$. Cette symétrie s'écrit $s = t_w \circ s_0$, où w est perpendiculaire à $\mathbb{R}(1+\omega_6)$, i.e., parallèle à $\mathbb{R}\omega_6^2$. De $s(\Gamma) \subset \Gamma$, on déduit que $s(0) = w$ appartient à Γ. Donc $w \in \Gamma \cap \mathbb{R}\omega_6^2 = \mathbb{Z}\omega_6^2$.

Ainsi, $s_0 = t_{-w} \circ s$ est bien dans G, comme attendu.

Série 5 2020 : corrigé de l'exercice 5

Exercice 5

1. D'abord on montre que l'action est transitive. Soit $z = x + iy \in \mathbb{C}$. Posons :
$$n = n(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$
$$a = a(y) = \begin{pmatrix} \sqrt{y} & 0 \\ 0 & \sqrt{1/y} \end{pmatrix}$$
Alors :
$$g := n.a = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & \sqrt{1/y} \end{pmatrix}$$
Et $g.i = \frac{\sqrt{y}i+x/\sqrt{y}}{\sqrt{1/y}} = x + iy = z$ Donc $\forall z \in \mathbb{C}, z \in G.i \iff$ Une seule orbite, donc action transitive.
On calcule maintenant le stabilisateur de i. Soit
$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}).$$
Alors $g.i = i \iff \frac{ai+b}{ci+d} = i \iff ai + b = di - c \iff a = d, b = -c \iff g \in K$. Par le théorème orbite-stabilisateur, on a une bijection entre $SL_2(\mathbb{R})/K$ et l'orbite de i, donc $\mathbb{H}$ par la première partie ci-dessus.
2. On vérifie juste les critères de sous-groupe.
Pour les isomorphismes, on pose :
$\varphi_1 : N \to (\mathbb{R}, +), n(x) \to x$
$\varphi_2 : A \to (\mathbb{R}_{>0}, *), a(y) \to y$
Et on vérifie facilement que ce sont bien des isomorphismes.
3. Montrons que $N.A = \{n.a, n \in N, a \in A\}$ est un sous groupe de $SL_2(\mathbb{R})$:
Soit, pour i=1,2 :
$$n_i = \begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix} \in N$$
$$a_i = \begin{pmatrix} \sqrt{y_i} & 0 \\ 0 & \sqrt{1/y_i} \end{pmatrix} \in A$$
Alors, comme ci-dessus,
$$n_i.a_i = \begin{pmatrix} \sqrt{y_i} & x_i/\sqrt{y_i} \\ 0 & \sqrt{1/y_i} \end{pmatrix} \in N.A$$
Et donc :
$$(n_1.a_1).(n_2.a_2) = \begin{pmatrix} \sqrt{y_1} & x_1/\sqrt{y_1} \\ 0 & \sqrt{1/y_1} \end{pmatrix} \begin{pmatrix} \sqrt{y_2} & x_2/\sqrt{y_2} \\ 0 & \sqrt{1/y_2} \end{pmatrix} = \begin{pmatrix} \sqrt{y_1 y_2} & \frac{(x_2 y_1 + x_1)}{\sqrt{(y_1 y_2)}} \\ 0 & \sqrt{1/(y_1 y_2)} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & x_2 y_1 + x_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{y_1 y_2} & 0 \\ 0 & \sqrt{1/(y_1 y_2)} \end{pmatrix} \in N.A$$

Donc $N.A$ est stable par multiplication.
Pour l'inverse de $n_1.a_1$, si on pose :

$$n = \begin{pmatrix} 1 & \frac{-x_1}{y_1} \\ 0 & 1 \end{pmatrix} \in N$$

et

$$a = a_1^{-1} = \begin{pmatrix} 1/\sqrt{y_1} & 0 \\ 0 & \sqrt{y_1} \end{pmatrix} \in A$$

Alors on vérifie que $n.a = (n_1.a_1)^{-1}$ et donc que l'inverse est vérifié. Donc $N.A$ est bien un sous-groupe.
Montrons que $N.A \cap K = \{Id\}$:
Soit $g = n.a = k \in N.A \cap K$, Alors g est de la forme :

$$g = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & \sqrt{1/y} \end{pmatrix} = \begin{pmatrix} u & -v \\ v & u \end{pmatrix}$$

Par identification, $v = 0 = x$, et $y = 1/y = 1$ Donc $g = Id$.

4. Si $n = n(x)$, $a = a(y)$ et $z \in (C)$, on a :
$n.z = \frac{1.z+x}{0.z+1} = z + x =$ translation par x réel $\Rightarrow$ Les orbites sont des bandes horizontales parallèles à Ox et un domaine fondamental est $i.\mathbb{R}$ l'axe vertical des imaginaires purs.
$a.z = \frac{\sqrt{y}.z+0}{0.z+1/\sqrt{y}} = z.y =$ homothétie par y réel $\Rightarrow$ Les orbites sont des demi-droites partant de z et passant par l'origine et un domaine fondamental est $\mathcal{C}^1 \cap \mathbb{H}$ le demi cercle unité supérieur.
5. Dans la question 1), on a montré qu'on pouvait effectivement trouver de tels a et n (par transitivité de l'action). Montrons donc leur unicité :
Supposons que $z = (na).i = (n'a').i$, alors :
$(na).i = (n'a').i \Leftrightarrow (n'a')^{-1}(na).i = i \Leftrightarrow (n'a')^{-1}(na) \in SL_2(\mathbb{R})_i = K$ par 2)
Mais on a aussi : $(n'a')^{-1}(na) \in N.A$, donc $(n'a')^{-1}(na) \in N.A \cap K = \{Id\}$ par 5)
$\Rightarrow (n'a')^{-1}(na) = Id \Leftrightarrow na = n'a' \Leftrightarrow a'^{-1}a = n^{-1}n' \Leftrightarrow n = n', a = a'$ car $N \cap A = \{Id\}$
6. Considérons $z := g.i$, c'est un nombre complexe obtenu à partir de i par action de g. Par 6), on peut écrire ce nouveau nombre complexe de façon unique comme : $z = na.i$, on a donc les égalités suivantes :
$g.i = z = na.i \Leftrightarrow na.i = g.i \Leftrightarrow g^{-1}na.i = i \Leftrightarrow g^{-1}na \in SL_2(\mathbb{R})_i = K$
$\Rightarrow \exists k' \in K$ tq, $g^{-1}na = k' \Leftrightarrow g = nak'^{-1} = nak$
7. Supposons que $g = n_1a_1k_1 = n_2a_2k_2$, alors :
$n_1a_1k_1 = n_2a_2k_2 \Leftrightarrow N.A \ni (n_2a_2)^{-1}n_1a_1 = k_2k_1^{-1} \in K$
Or $N.A \cap K = \{Id\} \Rightarrow (n_2a_2)^{-1}n_1a_1 = Id = k_2k_1^{-1}$
$\Rightarrow n_1a_1 = n_2a_2$, $k_1 = k_2$. Par le mÎme argument que précédemment, on a :
$k_1 = k_2$, $a_1 = a_2$, $n_1 = n_2$