.

Examen B03 du 9 janvier 2007 (2h.).

Avertissement :

L'énoncé comporte trois pages, trois exercices et un problème (exercice long). Le barème est indicatif. Des résultats utilisables pour la résolution des questions sont donnés à la fin de cet avertissement. Les documents, téléphones et calculettes sont **interdits**.

On rappelle qu'au sein d'un exercice on peut répondre à une question en utilisant les résultats précédents même si ceux-ci n'ont pas été démontrés. On rappelle aussi que, sauf mention contraire explicite, toute réponse à une question doit être justifiée.

On pourra utiliser sans démonstration les résultats suivants.

R1 : Soit $(a, b, c) \in \mathbb{C}$. On a

$$(a = b) \Longleftrightarrow (a + c = b + c) \qquad \text{et, si } c \neq 0\,, \quad (a = b) \Longleftrightarrow (ac = bc)\,.$$

R2 : Soit E un ensemble et $\mathcal{F}(E)$ l'ensemble des applications de E dans E. La composée $g \circ f$ de deux fonctions f, g de $\mathcal{F}(E)$ est la fonction de $\mathcal{F}(E)$ définie par $g \circ f(x) = g(f(x))$. La composition $\circ$ est une loi de composition interne associative sur $\mathcal{F}(E)$.

Exercice 1. : (4 points) Questions de cours.

1- Soit E, F deux ensembles et $f : E \longrightarrow F$. Définir la phrase : "f est injective".

2- Quelle est la définition de $\mathbb{Z}$, l'ensemble des entiers relatifs ?

3- Ranger dans l'ordre croissant, sans justification, les entiers naturels n_1, n_2 et n_3, dont l'écriture en base 2 est donnée par $\overline{100111100}$, $\overline{1010110001}$ et $\overline{1010101111}$, respectivement.

Exercice 2. : (3 points) On note par $\oplus$ et $\otimes$, respectivement, l'addition et la multiplication de $\mathbb{Z}/16Z$. Pour $Y \in \mathbb{Z}/16Z$, $\ominus Y$ désigne l'opposé de Y. Résoudre séparément les deux équations d'inconnue X dans $\mathbb{Z}/16Z$ données par

$$\begin{aligned} (\overline{3} \otimes X) \oplus (\ominus \overline{2}) &= \overline{0} \qquad (E1)\,, \\ \overline{2} \otimes X &= \overline{1} \qquad (E2)\,. \end{aligned}$$

Exercice 3. : (4 points) On définit sur $\mathbb{R} \times \mathbb{R}$ la relation $\mathcal{R}$ par :

$$(x, y)\mathcal{R}(x', y') \text{ si } (x \leq x' \text{ et } y \leq y')$$

1- Montrer que $\mathcal{R}$ est une relation d'ordre sur $\mathbb{R} \times \mathbb{R}$. Est-elle une relation d'ordre total ?

2- Déterminer l'ensemble des minorants de $(1, 1)$.

3- Soit
$$C = \left\{(x, y) \in \mathbb{R} \times \mathbb{R}; x \geq 0, y \geq 0, x^2 + y^2 \leq 1\right\}$$

a- Montrer que $(0, 0)$ est un plus petit élément de C.

b- Montrer que $(1, 1)$ est un majorant de C. Est-il un plus grand élément de C ?

Problème (11 points)

Soit $\mathcal{D} = \{(a, b, c, d) \in \mathbb{C}^4; ad - bc \neq 0\}$ où $\mathbb{C}$ désigne l'ensemble des nombres complexes.

A) Pour chaque élément (a, b, c, d) de $\mathcal{D}$, on associe une fonction f définie,

pour $c \neq 0$, par
$$\begin{array}{rcccl} f & : & \mathbb{C} \setminus \{-d/c\} & \longrightarrow & \mathbb{C} \\ & & z & \longmapsto & \frac{az+b}{cz+d} \end{array},$$

et pour $c = 0$, par
$$\begin{array}{rcccl} f & : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & & z & \longmapsto & \frac{az+b}{d} \end{array}.$$

A)1. Montrer l'implication

$$\Big(c = 0 \text{ et } (a, b, c, d) \in \mathcal{D}\Big) \Longrightarrow (a \neq 0 \text{ et } d \neq 0)\,.$$

En particulier, la fonction f est bien définie dans le cas $c = 0$.

A)2. Pour $(a, b, c, d) \in \mathcal{D}$ avec $c \neq 0$, pour $(y, z) \in \mathbb{C}^2$, montrer l'équivalence

$$\Big(az + b = y(cz + d) \text{ et } z \neq -d/c\Big) \Longleftrightarrow \Big(az + b = y(cz + d)\Big)\,.$$

A)3. Pour $(a, b, c, d) \in \mathcal{D}$ avec $c \neq 0$, pour $(y, z) \in \mathbb{C}^2$, montrer l'équivalence

$$\Big(z(a - cy) = yd - b \text{ et } y \neq a/c\Big) \Longleftrightarrow \Big(z(a - cy) = yd - b\Big)\,.$$

A)4. Pour $(a, b, c, d) \in \mathcal{D}$ avec $c \neq 0$, montrer que l'image de f, la fonction associée à (a, b, c, d), est incluse dans $\mathbb{C} \setminus \{a/c\}$.

A)5. Pour $(a,b,c,d) \in \mathcal{D}$, montrer que f, la fonction associée à (a,b,c,d), est bijective et calculer sa bijection réciproque $f^{\langle -1 \rangle}$ (Indication : distinguer les cas $c = 0$ et $c \neq 0$).

B) Soit ∞ un symbol appelé “infini”. Il n'appartient pas à $\mathbb{C}$. Soit $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Pour chaque élément (a,b,c,d) de $\mathcal{D}$, on associe une fonction F définie,

pour $c \neq 0$, par

$$\begin{array}{rcccl} F & : & \overline{\mathbb{C}} & \longrightarrow & \overline{\mathbb{C}} \\ & & z & \mapsto & f(z) \quad \text{si } z \in \mathbb{C} \setminus \{-d/c\}\,, \\ & & & & \infty \quad \text{si } z = -d/c\,, \\ & & & & a/c \quad \text{si } z = \infty\,, \end{array}$$

et pour $c = 0$, par

$$\begin{array}{rcccl} F & : & \overline{\mathbb{C}} & \longrightarrow & \overline{\mathbb{C}} \\ & & z & \mapsto & f(z) \quad \text{si } z \in \mathbb{C}\,, \\ & & & & \infty \quad \text{si } z = \infty\,. \end{array}$$

Soit $\mathcal{G}$ l'ensemble des fonctions F associées à un élément (a,b,c,d) de $\mathcal{D}$.

B)1. Montrer que, pour tout $(a,b,c,d) \in \mathcal{D}$, la fonction F associée est bijective et déterminer sa bijection réciproque $F^{\langle -1 \rangle}$ (Indication : distinguer les cas $c = 0$ et $c \neq 0$).

B)2. Montrer que l'application I définie par

$$\begin{array}{rcccc} I & : & \overline{\mathbb{C}} & \longrightarrow & \overline{\mathbb{C}} \\ & & z & \mapsto & z \end{array}$$

appartient à $\mathcal{G}$.

B)3. Soit $(a,b,c,d) \in \mathcal{D}$ et F l'application associée. Soit $(a',b',c',d') \in \mathcal{D}$ et F' l'application associée. Montrer que la composée $F' \circ F$ appartient à $\mathcal{G}$.

B)4. Montrer que $(\mathcal{G}, \circ)$ est un groupe.

Corrigé de l'examen B03 du 9 janvier 2007.

La correction proposée est très détaillée afin que le lecteur puisse se faire une idée précise des arguments utilisés. Lors de la correction des copies, les points ont souvent été mis pour des réponses moins complètes.

Exercice 1 : Pour les questions 1 (2 pts) et 2 (1 pt) voir le cours. L'ordre croissant dans la question 3 (1 pt) est : $n_1 < n_3 < n_2$.

Exercice 2 : Comme $\overline{3} \otimes \overline{11} = \overline{33} = \overline{1}$, $\overline{3}$ est inversible dans $\mathbb{Z}/16Z$. Par un résultat du cours, l'équation $(E1)$ admet une solution unique donnée par $\overline{2} \otimes \overline{11}$.
Ceci donne 2 pts.
L'équation $(E2)$ n'a pas de solution. On peut voir cela en effectuant les produits $\overline{2} \otimes X$ lorsque X décrit $\{\overline{0}; \overline{1}; \cdots \overline{15}\}$ et en constatant qu'on ne tombe jamais sur $\overline{1}$. On peut aussi procéder par l'absurde. Supposons qu'on ait une solution $X = \overline{x}$ (avec $x \in \mathbb{Z}$) de $(E2)$. Donc $2x \equiv 1 \mod 16$. Il existe donc $k \in \mathbb{Z}$ tel que $1 = 2x + 16k$. On a une contradiction car 1 n'est pas pair.
Ceci donne 1 pt.

Exercice 3 : Question 1 : Pour tout $(x, y) \in \mathbb{R}\times\mathbb{R}$, on a $x \leq x$ et $y \leq y$ donc $(x, y)\mathcal{R}(x, y)$. Pour $(x, y) \in \mathbb{R}\times\mathbb{R}$ et $(x', y') \in \mathbb{R}\times\mathbb{R}$ tels que $(x, y)\mathcal{R}(x', y')$ et $(x', y')\mathcal{R}(x, y)$, on a $x \leq x'$, $x' \leq x$, $y \leq y'$ et $y' \leq y$, donc $x = x'$ et $y = y'$. Pour $(x, y) \in \mathbb{R} \times \mathbb{R}$, $(x', y') \in \mathbb{R} \times \mathbb{R}$ et $(x'', y'') \in \mathbb{R} \times \mathbb{R}$, tels que $(x, y)\mathcal{R}(x', y')$ et $(x', y')\mathcal{R}(x'', y'')$, on a $x \leq x'$, $x' \leq x''$, $y \leq y'$ et $y' \leq y''$, donc $x =\leq x''$ et $y \leq y''$ soit $(x, y)\mathcal{R}(x'', y'')$. $\mathcal{R}$ est donc une relation d'équivalence.
Ceci donne 1,5 pts.
$(1, 0)\mathcal{R}(-1, 2)$ est faux car $1 \leq -1$ l'est. $(-1, 2)\mathcal{R}(1, 0)$ est faux car $2 \leq 0$ l'est. Les éléments $(-1, 2)$ et $(1, 0)$ sont incomparables pour $\mathcal{R}$ donc $\mathcal{R}$ n'est pas une relation d'ordre total.
Ceci donne 0,5 pt.
Question 2 : L'ensemble des minorants de $(1, 1)$ est, par définition,

$$\{(x, y) \in \mathbb{R} \times \mathbb{R};\ (x, y)\mathcal{R}(1, 1)\} .$$

Or $((x, y)\mathcal{R}(1, 1))$ équivaut à ($x \leq 1$ et $y \leq 1$) donc, cet ensemble est

$$\{(x, y) \in \mathbb{R} \times \mathbb{R};\ x \leq 1 \text{ et } y \leq 1\} .$$

Ceci donne 1 pt.
Question 2 : Comme $0 \geq 0$ et $0^2 + 0^2 \leq 1$, $(0, 0) \in C$. Pour $(x, y) \in C$, on a $0 \leq x$ et $0 \leq y$ donc $(0, 0)\mathcal{R}(x, y)$. Donc $(0, 0)$ minore C et comme il appartient à C, c'est un plus petit élément de C.

Ceci donne 0,5 pt.
Pour tout $(x, y) \in C$, $x^2 + y^2 \leq 1$ donc $x^2 \leq 1$ et $y^2 \leq 1$. Comme $x \geq 0$ et $y \geq 0$, on en déduit que $x \leq 1$ et $y \leq 1$, c'est-à-dire que $(x, y)\mathcal{R}(1, 1)$. Donc $(1, 1)$ majore C.
Ceci donne 0,5 pt.
Comme $1^2 + 1^2 = 2 > 1$, $(1, 1) \notin C$. Il ne peut donc être un plus grand élément de C.
Ceci donne 0,5 pt.

Problème :

A)1. C'est le résultat de cette question qui permet de dire que la fonction f est bien définie lorsque $c = 0$ et pas le contraire.
On suppose $(a, b, 0, d) \in \mathcal{D}$. On a $bc = 0$ et $ad - bc \neq 0$ donc $ad \neq 0$ soit $a \neq 0$ et $d \neq 0$. On a montré l'implication.
Ceci donne 1 pt.
A)2. En supposant la proposition de gauche vraie, celle de droite l'est aussi par définition de l'opérateur logique "et".
Ceci donne 0,5 pt.
Pour la réciproque, on suppose $az+b = y(cz+d)$ vraie. Il suffit de montrer que $z \neq -d/c$. On procède par l'absurde. Supposons que $z = -d/c$ alors $-ad/c + b = y \cdot 0 = 0$ soit $-ad = -bc$ par R1. Ceci contredit l'hypothèse $(a, b, c, d) \in \mathcal{D}$. Donc $z \neq -d/c$.
Ceci donne 1 pt.
A)3. Comme précédemment, l'implication vers la droite vient de la définition de l'opérateur logique "et".
Ceci donne 0,5 pt.
Pour la réciproque, on suppose $z(a - cy) = yd - b$ vraie. Il suffit de montrer que $y \neq a/c$. On procède par l'absurde. Supposons que $y = a/c$ alors $ad/c - b = z \cdot 0 = 0$ soit $ad = bc$ par R1. Ceci contredit l'hypothèse $(a, b, c, d) \in \mathcal{D}$. Donc $y \neq a/c$.
Ceci donne 1 pt.
A)4. Il suffit de montrer que, si $y \in \mathbb{C}$ est dans l'image de f alors $y \neq a/c$. Soit $y \in \mathbb{C}$ tel qu'il existe $z \in \mathbb{C}\setminus\{-d/c\}$ tel que $f(z) = y$. On a donc, en utilisant R1, $az+b = y(cz+d)$. Donc $z(a - cy) = yd - b$. En utilisant l'implication vers la gauche de A)3., on en déduit que $y \neq a/c$.
Ceci donne 1 pt.
A)5. **Ici l'énoncé est incorrect.** Il fallait lire que "f est bijective sur son image". Une autre façon de le dire est de dire que :
f est bijective si $c = 0$ et, pour $c \neq 0$, l'application

$$f \;:\; \begin{array}{ccc} \mathbb{C} \setminus \{-d/c\} & \longrightarrow & \mathbb{C} \setminus \{a/c\} \\ z & \longmapsto & \frac{az+b}{cz+d} \end{array},$$

notée encore f, est bijective.
Pour répondre à cette question, on peut montrer que f est injective et surjective puis calculer sa bijection réciproque. Il est plus économique de montrer que l'equation $y = f(z)$ d'inconnue z a une unique solution pour tout y dans l'ensemble d'arrivée de f.

Prenons le cas où $c \neq 0$. Soit $y \in \mathbb{C}$ et on résoud l'équation $y = f(z)$ d'inconnue z. On a

$$\big(f(z) = y\big) \iff \big(f(z) = y \text{ et } z \neq -d/c\big)$$

et, par R1,

$$\big(f(z) = y\big) \iff \big(az + b = y(cz + d) \text{ et } z \neq -d/c\big)\,.$$

En utilisant A)2,

$$\big(f(z) = y\big) \iff \big(az + b = y(cz + d)\big)\,.$$

Encore par R1,

$$\big(az + b = y(cz + d)\big) \iff \big(z(a - cy) = yd - b\big)\,.$$

On utilise maintenant A)3 et on obtient

$$\big(f(z) = y\big) \iff \big(z(a - cy) = yd - b \text{ et } y \neq a/c\big)\,.$$

Or

$$\big(z(a - cy) = yd - b \text{ et } y \neq a/c\big) \iff \left(z = \frac{yd - b}{a - cy} \text{ et } y \neq a/c\right)$$

donc

$$\big(f(z) = y\big) \iff \left(z = \frac{yd - b}{a - cy} \text{ et } y \neq a/c\right)\,.$$

L'équation en question a une solution unique pour $y \neq a/c$ (et pas de solution si $y = a/c$) donc f est bijective sur $\mathbb{C} \setminus \{a/c\}$ et la bijection réciproque est donnée par

$$\begin{array}{rccc} f^{\langle -1 \rangle} & : & \mathbb{C} \setminus \{a/c\} & \longrightarrow & \mathbb{C} \setminus \{-d/c\} \\ & & y & \longmapsto & \frac{yd-b}{a-cy}\,. \end{array}$$

Passons au cas où $c = 0$. Soit $y \in \mathbb{C}$. On a, par R1,

$$\big(f(z) = y\big) \iff \big(az = yd - b\big)\,.$$

Or, on sait que $a \neq 0$ par A)1 donc, par R1,

$$\big(f(z) = y\big) \iff \big(z = (yd - b)/a\big)\,.$$

L'équation en question a une solution unique pour tout y donc f est bijective et la bijection réciproque est donnée par

$$\begin{array}{rcccc} f^{\langle -1 \rangle} & : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & & y & \longmapsto & \frac{yd-b}{a}\,. \end{array}$$

Ceci donne 2 pts.

B)1. Là encore on peut montrer que F est injective et surjective (attention cela n'a pas de sens de dire que F est injective sur $\mathbb{C}$). On préfère ici reprendre la démarche du A)5. Prenons le cas où $c \neq 0$. Soit $y \in \overline{\mathbb{C}}$ et on résoud l'équation $y = F(z)$ d'inconnue z. Si $y \in \mathbb{C} \setminus \{a/c\}$, il y a une solution unique par A)5 et du fait que ∞ ne peut être solution. Si $y = a/c$, $y = f(z)$ n'a pas de solution par A)5. Donc $y = F(z)$ a une unique solution à savoir ∞. Si $y=\infty$, la seule solution est $z=-d/c$. F est donc bijective et la bijection réciproque est donnée par

$$\begin{array}{rcccl} F^{\langle -1\rangle} & : & \overline{\mathbb{C}} & \longrightarrow & \overline{\mathbb{C}} \\ & & y & \mapsto & f^{\langle -1\rangle}(y) \quad \text{si } y\in\mathbb{C}\setminus\{a/c\}\,, \\ & & & & \infty \quad \text{si } y=a/c\,, \\ & & & & -d/c \quad \text{si } y=\infty\,. \end{array}$$

Passons au cas où $c=0$. Soit $y\in\overline{\mathbb{C}}$. Si $y\in\mathbb{C}$, $(y=F(z))$ équivaut à $(y=f(z))$ car $F(\infty)=\infty$ donc l'équation a une solution unique par A)5. Si $y=\infty$, l'équation ne peut avoir de solution dans $\mathbb{C}$ donc ∞ est la seule solution. F est donc bijective et la bijection réciproque est donnée par

$$\begin{array}{rcccl} F^{\langle -1\rangle} & : & \overline{\mathbb{C}} & \longrightarrow & \overline{\mathbb{C}} \\ & & y & \mapsto & f^{\langle -1\rangle}(y) \quad \text{si } y\in\mathbb{C}\,, \\ & & & & \infty \quad \text{si } y=\infty\,. \end{array}$$

Ceci donne 1 pt.
B)2. L'application I est associée à $(1,0,0,1)$, qui appartient bien à $\mathcal{D}$. Donc elle appartient à $\mathcal{G}$.
Ceci donne 0,5 pt.
B)3. La réponse à cette question est très longue et est notée sur 5 pts. Voir les détails plus bas.
B)4. La composition $\circ$ est une loi associative sur $\mathcal{F}(\overline{\mathbb{C}})$ (cf. R2) et l'application I est l'élément neutre. D'après B)3, la composition $\circ$ est une loi de composition interne pour $\mathcal{G}$. D'après B)2, l'élément neutre I appartient à $\mathcal{G}$. Par B)1, tout élément de $\mathcal{G}$ admet un symétrique pour cette loi. $(\mathcal{G},\circ)$ est donc un groupe.

Détails de la question B)3 : On montre, dans tous les cas possibles, qu'il existe une fonction $F'':\overline{\mathbb{C}}\longrightarrow\overline{\mathbb{C}}$ associé à $(a'',b'',c'',d'')\in\mathcal{D}$ (elle appartient donc à $\mathcal{G}$) telle que $F'\circ F=F''$.
Premier cas : $c=c'=0$.
En particulier, a,d,a',d' sont tous non nuls (par A)1). Soit $(a'',b'',c'',d'')=(aa',a'b+b'd,0,d')$. Comme $a''d''-b''c''=aa'd\neq 0$, il est bien dans $\mathcal{D}$. Pour $z\in\mathbb{C}$, on a

$$F'\circ F(z)=\frac{a'(az+b)/d+b'}{d'}=\frac{a'az+a'b+b'd}{d'}=F''(z)\,.$$

De plus, $F'\circ F(\infty)=F'(\infty)=\infty=F''(\infty)$. Donc $F'\circ F=F''$.
Deuxième cas : $c=0$, $c'\neq 0$.
On sait que a et d sont non nuls. Soit $(a'',b'',c'',d'')=(aa',a'b+b'd,ac',c'b+dd')$. On a

$$a''d''-b''c''=a\Big(a'dd'-b'c'd\Big)=ad(a'd'-b'c')\neq 0$$

donc $(a'',b'',c'',d'')\in\mathcal{D}$. On a $F'\circ F(\infty)=F'(\infty)=a'/c'=a''/c''=F''(\infty)$. Comme

$$F(-d''/c'')=\frac{1}{d}\Big(-\frac{c'b+dd'}{c'}+b\Big)=\frac{1}{d}\cdot\frac{-dd'}{c'}=\frac{-d'}{c'}\,,$$

$F'\circ F(-d''/c'') = F'(-d'/c') = \infty = F''(-d''/c'')$. Pour $z \in \mathbb{C} \setminus \{-d''/c''\}$, $F(z) \neq F(-d''/c'')$ car F est injective donc $F(z) \neq -d'/c'$ et

$$F'\circ F(z) = \frac{a'(az+b)/d+b'}{c'(az+b)/d+d'} = \frac{a'az+a'b+b'd}{c'az+c'b+d'd} = F''(z)\,.$$

Donc $F'\circ F = F''$.

Troisième cas : $c \neq 0$, $c' = 0$.

On sait que a' et d' sont non nuls. Soit $(a'',b'',c'',d'') = (aa'+b'c, a'b+b'd, d'c, dd')$. On a

$$a''d''-b''c'' = d'\Big(a'ad+b'cd-a'bc-b'cd\Big) = a'd'(ad-bc) \neq 0$$

donc $(a'',b'',c'',d'') \in \mathcal{D}$. On a

$$F'\circ F(\infty) = F'(a/c) = \frac{a'a/c+b'}{d'} = \frac{a'a+b'c}{cd'} = \frac{a''}{c''} = F''(\infty)\,.$$

On a $F'\circ F(-d''/c'') = F'\circ F(-d/c) = F'(\infty) = \infty = F''(-d''/c'')$. Pour $z \in \mathbb{C}\setminus\{-d''/c''\}$, $z \neq -d/c$ donc

$$F'\circ F(z) = \frac{a'\frac{az+b}{cz+d}+b'}{d'} = \frac{a'(az+b)+b'(cz+d)}{d'(cz+d)} = \frac{(aa'+b'c)z+a'b+b'd}{d'cz+d'd} = F''(z)\,.$$

Donc $F'\circ F = F''$.

Quatrième cas : $c \neq 0$, $c' \neq 0$.

Soit $(a'',b'',c'',d'') = (aa'+b'c, a'b+b'd, c'a+d'c, c'b+dd')$. On a

$$\begin{aligned} a''d''-b''c'' &= a'c'ab+a'd'ad+b'c'bc+b'd'cd-a'c'ab-a'd'bc-b'c'ad-b'd'cd \\ &= b'c'\Big(bc-ad\Big)+a'd'\Big(ad-bc\Big) = \Big(ad-bc\Big)\Big(a'd'-b'c'\Big) \neq 0\,. \end{aligned}$$

On a $F'\circ F(-d/c) = F'(\infty) = a'/c'$. On remarque que $c'' = 0$ si et seulement si $a/c = -d'/c'$.

Premier sous-cas : $c'' = 0$. On a $a/c = -d'/c'$ et

$$F''(-d/c) = \frac{-d(aa'+b'c)+a'bc+b'cd}{c(c'b+d'd)} = \frac{a'(bc-ad)}{c'(bc-ad)} = \frac{a'}{c'} = F'\circ F(-d/c)\,.$$

On a $F'\circ F(\infty) = F'(a/c) = F'(-d'/c') = \infty = F''(\infty)$. Pour $z \in \mathbb{C}\setminus\{-d/c\}$, $F(z) \neq F(\infty)$ (F est injective) donc $F(z) \neq -d'/c'$ et

$$F'\circ F(z) = \frac{a'(az+b)+b'(cz+d)}{c'(az+b)+d'(cz+d)} = \frac{(aa'+b'c)z+a'b+b'd}{(c'a+d'c)z+c'b+d'd} = F''(z)\,.$$

Second sous-cas : $c'' \neq 0$. On a donc $a/c \neq -d'/c'$. En utilisant B)1, on voit que, pour $z \in \mathbb{C}$, $F(z) = -d'/c'$ équivaut à $z = -d''/c''$. De plus, si $-d/c = -d''/c''$ alors $dc'a = cc'b$ et $ad = bc$, contradiction. Donc $-d/c \neq -d''/c''$. On a donc

$$F''(-d/c) = \frac{-d(aa'+b'c)+a'bc+b'cd}{-d(c'a+d'c)+c'bc+d'cd} = \frac{a'(bc-ad)}{c'(bc-ad)} = \frac{a'}{c'} = F'\circ F(-d/c)\,.$$

Comme $a/c \neq -d'/c'$, $F(\infty) \neq -d'/c'$ donc

$$F' \circ F(\infty) = F'(a/c) = \frac{a'a/c + b'}{c'a/c + d'} = \frac{aa' + b'c}{c'a + d'c} = \frac{a''}{c''} = F''(z) \; .$$

On a $F' \circ F(-d''/c'') = F'(-d'/c') = \infty = F''(-d''/c'')$. Pour $z \in \mathbb{C} \setminus \{-d/c; -d''/c''\}$, $F(z) \neq F(-d''/c'')$ donc $F(z) \neq -d'/c'$ et

$$F' \circ F(z) = \frac{a'(az + b) + b'(cz + d)}{c'(az + b) + d'(cz + d)} = \frac{(aa' + b'c)z + a'b + b'd}{(c'a + d'c)z + c'b + d'd} = F''(z) \; .$$

On a donc $F' \circ F = F''$.

.

Examen B03 du 13 juin 2007 (2h.).

Avertissement :

L'énoncé comporte trois pages, trois exercices et un problème (exercice long). Le barème est indicatif. Les documents, téléphones et calculettes sont **interdits**.

On rappelle qu'au sein d'un exercice on peut répondre à une question en utilisant les résultats précédents même si ceux-ci n'ont pas été démontrés. On rappelle aussi que, sauf mention contraire explicite, toute réponse à une question doit être justifiée.

Exercice 1. : (4 points) Questions de cours.

1- Soit E, F deux ensembles et $f : E \longrightarrow F$. Définir la phrase : "f est surjective.".

2- Quelle est la définition de $\mathbb{Z}$, l'ensemble des entiers relatifs ?

3- Soit $(E, \leq)$ un ensemble muni d'une relation d'ordre $\leq$. Soit F une partie de E et a un élément de E. Définir la phrase : "a est un minorant de F.".

4- Comment qualifie-t-on une loi de composition interne $*$ sur un ensemble E qui vérifie : $\forall (x, y, z) \in E^3$, $x * (y * z) = (x * y) * z$?

Exercice 2. : (3 points) Soit $n \in \mathbb{N}$ tel que $n \geq 2$. On note par $\oplus$ et $\otimes$, respectivement, l'addition et la multiplication de $\mathbb{Z}/n\mathbb{Z}$. Pour $Y \in \mathbb{Z}/n\mathbb{Z}$, $\ominus Y$ désigne l'opposé de Y.

1- Résoudre dans $\mathbb{Z}/8\mathbb{Z}$ l'équation d'inconnue X donnée par

$$(\overline{5} \otimes X) \oplus (\ominus \overline{3}) \ = \ \overline{0}\,.$$

2- Résoudre dans $\mathbb{Z}/150\mathbb{Z}$ l'équation d'inconnue X donnée par

$$\overline{3} \otimes X \ = \ \overline{1}\,.$$

(Ind. : on pourra remarquer que 150 est un multiple de 3).

Exercice 3. : (3 points) Soit $f : \mathbb{C} \longrightarrow \mathbb{C}$ définie par $f(z) = \frac{z}{1+|z|}$.

1) Soit $z, z' \in \mathbb{C}$ tel que $f(z) = f(z')$. Montrer que $|z| = |z'|$.

2) En déduire que f est injective.

3) Soit $D = \{z \in \mathbb{C}; |z| < 1\}$. Montrer que $f(\mathbb{C})$, l'image de f, est incluse dans D.

4) f est-elle une bijection de $\mathbb{C}$ sur D ?

Problème (12 points)

L'ensemble $\mathbb{R}$ des nombres réels muni de l'addition est un groupe commutatif. Dans ce problème, on se propose de décrire les sous-groupes de $(\mathbb{R}, +)$. On rappelle les choses suivantes (que l'on pourra utiliser sans démonstration) :

- L'ensemble $\mathbb{R}$ muni de sa relation d'ordre usuelle $\leq$ vérifie la propriété dite de la borne supérieure suivante : Toute partie de $\mathbb{R}$ non vide majorée (resp. minorée) admet une borne supérieure (resp. inférieure).

- Un sous-groupe G de $(\mathbb{R}, +)$ est une partie non vide G de $\mathbb{R}$ telle que G muni de l'addition soit un groupe. Pour une telle partie G, l'addition de deux éléments de G est encore dans G et l'opposé d'un élément de G est un élément de G. Plus précisément, une partie non vide G de $\mathbb{R}$ est un sous-groupe de $(\mathbb{R}, +)$ si et seulement si l'une des propriétés équivalentes suivantes est vraie :

$$\mathcal{Q}_1 = \Big(\big(\forall (x, y) \in G\,, x + y \in G\big) \quad \text{et} \quad \big(\forall x \in G\,, -x \in G\big) \Big),$$

$$\mathcal{Q}_2 = \big(\forall (x, y) \in G^2\,, x - y \in G\big).$$

On note $\mathbb{R}^{+*} = \mathbb{R} \cup]0; +\infty[$ et, pour tout $r \in \mathbb{R}$, $r\mathbb{Z} = \{nr; n \in \mathbb{Z}\}$.

A) Soit G un sous-groupe de $(\mathbb{R}, +)$.

A)1- Soit $r \in G$. Montrer que, pour tout $n \in \mathbb{N}$, $nr \in G$.

A)2- Soit $r \in G$. Montrer que, pour tout $n \in \mathbb{Z}$, $nr \in G$.

A)3- En déduire l'implication : $(r \in G \Longrightarrow r\mathbb{Z} \subset G)$.

A)4- Montrer que $r\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.

A)5- Montrer que, ou bien $G = \{0\}$ ou bien il existe $b \in G \cap \mathbb{R}^{+*}$.

B) Soit $\mathcal{E}$ l'ensemble des sous-groupes de $(\mathbb{R}, +)$. Muni de l'inclusion, c'est un ensemble ordonné. Soit $r \in \mathbb{R}$. Montrer que l'ensemble $\mathcal{E}_r$ des sous-groupes de $(\mathbb{R}, +)$ qui contiennent r admet un plus petit élément, à savoir $r\mathbb{Z}$.

C) Soit G un sous-groupe de $(\mathbb{R},+)$ tel que $G \neq \{0\}$. D'après A)5-, l'ensemble $G \cap \mathbb{R}^{+*}$ est non vide. Comme il est minoré, il admet une borne inférieure réelle notée a. On suppose que $a > 0$.

C)1- Soit $y \in G$. Montrer que $y \in a\mathbb{Z}$. (Ind. : utiliser la division euclidienne de y par a).

C)2- En déduire que $G \subset a\mathbb{Z}$.

C)3- Montrer par l'absurde que $a \in G$. (Ind. : supposer que $a \notin G$, montrer que $2a$ minore $G \cap \mathbb{R}^{+*}$ et trouver une contradiction).

C)4- En déduire que $G = a\mathbb{Z}$.

D) Soit G un sous-groupe de $(\mathbb{R},+)$ tel que $G \neq \{0\}$ et $a = \inf G \cap \mathbb{R}^{+*}$. On suppose maintenant que $a = 0$. Pour tout $y \in \mathbb{R}$, on va montrer la proposition

$$\mathcal{P}(y) \;=\; \Big(\forall \epsilon > 0\,,\; G \cap]y-\epsilon; y+\epsilon[\neq \emptyset\Big)\,.$$

D)1- Soit $y \in \mathbb{R}$ et $\epsilon > 0$. Pourquoi existe-t-il un réel $b \in G$ tel que $0 < b < \epsilon$? (Ind. : exploiter le fait que $a = 0$).

D)2- Montrer qu'un multiple entier de b appartient à $]y-\epsilon; y+\epsilon[$.

D)3- En déduire que $\mathcal{P}(y)$ est vraie.

Corrigé de l'examen B03 du 13 juin 2007.

La correction proposée est très détaillée afin que le lecteur puisse se faire une idée précise des arguments utilisés. Lors de la correction des copies, les points ont souvent été mis pour des réponses moins complètes.

Exercice 1 : 4 points.

1- (1 pt). f est surjective si, pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$. On peut aussi dire : f est surjective si la proposition

$$\Big(\forall y \in F \ , \ \exists x \in E \ ; \ f(x) = y\Big)$$

est vraie.

2- (1 pt). Soit $\mathcal{R}$ la relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$ définie par

$$\forall\Big((a_1, a_2), (b_1, b_2)\Big) \in (\mathbb{N} \times \mathbb{N})^2 \ , \ (a_1, a_2)\mathcal{R}(b_1, b_2) \text{ si } a_1 + b_2 = a_2 + b_1 \ .$$

L'ensemble $\mathbb{Z}$ est le quotient $(\mathbb{N} \times \mathbb{N})/\mathcal{R}$ de l'ensemble $\mathbb{N} \times \mathbb{N}$ par la relation d'équivalence $\mathcal{R}$.

3- (1 pt). a est un minorant de F si, pour tout $y \in F$, on a $a \leq y$. On peut aussi dire : a est un minorant de F si la proposition

$$\Big(\forall y \in F \ , \ a \leq y\Big)$$

est vraie.

4- (1 pt). Cette loi est associative.

Exercice 2 : 3 points.

1- (2 pts). Comme $\overline{5} \otimes \overline{5} = \overline{25} = \overline{24} \oplus \overline{1} = \overline{1}$, car 24 est un multiple de 8, $\overline{5}$ admet un inverse dans $\mathbb{Z}/8\mathbb{Z}$, à savoir lui-même. Donc, par le cours, l'équation admet une unique solution donnée par

$$X \ = \ \ominus(\ominus\overline{3}) \otimes \overline{5} \ = \ \overline{15} \ = \ \ominus\overline{1} \ = \ \overline{7} \, .$$

2- (1 pt). Comme 3 divise 150, $\overline{3}$ n'est pas inversible dans $\mathbb{Z}/150\mathbb{Z}$. En effet, si $\overline{x} \otimes \overline{3} = \overline{1}$ alors on aurait $\overline{50} \otimes \overline{x} \otimes \overline{3} = \overline{50}$ soit $\overline{50} = \overline{x} \otimes \overline{150} = \overline{0}$, contradiction. Donc l'indication visait à faire remarquer que l'on ne peut pas appliquer le résultat du cours comme au 1-. On a fait remarquer dans le cours que l'équation peut avoir plusieurs solutions

ou pas du tout. Comme il est un peu pénible d'essayer tous les éléments de $\mathbb{Z}/150\mathbb{Z}$, on va reformuler la question autrement. Dire que $\overline{3} \otimes X = \overline{1}$ signifie que, pour tout $x \in X$, $\overline{1} = \overline{3} \otimes \overline{x} = \overline{3x}$. Donc, pour tout $x \in X$, il existe $k \in \mathbb{Z}$ tel que $1 = 3x + 150 \cdot k$. On voit que ce n'est pas possible car le terme de droite est un multiple de 3 et 1 n'en est pas.
On peut répondre à la question comme suit.
[Supposons que X soit une solution de l'équation. Soit $x \in X$. On a donc $X = \overline{x}$ et $\overline{1} = \overline{3} \otimes \overline{x} = \overline{3x}$. Il existe donc un $k \in \mathbb{Z}$ tel que $1 = 3x + 150 \cdot k$. Le terme de droite est un multiple de 3 car $150 = 3 \times 50$ et 1 n'en est pas. On a donc une contradiction. L'équation n'a donc pas de solution.]
On peut reformuler l'argument après la phrase " ....$k \in \mathbb{Z}$ tel que $1 = 3x + 150 \cdot k$.". Comme ces deux entiers sont égaux, ils ont la même classe dans $\mathbb{Z}/3\mathbb{Z}$: $\overline{1} = \overline{0}$, car $3x + 150 \cdot k$ est un multiple de trois. On a donc une contradiction.
Il est à noter que le texte entre crochets [,] suffit sur la copie.

Exercice 3 : 3,5 points.

1) (0,5 pt). Comme $f(z) = f(z')$, $|f(z)| = |f(z')|$, donc

$$\frac{|z|}{1+|z|} = \frac{|z'|}{1+|z'|}$$

ce qui équivaut à $|z| + |z| \cdot |z'| = |z'| + |z| \cdot |z'|$. Ceci implique $|z| = |z'|$.
On peut aussi signaler que la fonction $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ définie par $g(r) = r/(1+r)$ est dérivable de dérivée

$$g'(r) = \frac{1+r-r}{(1+r)^2} = \frac{1}{(1+r)^2} > 0 .$$

La fonction est donc strictement croissante donc injective. Si $f(z) = f(z')$, $|f(z)| = |f(z')|$ et $g(|z|) = g(|z'|)$, donc par injectivité de g, $|z| = |z'|$.

2) (1 pt). Soit z, z' dans $\mathbb{C}$ tels que $f(z) = f(z')$. Par 1), $|z| = |z'|$ donc

$$\frac{z}{1+|z|} = f(z) = f(z') = \frac{z'}{1+|z|}$$

et, par simplification par $1/(1+|z|)$, $z = z'$. f est donc bien injective.

3) (1 pt). Pour tout $z \in \mathbb{C}$, $|z| < 1 + |z|$, donc $|f(z)| < 1$ et donc $f(z) \in D$. On a montré que $f(\mathbb{C}) \subset D$.

4) (1 pt). Soit $z_0 \in D$. Il existe $r_0 \in [0, 1[$ et $\theta \in \mathbb{R}$ tel que $z_0 = r_0 e^{i\theta}$ (si $z_0 \neq 0$, c'est connu et pour $z_0 = 0$, on écrit $0 = 0e^{i0}$). On résoud l'équation d'inconnue $t \geq 0$ donnée par $r_0 = t/(1+t)$. On a, comme $r_0 \neq 1$,

$$r_0 = t/(1+t) \iff (1+t)r_0 = t \iff r_0 = t(1-r_0) \iff t = r_0/(1-r_0) .$$

Comme $r_0 < 1$, $r_0/(1-r_0) > 0$ et c'est l'unique solution de notre équation. Soit $r = r_0/(1-r_0)$ et $z = re^{i\theta}$. On a

$$f(z) \;=\; \frac{r}{1+r}\cdot e^{i\theta} \;=\; r_0 e^{i\theta} \;=\; z_0\,.$$

On a montré que f est surjective sur D. Comme elle est injective par 3), elle est bijective de $\mathbb{C}$ sur D.

Problème : 12 points.

A)1- (1,5 pts). Pour $n \in \mathbb{N}$ soit $\mathcal{P}(n)$ la propriété : $nr \in G$. Comme $r \in G$, $\mathcal{P}(1)$ est vraie. Supposons $\mathcal{P}(n)$ vraie pour un $n \geq 1$. Comme $r \in G$ et $nr \in G$ par hypothèse de récurrence, on a $nr + r \in G$ puisque G est un groupe (cf. la première proposition dans $\mathcal{Q}_1$). Donc $(n+1)r \in G$ et la propriété $\mathcal{P}(n)$ est héréditaire. Par le théorème de récurrence, elle est vraie pour tout $n \geq 1$. Et pour $n = 0$? Comme $r \in G$, $0 = r - r \in G$ puisque G est un sous-groupe de $(\mathbb{R}, +)$ (cf. $\mathcal{Q}_2$).
Autre argument : Comme $r \in G$, $-r \in G$ car G est un sous-groupe de $(\mathbb{R}, +)$ (cf. la seconde proposition dans $\mathcal{Q}_1$). Donc $0 = r + (-r) \in G$ puisque G est un sous-groupe de $(\mathbb{R}, +)$ (cf. la première proposition dans $\mathcal{Q}_1$).

A)2- (0,5 pt). Soit $n \in \mathbb{Z}$. Si $n \in \mathbb{N}$, $nr \in G$ par A)1-. Sinon $-n \in \mathbb{N}$ donc $-nr \in G$ par A)1-. D'où $nr = -(-nr) \in G$ par $\mathcal{Q}_1$.

A)3- (1 pt). Pour montrer l'implication, il suffit de prendre un $r \in G$ et de montrer que $r\mathbb{Z} \subset G$. Soit $r \in G$, il suffit de montrer que tout élément de $r\mathbb{Z}$ appartient à G. Mais c'est précisément ce que dit A)2-.

A)4- (1 pt). $r\mathbb{Z}$ contient 0 (et r) donc est non vide. Soit $n, n' \in \mathbb{Z}$. On a $nr - n'r = (n-n')r \in r\mathbb{Z}$ car $(n-n') \in \mathbb{Z}$. Par $\mathcal{Q}_2$, $r\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$.
Remarque : on peut aussi utiliser $\mathcal{Q}_1$.

A)5- (1 pt). Il suffit de montrer que, si $G \neq \{0\}$ alors $G \cap \mathbb{R}^{+*}$ n'est pas vide. Supposons $G \neq \{0\}$. Il existe donc un élément non nul b_1 dans G. Si $b_1 > 0$, il appartient à $G \cap \mathbb{R}^{+*}$. Si $b_1 < 0$, $b = -b_1 \in G$ par $\mathcal{Q}_1$ et $b > 0$ donc $b \in G \cap \mathbb{R}^{+*}$.

B) (1 pt). D'après A)4-, $r\mathbb{Z}$ appartient bien à $\mathcal{E}_r$. Il suffit de montrer qu'il minore $\mathcal{E}_r$. Soit $G \in \mathcal{E}_r$. Comme G contient r, $r\mathbb{Z} \subset G$ d'après A)3-. Ceci étant vrai pour tout $G \in \mathcal{E}_r$, $r\mathbb{Z}$ minore $\mathcal{E}_r$.

C)1- (2 pts). Le résultat demandé est vrai pour $y = 0$. Il suffit de le montrer pour $y > 0$. En effet, si ce dernier est vrai et si $y < 0$ alors $-y \in G$ et $-y > 0$ donc $-y$ s'écrit ka avec $k \in \mathbb{Z}$ et $y = -(-y) = -(ka) = (-k)a$ appartient bien à $a\mathbb{Z}$.
On suppose $y > 0$. Soit $y = aq + r$ avec $q \in \mathbb{N}$ et $r \in [0; a[$, la division euclidienne de y par a. Si $q = 0$, alors $r = y$ et $r \in G \cap \mathbb{R}^{+*}$. Contradiction avec $r < a = \inf G \cap \mathbb{R}^{+*}$.

Donc $q > 0$. On suppose $r > 0$. Comme $a + r/q > a$, $a + r/q$ ne minore pas $G \cap \mathbb{R}^{+*}$ (par définition de a). Il existe donc $g \in G \cap \mathbb{R}^{+*}$ tel que $a \leq g < a + r/q$. En particulier, $qg < qa + r = y$ soit $y - qg > 0$. Comme $y, g \in G$, $y - qg \in G \cap \mathbb{R}^{+*}$ (cf. A)2- et $\mathcal{Q}_2$). D'autre part, $y - qg = r - q(g - a) \leq r < a$, car $g \geq a$. On a donc encore une contradiction avec $a = \inf G \cap \mathbb{R}^{+*}$. Donc $r = 0$ et $y \in a\mathbb{Z}$.

C)2- (0,5 pt). Comme le résultat de C)1- est valable pour tout $y \in G$, G est inclu dans $a\mathbb{Z}$.

C)3- (1 pt). On suppose $a \notin G$. Comme $G \subset a\mathbb{Z}$ par C)2-, $G \cap \mathbb{R}^{+*} \subset a\mathbb{Z} \cap \mathbb{R}^{+*} = a\mathbb{N}^*$. Comme $a \notin G$, $G \cap \mathbb{R}^{+*} \subset [2a; +\infty[$. Donc $2a$ minore $G \cap \mathbb{R}^{+*}$. Par définition de a, $2a \leq a$ soit $a \leq 0$. Contradiction avec l'hypothèse $a > 0$. Conclusion : $a \in G$.

C)4- (1 pt). Comme $a \in G$ par C)3-, on a $a\mathbb{Z} \subset G$ par B) (ou bien A)3-). Par C)2-, $G \subset a\mathbb{Z}$ donc $G = a\mathbb{Z}$.

D)1- (0,5 pt). Soit $\epsilon > 0$. Comme $a = \inf G \cap \mathbb{R}^{+*} = 0$, ϵ ne minore pas $G \cap \mathbb{R}^{+*}$ donc il existe $b \in G \cap \mathbb{R}^{+*}$ tel que $b < \epsilon$.

D)2- (1 pt). Soit $y = bq + r$ avec $q \in \mathbb{Z}$ et $r \in [0; b[$ la division euclidienne de y par b. On a $|y - bq| = r < b < \epsilon$ donc $bq \in]y - \epsilon; y + \epsilon[$.

D)3- (1 pt). Par A)2-, $bq \in G$. Par D)2-, $]y - \epsilon; y + \epsilon[$ contient donc un élément de G soit $G \cap]y - \epsilon; y + \epsilon[\neq \emptyset$. Ceci étant vrai pour tout $\epsilon > 0$, on a démontré la proposition $\mathcal{P}(y)$.