FACULTÉ DES SCIENCES DE MARSEILLE SAINT-JÉRÔME

ANNALES D'ALGÈBRE ET ANALYSE I – 2001/2002

THOMAS REY & EMMANUEL RUSS

Sommaire

1. T.D.1 - Le raisonnement

Exercice 1. (*a*) Soient A, B et C des assertions. Les assertions suivantes sont-elles vraies ou fausses ? Justifier à chaque fois.

$$A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$$

$$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C).$$

(*b*) Soient P et Q deux assertions. Montrer que la proposition suivante est vraie:

$$(P \Longrightarrow Q) \iff (\neg Q \Longrightarrow \neg P).$$

(*c*) Soient P, Q et R des assertions. Montrer que les assertions

$$(P \Longrightarrow Q) \Longrightarrow R \text{ et } P \Longrightarrow (Q \Longrightarrow R)$$

ne sont PAS logiquement équivalentes.

Exercice 2. Soit $x \in \mathbb{R}$. On considère les propositions suivantes:

$$P:\ x = 0 \quad Q:\ \forall \varepsilon > 0\ \ |x| < \varepsilon \quad R:\ \forall \varepsilon > 0\ \ |x| \leq \varepsilon.$$

Montrer que ces trois propositions sont équivalentes (on montrera successivement $P \Longrightarrow Q$, $Q \Longrightarrow R$ et $R \Longrightarrow P$).

Exercice 3. Soient b et c des réels. On définit, pour tout $x \in \mathbb{R}$, $f(x) = x^2 + bx + c$. Montrer l'équivalence des trois propositions suivantes:

$$\forall x \in \mathbb{R},\ f(x) > 0$$

$$\forall x \in \mathbb{R},\ f(x) \neq 0,$$

$$b^2 - 4c < 0.$$

Exercice 4. Soit I un intervalle de $\mathbb{R}$ non vide et non réduit à un point, $f : I \to \mathbb{R}$ une fonction, x_0 un point de I et $l \in \mathbb{R}$.

On dit que f a pour limite l au point x_0 par valeurs différentes si, et seulement si, pour tout $\varepsilon > 0$, il existe $\alpha > 0$ tel que, pour tout $x \in I$, si $0 < |x - x_0| < \alpha$, alors $|f(x) - l| < \varepsilon$.

On dit que f est continue au point x_0 si, et seulement si, pour tout $\varepsilon > 0$, il existe $\alpha > 0$ tel que, pour tout $x \in I$, si $|x - x_0| < \alpha$, alors $|f(x) - f(x_0)| < \varepsilon$.

(*a*) Ecrire ces deux propriétés en utilisant des quantificateurs. Ecrire aussi leur négation.

(*b*) Si f a pour limite l au point x_0 par valeurs différentes, f est-elle continue en x_0?

(*c*) Si f est continue en x_0, f a-t-elle une limite en x_0 par valeurs différentes?

Exercice 5. Montrer que, pour tout entier $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k^4 = \frac{n(n+1)}{30}\left(6n^3+9n^2+n-1\right).$$

Exercice 6. (*a*) Montrer que, pour tous réels $x, y > 0$ et tout $t \in [0,1]$,

$$(1-t)\operatorname{Log} x + t \operatorname{Log} y \leq \operatorname{Log}\left((1-t)x+ty\right).$$

On pourra, pour x et y fixés, étudier la fonction $g(t) = (1-t)\operatorname{Log} x + t\operatorname{Log} y - \operatorname{Log}\left((1-t)x+ty\right)$.

(*b*) En déduire que, pour tout $n \in \mathbb{N}^*$, pour tous réels strictement positifs $x_1, ..., x_n$ et tous réels $\alpha_1, ..., \alpha_n$ positifs ou nuls vérifiant $\sum_{k=1}^{n} \alpha_k = 1$,

$$\sum_{k=1}^{n} \alpha_k \operatorname{Log} x_k \leq \operatorname{Log}\left(\sum_{k=1}^{n} \alpha_k x_k\right).$$

(*c*) Montrer que, pour tout $n \in \mathbb{N}^*$ et tous réels $x_1, ..., x_n > 0$,

$$\left(\prod_{k=1}^{n} x_k\right)^{1/n} \leq \frac{\sum_{k=1}^{n} x_k}{n}.$$

Exercice 7. Soit n un entier supérieur ou égal à 2. On dit que n est un nombre premier si, et seulement si, les seuls diviseurs de n sont 1 et n.

(*a*) Montrer par récurrence sur n que tout entier $n \geq 2$ possède un diviseur premier.

(*b*) Soient $k \in \mathbb{N}^*$ et $n_1, ..., n_k$ des entiers strictement positifs. On pose

$$N = 1 + \prod_{l=1}^{k} n_l.$$

Montrer que, quel que soit $l \in \{1, \ldots, k\}$, N n'est pas divisible par n_l.

(*c*) Déduire de ce qui précède qu'il existe une infinité de nombres premiers.

2. T.D.2 - Fonctions

Exercice 8. Soient E, F, G et H des ensembles, h une fonction de E dans F, g une fonction de F dans G et f une fonction de G dans H. On suppose que $f \circ g \circ h$ est bijective. Montrez qu'alors : f est surjective et h injective.

Exercice 9. Soit f une fonction. On suppose que le graphe de $f : [-1, 1] \to \mathbb{R}$ est un demi-cercle. Que vaut $f(1) - f(-1)$?

Exercice 10. Soit $f : \mathbb{R}^2 \to \mathbb{R}$ définie par : $f(x, y) = \sqrt{x^2 + y^2}$
Soit $J = \{(x, y) / \, |x| \leq 1 \, et \, |y| \leq 1\}$

1. Tracez J.
2. Que vaut $f(J)$?
3. Que vaut $f^{-1}(f(J))$? A-t-on $f^{-1}(f(J)) = J$?
4. Que vaut $f^{-1}(1)$?

Exercice 11. Soit $f : [0, 1] \to [0, 1]$ définie par :
$f(t) = t$ si $t \notin \mathbb{Q}$
$f(t) = 1 - t$ si $t \in \mathbb{Q}$
Cette fonction est-elle bijective ?

Exercice 12. Soit une fonction $f : E \to F$. Soient A,A_1,A_2 trois sous-ensembles de E et B,B_1,B_2 trois sous-ensembles de F. Montrer qu'on a :

(a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
(b) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$
(c) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
(d) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
(e) $f(f^{-1}(B)) = B \cap f(E)$
(f) $A \subset f^{-1}(f(A))$

Montrer par des exemples que les inclusions dans (b) et (f) peuvent être strictes.

Exercice 13. *Etude de la fonction sinus hyperbolique et de sa réciproque.*

Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction définie par $f(x) = \sinh x = \frac{1}{2}(e^x - e^{-x})$. (cette fonction est appelée "sinus hyperbolique").

(*a*) Pour $y \in \mathbb{R}$ quelconque, montrer qu'il existe un unique $X \in \mathbb{R}$ vérifiant $X^2 - 2yX - 1 = 0$.

(*b*) En utilisant la question (*a*), montrer que pour tout $y \in \mathbb{R}$, il existe un unique $x \in \mathbb{R}$ tel que $\sinh x = y$. On pourra poser $X = e^x$.

(*c*) En déduire que la fonction f est bijective. On note $f^{-1} = \operatorname{Arg\,sh}$.

(*d*) Donner une expression de $\operatorname{Arg\,sh}$ en fonction de ln.

Exercice 14. Soit E un ensemble et $f : E \to \mathcal{P}(E)$ une application. On définit

$$A = \{x \in E;\ x \notin f(x)\}.$$

(*a*) Montrer qu'il n'existe pas de $x \in E$ tel que $f(x) = A$.

(*b*) En déduire que f n'est pas surjective.

(*c*) Dans le cas où E est fini, donner une autre démonstration de la question (*b*).

Exercice 15. Soient n et p deux entiers, $E = \{1 \dots p\}$ et $F = \{1 \dots n\}$

(*a*) Calculez le nombre de fonctions strictement croissantes de E dans F.

(*b*) Calculez le nombre de fonctions croissantes (au sens large) de E dans F. (Remarquer que, si f est croissante, la fonction $g(k) = f(k) + k - 1$ est strictement croissante).

Exercice 16.

(*a*) Montrez que $k\binom{n}{k} = n\binom{n-1}{k-1}$ pour tout $n \geq k \geq 1$.

(*b*) A l'aide de la question précédente, calculez : $S_\alpha = \sum_{k=0}^{n} (-1)^k \binom{n}{k} k^\alpha$ pour $\alpha = 0, 1, 2$ et $n \geq \alpha$ (Attention aux cas particuliers, par exemple $\alpha = 2$ et $n = 2$).

3. T.D.3 - Relations

Exercice 17.

(*a*) Soit A un ensemble ordonné. Montrez qu'un ensemble A admet un de ses éléments pour borne inférieure si, et seulement si, A admet un plus petit élément (on a alors : $minA = infA$).

(*b*) Dans $(\mathbb{R}, \leq)$, soit $A = \{x \in \mathbb{R};\ 0 \leq x < 1\}$. A possède-t-il un plus grand élément (resp. plus petit élément) ? A possède-t-il une borne supérieure (resp. borne inférieure) et, si oui, quelle est sa valeur ?

Exercice 18. Soit $(E, \leq)$ un ensemble totalement ordonné et A une partie de E. Soit a un élément maximal de A. Montrez que a est le plus grand élément de A.

Exercice 19. On rappelle que $\sqrt{3}$ est irrationnel.

(*a*) Dans $(\mathbb{R}, \leq)$, soit $A = \left\{x \in \mathbb{R};\ x^2 < 3\right\}$. Montrer que A possède une borne supérieure et la calculer. L'ensemble A a-t-il un plus grand élément?

(*b*) Dans $(\mathbb{Q}, \leq)$, soit $B = \left\{x \in \mathbb{Q};\ x^2 < 3\right\}$. B possède-t-il des majorants ? B possède-t-il une borne supérieure ?

Exercice 20. Soient A et B deux parties de $\mathbb{R}$ non vides et majorées.

(*a*) On note

$$A + B = \{x \in \mathbb{R};\ \exists a \in A,\ \exists b \in B,\ x = a + b\}.$$

Montrer que $A + B$ est non vide et majoré, et que

$$\sup(A + B) = \sup A + \sup B.$$

(*b*) On note

$$AB = \{x \in \mathbb{R};\ \exists a \in A,\ b \in B,\ x = ab\}.$$

Montrer que, si $A \subset [0, +\infty[$ et $B \subset [0, +\infty[$, alors AB est non vide et majoré, et que

$$\sup(AB) = \sup A \sup B.$$

Donner un exemple de parties A et B de $\mathbb{R}$ non vides et majorées telles que AB ne soit pas majoré.

Exercice 21. Sur $\mathbb{N}$ on définit $\lhd$ par : $n \lhd m \iff \exists p \in \mathbb{N}$ tel que : $m = np$ (on écrit aussi : $n|m$).

(a) Montrez que $(\mathbb{N}, \lhd)$ est un ensemble ordonné. Est-il totalement ordonné ? Déterminer les éléments minimaux et maximaux.

(b) Mêmes questions avec $(\mathbb{N}\backslash\{1\}, \lhd)$

(c) Dans $(\mathbb{N}, \lhd)$, soit $B = \{0, 4, 5, 6, 8\}$. Quels sont les éléments maximaux de B ? Est-ce que B possède, dans $\mathbb{N}$ des majorants (resp. des minorants) ? Si oui, y a-t-il une borne supérieure (resp. borne inférieure).

Même question pour $B_1 = \{4, 5, 6, 8\}$.

Exercice 22. Soient $(A, \lhd_1)$ et $(B, \lhd_2)$ deux ensembles ordonnés.

(a) Sur $A \times B$ on définit la relation : $(a, b) \lhd (a', b') \iff \begin{cases} a \neq a' \text{ et } a \lhd_1 a' \\ \text{ou} \\ a = a' \text{ et } b \lhd_2 b' \end{cases}$ Montrez que $\lhd$ est un ordre sur $A \times B$. Il est appelé ordre lexicographique, pourquoi ?

Si $(A, \lhd_1) = (B, \lhd_2) = (\mathbb{N}, \leq)$, dessinez tous les éléments de $\mathbb{N} \times \mathbb{N}$ inférieurs à un élément (n, m) donné de $\mathbb{N} \times \mathbb{N}$.

(b) Sur $A \times B$ on définit la relation : $(a, b) \prec (a', b') \iff \begin{cases} a \lhd_1 a' \\ et \\ b \lhd_2 b' \end{cases}$

Montrez que $\prec$ est un ordre sur $A \times B$.

Si $(A, \lhd_1) = (B, \lhd_2) = (\mathbb{N}, \leq)$, dessinez tous les éléments de $\mathbb{N} \times \mathbb{N}$ inférieurs à un élément donné (n, m) de $\mathbb{N} \times \mathbb{N}$ pour l'ordre $\prec$.

(c) Si $\lhd_1$ et $\lhd_2$ sont des ordres totaux, qu'en est-il de $\lhd$ et $\prec$?

Exercice 23. Soit A un ensemble non vide.

(a) Prouvez que $(\P(A), \subset)$ est un ensemble ordonné. Montrez que, si A comporte au moins deux éléments, $(\P(A), \subset)$ n'est pas totalement ordonné.

(b) Soit X un ensemble et $\leq$ une relation d'ordre sur cet ensemble. On dit que $(X, \leq)$ est un treillis (on dit aussi "ensemble réticulé") si, et seulement si, pour tout x et tout x' appartenant à X, $sup(x, x')$ et $inf(x, x')$ existent dans X.

Montrez que $(\mathfrak{P}(A), \subset)$ est un treillis.

(c) On dit que X est complet pour son ordre $\leq$ si, et seulement si, pour tout sous-ensemble X' borné de X, $supX'$ et $infX'$ existent.

Montrez que $(\mathfrak{P}(A), \subset)$ est complet.

(d) Démontrez qu'un ensemble totalement ordonné est un treillis.

Exercice 24. Soit $(E, \leq)$ un ensemble ordonné.

(*a*) Montrez que le plus petit élément d'un sous-ensemble de E, s'il existe, est unique.

(*b*) On suppose ici que tout sous-ensemble non vide de E admet un plus petit élément. On dit dans ce cas que $(E, \leq)$ est bien ordonné. Montrez que si $(E, \leq)$ et $(E, \geq)$ sont tous les deux bien ordonnés, alors E est fini.

(*c*) Montrez que tout sous-ensemble fini et totalement ordonné est bien ordonné.

(*d*) Montrez que $(\mathbb{N}, \leq)$ est bien ordonné, et que $(\mathbb{Z}, \leq)$ ne l'est pas.

Exercice 25. Sur $E = \mathbb{Z} \times \mathbb{Z}^*$, on définit la relation $\mathcal{R}$ par : $\forall((a,b),(a',b')) \in E \times E,\ ((a,b),(a',b')) \in \mathcal{R} \iff ab' = a'b$. Montrez que $\mathcal{R}$ est une relation d'équivalence.

Exercice 26. Dans ce qui suit, $\underline{n = 3}$. On cherche à définir une addition et une multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

(*a*) Soient deux éléments C_1 et C_2 dans $\mathbb{Z}/n\mathbb{Z}$. On choisit $k \in C_1$ et $l \in C_2$, et on définit $C = C_1 + C_2$ comme étant la classe d'équivalence de $k + l$. Vérifier que cette définition est correcte, c'est-à-dire qu'elle ne dépend pas du choix de $k \in C_1$ et de $l \in C_2$.

(*b*) Procéder de manière analogue pour définir une multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

(*c*) Soit $k \in \{0, \dots, n-1\}$. A quelle condition sur k existe-t-il $l \in \{0, \dots, n-1\}$ tel que $\overline{k}\ \overline{l} = \overline{1}$?

(*d*) Refaire les questions précédentes dans le cas où $n \in \mathbb{N}^* \setminus \{1\}$ est quelconque.

Exercice 27. Soient E et F deux ensembles, munis respectivement des relations d'équivalence $\mathcal{R}$ et $\mathcal{S}$. Dans $E \times F$, on définit la relation $\mathcal{T}$ par :
$((x,y),(x',y')) \in \mathcal{T} \iff (x,x') \in \mathcal{R}\ et\ (y,y') \in \mathcal{S}$.
Montrez que $\mathcal{T}$ est une relation d'équivalence. Montrez qu'il existe une bijection entre $(E \times F)/\mathcal{T}$ et $(E/\mathcal{R}) \times (F/\mathcal{S})$.

4. T.D.4 - Groupes

Les exercices ou les questions les plus difficiles sont signalés par une étoile.

Exercice 28. On définit sur $\mathbb{R}$ la loi de composition $\star$ de la façon suivante :

$$\forall (x,y) \in \mathbb{R}^2, x \star y = x + y - xy.$$

1) Montrer que $\star$ est associative, commutative et admet 0 comme élément neutre.

2) Montrer que tout nombre réel différent de 1 admet un symétrique unique dont on calculera explicitement la valeur. $(\mathbb{R}, \star)$ est-il un groupe ?

3) Vérifier que, $\forall (x,y) \in \mathbb{R}^2$, on a :

$$x \star y = 1 - (x-1)(y-1).$$

En déduire que $\star$ est une loi de composition interne sur $\mathbb{R} \setminus \{1\}$. Montrer que $(\mathbb{R} \setminus \{1\}, \star)$ est un groupe commutatif.

4)Montrer que l'application :

$$\begin{array}{rccc} f: & \mathbb{R} \setminus \{1\} & \to & \mathbb{R}^* \\ & x & \mapsto & 1-x \end{array}$$

est un isomorphisme de groupes de $(\mathbb{R} \setminus \{1\}, *)$ sur $(\mathbb{R}, \times)$.

5) Pour tout $x \in \mathbb{R}$, et pour tout entier naturel n, calculer, par récurrence, $x^{(n)}$ (où $x^{(n)} = x \star x^{(n-1)}$ et $x^1 = x$)

Exercice 29. Soit $(G, .)$ un groupe d'ordre 4. On suppose de plus que ce groupe est monogène (i.e. il existe $a \in G$ tel que : $G = \{a^n, n \in \mathbb{Z}\}$).

1. Montrez que a est d'ordre 4.
2. Montrer qu'il existe un isomorphisme de groupe de $(G, .)$ sur $(\mathbb{Z}/4\mathbb{Z}, +)$.

Exercice 30 (Groupe de Klein)**.** Soit $\mathbb{K} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de la loi de composition interne $\star$ définie par : $\forall (x,y) \in \mathbb{K}$, $\forall (x',y') \in \mathbb{K}$: $(x,y) \star (x',y') = (x+x', y+y')$, où $+$ est l'addition $\mathbb{Z}/2\mathbb{Z}$.

1. Vérifier que $(\mathbb{K}, \star)$ est un groupe commutatif. Construire sa table.
2. Donner l'ordre de chaque élément de $\mathbb{K}$. En déduire que $(\mathbb{K}, \star)$ n'est pas isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$.
3. L'espace $\mathbb{R}^3$ étant rapporté au repère $Oxyz$, on considère les symétries orthogonales S_x, S_y, S_z par rapport aux axes de coordonnées. Montrer que l'ensemble $G = \{\mathrm{id}, S_x, S_y, S_z\}$ est un groupe pour la loi de composition des applications et que ce groupe est isomorphe à $(\mathbb{K}, \star)$.

Exercice 31. Construire, à isomorphisme près, les groupes d'ordre n avec $n \in \{1, 2, 3, 4, 5\}$ (et identifier parmi ces groupes $\mathbb{Z}/4\mathbb{Z}$ et le groupe de Klein des 2 exercices précédents).

Exercice 32. Soient H et K deux sous-groupes d'un groupe G.

1. Montrer que $H \cap K$ est un sous-groupe de G. Que pensez-vous d'une intersection quelconque de sous-groupes de G ?
2. Démontrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.
3. Montrer que $HK = \{x \in G \text{ tels que : } \exists h \in H \text{ et } \exists k \in K \ / \ x = hk\}$ est un sous-groupe de G si et seulement si $HK = KH$.

Exercice 33. Soit $(G, .)$ un groupe d'élément neutre e. Soit x un élément de G, tel qu'il existe un entier n tel que $x^n = e$, on note alors $\omega(x)$ l'ordre de x dans $(G, .)$.
Soient a et b deux éléments de G tels que $\omega(a)$ et $\omega(b)$ soient prermiers entre eux. Montrez alors, en utilisant le théorème de Bezout, que : $\omega(a.b) = \omega(a).\omega(b)$.

Exercice 34. Soit σ un élément du groupe $(\Sigma_7, \circ)$ (Σ_7 est l'ensemble des permutations à 7 éléments, $\circ$ est la composition des applications). σ est défini par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 2 & 6 & 3 & 7 \end{pmatrix}$$

1. Montrer que σ s'écrit comme le produit d'une transposition et d'une permutation d'ordre 3.
2. Montrer, en utilisant l'exercice précédent que σ est d'ordre 6.
3. Calculer σ^{38}.

Exercice 35 (Racines de l'unité dans $\mathbb{C}$)**.** Soit $n \geq 1$ un entier.

(*a*) Résoudre dans $\mathbb{C}$ l'équation $z^n = 1$. On note U_n l'ensemble des solutions de cette équation.
(*b*) Déterminer un $\omega \in U_n$ tel que $U_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.
(*c*) Vérifier que $(U_n, \cdot)$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$.
(*d*) Montrer qu'il existe une application linéaire bijective φ de $(U_n, \cdot)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$ telle que $\varphi(a \cdot b) = \varphi(a) + \varphi(b)$ pour tout $a, b \in U_n$; φ est un isomorphisme de groupes.

Exercice 36 (Groupe Diédral)**.** On appelle D_4 l'ensemble des isométries d'un plan affine euclidien qui conservent l'ensemble des sommets d'un carré.

(*a*) Montrer que l'ensemble D_4, muni de la loi de composition des applications $\circ$, est un groupe d'ordre 8 non commutatif.

(*b*) Pour $n \geq 3$, soit D_n l'ensemble des isométries d'un plan affine euclidien qui conservent l'ensemble des sommets d'un polygone régulier à n côtés que l'on note P (faire une figure).

Généraliser le résultat de la question précédente en montrant que D_n, muni de la loi de composition des applications, est un groupe non commutatif (ce groupe est appellé le groupe diédral).

(*c*) Soit O le centre de P et A un de ses sommets. Soit r la rotation de centre O et d'angle $2\pi/n$. Soit s la symétrie orthogonale d'axe (OA).

Montrer que G est engendré par r et s. Ecrire alors les éléments de D_n en fonction de r et s. Quel est l'ordre de $(D_n, \circ)$?

Remarque : On montre que tout groupe d'ordre 8 *engendré par deux éléments d'ordres* 4 *et* 2 *respectivement est isomorphe à* $(D_4, \circ)$.

5. T.D.5 - Anneaux, corps, suites

Les exercices ou les questions les plus difficiles sont signalés par une étoile.

Exercice 37. Soient A et A' des anneaux. Si (x, x') et (y, y') sont dans $A \times A'$, on pose

$$(x, y) + (x', y') = (x + x', y + y') \text{ et } (x, y).(x', y') = (xx', yy').$$

(a) Montrer que $(A \times A', +, .)$ est un anneau.

(b) On suppose A et A' intègres. L'anneau $A \times A'$ est-il intègre ?

Exercice 38. Soit $(A, +, .)$ un anneau commutatif et unitaire (soit e son élément unité). On dit qu'un élément x de A est *nilpotent* s'il existe un entier $n \geq 1$ tel que $x^n = 0$.

1. Montrer que l'ensemble des éléments nilpotents est un sous-groupe de $(A, +)$.
2. Montrer que, si x est nilpotent, $e - x$ est inversible.
3. Montrer que l'ensemble des diviseurs de 0 dans A (c'est-à-dire, l'ensemble des éléments $a \in A$ tels qu'il existe $b \in A$, $b \neq 0$ et $a.b = 0$) contient le sous-groupe des éléments nilpotents. L'ensemble des diviseurs de 0 est-il un groupe?
4. Dans $\mathbb{Z}/24\mathbb{Z}$, déterminer les éléments nilpotents, les diviseurs de 0 et les éléments inversibles, et vérifier les propriétés précédentes. Quel est l'ordre du groupe des éléments nilpotents? A quel groupe connu est-il isomorphe?

Exercice 39. Montrer que tout homomorphisme d'anneaux f de $\mathbf{Q}$ dans $\mathbf{Q}$, non identiquement nul, est égal à l'identité.
[[On commencera par montrer que, pour tout nombre entier naturel n, $f(n) = n$, puis que la propriété est vraie pour tout nombre entier relatif et enfin pour tout nombre rationnel.]]

Exercice 40. Soit A un anneau intègre fini. Montrer que A est un corps.

Exercice 41. Soit K un corps. On suppose que tout élément non nul a vérifie : $a^{-1} = -a$.
1) Montrer que, pour tout élément a de K, on a : $a + a = 0$.
2) En déduire que K ne contient que les deux éléments 0 et 1. Montrez alors que : K est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exercice 42. 1. Soit $A = \{x \in \mathbb{R};\ \exists a, b \in \mathbf{Q}\ :\ x = a + b\sqrt{2}\}$. Montrer que $(A, +, \cdot)$ est un corps.

2. Soit $B = \{z \in \mathbf{C};\ \exists a, b \in \mathbb{Z}\ :\ z = a + i.b\}$. Montrer que $(B, +, \cdot)$ est un anneau. On appelle B l'anneau des entiers de Gauss.
3. Quels sont les éléments inversibles de B ?
4. *** Montrez que J est un idéal de B si, et seulement si, J est de la forme λB avec $\lambda \in B$.

Exercice 43. Soit $(u_n)_{n\in\mathbb{N}}$ une suite numérique. Montrer que si (u_n) tend vers $l \in \mathbf{C}$ alors $(|u_n|)$ tend vers $|l|$.

Montrez que la réciproque est fausse (donnez un contre exemple).

Exercice 44. 1) Soit $(u_n)_{n\in\mathbb{N}}$ une suite numérique, on définit la suite $(v_n)_{n\in\mathbb{N}}$ par :

$$v_n = \tfrac{1}{n+1}(u_0 + u_1 + \cdots + u_n).$$

a) On suppose que $(u_n)_{n\in\mathbb{N}}$ est convergente, de limite 0 ; montrer que la suite $(v_n)_{n\in\mathbb{N}}$ est convergente, de limite 0.

b) On suppose que $(u_n)_{n\in\mathbb{N}}$ est convergente, de limite L ; montrer que $(v_n)_{n\in\mathbb{N}}$ est convergente, de limite L (poser $w_n = u_n - L$ et utiliser le a)).

2) Déduire de la question 1, que, si $(x_n)_{n\in\mathbb{N}}$ est une suite qui vérifie $\lim_{n\to\infty} x_{n+1} - x_n = L$, alors la suite de terme général x_n/n tend vers L (poser $u_n = x_{n+1} - x_n$).

3) Supposons que x_n/n tende vers L, peut-on dire que $\lim_{n\to\infty} x_{n+1} - x_n = L$? On pourra donner une démonstration ou trouver un contre-exemple.

4) Soit $(u_n)_{n\in\mathbb{N}}$ une suite à termes strictement positifs, vérifiant $\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = L$. Montrer que : $\lim_{n\to\infty}[(u_n)^{\frac{1}{n}}] = L$

Exercice 45. Suites classiques

(a) Soit $\alpha \in \mathbb{R}$. Pour tout $n \in \mathbb{N}^*$, on pose $x_n = n^\alpha$.
  (i) Montrer que, si $\alpha > 0$, la suite $(x_n)_{n\in\mathbb{N}^*}$ tend vers $+\infty$.
  (ii) Montrer que, si $\alpha < 0$, la suite $(x_n)_{n\in\mathbb{N}^*}$ tend vers 0.
  (iii) Quel est le comportement de la suite $(x_n)_{n\in\mathbb{N}^*}$ si $\alpha = 0$?

(b) Soit $a \in \mathbb{R}$. On pose pour tout $n \in \mathbb{N}$, $x_n = a^n$.
  (i) Montrer que, si $a > 1$, la suite $(x_n)_{n\in\mathbb{N}}$ tend vers $+\infty$.
  (ii) Montrer que, si $|a| < 1$, la suite $(x_n)_{n\in\mathbb{N}}$ tend vers 0.
  (iii) Quel est le comportement de la suite si $a = 1$, si $a = -1$, si $a < -1$?

6. T.D.6 - Suites, Polynômes

Exercice 46. Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans $\mathbb{C}$ et $l \in \mathbb{C}$. Montrer que si $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ convergent vers l, alors $(u_n)_{n\in\mathbb{N}}$ converge vers l.

Exercice 47. Soit $(u_n)_{n\in\mathbb{N}}$ de terme général $u_n = sin(n\frac{\pi}{6})$

(a) Exprimez en fonction de n les suites : $r_n = u_{6n}$, $s_n = u_{6n+3}$, $t_n = u_{2n}$. Ces suites sont-elles périodiques, et, si oui, quelle est leur période ?

(b) Les sous-suites de $(u_n)_{n\in\mathbb{N}}$ sont-elles toutes périodiques ?

(c) Exhibez deux sous-suites de $(u_n)_{n\in\mathbb{N}}$ dont l'une tend vers $+1$ et l'autre tend vers -1 quand n tend vers $+\infty$. Est-ce que la suite $(u_n)_{n\in\mathbb{N}}$ a une limite quand n tend vers $+\infty$?

Exercice 48. Soient a, b et c des réels, avec $a \neq 1$. On définit

$$u_0 = c,\ u_{n+1} = au_n + b\ \forall n \in \mathbb{N}.$$

(a) Trouver $d \in \mathbb{R}$ tel que la suite $v_n = u_n - d$ soit géométrique.

(b) En déduire l'expression de u_n en fonction de n.

(c) La suite $(u_n)_{n\in\mathbb{N}}$ possède-t-elle une limite ?

(d) Que se passe-t-il si $a = 1$?

Exercice 49. Moyenne arithmético-géométrique.

Soient a et b deux réels tels que $0 < a \leq b$ et les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ définies par : $u_0 = a$, $v_0 = b$, $u_{n+1} = \sqrt{u_n.v_n}$, $v_{n+1} = \dfrac{u_n + v_n}{2}$

(a) Montrer que, pour tous réels x et y,

$$2xy \leq x^2 + y^2.$$

En déduire que, pour tout $n \geq 0$, $u_n \leq v_n$.

(b) Utiliser la question (a) pour montrer que la suite $(u_n)_{n\geq 0}$ est croissante et la suite $(v_n)_{n\geq 0}$ décroissante.

(c) Exprimer $v_{n+1} - u_{n+1}$ en fonction de v_n et u_n. En déduire que les deux suites sont adjacentes, puis qu'elles ont une limite commune. Cette limite s'appelle la moyenne arithmético-géométrique des nombres a et b.

Exercice 50. *Suites homographiques*

On se propose d' étudier ici la suite $(u_n)_{n\in\mathbb{N}}$ définie par :

$u_0 = a \in \mathbb{R}$ et $u_{n+1} = \frac{3u_n+6}{u_n+4}$.

De plus, on note

$$E = \{a \in \mathbb{R};\ \text{la suite } (u_n)_{n\in\mathbb{N}} \text{ est bien définie}\}.$$

(1) Si $a \notin E$, que se passe-t-il ?

(2) Soit f la fonction définie sur $\mathbb{R} \setminus \{-4\}$ par : $f(x) = \frac{3x+6}{x+4}$. Résoudre l' équation $f(x) = x$. On note par la suite α et β (avec $\alpha \leq \beta$) les deux solutions de cette équation.

(3) Si $a \in \{\alpha, \beta\}$, comment se comporte la suite $(u_n)_{n\in\mathbb{N}}$?

On suppose désormais que $a \in E \setminus \{\alpha, \beta\}$.

(4) Montrer que la suite $(w_n)_{n\in\mathbb{N}}$ définie par $w_n = \dfrac{u_n - \alpha}{u_n - \beta}$ est bien définie et est une suite géométrique dont on déterminera la raison.

[[Indication : calculer $\dfrac{w_{n+1}}{w_n}$]]

(5) En utilisant la question précédente, exprimez w_n en fonction de n. En déduire l'expression de u_n en fonction de n.

A l'aide de cette expression, calculez : $\lim_{n\to+\infty} u_n$.

Exercice 51. Approximations de réels.

Soit $a \in \mathbb{R}_+^*$ et $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 > 0$ et $u_{n+1} = \frac{1}{2}(u_n + \frac{a}{u_n})$.

(*a*) Montrez que $\forall n \in \mathbb{N}^*$, $u_n \geq \sqrt{a}$, et que $(u_n)_{n\in\mathbb{N}}$ est décroissante et converge vers $\sqrt{a}$.

(*b*) Montrez que $\frac{u_{n+1}-\sqrt{a}}{u_{n+1}+\sqrt{a}} = (\frac{u_0-\sqrt{a}}{u_0+\sqrt{a}})^{2^n}$

(*c*) En prenant $a = 2$ et $u_0 = 1$ et en utilisant la question précédente, calculez une valeur approchée de $\sqrt{2}$ à 10^{-10} près sachant que $1 < \sqrt{2} < 2$.

Exercice 52. On considère une suite $(u_n)_{n\in\mathbb{N}}$ définie par la donnée de $u_0 \in \mathbb{R}$ et la relation de récurrence $u_{n+1} = f(u_n)$ où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Dans toute la suite, on considère un intervalle I stable par f, c'est-à-dire vérifiant : $f(I) \subset I$ et l'on suppose que $u_0 \in I$.

(1) Montrez que $\forall n \in \mathbb{N}$, $u_n \in I$.

(2) Montrez que si f est croissante sur I, alors $(u_n)_{n\in\mathbb{N}}$ est monotone.

(3) Montrez que si f est décroissante sur I, alors les deux suites $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont monotones de sens de monotonie contraires.

(4) Montrez que si $\forall x \in I$, $f(x) \geq x$ alors $(u_n)_{n\in\mathbb{N}}$ est croissante et si $\forall x \in I$, $f(x) \leq x$ alors $(u_n)_{n\in\mathbb{N}}$ est décroissante.

(5) Utilisez les résultats précédents pour étudier les suites vérifiant :

(*a*) $u_{n+1} = \frac{1}{2}u_n^2 + 2u_n + \frac{1}{2}$

(*b*) $u_{n+1} = \frac{6}{2+u_n^2}$

Exercice 53. On définit la suite de polynômes $(P_n)_{n\in\mathbb{N}} \in \mathbb{R}[X]$ par

$$P_0 = 1,\ P_1 = X,\ P_{n+2} = XP_{n+1} - P_n \text{ si } n \in \mathbb{N}.$$

(*a*) Montrer que, pour tout $n \geq 1$,

$$P_n^2 - P_{n-1}P_{n+1} = 1.$$

Indication: raisonner par récurrence sur n.

(*b*) En déduire que, pour tout $n \in \mathbb{N}$, les seuls polynômes qui divisent à la fois P_n et P_{n+1} sont constants.

Exercice 54. (*a*) Dans $\mathbb{R}[X]$, effectuer la division euclidienne de $P = X^4 + 8X^3 - 3X^2 + 1$ par $Q = 2X^2 - 5X + 3$.

(*b*) Ici, $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$. On pose

$$P = X^3 + \overline{2}X - \overline{3},\ Q = X^2 + \overline{5}X - \overline{3}.$$

Effectuer la division euclidienne de P par Q.

Exercice 55. Quels sont tous les polynômes $P \in \mathbb{R}[X]$ tels que P' divise P?

Suggestion: écrire $P = QP'$ et regarder les degrés.

Exercice 56. Soient α et β des réels, $n \in \mathbb{N}$. On pose $P = X^{8n} + \alpha X^{4n} + \beta$ et $Q = X^8 + X^4 + 1$. Quelles sont les valeurs de α, β et n pour que Q divise P ?

Suggestion: chercher les racines de Q.

7. Devoir n^0 1 - Enoncé et corrigé

Exercice 1 *Théorème de Cantor-Bernstein*

(*a*) $\emptyset \in B$ car $f(\emptyset) = \emptyset$ et donc $g(F \setminus f(\emptyset)) = g(F \setminus \emptyset) = g(F) \subset E = E \setminus \emptyset$. Ainsi $B \neq \emptyset$.

(*b*) On a vu (TD2, exercice 5) que

$$f(C) = \bigcup_{A \in B} f(A).$$

La preuve a été faite dans le cas d'une union finie, mais le cas d'une union quelconque est identique. On a donc

$$F \setminus f(C) = \bigcap_{A \in B} F \setminus f(A),$$

donc

$$g(F \setminus f(C)) = g\left(\bigcap_{A \in B} F \setminus f(A) \right) \subset \bigcap_{A \in B} g(F \setminus f(A)).$$

La dernière inclusion a également été vue dans l'exercice 5 du TD2 dans le cas d'une intersection finie, et la même preuve marche pour une intersection quelconque. Or, par définition de B, pour tout $A \in B$,

$$g(F \setminus f(A)) \subset E \setminus A.$$

On en déduit que

$$g(F \setminus f(C)) \subset \bigcap_{A \in B} E \setminus A = E \setminus \bigcup_{A \in B} A = E \setminus C,$$

ce qui signifie que $C \in B$.

(*c*) Si $A \subset E$ vérifie l'inclusion : $g\left(F \setminus f(A)\right) \subset E \setminus A$,

alors $A \in B$ vu la définition de B. Donc $A \subset C$.

Montrons à présent que : $g\left(F \setminus f(C)\right) = E \setminus C$. Compte tenu de la question (*b*), il suffit de montrer que : $(E \setminus C) \setminus g\left(F \setminus f(C)\right) = \emptyset$.

On définit $D = \{x \in E \setminus C; x \notin g(F \setminus f(C))$ et $C' = C \cup D$, et on montre que (*voir figure 1 en fin de correction*) :

$$g(F \setminus f(C')) \subset E \setminus C'.$$

Soit $x \in g(F \setminus f(C'))$. Il existe donc $y \in F \setminus f(C')$ tel que $x = g(y)$. On a $y \notin f(C)$ et $y \notin f(D)$. Comme $y \in F \setminus f(C)$, on obtient que $x \in g(F \setminus f(C)) \subset E \setminus C$, c'est-à-dire que $x \notin C$.

Il reste donc à montrer que $x \notin D$. Comme $x \in E \setminus C$, cela revient à prouver que $x \in g(F \setminus f(C))$, ce qui est vrai car $x = g(y)$ et $y \in F \setminus f(C)$.

Ainsi, on a bien montré que $g(F \setminus C') \subset E \setminus C'$. Donc $C' \subset C$, vu le premier résultat démontré dans cette question. Par ailleurs, comme $C' = C \cup D$, il est clair que $C \subset C'$. D'où : $C' = C$, et $D = \emptyset$, ce qui montre bien l'égalité

$$g(F \setminus f(C)) = E \setminus C.$$

(d) Soit $x \in E \setminus C$. Comme $g(F \setminus f(C)) = E \setminus C$, il existe $y \in F \setminus f(C)$ tel que $g(y) = x$. A fortiori, $y \in F$. De plus, un tel y est unique car la fonction g est injective par hypothèse. Cela donne bien l'intégralité du résultat à démontrer.

(e) On remarque au préalable que, par sa construction, h vérifie les deux propriétes suivantes :

(1) La restriction de h à C est une bijection de C sur $f(C)$.

(2) La restriction de h à $E \setminus C$ est une bijection de $E \setminus C$ sur $F \setminus f(C)$.

Soit $y \in F$. On veut montrer qu'il existe un unique élément $x \in E$ tel que $h(x) = y$. On a 2 cas :

- Premier cas : $y \in f(C)$. Dans ce cas, comme f est bijective de C sur $f(C)$ (car f est injective par hypothèse), il existe un unique $x \in C$ tel que $f(x) = y$. Comme $x \in C$, on a donc aussi par définition de h sur C : $h(x) = y$. Dans C, vu la définition de h sur C et vu que f est injective, x est l'unique élément de C ayant y comme image par h.

Par ailleurs, pour $z \in E \setminus C$, on sait, vu la définition de h et vu que g est une bijection de $F \setminus f(C)$ sur $E \setminus C$, que $h(z) \in F \setminus f(C)$. Donc $h(z) \notin f(C)$, en particulier $h(z) \neq y$.

Ainsi, pour $y \in f(C)$, il existe un unique $x \in E$ (et on sait même que $x \in C$) tel que : $h(x) = y$

- Second cas : $y \in F \setminus f(C)$. Pour tout $x \in C$, $h(x) \in f(C)$. Donc, le ou les antécédents de y ne peuvent se trouver que dans $E \setminus C$. Comme on l'a déjà remarqué en (2), la restriction de h sur $E \setminus C$ est une bijection de $E \setminus C$ sur $F \setminus f(C)$. Donc, y a, par la fonction h, un unique antécédent et il appartient à $F \setminus f(C)$.

Ainsi tout $y \in F$ a un unique antécédent dans E par la fonction h. Donc h est une bjection de E sur F.

(f) Cas fini :

Le fait qu'il existe une injection de E dans F implique que : $card(E) \leq card(F)$.

Le fait qu'il existe une injection de F dans E implique que : $card(F) \leq card(E)$.

Par conséquent : $card(F) = card(E)$, ce qui implique qu'il existe une bijection de E sur F.

Exercice 2

(*a*) Soit n un entier impair. Il existe donc un entier k tel que $n = 2k + 1$. Par suite, $3n = 6k + 3$ est impair aussi.

On montre par récurrence sur k que, pour tout $k \in \mathbb{N}$, 3^k est impair. C'est vrai pour $k = 0$, car $3^0 = 1$. Si, pour un entier $k \in \mathbb{N}$, 3^k est impair, alors $3^{k+1} = 3 \times 3^k$ est impair aussi. On obtient bien que pour tout $k \in \mathbb{N}$, 3^k est impair.

(*b*) Soient (n, m) et (n', m') deux couples d'entiers tels que $f(n, m) = f(n', m')$, ce qui signifie que $2^{n-n'} = 3^{m'-m}$. On pose $l = n - n'$ et $k = m' - m$.

Supposons $l \geq 0$. On a donc $3^k = 2^l \geq 1$, donc $k \geq 0$. La question (*a*) montre que 3^k est impair. Comme, pour tout $l \in \mathbb{N}^*$, 2^l est pair, on a nécessairement $l = 0$, donc $3^k = 1$, ce qui montre que $k = 0$. On a donc obtenu $n = n'$ et $m = m'$.

Si maintenant $l \leq 0$, on écrit que $3^{-k} = 2^{-l}$. Comme $-l \geq 0$, le raisonnement précédent montre que $l = k = 0$, c'est-à-dire que $n = n'$ et $m = m'$.

Ainsi, f est injective.

(*c*) Soit $A = f(\mathbb{N} \times \mathbb{N})$. La fonction f est une bijection de $\mathbb{N} \times \mathbb{N}$ sur A, car on a vu qu'elle est injective (question (*b*)) et, par définition de A, f est une surjection de $\mathbb{N} \times \mathbb{N}$ sur A. Comme l'ensemble $\mathbb{N} \times \mathbb{N}$ est infini, l'ensemble A est infini également. Comme A est une partie infinie de $\mathbb{N}$, A est dénombrable. On a donc construit une bijection de $\mathbb{N} \times \mathbb{N}$ sur un ensemble dénombrable, ce qui montre que $\mathbb{N} \times \mathbb{N}$ est dénombrable.

(*d*) Soient maintenant E et F deux ensembles dénombrables. Il existe donc une bijection f de $\mathbb{N}$ sur E et une bijection g de $\mathbb{N}$ sur F. Pour tout $(n, m) \in \mathbb{N} \times \mathbb{N}$, on définit

$$h((n, m)) = (f(n), g(m)).$$

L'application h est une bijection de $\mathbb{N} \times \mathbb{N}$ sur $E \times F$. Sa bijection réciproque est donnée par

$$h^{-1}((x, y)) = (f^{-1}(x), g^{-1}(y))$$

pour tout $(x, y) \in E \times F$. Ainsi, $E \times F$ est dénombrable.

(*e*) On montre par récurrence sur $n \in \mathbb{N}^*$ que, pour tout $n \in \mathbb{N}^*$, pour tous ensembles dénombrables $E_1, ..., E_n$, $E_1 \times ... \times E_n$ est dénombrable.

C'est immédiat pour $n = 1$. On suppose que c'est vrai pour un entier $n \geq 1$. Soient $E_1, ..., E_{n+1}$ des ensembles dénombrables. Par hypothèse de récurrence, $E_1 \times ... \times E_n$ est dénombrable. Soit donc f une bijection de $E_1 \times ... \times E_n$ sur $\mathbb{N}$, et g une bijection de E_{n+1} sur $\mathbb{N}$. Pour tout élément $(x_1, ..., x_{n+1}) \in E_1 \times ...E_{n+1}$, on définit

$$h((x_1, ..., x_{n+1})) = (f((x_1, ..., x_n)), g(x_{n+1})).$$

On vérifie facilement que h est une bijection de $E_1 \times ...E_{n+1}$ sur $\mathbb{N}\times\mathbb{N}$. De plus, on a vu à la question (c) que $\mathbb{N} \times \mathbb{N}$ est dénombrable, soit donc ϕ une bijection de $\mathbb{N} \times \mathbb{N}$ sur $\mathbb{N}$. Alors, l'application $\phi \circ h$ est une bijection de $E_1 \times ...E_{n+1}$ sur $\mathbb{N}$. On a donc bien montré que $E_1 \times ...E_{n+1}$ est dénombrable, ce qui termine la démonstration.

(f) Pour tout couple $(n, m) \in \mathbb{N} \times \mathbb{N}$, on définit

$$\phi((n, m)) = \phi_n(m).$$

L'application ϕ est une surjection de $\mathbb{N}\times\mathbb{N}$ sur E. En effet, si $x \in E$, il existe $n \in \mathbb{N}$ tel que $x \in E_n$. Comme ϕ_n est une bijection de $\mathbb{N}$ sur E_n, il existe $m \in \mathbb{N}$ tel que $x = \phi_n(m)$. Ainsi, $x = \phi((n, m))$.

A tout $x \in E$, on peut donc associer un couple $(n, m) \in \mathbb{N} \times \mathbb{N}$ tel que $x = \phi((n, m))$. On définit ainsi une application h de E dans $\mathbb{N} \times \mathbb{N}$. Or h est injective. En effet, soient x et x' dans E tels que $h(x) = h(x') = (n, m)$. On a

$$x = \phi((n, m)) = x'.$$

Il existe donc une application injective h de E dans $\mathbb{N} \times \mathbb{N}$. En raisonnant comme à la question (c), on conclut que E est dénombrable.

Remarque: Un produit dénombrables d'ensembles finis n'est pas dénombrable en général. Ainsi, on montre que $\{0, 1\}^{\mathbb{N}}$ est en bijection avec $\mathcal{P}(\mathbb{N})$, qui n'est pas en bijection avec $\mathbb{N}$ (cf. TD2, exercice 7). Pour mettre en bijection $\mathcal{P}(\mathbb{N})$ avec $\{0, 1\}^{\mathbb{N}}$, on associe à toute partie A de $\mathbb{N}$ la suite $(u_n)_{n\in\mathbb{N}}$ qui vaut 1 si $n \in A$ et 0 si $n \notin A$.

8. Devoir n^0 2 - Enoncé

Exercice 1 - Soient X et Y deux ensembles. On note $\mathcal{E}$ l'ensemble des fonctions dont le domaine de définition est une partie quelconque de X et dont le domaine des valeurs est Y. Pour toute fonction $f \in \mathcal{E}$, on notera D_f le domaine de définition de f.

Sur $\mathcal{E}$ on définit la relation $\lhd$ par : $f \lhd g$ si, et seulement si, $D_f \subset D_g$ et $\forall x \in D_f,\ g(x) = f(x)$.

(*a*) $\lhd$ est-elle une relation d'ordre ? Si oui, est-elle totale ?

(*b*) Quels sont les éléments maximaux de $\mathcal{E}$ pour cette relation?

Exercice 2 - On considère $A = [0,1]$ et $B =]0,1]$. On munit $\mathbb{R}^2$ de l'ordre lexicographiqe, noté $\lhd$ et défini par : pour tous couples (a,b) et (a',b') de $\mathbb{R}^2$, $(a,b) \lhd (a',b') \iff \begin{cases} a \neq a' \text{ et } a \leq a' \\ \text{ou} \\ a = a' \text{ et } b \leq b' \end{cases}$

Dans $(\mathbb{R}^2, \lhd)$, montrez que toute partie non vide de $A \times A$ admet une borne supérieure. Est-ce que $A \times B$ possède la même propriété ?

Exercice 3 - Soit $n \in \mathbb{N}^*$ et $E = \{1, \ldots, n\}$.

(*a*) Combien y a-t-il de lois de composition interne sur E ?

(*b*) Combien y a-t-il de couples (i,j) avec $i \in E$, $j \in E$ et $i \leq j$?

(*c*) Combien y a-t-il de lois de composition interne commutatives sur E ? On utilisera la question (*b*).

Exercice 4 - Soient E et F deux ensembles. On fixe $f : E \to F$ une fonction quelconque. On veut montrer que f peut se décomposer de la manière suivante : $f = i \circ \overline{f} \circ s$ avec i une injection, $\overline{f}$ une bijection et s une surjection.

De plus, on définit sur E la relation $\mathcal{R}$ par : $\forall (x,x') \in \mathbb{R}^2,\ (x,x') \in \mathcal{R} \iff f(x) = f(x')$.

(*a*) Montrez que $\mathcal{R}$ est une relation d'équivalence.

(*b*) Soit $s : E \to E/\mathcal{R}$, la fonction définie par : $\forall x \in E, s(x) = \overline{x} = \{x' \in E;\ (x;x') \in \mathcal{R}\}$ = la classe de x suivant $\mathcal{R}$.

Montrez que s est bien une fonction surjective.

(*c*) On définit $\overline{f} : E/\mathcal{R} \to f(E)$ par $\forall \overline{x} \in E/\mathcal{R},\ \overline{f}(\overline{x}) = f(x)$

Vérifiez que $\overline{f}$ est bien définie (i.e. que la valeur de $\overline{f}(\overline{x})$ ne dépend pas du représentant choisi) et que $\overline{f}$ est bijective.

(*d*) Soit i la fonction de $f(E)$ dans F définie par : $\forall y \in f(E), i(y) = y$.

Montrez que i est injective. (i est appelée l'injection canonique de $f(E)$ dans F.

(*e*) Vérifiez qu'on a : $f = i \circ \overline{f} \circ s$ avec i une injection, $\overline{f}$ une bijection et s une surjection.

9. Devoir n^0 3 - Enoncé et corrigé

Exercice 1

(*a*) L'ensemble $f(A)$ est une partie non vide de $\mathbb{R}$ et majorée par hypothèse. Elle possède donc une borne supérieure. On raisonne de même pour $f(B)$.

(*b*) Soit $x \in A$. Alors $f(x) \leq \sup_A f$ et $g(x) \leq \sup_A g$. Donc $f(x)+g(x) \leq \left(\sup_A f\right) + \left(\sup_A g\right)$, ce qui montre que l'ensemble $(f+g)(A)$ est majoré par $\left(\sup_A f\right) + \left(\sup_A g\right)$.

On en déduit que $(f+g)(A)$ est une partie non vide majorée de $\mathbb{R}$. Elle admet donc une borne supérieure, qui est inférieure ou égale à n'importe lequel de ses majorants , donc à $\left(\sup_A f\right) + \left(\sup_A g\right)$.

(*c*) Soit $x \in A$. Alors $f(x) \leq \sup_A f$ et $g(x) \leq \sup_A g$. Donc, comme $f(x) \geq 0$ et $g(x) \geq 0$, $f(x)g(x) \leq \left(\sup_A f\right)\left(\sup_A g\right)$, ce qui montre que l'ensemble $(fg)(A)$ est majoré par $\left(\sup_A f\right)\left(\sup_A g\right)$. On conclut comme pour la question précédente.

(*d*) On pose $f(x) = x$ et $g(x) = 1-x$. Alors f et g sont positives sur $[0,1]$ et elles sont majorées par 1. On a

$$\sup_{[0,1]} f = 1, \ \sup_{[0,1]} g = 1.$$

De plus, pour tout $x \in [0,1]$, $f(x)+g(x) = 1$, donc

$$\sup_{[0,1]}(f+g) = 1 < \left(\sup_{[0,1]} f\right) + \left(\sup_{[0,1]} g\right).$$

De plus, $f(x)g(x) = x(1-x) \leq \dfrac{1}{4}$ pour tout $x \in [0,1]$. Comme $f\left(\dfrac{1}{2}\right) g\left(\dfrac{1}{2}\right) = \dfrac{1}{4}$, on a

$$\sup_{[0,1]}(fg) = \frac{1}{4} < \left(\sup_{[0,1]} f\right)\left(\sup_{[0,1]} g\right).$$

(*e*) Si $f(x) = g(x) = -\dfrac{1}{x}$ pour tout $x \in]0,1]$, f et g sont majorées par 0 sur $]0,1]$, et $f(x)g(x) = \dfrac{1}{x^2}$, qui n'est pas majorée sur $]0,1]$. En effet, si $A > 0$, on a

$$f\left(\frac{1}{2\sqrt{A}}\right) g\left(\frac{1}{2\sqrt{A}}\right) = 2A > A.$$

Or, si $A > \dfrac{1}{4}$, $\dfrac{1}{2\sqrt{A}} \in]0,1]$, donc fg n'est pas majorée par A sur $]0,1]$. On en déduit que fg n'est pas majorée sur $]0,1]$.

Exercice 2

(*a*) L'ensemble A est une partie non vide de $\mathbb{R}$ (car $0 \in A$), et majorée par 1. Donc A possède une borne supérieure. Soit c cette borne supéreure.

(*b*) Si $f(c) > c$, alors comme f est croissante $f(f(c)) \geq f(c)$, donc $f(c) \in A$. Comme c est la borne supérieure de A, en particulier c'est un majorant de A, on a donc : $f(c) \leq c$, ce qui contredit $f(c) > c$. Cette hypothèse est donc absurde, et on a donc bien $f(c) \leq c$.

(*c*) Si $f(c) < c$: déjà, pour tout $d \in A$, on a : $d \leq c$ car c est un majorant de A

Par l'absurde, si $\forall d \in A$, $d \leq f(c)$, alors $f(c)$ est un majorant de A. Ceci et $f(c) < c$ apporte une contradiction au fait que c est le plus petit majorant de A (par définition de la borne supérieure d'un ensemble).

Ainsi, il existe $d \in A$ tel que $f(c) < d \leq c$.

Comme $c \geq d$ et f croissante, on a : $f(c) \geq f(d)$. De plus, $d \in A$ donc $f(d) \geq d$. Ainsi : $f(c) \geq f(d) \geq d$. En particulier : $f(c) \geq d$.

En résumé, on a montré que : si $f(c) < c$ alors il existait $d \in A$ tel que : $f(c) < d$ et on montrait alors que : $d \leq f(c)$. contradiction.

Ainsi $f(c) \geq c$. Comme à la question précédente on a montré que $f(c) \leq c$, on en déduit que : $f(c) = c$.

(*d*) On vérifie que la fonction $f : [0,1] \to \mathbb{R}$, définie par $f(x) = \frac{1}{2}x + \frac{1}{4}$ arrive bien dans $[0,1]$, est croissante sur $[0,1]$ et a bien un unique point fixe, de valeur $\frac{1}{2}$ car il est aisé de vérifier que l'équation $f(x) = x$ a pour unique solution $x = \frac{1}{2}$.

(*e*) On vérifie que la fonction $f : [0,1] \to \mathbb{R}$, définie par $f(x) = x$ arrive bien dans $[0,1]$, est croissante sur $[0,1]$ et a une infinité de points fixes (en fait tout $x \in [0,1]$ est point fixe de f).

(*f*) Il est aisé de vérifier que la fonction proposée par l'énoncé est bien décroissante sur $[0,1]$. Par ailleurs, f n'a pas de points fixes : en effet, pour $x = 0$, on a $f(0) = 1 \neq 0$, et pour $x \neq 0$, on a $f(x) = 0 \neq x$.

Exercice 3

(*a*) Vérifions que $Z(G)$ est un sous-groupe de G :

• Soit e l'élément neutre de G, $e \in Z(G)$ car $\forall y \in G, e * y = y * e = y$.

• Soient x_1 et x_2 deux éléments quelconques de $Z(G)$ alors on a : $x_1 * x_2 \in Z(G)$. En effet :

$\forall y \in G, (x_1 * x_2) * y = x_1 * (x_2 * y) = x_1 * (y * x_2)$ en utilisant successivement l'associativité de $*$ et le fait que $x_2 \in Z(G)$. D'où :

$\forall y \in G, (x_1 * x_2) * y = (x_1 * y) * x_2 = (y * x_1) * x_2 = y * (x_1 * x_2)$ en utilisant successivement l'associativité de $*$ et le fait que $x_2 \in Z(G)$. Donc $Z(G)$ est stable par $*$.

• Soient x un élément quelconque de $Z(G)$ alors on a : $x^{-1} \in Z(G)$. En effet, comme $x \in Z(G)$, on a :

$\forall y \in G, x*y = y*x$. D'où, par multiplication par x^{-1} à droite puis à gauche : $\forall y \in G, y*x^{-1} = x^{-1}*y$. Donc $Z(G)$ est stable par passage à l'inverse.

Ainsi, on a montré que $Z(G)$ est un sous-groupe de G.

(*b*) Soit $\sigma \in Z(\mathcal{S}_n)$. Supposons qu'il existe $i \in \{1, \dots n\}$ tel que $\sigma(i) \neq i$. Soit $j \in \{1, \dots n\}$ tel que $j \neq i$ (un tel j existe car $n \geq 2$).

Comme $\sigma \in Z(\mathcal{S}_n)$, σ commute en particulier avec $\tau_{i,j}$, c'est-à-dire :

$\sigma \circ \tau_{i,j} = \tau_{i,j} \circ \sigma$. On a, en appliquant la dernière égalité au point i : $\sigma \circ \tau_{i,j}(i) = \tau_{i,j} \circ \sigma(i)$. Soit :

$\sigma(j) = \tau_{i,j}(\sigma(i))$

Or, vu cette dernière égalité, comme $\sigma(i) \neq \sigma(j)$ car σ est une bijection, et comme τ laisse invariants tous les points de $\{1, \dots n\}$ sauf i et j, on obtient que : $\sigma(i) \in \{i, j\}$. Or, par hypothèse $\sigma(i) \neq i$, donc : $\sigma(i) = j$. Ceci est valable pour tout $j \neq i$.

(*c*) • Soit $\sigma \in Z(\mathcal{S}_n)$ (avec $n \geq 3$).

Par l'absurde, s'il existe $i \in \{1, \dots n\}$ tel que $\sigma(i) \neq i$. Comme $n \geq 3$, on peut prendre j et k , deux points de $\{1, \dots n\}$, tous deux différents de i et différents entre eux. Vu le résultat de la question précédente, on a : $\sigma(i) = j$ et $\sigma(i) = k$. Ceci et $j \neq k$ apporte une contradiction avec le fait que σ est une fonction.

Ainsi, $\forall i \in \{1, \dots n\}$, $\sigma(i) = i$. Donc, $\sigma = Id$.

Conclusion : Pour $n \geq 3$, $Z(\mathcal{S}_n) = \{Id\}$.

(*d*) • Pour $Z(\mathcal{S}_1)$, on sait que $\mathcal{S}_1 = \{Id\}$. Ainsi, comme $Id \in Z(\mathcal{S}_1)$ car $Z(\mathcal{S}_1)$ est un sous-groupe, on a : $Z(\mathcal{S}_1) = \mathcal{S}_1 = Id$.

• Pour $Z(\mathcal{S}_2)$, on sait que $\mathcal{S}_1 = \{Id, \tau_{1,2}\}$. Or, $Id \in Z(\mathcal{S}_2)$ car $Z(\mathcal{S}_2)$ est un sous-groupe, et $\tau_{1,2} \in Z(\mathcal{S}_2)$ car $\tau_{1,2}$ commute avec tous les éléments de $Z(\mathcal{S}_2)$ (i.e. Id et lui-même). Donc, on a : $Z(\mathcal{S}_2) = \mathcal{S}_2 = \{Id, \tau_{1,2}\}$.

10. Devoir n^0 4 - Enoncé et corrigé

Exercice 1

1. Soient $\alpha \in \mathbb{C}^*$ et $\beta \in \mathbb{C}$. Si $z, z' \in \mathbb{C}$,
$$\phi_{\alpha,\beta}(z) = z' \Leftrightarrow z = \frac{1}{\alpha}(z' - \beta) \Leftrightarrow \phi_{\frac{1}{\alpha},-\frac{\beta}{\alpha}}(z') = z.$$
Cela montre que $\phi_{\alpha,\beta}$ est une bijection de $\mathbb{C}$ sur $\mathbb{C}$, et que sa réciproque est $\phi_{\frac{1}{\alpha},-\frac{\beta}{\alpha}}$.

   On vérifie alors que G est un sous-groupe du groupe des bijections de $\mathbb{C}$ sur $\mathbb{C}$. En effet, $\mathrm{Id} = \phi_{1,0} \in G$. Si $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$ avec $\alpha \neq 0$, $\alpha' \neq 0$, alors
$$\phi_{\alpha,\beta} \circ \phi_{\alpha',\beta'} = \phi_{\alpha\alpha',\alpha\beta'+\beta} \in G.$$
Enfin, on a vu que, si $\alpha \in \mathbb{C}^*$ et $\beta \in \mathbb{C}$,
$$\phi_{\alpha,\beta}^{-1} = \phi_{\frac{1}{\alpha},-\frac{\beta}{\alpha}} \in G.$$
2. On vérifie que $\mathrm{Id} = \phi_{1,0} \in H$. Si $|\alpha| = |\alpha'| = 1$, alors
$$\phi_{\alpha,0} \circ \phi_{\alpha',0} = \phi_{\alpha\alpha',0} \in H,$$
car $|\alpha\alpha'| = 1$. Enfin, si $|\alpha| = 1$,
$$\phi_{\alpha,0}^{-1} = \phi_{\frac{1}{\alpha},0} \in H,$$
car $\left|\frac{1}{\alpha}\right| = 1$. Ainsi, H est un sous-groupe de G.
3. Soit α un nombre complexe de module 1 et $n \in \mathbb{N}^*$. Alors
$$\phi_{\alpha,0}^{(n)} = \phi_{\alpha^n,0},$$
où $\phi_{\alpha,0}^{(n)}$ désigne la composée de $\phi_{\alpha,0}$ avec elle-même n fois. Donc, $\phi_{\alpha,0}$ est d'ordre n si, et seulement si, $\alpha^n = 1$. Les éléments $\phi_{\alpha,0}$ d'ordre fini sont donc ceux pour lesquels il existe $n \in \mathbb{N}^*$ tel que $\alpha^n = 1$.

   Si $\alpha = e^{i\theta}$ avec $\theta \in [0, 2\pi[$ et $n \in \mathbb{N}^*$, alors
$$\alpha^n = 1 \Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } n\theta = 2k\pi.$$
Ainsi, $\phi_{\alpha,0}$ est d'ordre fini si, et seulement si, il existe $k \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ tels que
$$\theta = \frac{2k\pi}{n},$$
c'est-à-dire qu'il existe $r \in \mathbb{Q}$ tel que $\theta = r\pi$.

   Si $\alpha = e^{i\theta}$, la fonction $\phi_{\alpha,0}$ représente la rotation d'angle θ et de centre 0 (ce qui signifie que, si $z = x + iy$ avec $x \in \mathbb{R}$ et $y \in \mathbb{R}$, et si $\phi_{\alpha,0}(z) = x' + iy'$ avec $x' \in \mathbb{R}$ et $y' \in \mathbb{R}$, le point M de coordonnées (x, y) a pour image le point M' de coordonnées (x', y') par la rotation de centre 0 et d'angle θ). Les éléments de H d'ordre fini correspondent aux rotations de centre 0 et d'angle $r\pi$ avec $r \in \mathbb{Q}$.

Exercice 2

1. • On a par définition de $\mathcal{R}$: $x\mathcal{R}y \Leftrightarrow \phi(xy^{-1}) = e'$. Comme ϕ est un morphisme de groupe, ceci équivaut à : $\phi(x) \star \phi(y)^{-1} = e'$, c'est-à-dire : $\phi(x) = \phi(y)$.

   Ainsi : $x\mathcal{R}y \Leftrightarrow \phi(x) = \phi(y)$. (1)

   • $\mathcal{R}$ est bien une relation d'équivalence car $\mathcal{R}$ est :

   - réflexive : pour tout $x \in G$ il est trivial que $\phi(x) = \phi(x)$ et, vu (1), ceci équivaut à : $x\mathcal{R}x$.

   - symétrique : car en utilisant (1) on a, pour tout $(x, y) \in G \times G$: $x\mathcal{R}y \Leftrightarrow \phi(x) = \phi(y) \Leftrightarrow \phi(y) = \phi(x) \Leftrightarrow y\mathcal{R}x$.

   - transitive : car , soit $(x, y, z) \in G \times G \times G$, si on suppose que $x\mathcal{R}y$ et $y\mathcal{R}z$ alors on a : $\phi(x) = \phi(y)$ et $\phi(y) = \phi(z)$, donc $\phi(x) = \phi(z)$, c'est-à-dire : $x\mathcal{R}z$.

2. Soient $(x, y) \in G \times G$ et $(x', y') \in G \times G$ tels que $x\mathcal{R}y$ et $x'\mathcal{R}y'$. Vu la relation (1), on a donc : $\phi(x) = \phi(y)$ et $\phi(x') = \phi(y')$. Par conséquent, on obtient : $\phi(x.x') = \phi(x) \star \phi(x') = \phi(y) \star \phi(y') = \phi(y.y')$. Donc, vu (1), on a : $(x.x')\mathcal{R}(y.y')$.

   Ainsi, la loi . est bien compatible avec la relation d'équivalence $\mathcal{R}$.

   On peut donc munir $G/\mathcal{R}$ d'une loi quotient (notée elle aussi .) définie par : $\forall(\overline{x}, \overline{y}) \in (G/\mathcal{R}) \times (G/\mathcal{R})$, $\overline{x}.\overline{y} = \overline{x.y}$ (dans cette dernière égalité on remarquera que . est, dans le membre de gauche, la loi quotient sur $G/\mathcal{R}$ et, dans le membre de droite, la loi initiale sur G).

   On montre alors aisément que $G/\mathcal{R}$ muni de la loi quotient . est un groupe : on laisse ici le soin au lecteur de vérifier que $\overline{e}$ est l' élément neutre de $(G/\mathcal{R}, .)$, que la loi quotient . est associative, et que pour cette loi tout élément $\overline{x}$ de $G/\mathcal{R}$ a un inverse, égal à $\overline{x^{-1}}$.

3. • s est une surjection : en effet, soit $w \in G/\mathcal{R}$. Dans la classe w prenons un représentant x (i.e. soit $x \in w$). On sait que : $\overline{x} = w$. Donc, par définition de s, on a : $s(x) = w$. Donc s est surjective.

   • s est un morphisme de groupe : en effet, soit $(x, y) \in G \times G$, on a : $s(x.y) = \overline{x.y}$. De plus, vu la conclusion de la question (2), on a, par définition de la loi quotient : $\overline{x.y} = \overline{x}.\overline{y}$.

   D'où : $s(x.y) = \overline{x}.\overline{y} = s(x).s(y)$.

   Ainsi, s est bien un morphisme de groupe de $(G, .)$ dans $(G/\mathcal{R}, .)$.

4. • On a le résultat général suivant : l'image de G par un morphisme de groupe de G dans G' est un sous-groupe de G'. Donc $\phi(G)$ est un sous-groupe de $(G', \star)$.

   [[On peut aussi démontrer ce dernier résultat explicitement :

   - $e' \in \phi(G)$ car $\phi(e) = e'$.

   - soit $(x', y') \in \phi(G) \times \phi(G)$, donc il existe x et y dans G tels que : $\phi(x) = x'$ et $\phi(y) = y'$. On a alors : $x' \star y'^{-1} = \phi(x) \star \phi(y)^{-1} = \phi(x.y^{-1}) \in \phi(G)$.

   Donc $\phi(G)$ est un sous-groupe de $(G', \star)$.]]

   [[*les deux points qui suivent ont déjà été vus lors du Devoir 2 Exercice 4 Question c)]]

   • Montrons d'abord que $\overline{\phi}$ est bien définie :

Soit $\overline{x}$ un élément quelconque de $G/\mathcal{R}$, soit x_1 et x_2 deux représentants dans G de la classe $\overline{x}$.

La définition de $\overline{\phi}(\overline{x})$ en prenant x_1 comme représentant de $\overline{x}$ donne : $\overline{\phi}(\overline{x}) = \phi(x_1)$. Cette même définition en prenant x_2 comme représentant de $\overline{x}$ donne : $\overline{\phi}(\overline{x}) = \phi(x_2)$.

Pour montrer que la définition de $\overline{\phi}$ ne dépend pas du représentant choisi, il faut donc vérifier que $\phi(x_1) = \phi(x_2)$. Or, par hypothèse x_1 et x_2 sont dans la même classe d'équivalence modulo $\mathcal{R}$ (cette classe est $\overline{x}$), donc par définition de $\mathcal{R}$ on a : $\phi(x_1) = \phi(x_2)$. c.q.f.d.

• Montrons que $\overline{\phi}$ est bijective :

- $\overline{\phi}$ est injective : en effet, soit $\overline{x}$ et $\overline{z}$ deux éléments de $G/\mathcal{R}$. Si $\overline{\phi}(\overline{x}) = \overline{\phi}(\overline{z})$ alors, vu la définition de $\overline{\phi}$, on a : $\phi(x') = \phi(z')$ (avec x' un représentant de $\overline{x}$ et z' un représentant de $\overline{z}$). D'où, en appliquant (1) de la question 1 : $x'\mathcal{R}z'$. Ce qui signifie que x' et z' sont dans la même classe modulo $\mathcal{R}$, i.e. $\overline{x'} = \overline{z'}$. D'où : $\overline{x} = \overline{z}$.

- $\overline{\phi}$ est surjective : soit $y \in \phi(G)$, par définition de $\phi(G)$ on sait qu'il existe $x \in G$ tel que $\phi(x) = y$. Donc, par définition de $\overline{\phi}$, on a : $\overline{\phi}(\overline{x}) = \phi(x) = y$ avec $\overline{x} \in G/\mathcal{R}$.

• Montrons que $\overline{\phi}$ est un morphisme :

En effet, en utilisant la définition de la loi quotient puis la définition de $\overline{\phi}$, on a : $\overline{\phi}(\overline{x}.\overline{y}) = \overline{\phi}(\overline{x.y}) = \phi(x.y)$.

Comme ϕ est un morphisme, on a : $\phi(x.y) = \phi(x) \star \phi(y)$.

D'où, en utilisant à nouveau la définition de ϕ : $\overline{\phi}(\overline{x}.\overline{y}) = \phi(x) \star \phi(y) = \overline{\phi}(\overline{x}) \star \overline{\phi}(\overline{y})$. Donc $\overline{\phi}$ est un morphisme.

Conclusion : $\overline{\phi}$ est bien un isomorphisme de groupe de $G/\mathcal{R}$ sur $\phi(G)$.

5. Soit $x \in G$, en appliquant successivement la définition de s, de $\overline{\phi}$ et de i, on obtient : $i \circ \overline{\phi} \circ s(x) = i \circ \overline{\phi}(\overline{x}) = i \circ \phi(x) = \phi(x)$. D'où : $i \circ \overline{\phi} \circ s = \phi$.

Remarque : Ce dernier résultat montre que, quel quesoit ϕ un morphisme de groupe, il est possible de l'écrire comme la composée d'un morphisme injectif i, d'un isomorphisme $\overline{\phi}$, et d'un morphisme surjectif s.

6. • ϕ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathcal{U}_5, .)$:

En effet, $(\mathbb{Z}, +)$ et $(\mathcal{U}_5, .)$ sont bien des groupes. De plus, soit $(n, m) \in \mathbb{Z}^2$, on a : $\phi(n + m) = \omega^{n+m} = \omega^n.\omega^m = \phi(n).\phi(m)$ c.q.f.d.

• Déterminons le noyau de ϕ :

Par définition du noyau d'un morphisme de groupe, on a :

$\ker \phi = \{n \in \mathbb{Z}; \phi(n) = 1\}$

Or $\phi(n) = 1 \Leftrightarrow \omega^n = 1 \Leftrightarrow e^{\frac{2in\pi}{5}} = 1 \Leftrightarrow \exists k \in \mathbb{Z}$ tel que : $\dfrac{2n\pi}{5} = 2k\pi \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $n = 5k$.

Ainsi : $\ker \phi = \{n \in \mathbb{Z}; \exists k \in \mathbb{Z}$ tel que $n = 5k\} = 5\mathbb{Z}$.

• Montrons que $(\mathbb{Z}/5\mathbb{Z}, +)$ et $(\mathcal{U}_5, .)$ sont isomorphes :

En appliquant les résultats des questions précédentes à ϕ, on sait qu'il existe un isomorphisme de groupe $\overline{\phi}$ de $(\mathbb{Z}/\mathcal{R}, +)$ dans $(\phi(\mathbb{Z}), .)$, en notant $\mathcal{R}$ la relation d'équivalence définie par : $\forall (n, m) \in \mathbb{Z}^2$, $n\mathcal{R}m \Leftrightarrow n - m \in \ker \phi = 5\mathbb{Z}$.

Ainsi, $n\mathcal{R}m \Leftrightarrow 5/(n - m) \Leftrightarrow n = m[5]$. Donc, $(\mathbb{Z}/\mathcal{R}, +) = (\mathbb{Z}/5\mathbb{Z}, +)$ car ces deux groupes sont obtenus en quotientant le groupe $(\mathbb{Z}, +)$ par la même relation d'équivalence.

Par ailleurs, $\phi(\mathbb{Z}) = \mathcal{U}_5$ (ce qui revient à dire que ϕ est surjective). En effet, il est connu que $\mathcal{U}_5 = \{1, \omega, \omega^2, \omega^3, \omega^4\}$, et on a, pour $i = \{0, 1, 2, 3, 4\}$: $\phi(i) = \omega^i$.

Ainsi, on vient de montrer que : $(\phi(\mathbb{Z}), +) = (\mathcal{U}_5, .)$ et $(\mathbb{Z}/\mathcal{R}, +) = (\mathbb{Z}/5\mathbb{Z}, +)$. Par ailleurs, comme $(\mathbb{Z}/\mathcal{R}, +)$ et $(\phi(\mathbb{Z}), .)$ sont isomorphes, il est équivalent de dire que : $(\mathbb{Z}/5\mathbb{Z}, +)$ et $(\mathcal{U}_5, .)$ sont isomorphes.

11. Devoir n^o 5 - Enoncé

Exercice 1 - Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans $\mathbb{Z}$. On suppose que

$$\lim_{n\to+\infty} u_n = l \in \mathbb{R}.$$

Montrer que $l \in \mathbb{Z}$ (raisonner par l'absurde).

Exercice 2 - Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels positifs ou nuls qui ne tend pas vers $+\infty$.

(*a*) Montrer qu'on peut extraire de $(u_n)_{n\in\mathbb{N}}$ une suite bornée.

(*b*) En déduire qu'on peut extraire de $(u_n)_{n\in\mathbb{N}}$ une suite convergente.

Exercice 3 - Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites à termes dans $\mathbb{N}^*$, et vérifiant : $\lim_{n\to+\infty} \frac{a_n}{b_n} = \sqrt{2}$. On veut prouver que $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ tendent vers $+\infty$ quand $n \to +\infty$. Pour cela, on raisonne par l'absurde et on suppose que $(b_n)_{n\in\mathbb{N}}$ ne tend pas vers $+\infty$.

(*a*) Montrer qu'on peut extraire de $(b_n)_{n\in\mathbb{N}}$ une suite convergente (appliquer l'exercice 2), qu'on notera $(b_{\phi(n)})_{n\in\mathbb{N}}$. On notera b la limite de $(b_{\phi(n)})_{n\in\mathbb{N}}$.

(*b*) Montrer que $(a_{\phi(n)})_{n\in\mathbb{N}}$ est convergente, soit a sa limite.

(*c*) Montrer que a et b sont des entiers (voir l'exercice 1), aboutir à une contradiction.

(*d*) Conclure.

Exercice 4 - *Polynômes Cyclotomiques*

Soient $n \in \mathbb{N}^*$ et $\xi \in \mathbb{C}$ une racine $n^{ème}$ de 1 (ce qui veut dire que $\xi^n = 1$). On dit que est ξ est une racine primitive $n^{ème}$ de 1 si, et seulement si, le plus petit entier $k \geq 1$ tel que $\xi^k = 1$ est n. En d'autres termes, cela signifie que l'ordre de ξ dans le groupe $(\mathbb{C}^*, .)$ est n.

On note ξ_1, ...,ξ_k les racines primitives $n^{èmes}$ de 1 et Φ_n le polynôme :

$$\Phi_n = \prod_{i=1}^{k} (X - \xi_i).$$

1) Calculer Φ_1, Φ_2, Φ_3, Φ_4.

2) Montrer que Φ_n divise $X^n - 1$.

3) Soient A et B deux polynômes à coefficients dans $\mathbb{Q}$, on suppose qu'il existe un polynôme P à coefficients dans $\mathbb{C}$ tels que :

$$A = BP.$$

Montrer que P est un polynôme à coefficients dans $\mathbb{Q}$. On utilisera la division euclidienne.

4) Soit $k \in \{0, 1, \dots n-1\}$, montrer que $e^{\frac{2ik\pi}{n}}$ est racine primitive $n^{ème}$ de 1 si, et seulement si, k et n sont premiers entre eux.

5) Montrer que, pour tout entier n,

$$\prod_{d/n} \Phi_d = X^n - 1.$$

Le produit porte sur tous les entiers $d \in \{1, \dots, n\}$ qui divisent n.

6) Montrer, par récurrence sur n, en utilisant les questions 3) et 5), que Φ_n est un polynôme à coefficients dans $\mathbb{Q}$.

[[On peut montrer, mais c'est plus difficile, que Φ_n est un polynôme à coefficients dans $\mathbb{Z}$]].

12. Interrogation écrite du 7 novembre 2001 - Enoncé et corrigé

Enoncé

Question de cours

(*a*) Soient E un ensemble, $\mathcal{R}$ une relation d'ordre sur E et $A \subset E$. Rappeler la définition de la borne supérieure de A dans E.

(*b*) Dans cette question, $E = \mathbb{N} \setminus \{0\}$ et $\mathcal{R}$ est définie par:

$$\forall (n,m) \in \mathbb{N}^2,\ (n,m) \in \mathcal{R} \Leftrightarrow n \text{ divise } m.$$

Soit $A = \{2,3,4\}$. Déterminer la borne supérieure de A dans E.

Exercice 1

On définit la fonction f de $\mathbb{Z}$ dans $\mathbb{N}$ de la manière suivante:

$$f(n) = \begin{cases} 2n-1 & \text{si } n \geq 1 \\ -2n & \text{si } n \leq -1 \\ 0 & \text{si } n = 0. \end{cases}$$

(*a*) Montrer que f est injective.

(*b*) Prouver que f est surjective.

(*c*) En déduire que $\mathbb{Z}$ est dénombrable.

Exercice 2

On note E l'ensemble des fonctions de $\mathbb{N}$ dans $\{0,1\}$. Pour toute partie A de $\mathbb{N}$, on note χ_A la fonction caractéristique de A, c'est-à-dire la fonction de $\mathbb{N}$ dans $\{0,1\}$ qui vaut 1 en tout point de A et 0 en tout point de $\mathbb{N} \setminus A$.

Enfin, on appelle ϕ la fonction de $\mathcal{P}(\mathbb{N})$ dans E donnée par

$$\phi(A) = \chi_A$$

pour tout $A \in \mathcal{P}(\mathbb{N})$.

(*a*) Montrer que ϕ est injective.

(*b*) Soit $f \in E$. Déterminer une partie A de $\mathbb{N}$ telle que $f = \chi_A$. En déduire que ϕ est surjective.

(*c*) Soit h une application de $\mathbb{N}$ dans $\mathcal{P}(\mathbb{N})$. En considérant

$$C = \{x \in \mathbb{N};\ x \notin h(x)\},$$

montrer que h n'est pas surjective.

(*d*) Déduire de ce qui précède que E n'est pas dénombrable.

Exercice 3

(*a*) Soit $n \in \mathbb{N}$. Combien y a-t-il de couples d'entiers $(a, b) \in \mathbb{N} \times \mathbb{N}$ tels que $a + b = n$?

(*b*) Soit $n \in \mathbb{N}$. Combien y a-t-il de triplets d'entiers $(a, b, c) \in \mathbb{N}^3$ tels que $a + b + c = n$? On utilisera la question (*a*).

(*c*) Soit $n \in \mathbb{N}$. Combien y a-t-il de triplets d'entiers $(a, b, c) \in \mathbb{N}^3$ tels que $a + b + c \leq n$?

Corrigé

Question de cours

(*a*) Soit B l'ensemble des majorants de A dans E, c'est-à-dire

$$B = \{x \in E;\ \forall y \in A,\ y \leq x\}.$$

La borne supérieure de A dans E est le plus petit élément de B, si ce plus petit élément existe.

(*b*) Soit $n \in \mathbb{N} \setminus \{0\}$. Alors n est un majorant de A si, et seulement si, n est divisible par $2, 3$ et 4, c'est-à-dire n divisible par 12. La borne supérieure de A, c'est-à-dire le plus petit élément de l'ensemble des majorants de A dans $\mathbb{N} \setminus \{0\}$, est donc 12.

Exercice 1

(*a*) Soient n et m dans $\mathbb{Z}$ tels que $f(n) = f(m)$. On remarque que si $p \geq 1$, $f(p)$ est impair, alors que, si $p \leq 0$, $f(p)$ est pair. On a donc soit $n \geq 1$ et $m \geq 1$, soit $n \leq 0$ et $m \leq 0$. Dans le premier cas, $f(n) = 2n - 1$ et $f(m) = 2m - 1$, ce qui implique $m = n$. Dans le second cas, $f(n) = -2n$ et $f(m) = -2m$, ce qui implique encore $m = n$. Ainsi, f est injective.

(*b*) Soit $m \in \mathbb{N}$. Si m est pair, il existe $k \in \mathbb{N}$ tel que $m = 2k$, et on a donc $m = f(-k)$ puisque $-k \leq 0$. Si m est impair, il existe $k \in \mathbb{N}^*$ tel que $m = 2k - 1$, et on a donc $f(k) = m$. La fonction f est donc surjective.

(*c*) Les questions (*a*) et (*b*) montrent que f est une bijection de $\mathbb{Z}$ sur $\mathbb{N}$, ce qui signifie que $\mathbb{Z}$ est dénombrable.

Exercice 2

(*a*) Soient A et B des parties de $\mathbb{N}$ telles que $\phi(A) = \phi(B)$, c'est-à-dire $\chi_A = \chi_B$. Si $x \in A$, on a $\chi_A(x) = 1$, donc $\chi_B(x) = 1$, d'où $x \in B$. Ainsi, $A \subset B$. Symétriquement, on montre $B \subset A$. Finalement, $A = B$ et ϕ est injective.

(*b*) Soit $f \in E$. On définit

$$A = f^{-1}(\{1\}) = \{x \in \mathbb{N};\ f(x) = 1\}.$$

Alors $f = \chi_A$. En effet, soit $x \in \mathbb{N}$. Si $x \in A$, $f(x) = 1 = \chi_A(x)$. Si $x \notin A$, $f(x) \neq 1$, donc $f(x) = 0$ car $f \in E$, or $0 = \chi_A(x)$.

On en déduit que, pour toute $f \in E$, il existe $A \in \mathcal{P}(\mathbb{N})$ tel que $f = \chi_A = \phi(A)$, ce qui signifie que ϕ est surjective.

(*c*) On suppose qu'il existe $x \in \mathbb{N}$ tel que $h(x) = C$. Alors, si $x \in C$, la définition de C montre que $x \notin h(x)$, c'est-à-dire que $x \notin C$, ce qui est impossible. Si $x \notin C$, on a $x \in h(x) = C$, ce qui est impossible aussi. Il n'existe donc pas de $x \in \mathbb{N}$ tel que $h(x) = C$, ce qui montre que h n'est pas surjective.

(*d*) On suppose E dénombrable. Il existe donc une bijection ψ de E sur $\mathbb{N}$. Alors, comme ϕ est une bijection de $\mathcal{P}(\mathbb{N})$ sur E, $\psi \circ \phi$ est une bijection de $\mathcal{P}(\mathbb{N})$ sur $\mathbb{N}$. Or, d'après la question (*c*), une telle bijection n'existe pas. L'ensemble E n'est donc pas dénombrable.

Exercice 3

(*a*) On note

$$E = \{(a, b) \in \mathbb{N} \times \mathbb{N};\ a + b = n\}.$$

On définit une fonction f de E dans $\{0, ..., n\}$ par

$$f(a, b) = a.$$

On vérifie que f est bien à valeurs dans $\{0, ..., n\}$, car si $a + b = n$ avec $a \geq 0$ et $b \geq 0$, on a bien $a \in \{0, ..., n\}$. La fonction f est injective, car si $f(a, b) = f(a', b')$, on a $a = a'$, puis $b = n - a = n - a' = b'$. De plus, f est surjective, car si $k \in \{0, ..., n\}$, on pose $l = n - k$, on a bien $l \in \{0, ..., n\}$ et $f(k, l) = k$.

La fonction f est donc une bijection de E sur $\{0, ..., n\}$. Le cardinal de E est donc $n + 1$.

(*b*) On note

$$F = \left\{(a, b, c) \in \mathbb{N}^3;\ a + b + c = n\right\}.$$

Pour tout $k \in \{0, ..., n\}$, on définit

$$F_k = \left\{(a, b) \in \mathbb{N}^2;\ a + b = k\right\}.$$

On a alors

$$F = \bigcup_{k=0}^{n} (F_k \times \{n - k\}).$$

En effet, si $(a, b, c) \in F$, on pose $a + b = k$. Alors $k \in \{0, ..., n\}$ et $c = n - k$, donc $(a, b, c) \in F_k \times \{n - k\}$. Réciproquement, si $(a, b, c) \in F_k \times \{n - k\}$ pour un $k \in \{0, ..., n\}$, alors $(a, b, c) \in F$.

Or les ensembles F_k sont deux à deux disjoints et le cardinal de F_k est $k+1$, d'après la question (a). On en déduit que le cardinal de F est

$$\sum_{k=0}^{n} \text{card } F_k = \sum_{k=0}^{n}(k+1) = \sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}.$$

(c) On note

$$G = \left\{(a,b,c) \in \mathbb{N}^3;\ a+b+c \leq n\right\}$$

et, pour tout $k \in \{0,...,n\}$,

$$G_k = \left\{(a,b,c) \in \mathbb{N}^3;\ a+b+c = k\right\}.$$

Alors

$$G = \bigcup_{k=0}^{n} G_k,$$

et les G_k sont deux à deux disjoints. De plus, d'après la question (b), le cardinal de G_k est $\dfrac{(k+1)(k+2)}{2}$. On obtient donc que le cardinal de G est

$$\sum_{k=0}^{n} \text{card } G_k = \frac{1}{2}\sum_{k=0}^{n}(k+1)(k+2) = \frac{1}{2}\sum_{k=0}^{n}\left(k^2+3k+2\right).$$

Or

$$\sum_{k=0}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1).$$

Le cardinal de G est donc

$$\frac{1}{12}n(n+1)(2n+1) + \frac{3}{4}n(n+1) + (n+1) = \frac{n+1}{12}\left(2n^2+10n+12\right).$$

13. Interrogation écrite du Mardi 18 décembre 2001 - Enoncé

I

1 - Pour chaque entier $k \geq 1$ on note

$$u_k = \frac{(-1)^1}{1} + \frac{(-1)^2}{2} + \frac{(-1)^3}{3} + \cdots + \frac{(-1)^{2k-1}}{2k-1} \quad \text{et} \quad v_k = u_k + \frac{1}{2k}\cdot$$

Montrer que les suites $(u_k)_{k\geq 1}$ et $(v_k)_{k\geq 1}$ sont convergentes et ont la même limite.

II

On munit l'ensemble $A = \mathbb{Z} \times \mathbb{Z}$ des deux opérations

$$(a,b) + (a',b') = (a+a', b+b')$$

$$(a,b)(a',b') = (aa' + bb', ab' + a'b)$$

1 - Montrer que A est un anneau commutatif unitaire.

2 - Déterminer les éléments inversibles de A.

3 - Dans quel cas l'égalité $(a,b)(x,y) = (0,0)$ implique-t-elle $x = 0$ et $y = 0$?

14. Epreuve écrite du 16 janvier 2002 - Enoncé et corrigé

I

1 - Soit $(a_n)_{n\geq 1}$ une suite décroissante de réels qui converge vers 0.

a) Montrer que, pour chaque entier $n \geq 1$, on a $0 \leq a_n$.

Pour chaque entier $n \geq 1$ on note

$$x_n = (-1)^1 a_1 + (-1)^2 a_2 + (-1)^3 a_3 + \cdots + (-1)^{2n-1} a_{2n-1} \quad \text{et} \quad y_n = x_n + a_{2n}\,.$$

b) Quelle relation y a-t-il entre y_n et x_{n+1} ?

c) Montrer que les suites $(x_n)_{n\geq 1}$ et $(y_n)_{n\geq 1}$ sont convergentes et ont la même limite notée l. Montrer que, si p et q sont deux entiers ≥ 1, on a $x_p \leq l \leq y_q$.

2 - a) Montrer que, pour chaque entier $n \geq 1$, on a

$$\frac{1}{(n+1)^2} \leq \frac{1}{n} - \frac{1}{n+1}\,.$$

b) On pose, pour chaque entier $n \geq 1$,

$$z_n = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}\,.$$

Démontrer que, pour $1 \leq n < m$, on a

$$0 \leq z_m - z_n \leq \frac{1}{n} - \frac{1}{m}\,.$$

En déduire la convergence de la suite $(z_n)_{n\geq 1}$.

II

On cherche à résoudre dans $\mathbb{R}$ l'équation

$$x^3 - 3x - 1 = 0\,. \tag{1}$$

1 - Montrer que $x = u + v$ est solution de (1) si, et seulement si,

$$u^3 + v^3 + 3(u+v)(uv-1) - 1 = 0\,.$$

2 - On suppose que $x = u+v$ est une solution de (1) telle que $uv = 1$. Montrer que u^3 et v^3 sont solutions d'une équation du second degré que l'on précisera. 3 - Montrer que (1) possède deux solutions

III

On désigne par P le polynôme à coefficients réels $X^3 - 3X - 1$.

1 - Montrer que P possède trois racines réelles distinctes.

2 - Montrer qu'aucune des racines de P n'est rationnelle. [On pourra supposer qu'un nombre rationnel q écrit sous la forme $\frac{r}{s}$ avec r et s premiers entre-eux est racine de P et montrer que cela conduit à une contradiction]

3 - Montrer que P ne peut pas être écrit comme le produit de deux polynômes à coefficients rationnels de degré ≥ 1.

4 - Montrer que, si Q est un polynôme à coefficents rationnels qui n'est pas divisible par P, il existe $U, V \in \mathbb{Q}[X]$ tels que

$$UP + VQ = 1\,.$$

5 - Soit θ une racine de P. On note

$$A = \{\, x \in \mathbb{R}\,;\, \exists p, q, r \in \mathbb{Q} \text{ tels que } x = p + q\theta + r\theta^2 \,\}\,.$$

a) Montrer que A est un sous-anneau de $\mathbb{R}$.

b) Montrer que A est un corps. [On pourra utiliser 4 avec un polynôme Q judicieusement choisi]

Corrigé de l'épreuve écrite du 16 janvier 2002

I

1 - a) Supposons que, pour un entier N, on ait $a_N < 0$; alors, pour chaque entier $n \geq N$, on a $|a_n| \geq |a_N| > 0$ ce qui est contradictoire avec la convergence de la suite $(a_n)_n$ vers 0.

b) On a, pour chaque entier k,

$$(1) \qquad x_{k+1} - x_k = a_{2k} - a_{2k+1} \geq 0$$

$$(2) \qquad y_{k+1} - y_k = a_{2k+2} - a_{2k+1} \leq 0\,.$$

La relation (1) montre que la suite $(x_k)_k$ est croissante, la relation (2) montre que la suite $(y_k)_k$ est décroissante. On a visiblement, pour chaque entier k, $x_k \leq y_k$. Puisque la suite $(a_{2k})_k$ tend vers 0, les deux suites $(x_k)_k$ et $(y_k)_k$ sont adjacentes, elles convergent donc vers la même limite ℓ. De $\ell = \sup_p x_p = \inf_q y_q$ on déduit évidemment que $x_p \leq \ell \leq y_q$ pour chaque p et q.2 - a) La preuve est évidente.

b) Nous avons, pour $1 \leq n < m$, en utilisant a)

$$0 \leq z_m - z_n = \frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \cdots \frac{1}{m^2} \leq \left[\frac{1}{n} - \frac{1}{n+1}\right] + \left[\frac{1}{m-1} - \frac{1}{m}\right] = \frac{1}{n} - \frac{1}{m}\,.$$

Nous allons utiliser cette dernière relation pour montrer que la suite $(z_n)_{n\geq 1}$ est de Cauchy. Donnons-nous un réel $\varepsilon > 0$. Puisque la suite $\left(\frac{1}{k}\right)_{k\geq 1}$ tend vers 0 il existe un entier $N \geq 1$ tel $\frac{1}{N} \leq \varepsilon$. Pour deux entiers quelconques n, m vérifiant $N \leq n < m$ nous avons alors

$$0 \leq z_m - z_n \leq \frac{1}{n} - \frac{1}{m} \leq \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon$$

ce qui montre bien que a suite $(z_n)_{n\geq 1}$ est de Cauchy.

II

1 - En élevant $2\cos\theta = \mathrm{e}^{\imath\theta} + \mathrm{e}^{-\imath\theta}$ au cube et en utilisant la formule du binôme on obtient

$$8\cos^3\theta = \mathrm{e}^{3\imath\theta} + 3\mathrm{e}^{2\imath\theta}\mathrm{e}^{-\imath\theta} + 3\mathrm{e}^{\imath\theta}\mathrm{e}^{-2\imath\theta} + \mathrm{e}^{-3\imath\theta}$$

$$= 2\cos 3\theta + 6\cos\theta$$

d'où la formule demandée.

2 - Ecrivons les quotients et restes partiels

$$X^3 - 3X - 1 = X^2\left(X - 2\cos\frac{\pi}{9}\right) + 2\cos\frac{\pi}{9}X^2 - 3X - 1$$

$$2\cos\frac{\pi}{9}X^2 - 3X - 1 = 2\cos\frac{\pi}{9}X\left(X - 2\cos\frac{\pi}{9}\right) + \left(4\cos^2\frac{\pi}{9} - 3\right)X - 1$$

$$\left(4\cos^2\frac{\pi}{9} - 3\right)X - 1 = \left(4\cos^2\frac{\pi}{9} - 3\right)\left(X - 2\cos\frac{\pi}{9}\right) + 8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9} - 1$$

La formule (1) appliquée avec $\theta = \dfrac{\pi}{9}$ donne

$$8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9} - 1 = 0$$

donc

$$X^3 - 3X - 1 = \left[X^2 + 2\cos\frac{\pi}{9}X + \left(4\cos^2\frac{\pi}{9} - 3\right)\right]\left(X - 2\cos\frac{\pi}{9}\right)$$

ce qui montre que $2\cos\dfrac{\pi}{9}$ est racine de P.
En remplacant X par $2\cos\dfrac{\pi}{9}$ dans $X^2 + 2\cos\dfrac{\pi}{9}X + \left(4\cos^2\dfrac{\pi}{9} - 3\right)$ on obtient

$$12\cos^2\frac{\pi}{9} - 3 = 12\left(\cos^2\frac{\pi}{9} - \frac{1}{4}\right) = 12\left(\cos\frac{\pi}{9} - \frac{1}{2}\right)\left(\cos\frac{\pi}{9} + \frac{1}{2}\right) \neq 0$$

ce qui montre que $2\cos\dfrac{\pi}{9}$ est racine simple de P.

3 - Le discriminant réduit du trinôme $T = X^2 + 2\cos\dfrac{\pi}{9}X + \left(4\cos^2\dfrac{\pi}{9} - 3\right)$ égal à $3 - 3\cos^2\dfrac{\pi}{9}$ est > 0, il s'ensuit que T possède deux racines réelles distinctes; d'où le résultat demandé pour P.

4 - Montrons que P ne possède pas de racine entière. Supposons qu'un entier relatif n soit racine de P, il vérifie alors $n^3 - 3n = n(n^2 - 3) = 1$; il s'ensuit que n et $n^2 - 3$ sont inverses l'un de l'autre dans $\mathbb{Z}$; on a donc les relations $n = 1$ et $n^2 - 3 = 1$ ou $n = -1$ et $n^2 - 3 = -1$ qui sont toutes deux contradictoires.
Montrons que P ne possède pas de racine rationnelle. Supposons qu'un nombre rationnel q soit racine de P. Nous pouvons écrire $q = \pm\dfrac{r}{s}$ avec r et s deux entiers premiers entre eux. On obtient alors

$$\frac{r^3}{s^3} = 3\frac{r}{s} \pm 1$$

donc

$$r^3 = s^2(3r \pm s)\,.$$

Cette dernière relation montre que s divise r^3 ce qui est absurde car r et s sont premiers entre eux.

5 - Supposons qu'il existe un polynôme à coefficients rationnels R de degré égal à 1 ou 2 qui divise P. Alors tel que $P = RS$ est aussi à coefficients rationnels. En considérant les degrés respectifs, R ou S est de degré égal à 1. Le polynôme P possède donc une racine rationelle, ce qui est contradictoire avec la conclusion de la question précédente. Le polynôme P est donc irréductible sur $\mathbb{Q}$.

6 - Tout diviseur à coefficients rationnels de degré ≥ 1 de P étant associé à P ne peut donc pas diviser Q. P est Q sont premiers entre eux. Le théorème de Bezout pour les polynômes assure l'existence de $U, V \in \mathbb{Q}[X]$ tels que $UP + VQ = 1$.

7 - a) Nous démontrons l'affirmation par récurrence sur n. La propriété est évidente pour $n = 3$ car $\theta^3 = 3\theta + 1$; dans ce cas $R_3 = 3X + 1$. Soit $n \geq 3$ et supposons la propriété vraie pour n. Il existe alors $a_n, b_n, c_n \in \mathbb{Q}$ tels que $\theta^n = a_n + b_n\theta + c_n\theta^2$. En multipliant les deux membres par θ on obtient

$$\begin{aligned}\theta^{n+1} &= a_n\theta + b_n\theta^2 + c_n\theta^3 = a_n\theta + b_n\theta^2 + c_n(3\theta + 1)\\ &= c_n + (a_n + 3c_n)\theta + b_n\theta^2\,.\end{aligned}$$

On a donc $\theta^{n+1} = R_{n+1}(\theta)$ avec $R_{n+1} = b_nX^2 + (a_n + 3c_n)X + c_n$; on en déduit le résultat car $b_n, (a_n + 3c_n), c_n \in \mathbb{Q}$.

b) Il est clair que A contient 0, c'est donc un sous-ensemble non vide de $\mathbb{R}$. Vérifions que A est un sous-anneau de $\mathbb{R}$. Etant donnés $a = p + q\theta + r\theta^2, a' = p' + q'\theta + r'\theta^2$ avec $p, q, r, p', q', r' \in \mathbb{Q}$ nous avons $a - a' = (p - p') + (q - q')\theta + (r - r')\theta^2 \in A$ donc A est un sous-groupe du groupe commutatif $(\mathbb{R}, +)$. Nous avons aussi

$$aa' = pp' + (pq' + p'q)\theta + (pr' + qq' + p'r)\theta^2 + (qr' + q'r)\theta^3 + rr'\theta^4.$$

En utilisant la question précédente ou les relations $\theta^3 = 3\theta + 1$ et $\theta^4 = 3\theta^2 + \theta$ nous obtenons

$$aa' = pp' + qr' + q'r + (pq' + p'q + 3qr' + 3q'r + rr')\theta + (pr' + qq' + p'r + 3rr')\theta^2$$

ce qui montre que A est stable pour la multiplication.c) Soit $a = p + q\theta + r\theta^2$ un élément non nul de A. Nous allons montrer qu'il est inversible dans A. Les trois nombres rationnels p, q, r ne sont pas simultanément nuls. Le polynôme à coefficients rationnels $Q = rX^2 + qX + p$ n'étant pas divisible par P est premier avec lui. Soient U, V comme dans la question 6 tels que

$$U(\theta)P(\theta) + V(\theta)Q(\theta) = aV(\theta) = 1.$$

Nous savons, d'après a), que $V(\theta) \in A$. La multiplication étant commutative il est clair que $V(\theta)$ est l'inverse de a.

15. Epreuve écrite du 3 Septembre 2002

I

Soit $(G,.)$ un groupe dont l'élément neutre est noté e. On suppose qu'il existe une relation d'ordre sur G qui possède les propriétés suivantes :

$$\forall x,a,b\in G,\quad a\leq b\ \Rightarrow\begin{cases}a.x\leq b.x & (\alpha)\\ x.a\leq x.b & (\beta)\end{cases}$$

De plus, on note :

$$\begin{array}{rll} P & =\{\,x\in G\,;\,x\geq e\,\} & (\gamma)\\ P^{-1} & =\{\,x\in G\,;\,x^{-1}\geq e\,\} & (\delta)\\ P.P & =\{\,x\in G\,;\,\exists\,(y,z)\in P\times P\quad\text{tel que}\quad x=yz\,\} & (\varepsilon)\end{array}$$

1 - Montrer que : $a\leq b\ \Leftrightarrow\ b^{-1}\leq a^{-1}$.

2 - Montrer qu'on a les propriétés :

$$\begin{array}{ll} P.P\subset P & (1)\\ P\cap P^{-1}=\{e\} & (2)\\ \forall x\in G\,,\ x.P.x^{-1}\subset P & (3)\end{array}$$

3 - Réciproquement, soient G un groupe quelconque et P une partie de G vérifiant (1),(2),(3).

Montrer que la relation $\top$, définie par : $\forall(a,b)\in G\times G\,,\ a\top b\Leftrightarrow b.a^{-1}\in P$, est une relation d'ordre sur G vérifiant (α), (β), (γ).

II

Soit $(a_n)_{n\geq1}$ une suite d'éléments de $\mathbb{R}$, on définit les suites $(b_n)_{n\geq1}$ et $(c_n)_{n\geq1}$ par :

$$b_n=\frac{1}{n}(a_1+a_2+\cdots+a_n)\,,$$

$$c_n=\frac{1}{n^2}(a_1+2a_2+\cdots+na_n)$$

1 - Montrer que si la suite $(a_n)_{n\geq1}$ converge vers un réel λ alors la suite $(b_n)_{n\geq1}$ converge aussi vers λ.

2 - On veut montrer dans cette question que si la suite $(a_n)_{n\geq1}$ converge vers un réel λ alors $(c_n)_{n\geq1}$ est convergente vers $\dfrac{\lambda}{2}$.

a) Montrer que, pour tout $n\in\mathbb{N}\setminus\{0\}$, on a : $1+2+\cdots+n=\dfrac{n(n+1)}{2}$.

b) On suppose dans cette question que $\lambda=0$. Montrer que $\lim_{n\to\infty}c_n=0$

c) On revient pour toute la suite de l'exercice au cas général où λ est un réel quelconque.

On définit la suite $(d_n)_{n\geq1}$ par

$$d_n=\frac{\lambda}{n^2}(1+2+\cdots+n)\,.$$

Montrer que : $\lim_{n\to\infty}(c_n - d_n) = 0$. [On pourra pour cela utiliser le résultat de la question précédente appliqué à une suite appropriée]

d) En utilisant la question a) , montrer qu'on a $\lim_{n\to\infty} d_n = \dfrac{\lambda}{2}\cdot$

e) Déduire des questions précédentes que $\lim_{n\to\infty} c_n = \dfrac{\lambda}{2}\cdot$

III

Soit I un intervalle non réduit à un point et $f : I \to \mathbb{R}$ une application injective et continue sur I. On veut montrer dans cet exercice que f est strictement monotone.

Pour cela, on raisonne par l'absurde. On suppose donc qu'il existe $a, b, x, y \in I$ vérifiant les trois hypothèses suivantes :

$$a < b\,,$$

$$x < y\,,$$

$$(f(y) - f(x)).(f(b) - f(a)) \leq 0\,.$$

a) On introduit la fonction auxiliaire $\phi : [0,1] \to \mathbb{R}$, définie pour chaque $\lambda \in [0,1]$ par

$$\phi(\lambda) = f((1-\lambda)b + \lambda y) - f((1-\lambda)a + \lambda x)\,.$$

Montrer que ϕ est continue sur $[0,1]$.

b) Montrer que $\phi(0).\phi(1) \leq 0$. En vérifiant qu'on a bien les hypothèses exigées, appliquer le théorème des valeurs intermédiaires pour montrer qu'il existe $\lambda_0 \in [0,1]$ tel que $\phi(\lambda_0) = 0$.

c) En utilisant la question précédente et l'injectivité de f, en déduire une contradiction. Conclure.