**Licence MPCI**, 2e année
Algèbre Générale

**Devoir Surveillé**
12 Avril 2019

*Durée 2h*

# Exercices

**Exercice 1** (Groupe Affine)**.**

Pour tout $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, on note $f_{a,b}$ l'application suivante : $\begin{array}{rcl} f_{a,b} : \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & az+b \end{array}$

On considère l'ensemble $\mathcal{A} = \left\{ f_{a,b} \middle| \ a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$

(1) Montrer que $(\mathcal{A}, \circ)$ est un groupe (où $\circ$ désigne la composition des applications).

On montre que $\mathcal{A}$ est un sous-groupe de Bij($\mathbb{C}$). (Attention, l'ensemble des fonctions de $\mathbb{C}$ dans $\mathbb{C}$ n'est pas un groupe pour la composition $\circ$.)
— Soit $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$. Soit $z' \in \mathbb{C}$. L'équation $az+b = z'$ a une unique solution qui est $z = \frac{z'-b}{a}$. Donc $f_{a,b}$ est bijective. Donc $\mathcal{A} \subset$ Bij($\mathbb{C}$).
— L'identité $\mathrm{id}_{\mathbb{C}} = \mathrm{f}_{1,0} \in \mathcal{A}$
— Soient $f_{a,b}$ et $f_{c,d}$ dans $\mathcal{A}$ Alors

$$\forall z \in \mathbb{C}, f_{a,b} \circ f_{c,d}(z) = a(cz+d)+b = acz + (ad+b) = f_{ac,ad+b}$$

Donc $f_{a,b} \circ f_{c,d} \in \mathcal{A}$
— On a vu au premier point que $f_{a,b}^{-1} = f_{\frac{1}{a},-\frac{b}{a}} \in \mathcal{A}$.
Donc $\mathcal{A}$ est un sous-groupe de Bij($\mathbb{C}$).

(2) Déterminer l'ordre de $f_{i,1}$ dans $\mathcal{A}$.

Soit $z \in \mathbb{C}$

$$\begin{aligned} f_{i,1}(z) &= iz+1 \\ f_{i,1}^2(z) &= i(iz+1)+1 = -z+1+i \\ f_{i,1}^3(z) &= i(-z+1+i)+1 = -iz+i-1+1 = -iz+i \\ f_{i,1}^4(z) &= i(-iz+i)+1 = z-1+1 = z \end{aligned}$$

On voit que $f_{i,1}^4 = \mathrm{id}_{\mathbb{C}}$ et que $f_{i,1}^i \neq \mathrm{id}_{\mathbb{C}}$ pour $1 \leq i \leq 3$. Donc $f_{i,1}$ est d'ordre 4.

(3) Soient les applications suivantes :

$$\begin{array}{rcl} t : \mathcal{A} & \longrightarrow & \mathbb{C}^* \\ f & \longmapsto & f(1)-f(0) \end{array} , \qquad \begin{array}{rcl} h : \mathbb{C}^* & \longrightarrow & \mathcal{A} \\ a & \longmapsto & f_{a,0} \end{array}$$

Montrer $t$ et $h$ sont des morphismes.

Soit $f_{a,b}$ et $f_{c,d}$ dans $\mathcal{A}$

$$t(f_{a,b} \circ f_{c,d}) = t(f_{ac,ad+b}) = ac+ad+b-(ad+b) = ac = t(f_{a,b})t(f_{c,d})$$

Donc $t$ est un morphisme.
Soient $a, c \in \mathbb{C}^*$. Alors $h(ac) = f_{ac,0}$ Et d'autre part pour tout $z \in \mathbb{C}$, on a $f_{a,0} \circ f_{c,0}(z) = a(cz) = (ac)z = f_{ac,0}(z)$. Donc $h(ac) = h(a) \circ h(c)$.
Donc $h$ est un morphisme.

(4) On note $T = \ker(\mathrm{t})$ et $H = \mathrm{Im}(\mathrm{h})$. Montrer que $T$ est isomorphe à $\mathbb{C}$, et que $H$ est isomorphe à $\mathbb{C}^*$.

Il ne fallait pas utiliser le morphisme $t$ pour montrer l'isomorphisme.

$$T = \{f_{a,b} \in \mathcal{A}, f(1) - f(0) = 1\} = \{f_{a,b} \in \mathcal{A}, a = 1\} = \{f_{1,b}, b \in \mathbb{C}\}$$

On définit alors l'application $\phi : \mathbb{C} \to T$ par $\phi(b) = f_{1,b}$. On vérifie que c'est un morphisme $\phi(b + b') = f_{1,b+b'} = f_{1,b} \circ f_{1,b'}$. Il est surjectif d'après la carctérisation de $T$ au-dessus. Et il est injectif car $f_{1,b} = \mathrm{id}$ si et seulement si $b = 0$.
Pour la deuxième partie, $f_{a,0} = \mathrm{id}$ si et seulement si $a = 1$. Donc $\mathrm{Ker}(h) = \{1\}$ et donc $h$ est injectif. Donc $h$ est un isomorphisme sur son image $H$. Donc $H$ est isomorphe à $\mathbb{C}^*$.

(5) Montrer que pour tout élement de $f \in \mathcal{A}$ il existe un unique couple $(h, t) \in H \times T$ tel que $f = h \circ t$.

(Désolé pour la notation un peu malheureuse : le $h$ et le $t$ n'ont rien à voir avec les morphismes de la question 3.)
On voit que $f_{a,b} = f_{a,0} \circ f_{1,\frac{b}{a}}$ Et $f_{a,0} \in H$ et $f_{1,\frac{b}{a}} \in T$. On a donc l'existence du couple avec $h = f_{a,0}$ et $t = f_{1,\frac{b}{a}}$.
Supposons que $(h, t)$ et $(h', t')$ sont deux couples de $H \times T$ satisfaisant $h \circ t = h' \circ t'$. Alors $h'^{-1}h = t't^{-1}$. Or $h'^{-1}h \in H$ et $t't^{-1} \in T$ donc $h'^{-1}h = t't^{-1} \in H \cap T$.
Or on voit directement que $H \cap T = \{f_{1,0}\}$. Donc $h'^{-1}h = t't^{-1} = \mathrm{id}_{\mathbb{C}}$ et donc $h' = h$ et $t' = t$.

(6) (***) Est-ce que $\mathcal{A}$ est isomorphe au groupe produit $\mathbb{C}^* \times \mathbb{C}$ ? (Justifier votre réponse)

Le groupe $\mathcal{A}$ n'est pas commutatif. En effet, $f_{2,1} \circ f_{2,0} = f(4, 1)$ alors que $f_{2,0} \circ f_{2,1} = f_{4,2}$.
Par contre, le groupe $\mathbb{C}^* \times \mathbb{C}$ est commutatif. Les deux groupes ne peuvent donc pas être isomorphes !

**Exercice 2** (Matrices à coefficients entiers)**.**

On considère l'ensemble des matrices **à coefficients entiers** de déterminant 1 :

$$\mathrm{SL}(2, \mathbb{Z}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z}, \det(M) = 1 \right\}$$

On considère également les deux matrices.

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(1) Montrer que $\mathrm{SL}(2, \mathbb{Z})$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

— Soit $M \in \mathrm{SL}(2, \mathbb{Z})$. Alors $\det(M) \neq 0$ donc $M \in \mathrm{GL}(2, \mathbb{R})$. Donc $\mathrm{SL}(2, \mathbb{Z}) \subset \mathrm{GL}(2, \mathbb{R})$.
— La matrice $I_2$ est bien à coefficients entiers, et $\det(I_2) = 1$. Donc $I_2 \in \mathrm{SL}(2, \mathbb{Z})$.
— Soit $M, N \in \mathrm{SL}(2, \mathbb{Z})$. Et soit $L = MN$. Les coefficients de $L$ sont donnés par $L_{ij} = \sum_{k=1}^{2} M_{ik}N_{kj}$. Donc les coefficients de $L$ sont entiers et $\det(L) = \det(M)\det(N) = 1$. Donc $MN \in \mathrm{SL}(2, \mathbb{Z})$.
— Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. On a

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Comme $\det(M) = \pm 1$, on a $\frac{1}{\det(M)} = \det(M)$. Donc $M$ est à coefficients entiers. Et de plus, $\det(M^{-1}) = \frac{1}{\det(M)} = \det(M)$ donc $\det(M^{-1}) = \pm 1$. Donc $M^{-1} \in \mathrm{SL}(2, \mathbb{Z})$.

En conclusion, $\mathrm{SL}(2, \mathbb{Z})$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

(2) Soit $\mathcal{P} = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$. Justifier que $\mathcal{P} = \langle T \rangle$

On montre par (double) récurence que $\forall n \in \mathbb{Z}, T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. En effet pour $n = 0$ on a bien $T^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Et supposont que l'hypothèse est vrai au rang $n$ et au rang $-n$. Alors

$$T^{n+1} = T^n T = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

et

$$T^{-n-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n-1 \\ 0 & 1 \end{pmatrix}$$

D'autre part, on a $\langle T \rangle = \{T^n, n \in \mathbb{Z}\}$, donc $\mathcal{P} = \langle T \rangle$.

(3) Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Montrer que si $a = 0$ alors $RM \in \mathcal{P}$ ou $R^{-1}M \in \mathcal{P}$.

On a

$$RM = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ 0 & b \end{pmatrix}, \quad \text{et} \quad R^{-1}M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & -b \end{pmatrix}$$

On sait que $ad - bc = 1$ donc $-bc = 1$. Et comme $b$ et $c$ sont entiers, on en déduit $b = \pm 1$. Si $b = 1$, alors $c = -1$ et $RM \in \mathcal{P}$. Si $b = -1$ alors $c = 1$ et $R^{-1}M \in \mathcal{P}$.

(4) On suppose que $a \neq 0$. Montrer qu'il existe des entiers $q, r, d' \in \mathbb{Z}$ tels que

$$0 \leq r < |a|, \quad \text{et} \quad M = \begin{pmatrix} r & -a \\ d' & -c \end{pmatrix} R^{-1} T^q$$

(*indication : $q$ et $r$ sont le quotient et le reste d'une division euclidienne*)

On écrit la division euclidienne de $b$ par $a$ (qui est non-nul, ça tombe bien), sous la forme $b = qa + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < |a|$. Alors on calcule

$$MT^{-q}R = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b-qa \\ c & d-qb \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b-qa & -a \\ d-qb & -c \end{pmatrix}$$

Comme $b - qa = r$, il suffit de poser $d' = d - qb$ et on a l'égalité voulue.

(5) (***) Montrer que $\langle R, T \rangle = \mathrm{SL}(2, \mathbb{Z})$.

Soit $M \in \mathrm{SL}(2, \mathbb{Z})$.
On va construire une suite $M = M_0, M_1, \ldots, M_n$ telle que le dernier terme $M_n \in \mathcal{P}$ et $M_i = M_{i+1}A_i$ où $A_i \in \langle R, T \rangle$. Comme $\mathcal{P} \subset \langle R, T \rangle$, cela suffit à montrer que $M = M_n A_{n_1} \cdots A_1 \in \langle R, T \rangle$.

Supposons la suite construite jusqu'au rang $i$ avec $M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$

(a) Si $a_i = 0$ alors $M_i = RT^n$ ou $M = R^{-1}T^n$. Et on s'arrête.

(b) Si $a_i \neq 0$, alors d'après la question précédente, il existe $q$ et une matrice $M_{i+1}$ telle que $M_i = M_{i+1}R^{-1}T^q$. Donc on pose $A_i = T^{-q}R$.

D'après la construction, on $|a_{i+1}| < |a_i|$. Donc la suite des $|a_i|$ est à valeurs entières et strictement décroissante, donc elle est finie. Pour un certain rang $n$ on a $a_n = 0$. On a donc bien $M_n \in \langle R, T \rangle$. CQFD.

**Exercice 3** (Exposant d'un groupe)**.**

Soit $G$ un groupe fini d'ordre $n \geq 2$.

(1) On considère l'ensemble

$$E = \{k \in \mathbb{Z} \mid \forall g \in G, g^k = e\}$$

Montrer que $E$ est un sous-groupe de $\mathbb{Z}$ non trivial (c'est à dire $E \neq \{0\}$).

Montrons d'abord que $E$ est un sous-groupe de $\mathbb{Z}$.
— $\forall g \in G, g^0 = e$ donc $0 \in E$.
— Soit $k, l \in E$. Soit $g \in G$. On a $g^{k+l} = g^k g^l = ee = e$. Donc $k + l \in E$.
— On a $g^{-k} = (g^{-1})^k = e$. Donc $-k \in E$.
$E$ est bien un sous-groupe de $\mathbb{Z}$.
De plus, comme $G$ est un groupe fini d'ordre $n$, le théorème de Lagrange nous donne que $\forall g \in G$, $g^n = e$. Donc $n \in E$ et $E$ est un sous-groupe non-trivial.

(2) On appelle exposant de $G$, et on le note exp(G), le plus petit entier positif non-nul de $E$. Montrer que exp(G) divise $n$.

On a $E$ est un sous-groupe de $\mathbb{Z}$, et exp(G) est le plus petit entier non-nul de $E$, donc on a $E = \exp(\mathrm{G})\mathbb{Z}$. On sait que $n \in E$. Donc $n \in \exp(\mathrm{G})\mathbb{Z}$, ce qui nous donne que exp(G) divise $n$.

(3) Montrer que exp(G) est le PPCM de l'ensemble des ordres des élements de $G$. (On rappelle que le PPCM d'un ensemble de nombre $\{k_1, \ldots, k_n\}$, est le plus petit entier positif qui soit un multiple de chacun des $k_i$)

On décompose $E$ comme une intersection de sous-ensembles.

$$E = \bigcap_{g \in G} \{k \in \mathbb{Z}, g^k = e\}$$

Or $\{k \in \mathbb{Z}, g^k = e\} = o_g\mathbb{Z}$ où $o_g$ désigne l'ordre de $g$. On sait que $m\mathbb{Z} \cap m'\mathbb{Z} = ppcm(m, m')\mathbb{Z}$. On en déduit

$$E = \bigcap_{g \in G} o_g\mathbb{Z} = \mathrm{ppcm}(\mathrm{o}_1, \ldots, \mathrm{o}_\mathrm{n})\mathbb{Z}$$

Par unicité du générateur positif d'un sous-groupe de $\mathbb{Z}$, on en déduit donc que $\exp(\mathrm{G}) = \mathrm{ppcm}(\mathrm{o}_1, \ldots, \mathrm{o}_\mathrm{n})$.

(4) Soit $p$ un nombre premier et $a \geq 1$. Montrer que si $p^a$ divise exp(G) alors il existe un élement $g \in G$ d'ordre $p^a$.

On montre d'abord que l'un des $o_g$ est divisible par $p^a$.
On commence par la remarque suivante, si $o_1, \ldots, o_n$ sont des entiers, et on note $p_i$ l'exposant de $p$ dans la décomposition en facteur premier de $o_i$. On en déduit que l'exposant de $p$ dans $\mathrm{ppcm}(\mathrm{o}_1, \ldots, \mathrm{o}_\mathrm{n})$ est $p^{\max(a_i)}$.
Donc si $p^a$ divise exp(G), alors il existe un élément $g$ tel que $o_g$ est divisible par $p^a$. On note $o_g = p^a m$ avec $m \in \mathbb{N}$ et $m \wedge p = 1$.
Alors $g^m$ est un élément d'ordre $p^a$. En effet on a $(g^m)^{p^a} = e$ donc l'ordre de $g^m$ divise $p^a$, et si $k < p^a$ on a $(g^m)^k \neq e$ car $mk < o_g$.

(5) Soient $g, h \in G$ tels que $gh = hg$. Montrer que si $g$ et $h$ sont d'ordre respectifs $m$ et $n$, et que $m \wedge n = 1$, alors $gh$ est d'ordre $mn$.

Soit $k$ l'ordre de $gh$.
— on a $(gh)^{mn} = g^{mn}h^{mn}$ car $gh = hg$. on en déduit $(gh)^{mn} = (g^m)^n(h^n)^m = ee = e$. Donc $k$ divise $mn$.
— Réciproquement, on a $(gh)^k = e$. Donc $g^k = h^{-k} \in \langle g \rangle \cap \langle h \rangle$. Comme $\langle g \rangle \cap \langle h \rangle$ est un sous-groupe de $\langle g \rangle$, on peut utiliser le theorème de Lagrange et on a que $|\langle g \rangle \cap \langle h \rangle|$ divise $m$. De même $|\langle g \rangle \cap \langle h \rangle|$ divise $n$. Donc $|\langle g \rangle \cap \langle h \rangle|$ divise $m \wedge n = 1$.
On en déduit que $g^k = h^k = e$. Donc $m$ divise $k$ et $n$ divise $k$. Donc le ppcm de $m$ et $n$ divise $k$. Or le ppcm de $m$ et $n$ est $mn$. Donc $mn$ divise $k$.
On a donc bien $k = mn$.

(6) (***) En déduire que si $G$ est commutatif, il existe un élément dont l'ordre est égal à exp(G).

On décompose $\exp(\mathrm{G}) = \mathrm{p}_1^{\mathrm{a}_1} \cdots \mathrm{p}_\mathrm{k}^{\mathrm{a}_\mathrm{k}}$ avec les $p_i$ des nombres premiers distincts et $a_i \geq 1$.
Pour tout $1 \geq i \geq k$, il existe $g_i$ d'ordre $p_i^{a_i}$. On considère alors l'élement $g = g_1 \cdots g_k$. Cet élément est bien d'ordre $p_1^{a_1} \cdots p_k^{a_k}$ d'après la question précédente (après une petite induction sur $k$)