Arithmétique

Examen blanc – Décembre 2014

Durée : 1h30

Chaque réponse devra être justifiée et rédigée de manière rigoureuse. Si un résultat du cours est utilisé, il devra être clairement indiqué.

Exercice 1. (8 pts)

i) Soit $f : E \to F$ une fonction et $A, B \subset E$. Prouver que $f(A \cup B) = f(A) \cup f(B)$. Peut-on affirmer que $f(A \cap B) = f(A) \cap f(B)$? Justifier une réponse négative avec un contre-exemple.

ii) Soit la fonction

$$g : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & x^2 + y^2 \end{array}$$

(a) g est-elle injective ? surjective ? bijective ?.

(b) Calculer $g(\{(0, 0)\})$, $g^{-1}(\{0\})$, $g^{-1}(\{1\})$, $g\left([-1, 1] \times \left\{\sqrt{2}\right\}\right)$ et $g^{-1}\left(\left[-\sqrt{3}, -1\right[\right)$.

(c) Soit $\mathcal{R}$ une relation binaire sur $\mathbb{R}^2$ définie par :

$$(a, b)\mathcal{R}(c, d) \Longleftrightarrow g(a, b) = g(c, d), \quad \forall (a, b), (c, d) \in \mathbb{R}^2.$$

$\mathcal{R}$ est-elle une relation d'équivalence ? et d'ordre ?. Si $\mathcal{R}$ est une relation d'équivalence, décrire $\overline{(0,0)}^{\mathcal{R}}$ et $\overline{(0,1)}^{\mathcal{R}}$, les classes d'équivalence de $(0, 0)$ et $(0, 1)$ respectivement.

Exercice 2. (6 pts) Soit $G = \mathbb{R}^{*+} \times \mathbb{R}$. Étant données (a, b) et (c, d) dans G, on pose

$$(a, b) * (c, d) = (ac, b + d\sqrt{a})$$

Montrer que $(G, *)$ est un groupe. Est-il abélien ?

Exercice 3. (6+2 pts) Année 2214, le détective Jerry Cornelius arrive à bord de Herschel–IV, une station spatiale en orbite géostationnaire sur Uranus, sur laquelle la durée du jour est de 18 heures. Notre détective vient pour éclaircir l'assassinat d'un technicien qui s'est produit au bord de la station. À coté du corps, se trouve un robot policier avec les deux principaux suspects du crime.

i) Le robot policier, qui a été initialisé avec la station il y a longtemps, informe le détective que le technicien est mort à 35^{403} heures sur la station. De quelle heure (locale) parle-t-il ? (*Indication : utiliser des congruences.*)

ii) Cornelius interroge les suspects : le premier suspect explique au détective qu'il a fait 95 heures de travail continu entre la Terre et la station, tandis que le second suspect a fait 102 heures. Sachant que le voyage entre la Terre et Herschel–IV se fait par téléportation instantanée et qu'ils ne sont restés que des journées entières autant sur la Terre comme sur la station, déterminer lequel des suspects ne dit pas la vérité. (*Indication : poser le problème en équations dioffantiennes et étudier l'existence des solutions.*)

iii) **(Bilan extra : 2 pts)** En considérant uniquement le suspect qui ne ment pas, déterminez combien de jours est-il resté sur la station. (*Indication : résoudre dans $\mathbb{N} \times \mathbb{N}$ l'équation dioffantienne qui admet des solutions posée dans (ii).*)

Arithmétique

Solutions détaillées

Solution 1.

i) La preuve par double inclusion de $f(A \cup B) = f(A) \cup f(B)$ est bien détaillée dans le cours. En ce qui concerne à la seconde égalité on a prouvé dans le cours que $f(A \cap B) \subset f(A) \cap f(B)$, mais $f(A \cap B) \not\supset f(A) \cap f(B)$ en général.
On peut donner comme contre-exemple : soient $E = F = \mathbb{R}$ et $f(x) = x^2$ pour tout $x \in \mathbb{R}$. En prenant $A = [-1, 0]$ et $B = [0, 1]$, on a $A \cap B = \{0\}$ donc $f(A \cap B) = f(\{0\}) = \{f(x) \mid x \in \{0\}\} = \{f(0)\} = \{0\}$. Par contre, on a $f(A) = [0, 1] = f(B)$. Alors $f(A) \cap f(B) = [0, 1]$. Cet exemple montre clairement que $f(A \cap B) = \{0\} \subset [0, 1] = f(A) \cap f(B)$ mais $f(A \cap B) = \{0\} \not\supset [0, 1] = f(A) \cap f(B)$.

ii) (a) On étude les propriétés de la fonction :

- g est-elle injective ? : Fixons $(x, y), (x', y') \in \mathbb{R}^2$ et supposons $g(x, y) = g(x', y')$, est-ce que peut-on prouver que cette hypothèse implique $(x, y) = (x'y')$? On voit que :
$$g(x, y) = g(x', y') \iff x^2 + y^2 = (x')^2 + (y')^2$$
C'est mal tourné pour démontrer que $(x, y) = (x', y')$, on peut trouver facilement un contre-exemple : on a que $f(1, 0) = 1^2 + 0^2 = 1 = 0^2 + 1^2 = f(0, 1)$ mais $(1, 0) \neq (0, 1) \in \mathbb{R}^2$.
Donc f n'est pas injective.

- g est-elle surjective ? : Fixons un élément dans l'ensemble d'arrivée, $z \in \mathbb{R}$, est-ce qu'il existe un élément de l'ensemble de départ $(x, y) \in \mathbb{R}^2$ tel que z soit l'image de (x, y) par g, c'est-à-dire $z = g(x, y)$? Posons l'équation et essayons de trouver une solution (x, y) en fonction de z :
$$z = g(x, y) \iff z = x^2 + y^2$$
Clairement, si $z < 0$, l'équation précédente ne possède pas des solutions car $f(x, y) \geq 0$, pour tout $(x, y) \in \mathbb{R}^2$.
Donc g n'est pas surjective.

- g est-elle bijective ? : Non, car g n'est pas injective et non plus surjective.

(b) On se souvient de que, par définition
$$\begin{array}{ll} A \subset \mathbb{R}^2 : & g(A) = \{z \in \mathbb{R} \mid \exists (x, y) \in A : z = g(x, y)\} = \{g(x, y) \mid (x, y) \in A\} \\ B \subset \mathbb{R} : & g^{-1}(B) = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) \in B\} \end{array}$$
Alors :
- $g(\{(0, 0)\}) = \{g(x, y) \mid (x, y) \in \{(0, 0)\}\} = \{f(0, 0)\} = \{0\}$.

- $g^{-1}(\{0\}) = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) \in \{0\}\} = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) = 0\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\}$.
Fixons $(x, y) \in \mathbb{R}^2$. Il est clair que :
$$x^2 + y^2 = 0 \overset{x^2, y^2 \geq 0}{\iff} \left\{ \begin{array}{c} x^2 = 0 \\ \text{et} \\ y^2 = 0 \end{array} \right. \iff \left\{ \begin{array}{c} x = 0 \\ \text{et} \\ y = 0 \end{array} \right.$$

Alors $(x, y) = (0, 0)$ est la seule solution de l'équation précédente. On peut conclure donc $g^{-1}(\{0\}) = \{(0, 0)\}$.

- $g^{-1}(\{1\}) = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) \in \{1\}\} = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) = 1\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$.
  En regardant la dernière équation dedans la description de l'ensemble, on voit qu'elle correspond à l'équation de $C_1(0, 0)$, *le cercle dans le plan du centre* $(0, 0)$ *et rayon* 1. On conclut que $g^{-1}(\{0\}) = C_1(0, 0)$.

- $g\left([-1, 1] \times \left\{\sqrt{2}\right\}\right) = \{g(x, y) \mid (x, y) \in [-1, 1] \times \left\{\sqrt{2}\right\}\} = \{g(x, \sqrt{2}) \mid x \in [-1, 1]\} = \{x^2 + \left(\sqrt{2}\right)^2 \mid x \in [-1, 1]\} = \{x^2 + 2 \mid x \in [-1, 1]\}$.
  Supposons que $x \in [-1, 1]$. C'est équivalent à dire $-1 \leq x \leq 1$. Pour tout réel x, on a $x^2 = (-x)^2$ donc il suffit de étudier la cas positif. On a que $0 \leq x \leq 1$ implique $0 \leq x^2 \leq 1$. Si on somme 2, on a $2 \leq x^2 + 2 \leq 3$. Alors $g\left([-1, 1] \times \left\{\sqrt{2}\right\}\right) \subset [2, 3]$. Réciproquement, si $z \in [2, 3]$, alors $0 \leq (z - 2) + 2 \leq 1$ avec $(z - 2) \in [0, 1]$, qui peut être exprimé comme $(z - 2) = \left(\sqrt{z - 2}\right)^2$ où $\sqrt{z - 2} \in [0, 1]$. Alors,
  $$0 \leq \left(\sqrt{z-2}\right)^2 + 2 \leq 1 \iff 0 \leq \left(\sqrt{z-2}\right)^2 + \left(\sqrt{2}\right)^2 \leq 1 \iff 0 \leq g\left(\sqrt{z-2}, \sqrt{2}\right) \leq 1$$
  avec $\sqrt{z - 2} \in [0, 1] \subset [-1, 1]$. Donc, $g\left([-1, 1] \times \left\{\sqrt{2}\right\}\right) \supset [2, 3]$, qui nous donne l'égalité des ensembles par double contenu.

- $g^{-1}\left(\left[-\sqrt{3}, -1\right[\right) = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) \in \left[-\sqrt{3}, 1\right[\} = \{(x, y) \in \mathbb{R}^2 \mid -\sqrt{3} \leq x^2 + y^2 \leq -1\}$.
  Il est clair que $f(x, y) = x^2 + y^2 \geq 0$ pour tout $(x, y)\mathbb{R}^2$, donc $\nexists (x, y) \in \mathbb{R}^2$ tel que $-\sqrt{3} \leq x^2 + y^2 \leq -1 < 0$. Donc $g^{-1}\left(\left[-\sqrt{3}, -1\right[\right) = \emptyset$.

(c) Une relation binaire est une relation d'équivalence si elle vérifie les propriétés réflexive, symétrique et transitive.
(Réflexive) Fixons $(a, b) \in \mathbb{R}^2$. De façon triviale, on a $g(a, b) = g(a, b)$, alors $(a, b)\mathcal{R}(a, b)$.

(Symétrique) Soient $(a, b), (c, d) \in \mathbb{R}^2$. Supposons que $(a, b)\mathcal{R}(c, d)$, par définition :
$$(a, b)\mathcal{R}(c, d) \iff g(a, b) = g(c, d) \iff g(c, d) = g(a, b) \iff (c, d)\mathcal{R}(a, b).$$
Donc $(c, d)\mathcal{R}(a, b)$ et c'est symétrique.

(Transitive) Soient $(a, b), (c, d), (e, f) \in \mathbb{R}$. Supposons que $(a, b)\mathcal{R}(c, d)$ et $(c, d)\mathcal{R}(e, f)$, on a :
$$\left\{\begin{array}{c} (a, b)\mathcal{R}(c, d) \\ \text{et} \\ (c, d)\mathcal{R}(e, f) \end{array}\right. \iff \left\{\begin{array}{c} g(a, b) = g(c, d) \\ \text{et} \\ g(c, d) = g(e, f) \end{array}\right. \iff g(a, b) = g(c, d) = g(e, f) \iff (a, b)\mathcal{R}(e, f)$$
D'où $(a, b)\mathcal{R}(e, f)$, transitive.

On a démontré, alors, que $\mathcal{R}$ est bien une relation d'équivalence sur $\mathbb{R}^2$.
D'une autre coté, une relation binaire est une relation d'ordre si elle vérifie les propriétés réflexive, antisymétrique et transitive. D'après l'analyse précédente, il nous manque de vérifier que la propriété antisymétrique.
(Antisymétrique) Soient $(a, b), (c, d) \in \mathbb{R}^2$. Supposons que $(a, b)\mathcal{R}(c, d)$ et $(c, d)\mathcal{R}(a, b)$, est-ce que ça implique que $(a, b) = (c, d)$?
$$\left\{\begin{array}{c} (a, b)\mathcal{R}(c, d) \\ \text{et} \\ (c, d)\mathcal{R}(a, b) \end{array}\right. \iff \left\{\begin{array}{c} g(a, b) = g(c, d) \\ \text{et} \\ g(c, d) = g(a, b) \end{array}\right. \iff g(a, b) = g(c, d) \iff a^2 + b^2 = c^2 + d^2.$$

Mais, on a vu dans (ii)–(a) que g n'est pas injective, donc $\mathcal{R}$ n'est pas antisymétrique. Alors, on déduit que $\mathcal{R}$ n'est pas une relation d'ordre.
Pour les classes d'équivalence :

- $\overline{(0,0)}^{\mathcal{R}} = \{(a,b) \in \mathbb{R}^2 \mid (0,0)\mathcal{R}(a,b)\} = \{(a,b) \in \mathbb{R}^2 \mid g(0,0) = g(a,b)\} = \{(a,b) \in \mathbb{R}^2 \mid 0 = g(a,b)\} = g^{-1}(\{0\}) \overset{(ii)-(b)}{=} \{0\}$.
- $\overline{(0,1)}^{\mathcal{R}} = \{(a,b) \in \mathbb{R}^2 \mid (0,1)\mathcal{R}(a,b)\} = \{(a,b) \in \mathbb{R}^2 \mid g(0,1) = g(a,b)\} = \{(a,b) \in \mathbb{R}^2 \mid 1 = g(a,b)\} = g^{-1}(\{1\}) \overset{(ii)-(b)}{=} C_1(0,0)$, tous les points dans le plan contenus dans le cercle de centre $(0,0)$ et rayon 1.

Solution 2. $(G,*)$ forme une structure de groupe si $*$ est une loi de composition interne sur G, associative, possédant un élément neutre et par rapport à qui tout élément de G a un symétrique.

(L.C.I.) Soient $(a,b),(c,d) \in \mathbb{R}^{*+} \times \mathbb{R}$. Car $a,c \in \mathbb{R}^{+*}$, le produit ac est aussi dans $\mathbb{R}^{*+}$ et la racine carré $\sqrt{a}$ est définie. Alors :

$$\begin{array}{rccl} *: & G \times G & \longrightarrow & G \\ & ((a,b),(c,d)) & \longmapsto & (ac, b+\sqrt{a}) \end{array}$$

est bien définie partout et $*$ est une loi de composition interne sur G.

(A) Soient $(a,b),(c,d),(e,f) \in G$. Est-ce que $((a,b)*(c,d))*(e,f) = (a,b)*((c,d)*(e,f))$?

$$\begin{aligned} ((a,b)*(c,d))*(e,f) &= \big((ac, b+d\sqrt{a})\big)*(e,f) = \big(ace, b+d\sqrt{a}+f\sqrt{ac}\big) \\ &= \big(ace, b+\big(d+f\sqrt{c}\big)\sqrt{a}\big) = (a,b)*\big(ce, d+f\sqrt{c}\big) \\ &= (a,b)*((c,d)*(e,f)) \end{aligned}$$

Donc $*$ est associative.

(N) Fixons $(a,b) \in G$, est-ce qu'il existe un élément $(c,d) \in G$ tel que $(a,b)*(c,d) = (c,d)*(a,b) = (a,b)$?
En regardant l'expression du produit, on voit rapidement que :

$$\begin{aligned} (a,b)*(1,0) &= (a \cdot 1, b + 0 \cdot \sqrt{a}) = (a,b) \\ (1,0)*(a,b) &= (1 \cdot a, 0 + b \cdot \sqrt{1}) = (a,b) \end{aligned}$$

et $(1,0) \in G$. Alors G possède un élément neutre par $*$: $(1,0)$.

(S) Fixons $(a,b) \in G$, existe-t-il un élément $(a',b') \in G$ tel que $(a,b)*(a',b') = (a',b')*(a,b) = (1,0)$?
On fixe $(a',b') \in G$. Si on fait un analyse du symétrique à droite :

$$(a,b)*(a',b') = (1,0) \Longleftrightarrow \left\{\begin{array}{rcl} aa' &=& 1 \\ b+b'\sqrt{a} &=& 0 \end{array}\right. \overset{a\neq 0}{\Longleftrightarrow} \left\{\begin{array}{rcl} a' &=& 1/a \\ b' &=& -b/\sqrt{a} \end{array}\right.$$

En plus, $(1/a, -b/\sqrt{a}) \in \mathbb{R}^{*+} \times \mathbb{R} = G$. Cela montre que $(1/a, -b/\sqrt{a})$ est symétrique à gauche de (a,b). Est-il aussi symétrique de (a,b) à droite ?

$$(1/a, -b/\sqrt{a})*(a,b) = \Big((1/a)\cdot a, -b/\sqrt{a} + b\sqrt{1/a}\Big) = (1,0)$$

donc cet élément est également symétrique à droite de (a,b).

Alors, on a prouvé que $(G, *)$ a une structure de groupe.

Est-il abélien ? Les groupes abéliens sont ces dont la loi de composition interne est aussi commutative, c.-à.-d. pour tout $(a, b), (c, d) \in G$, on a que $(a, b) * (c, d) = (c, d) * (a, b)$. Par contre, on voit que :

$$
\begin{aligned}
(4, 0) * (1, 1) &= (4 \cdot 1, 0 + 1\sqrt{4}) = (4, 2) \\
(1, 1) * (4, 0) &= (1 \cdot 4, 1 + 0\sqrt{1}) = (4, 1)
\end{aligned}
$$

Alors, $*$ n'est pas une loi commutative, et $(G, *)$ n'est pas un groupe abélien.

Solution 3.

i) Car le jour sur la station a une durée de 18 heures, on doit faire calculs modulo 18 pour trouver le reste de la division euclidienne de 35^{403} par 18. On analyse en premier la base de la puissance. Facilement, par division euclidienne, on obtient :

$$35 = 18 \times 1 + 17 = 18 \times 2 - 1$$

qui est équivalent à dire que $35 \equiv 17 \equiv -1$ [18]. Les puissances de -1 sont plus faciles à calculer, et on sait que $x \equiv x'$ implique que $x^k \equiv (x')^k$ [18], quelque soit $k \in \mathbb{N}$. Alors :

$$35^{403} \equiv (-1)^{403} = (-1) \equiv 17 \ [18]$$

Donc, le technicien est mort à 17 heures du soir sur la station (une heure avant minuit en Uranus).

ii) On note t_1, u_1 le nombre de jours que le premier suspect est resté sur la Terre et sur la station de Uranus, respectivement. De la même façon, on note t_2, u_2 pour le seconde suspect. Le premier suspect affirme qu'il a fait 95 heures de travail continu par des journées entières entre les deux places. Comme une journée dans la Terre se compose de 24 heures et une journée dans Herschel–IV se compose de 18 heures, on peut poser l'équation dioffantienne représentant le temps total de travail :

$$24t_1 + 18u_1 = 95 \tag{E_1}$$

En suivant le même raisonnement pour le seconde suspect, qui affirme avoir travaillé 102 heures, on pose l'équation :

$$24t_2 + 18u_2 = 102 \tag{E_2}$$

On doit déterminer l'existence de solutions de (E_1) et (E_2). On a vu dans le cours qu'une équation du type

$$ax + by = c \tag{E}$$

avec $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$, admet des solutions dans $\mathbb{Z} \times \mathbb{Z}$ sii c est multiple de $\text{pgcd}(a, b)$. Les coefficients dans (E_1) et (E_2) sont invariantes et ce n'est que le terme indépendante des équations qui change. On doit donc calculer $\text{pgcd}(24, 18)$. On utilise l'algorithme d'Euclide :

$$
\begin{aligned}
24 &= 1 \times 18 + 6 \\
18 &= 3 \times 6 + 0
\end{aligned}
$$

Donc $\text{pgcd}(24, 18) = 6$. Maintenant, si on fait la division euclidienne de 95 et 102 par 6 :

$$
\begin{aligned}
95 &= 15 \times 6 + 5 \\
102 &= 17 \times 6 + 0
\end{aligned}
$$

Alors (E_1) n'a pas des solutions entières tandis que (E_2) oui, d'où on peut déduire que le premier suspect ne dit pas la vérité.

iii) **(Bilan extra : 2 pts)** Cherchons à résoudre dans $\mathbb{N} \times \mathbb{N}$ l'équation

$$24t_2 + 18u_2 = 102 \qquad (E_2)$$

Premièrement, on cherche une solution particulière. En utilisant l'algorithme d'Euclide à l'inverse, on a :

$$6 = 24 - 18 = 24 \cdot (1) + 18 \cdot (-1)$$

Comme $102 = 17 \times 6$, on multiplie l'équation par 15 pour obtenir :

$$102 = 24 \cdot (17) + 18 \cdot (-17)$$

Donc, une solution particulière de (E_2) est $(t_2^0, u_2^0) = (17, -17)$. Cette solution n'a pas de sens réel (on ne peut pas rester une quantité négative de jours sur la station !). On doit donc trouver la solution générale.
Soit $(t_2, u_2) \in \mathbb{Z}^2$:

$$\begin{aligned}(t_2, u_2) \text{ solution de } (E_2) &\iff 24t_2 + 18u_2 = 24t_2^0 + 18u_2^0 \\ &\iff 24(t_2 - t_2^0) = 18(u_2^0 - u_2) \\ &\iff 4(t_2 - t_2^0) = 3(u_2^0 - u_2)\end{aligned}$$

la dernière équivalence s'obtenant en divisant les deux membres de l'égalité par $\text{pgcd}(24, 18) = 6$.
Par suite, si (t_2, u_2) est solution, alors 3 divise $4(t_2 - t_2^0)$. Comme 3 est premier avec 4, le théorème de Gauss nous dit que 3 divise $(t_2 - t_2^0)$, c.-à.-d. qu'il existe $k \in \mathbb{Z}$ tel que $(t_2 - t_2^0) = 3k$, d'où $t_2 = t_2^0 + 3k$. Si on substitue dans la relation précédente :

$$4(t_2^0 + 3k - t_2^0) = 3(u_2^0 - u_2) \iff 12k = 3(u_2^0 - u_2) \iff 4k = u_2^0 - u_2$$

D'où $u_2 = u_2^0 - 4k$. Ainsi, si (t_2, u_2) est solution de (E_2) dans $\mathbb{Z}^2$, alors il existe $k \in \mathbb{Z}$ tel que $t_2 = t_2^0 + 3k$ et $u_2 = u_2^0 - 4k$.
Réciproquement, pour tout $k \in \mathbb{Z}$:

$$24(t_2^0 + 3k) + 18(u_2^0 - 4k) = 24 \cdot (17) + 18 \cdot (-17) + 72k - 72k = 408 - 306 = 102$$

Donc $(17 + 3k, -17 - 4k)$ est solution de (E_2). L'ensemble des solutions de (E_2) dans $\mathbb{Z}^2$ est donc

$$\mathscr{S}(E_2) = \{(17 + 3k, -17 - 4k) \in \mathbb{Z}^2 \mid k \in \mathbb{Z}\}$$

Maintenant, on doit chercher des solutions dans $\mathbb{N} \times \mathbb{N}$. Si on prend des valeurs de $k \in \mathbb{Z}$ dans $(17 + 3k, -17 - 4k)$ pour trouver des solutions positives :

$$\begin{aligned}k = -7 : &\quad (17 + 3k, -17 - 4k) = (-4, 11) \\ k = -6 : &\quad (17 + 3k, -17 - 4k) = (-1, 7) \\ k = -5 : &\quad (17 + 3k, -17 - 4k) = (2, 3) \\ k = -4 : &\quad (17 + 3k, -17 - 4k) = (5, -1)\end{aligned}$$

Remarquez que $17 + 3k$ et $-17 - 4k$ sont des fonctions croissante et décroissante sur $k \in \mathbb{Z}$, respectivement. Donc, la seule solution dans $\mathbb{N}^2$ est $(2, 3)$. Alors, le seconde suspect est resté 2 jours sur la Terre et 3 sur la station.