Devoir surveillé n° 5 – Sujet B

samedi 17 janvier 2026

La durée de l'épreuve est de 4 heures et aucune sortie définitive avant la fin n'est autorisée. Il est possible d'obtenir la note maximale sans avoir traité l'intégralité du sujet.

Avant de commencer, lisez l'intégralité du sujet.

Aucun document n'est autorisé. Les calculatrices et téléphones portables sont interdits.

*Rédigez sur une copie double **lisiblement et proprement**. Laissez une marge à gauche et de la place au début de la copie pour mes appréciations. Écrivez à l'encre bleue ou noire. N'utilisez pas de blanc correcteur. **Encadrez ou soulignez les résultats principaux.***

*Veuillez apporter un soin particulier à la rédaction, à la rigueur et aux raisonnements. **Tout résultat doit être justifié**. Ces éléments seront pris en compte dans la notation. N'oubliez pas d'introduire toutes les variables que vous utilisez, lorsqu'il le faut. Évitez les symboles $\forall$, $\exists$, $\Rightarrow$ et $\Leftrightarrow$ sauf si vous savez les utiliser correctement.*

Problème 1 : Les seigneurs des anneaux [1]

Partie A : Anneau $\mathbb{Z}[\mathrm{i}]$

On note $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \,|\, (a,b) \in \mathbb{Z}^2\}$. Pour tout $z \in \mathbb{Z}[\mathrm{i}]$, on note $N(z) = |z|^2 = z\overline{z}$.

1) Montrer que $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un anneau commutatif intègre.

2) a) On note $U(\mathbb{Z}[\mathrm{i}])$ l'ensemble des inversibles de $\mathbb{Z}[\mathrm{i}]$. Montrer que

$$U(\mathbb{Z}[\mathrm{i}]) = \{z \in \mathbb{Z}[\mathrm{i}] \,|\, N(z) = 1\}.$$

Expliciter alors $U(\mathbb{Z}[\mathrm{i}])$ (par extension).

b) $\mathbb{Z}[\mathrm{i}]$ est-il un corps ?

3) a) Montrer que $h : z \longmapsto \overline{z}$ est un automorphisme d'anneaux de $\mathbb{Z}[\mathrm{i}]$ (c'est-à-dire un isomorphisme d'anneaux de $\mathbb{Z}[\mathrm{i}]$ dans lui-même).

b) Soit f un morphisme d'anneaux de $\mathbb{Z}[\mathrm{i}]$ dans lui-même. Pour tout $n \in \mathbb{Z}$, donner la valeur de $f(n)$ en fonction de n. Que peut valoir $f(\mathrm{i})$?

c) En déduire qu'il existe deux morphismes d'anneaux de $\mathbb{Z}[\mathrm{i}]$ dans lui-même (que l'on explicitera) et que ce sont des automorphismes.

4) Soient $(x,y) \in \mathbb{Z}[\mathrm{i}]^2$ tels que $x \neq 0$. Notons a et b les parties réelles et imaginaires respectives du complexe $\dfrac{y}{x}$ de sorte que $\dfrac{y}{x} = a + \mathrm{i}b$.

a) Justifier qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $|u - a| \leqslant \dfrac{1}{2}$ et $|v - b| \leqslant \dfrac{1}{2}$.

b) On se donne un tel couple (u,v) et on note $q = u + \mathrm{i}v$ et $r = y - qx$. Justifier que $|r| < |x|$.
On commencera par écrire $\frac{r}{x}$ sous forme algébrique.

On vient de montrer que, pour tout $(x,y) \in \mathbb{Z}[\mathrm{i}]^2$ tel que $x \neq 0$, il existe un couple $(q,r) \in \mathbb{Z}[\mathrm{i}]^2$ tel que

$$y = qx + r \qquad \text{et} \qquad N(r) < N(x).$$

De tels q et r sont alors appelés respectivement quotient et reste de la division euclidienne de y par x.

5) Montrer que le reste et le quotient de la division euclidienne dans $\mathbb{Z}[\mathrm{i}]$ ne sont pas uniques en général.
On pourra former celle de $1 + \mathrm{i}$ par 2.

1. a.k.a anneaux euclidiens et principaux.

Partie B : Idéaux, idéaux principaux, anneaux euclidiens et principaux

On se donne dans cette partie un anneau $(A, +, \times)$ qui est **commutatif** et **intègre**. On note 0 et 1 les éléments neutres de A pour $+$ et $\times$ respectivement. On suppose aussi que $0 \neq 1$. Quelques définitions :

- On appelle **idéal** de A toute partie I de A telle que I est un sous groupe de $(A, +)$ et

$$\forall (x, a) \in I \times A, \qquad xa \in I.$$

- Pour tout $a \in A$, on note aA l'ensemble $\{au \,|u \in A\}$. Pour tout $(a, b) \in A^2$, on note $aA + bA$ l'ensemble $\{au + bv \,|(u, v) \in A^2\}$.
- Lorsque x et y sont deux éléments de A, on dit que y est **associé** à x s'il existe $\lambda \in A$ inversible tel que $y = \lambda x$. On vérifie aisément (on ne demande pas de le faire) que « être associé » est une relation d'équivalence. On pourra donc dire que deux éléments x et y de A sont associés lorsque x est associé à y ou le contraire.
- Pour tout $(a, b) \in A^2$, on dit que a est un **diviseur** de b s'il existe $c \in A$ tel que $b = ca$. On note alors $a|b$.
- Un élément p de A est dit **irréductible** s'il n'est pas inversible et si ses seuls diviseurs sont les inversibles de A et les éléments associés à p.
- On dit que A est **euclidien** s'il existe une application $\varphi : A\backslash\{0\} \longrightarrow \mathbb{N}$ vérifiant :

$$\forall (x, y) \in (A\backslash\{0\}) \times A, \qquad \exists (q, r) \in A^2, \qquad \begin{cases} y = qx + r \\ r = 0 \text{ ou } \varphi(r) < \varphi(x) \end{cases}$$

  Une telle application φ est appelée **stathme euclidien** sur A.

1) Montrer que, pour tout $(c, d) \in A^2$, $cA + dA$ est un idéal. En déduire que, pour tout $c \in A$, cA est un idéal de A.

2) Soit $p \in A$ non inversible. Montrer que, si p n'est pas irréductible, alors il existe $(u, v) \in A^2$ tel que $p = uv$ et u et v sont ni inversibles ni associés à p.

On dit qu'un idéal I de A est un **idéal principal** s'il existe $a \in A$ tel que $I = aA$. L'anneau A est dit **principal** si ses seuls idéaux sont les idéaux principaux.

3) Soit I un idéal de A. Justifier que, pour tous $(a, b) \in I^2$ et $u \in A$, $a - bu \in I$.

4) Supposons que A est un anneau euclidien. Soit φ un stathme euclidien sur A. Soit I un idéal de A non réduit à $\{0\}$.

   a) Justifier que $B = \{\varphi(x) \,|\, x \in I\backslash\{0\}\}$ admet un plus petit élément n_0.

   b) On se donne alors $c_0 \in I\backslash\{0\}$ tel que $\varphi(c_0) = n_0$. Justifier que $c_0 A \subset I$.

   c) Montrer que $I \subset c_0 A$.
   On pourra montrer que le reste de la « division euclidienne » d'un élément de I par c_0 est nul.

   d) Conclure que A est un anneau principal.

   On vient donc de montrer que tout anneau [1] euclidien est principal.

5) En déduire que $\mathbb{Z}$ et $\mathbb{Z}[\mathrm{i}]$ sont des anneaux principaux.

6) Supposons que A est un anneau principal. On considère $(a, b, p) \in A^3$ tel que p est irréductible et divise ab.

   a) Justifier qu'il existe $c \in A$ tel que $pA + bA = cA$.

   b) Justifier que $p \in cA$ puis montrer que c est ou bien inversible ou bien associé à p.

   c) Supposons que c est inversible. Montrer qu'il existe $(u, v) \in A^2$ tel que $pu + bv = 1$ et conclure que $p|a$.

   d) Supposons que c est associé à p. Prouver que $p|b$.

1. commutatif et intègre.

Nous venons de montrer le **lemme d'Euclide dans un anneau principal** : si p irréductible divise ab dans un anneau principal, alors p divise a ou p divise b (ou les deux) dans cet anneau.

Partie C : Application au théorème des deux carrés

L'objectif de cette partie est de montrer le théorème des deux carrés pour les nombres premiers : un nombre premier p est somme de deux carrés [1] si et seulement $p = 2$ ou $p \equiv 1\,[4]$.

1) Montrer que, si p un nombre premier qui est somme de deux carrés, alors $p = 2$ ou $p \equiv 1\,[4]$.

2) Soit p un nombre premier supérieur ou égal à 3.

   a) Montrer que, pour tout $x \in [\![1\,;p-1]\!]$, il existe un unique entier y de $[\![1\,;p-1]\!]$ tel que $xy \equiv 1\,[p]$.

   b) On définit sur $[\![1\,;p-1]\!]$ la relation $\sim$ par

   $$\forall (x,y) \in [\![1\,;p-1]\!]^2, \qquad x \sim y \quad \iff \quad x = y \text{ ou } xy \equiv 1\,[p]\,.$$

   Montrer que $\sim$ est une relation d'équivalence.

   Notons $\mathrm{R_{ep}}$ un ensemble de représentant des classes d'équivalences de $\sim$. Pour tout $r \in \mathrm{R_{ep}}$, notons $\mathrm{cl}(r)$ la classe d'équivalence de r par $\sim$.

   c) Déterminer $\mathrm{cl}(x)$ pour tout $x \in [\![1\,;p-1]\!]$. Quel est son cardinal ?
   On séparera les cas selon que $x = 1$, $x = p-1$ ou $x \in [\![2\,;p-2]\!]$.

   d) Notons $m = \dfrac{p-1}{2}$. Justifier que

   $$\prod_{k=1}^{m} k(p-k) = \prod_{r \in \mathrm{R_{ep}}} \prod_{x \in \mathrm{cl(r)}} x$$

   et conclure que $(m!)^2 \equiv (-1)^{m+1}\,[p]$.

3) Soit p un nombre premier tel que $p \equiv 1\,[4]$.

   a) Notons $m = \dfrac{p-1}{2}$. Justifier l'existence d'un entier x (explicite) tel que $x^2 \equiv -1\,[p]$.

   b) En raisonnant par l'absurde, montrer que p n'est pas irréductible dans $\mathbb{Z}[\mathrm{i}]$.
   Rappelons que nous avons montré que $\mathbb{Z}[\mathrm{i}]$ est principal.

   c) En déduire qu'il existe $(u,v) \in \mathbb{Z}[\mathrm{i}]^2$ tel que $|u| \neq 1$, $|v| \neq 1$ et $p = uv$.

   d) Montrer que $|u|^2 = |v|^2 = p$ et conclure qu'il existe $(a,b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.

Puisque $2 = 1^2 + 1^2$ est somme de deux carrés, on en déduit bien le théorème des deux carrés pour les nombres premiers. Pour la culture : la version général du théorème des deux carrés assure qu'un entier naturel non nul n est somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout nombre premier p congru à 3 modulo 4. La preuve est tout à fait accessible avec des arguments d'arithmétique dans $\mathbb{Z}$ mais arrêtons nous là pour cette fois... ce devoir est déjà bien assez long.

Problème 2 : Ensembles bien ordonnés

L'ensemble $\mathbb{N}$ des entiers naturels, muni de sa relation d'ordre naturelle, possède une propriété remarquable : tout sous-ensemble non vide $\mathbb{N}$ admet un minimum. Intéressons-nous dans ce problème aux ensembles ordonnés qui possèdent aussi cette propriété.

Soit $(E, \leqslant)$ un ensemble (non vide) ordonné. On dit que $\leqslant$ est un **bon ordre** sur E (ou que $(E, \leqslant)$ est **bien ordonné**), lorsque toute partie non vide de E admet un plus petit élément.

On admet (c'est même immédiat) que, pour toute partie F non vide d'un ensemble ordonné $(E, \leqslant)$,

- la restriction de $\leqslant$ à F est encore une relation d'ordre sur F et on la notera toujours $\leqslant$.
- si $(E, \leqslant)$ est bien ordonné, $(F, \leqslant)$ également.

1. ...somme de deux carrés d'**entiers** bien sûr ! Par exemple $29 = 2^2 + 5^2$.

Partie A : Exemples et premières propriétés

1) Soit $(E, \leqslant)$ un ensemble non vide bien ordonné. On note $<$ la relation d'ordre strict associée.

   a) Montrer que $\leqslant$ est un ordre total sur E.

   b) Soit A une partie non vide et majorée de E. Montrer que A admet une borne supérieure.

   c) Soit a un élément non maximal [1]. Justifier qu'il existe un unique élément $b \in E$ tel que $a < b$, et, pour tout $x \in E$, si $a < x$, alors $b \leqslant x$ (autrement dit, il s'agit de montrer l'existence du plus petit élément de E qui est supérieur strictement à a). On l'appelle le successeur de a.

2) Dans cette question, on munit $\mathbb{R}$ (et toutes ses parties non vides) de son ordre usuel (que l'on note $\leqslant$). Puisque $\mathbb{Z}$ n'admet pas de minimum, les ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas bien ordonnés pour l'ordre usuel. Voyons cela plus en détail.

   a) Soit B une partie non vide de $\mathbb{Z}$. Déterminer une condition nécessaire et suffisant sur B pour que $(B, \leqslant)$ soit bien ordonnée.

   b) Expliciter un sous-ensemble minoré de $\mathbb{Q}$ (muni de l'ordre naturel) qui n'admet pas de minimum.

   Il est immédiat que toute partie finie de $\mathbb{R}$ est bien ordonnée. Pour autant, il existe des parties infinies de $\mathbb{R}$ qui sont bien ordonnées ($\mathbb{N}$ par exemple).

   c) Soit F une partie de $\mathbb{R}$ infinie et bien ordonnée (pour l'ordre naturel). Montrer qu'il existe une injection de F dans $\mathbb{Q}$.
   On pourra commencer par justifier l'existence d'un rationnel entre tout réel de F et son successeur.

   On admet que F est alors en bijection avec $\mathbb{Q}$ et donc en bijection avec $\mathbb{N}$ (on dit que F est dénombrable).

3) Soit E un ensemble non vide tel qu'il existe une injection f de E dans $\mathbb{N}$. On définit $\preccurlyeq_f$ sur E par :

$$\forall (x, y) \in E^2, \qquad x \preccurlyeq_f y \iff f(x) \leqslant f(y).$$

   Montrer que $\preccurlyeq_f$ un bon ordre sur E.

4) Notons $\Omega = (\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\})$. On définit sur Ω une relation $\preccurlyeq$ par

$$\forall ((n, i), (p, j)) \in \Omega^2, \qquad (n, i) \preccurlyeq (p, j) \iff i < j \text{ ou } (i = j \text{ et } n \leqslant p).$$

   Montrer que $\preccurlyeq$ est un bon ordre sur Ω et expliciter une partie majorée de Ω dont la borne supérieure n'est pas le maximum.

Ce dernier exemple permet de comprendre que, dans un ensemble bien ordonné, tout ne se passe pas non plus comme dans $\mathbb{N}$ (ce qui pouvait sembler le cas au premier coup d'œil).

Partie B : Applications strictement croissantes entre ensembles ordonnés

Soient $(E, \leqslant)$ et $(F, \preccurlyeq)$ des ensembles ordonnés. Notons $<$ et $\prec$ leurs ordres stricts associés respectifs. On dit qu'une application $f : E \longrightarrow F$ est **strictement croissante** lorsque

$$\forall (x, y) \in E^2, \qquad x < y \implies f(x) \prec f(y).$$

On suppose que $(E, \leqslant)$ est bien ordonnée.

1) Montrer qu'une application strictement croissante de $(E, \leqslant)$ sur $(F, \preccurlyeq)$ est injective.

2) On suppose qu'il existe une bijection f strictement croissante de $(E, \leqslant)$ sur $(F, \preccurlyeq)$.

   a) Montrer que $(F, \preccurlyeq)$ est bien ordonné.
   On commencera par considérer l'image réciproque d'une partie non vide de F.

   b) Montrer que f^{-1} est strictement croissante de $(F, \preccurlyeq)$ dans $(E, \leqslant)$.

1. Comme $(E, \leqslant)$ est totalement ordonnée, cela signifie que, dans le cas où E admet un maximum, a n'est pas le maximum en question.

On dit qu'une application bijective et strictement croissante entre deux espaces bien ordonnés est un **isomorphisme**[1] (d'espaces bien ordonnés). On dit que deux ensembles bien ordonnés sont **isomorphes** lorsqu'il existe un isomorphisme[2] de l'un dans l'autre.

3) a) Soit $f : E \longrightarrow E$ strictement croissante. Montrer que, pour tout $x \in E$, $x \leqslant f(x)$.
On pourra considérer le minimum de la partie $\{x \in E \,|\, f(x) < x\}$, s'il existe.

b) Montrer alors que l'identité est le seul isomorphisme de $(E, \leqslant)$ sur lui-même.

c) En déduire qu'il existe au plus un isomorphisme de $(E, \leqslant)$ sur $(F, \preccurlyeq)$.

Partie C : Segments initiaux

Dans cette partie, on se donne $(E, \leqslant)$ un ensemble non vide bien ordonné. Notons m son minimum. On adopte les définitions suivantes :

- Pour tout $a \in E$, on note $S_a = \{x \in E \,|\, x < a\}$. On l'appelle le **segment initial** de a. Remarquons que $S_m = \varnothing$.
- On dit qu'une partie non vide A de E est **close par minoration** si elle vérifie : pour tout $x \in E$ et $y \in A$, si $x \leqslant y$, alors $x \in A$. On convient que $\varnothing$ est close par minoration.

1) Quels sont les segments initiaux de $\mathbb{N}$ muni de l'ordre usuel ? Même question avec l'ensemble Ω de la question A4.
On pourra se contenter de donner la réponse sans preuve.

On revient au cas général.

2) a) Soit $a \in E\backslash\{m\}$. Montrer que le segment initial S_a est close par minoration.

b) Il est immédiat que E est close par minoration mais est-il un segment initial ?

c) Soit A une partie non vide de E qui est close par minoration et qui n'est pas E. Montrer que A est un segment initial.
On pourra considérer le minimum de la partie $E\backslash A$.

Nous venons de montrer que les seules parties closes par minoration de E sont E et les segments initiaux.

3) Soit P une propriété portant sur les éléments de E telle que $P(m)$ est vraie et

$$\forall x \in E\backslash\{m\}, \qquad (\forall y \in S_x,\ P(y)) \quad \Longrightarrow \quad P(x).$$

Montrer que $P(x)$ est vraie pour tout $x \in E$. On parle alors de récurrence transfinie.
On pourra considérer $A = \{x \in E \,|\, P(x)$ est fausse$\}$.

4) On note $\mathrm{SEG} = \{S_a \,|\, a \in E\} \cup \{E\}$. Il s'agit aussi de l'ensemble des parties closes par minoration, compte tenu de la question C2a. Montrer que $\sigma : a \longmapsto S_a$ est une application strictement croissante de $(E, \leqslant)$ dans $(\mathrm{SEG}, \subset)$.

On en déduit que σ est injective (mais non bijective puisque E n'est pas un segment initial).

Nous allons alors ajouter artificiellement un élément ω à E et définir ainsi $\overline{E} = E \cup \{\omega\}$. On prolonge ensuite la relation d'ordre sur E à $\overline{E}$ de sorte que tous les éléments de E soient plus petits que ω. On admet que $(\overline{E}, \leqslant)$ est toujours bien ordonnée. On a alors $S_\omega = E$ (mais on ne dit pas qu'il s'agit d'un segment initial de E) et on prolonge la fonction σ sur $\overline{E}$ en posant $\sigma(\omega) = S_\omega = E$. Ainsi prolongée, il s'agit donc d'une bijection strictement croissante (on ne demande pas de le montrer) de $(\overline{E}, \leqslant)$ dans $(\mathrm{SEG}, \subset)$. La question B2a assure alors que $(\mathrm{SEG}, \subset)$ est bien ordonné et que σ est un isomorphisme d'ensembles bien ordonnés de $(\overline{E}, \leqslant)$ dans $(\mathrm{SEG}, \subset)$.

En particulier $(\mathrm{SEG}, \subset)$ est totalement ordonné et donc, lorsqu'on se donne deux segments initiaux, l'un est forcément inclus dans l'autre.

1. Rien à voir dans cet exercice avec les isomorphismes de groupes ou d'anneaux. Il n'y a aucune LCI ici !
2. On admet que « être isomorphe » est une relation d'équivalence. .

Partie D : Classification des ensembles bien ordonnés

On reprend les hypothèses et les notations de la partie précédente.

1) a) Montrer que E n'est isomorphe à aucun de ses segments initiaux.
Attention, on a dit que $E = S_\omega$ n'avait pas l'appellation de segment initial.

b) En déduire que que deux segments initiaux distincts de E ne sont pas isomorphes.

On se donne maintenant $(F, \preccurlyeq)$ un ensemble non vide bien ordonné. Supposons que, pour tout $y \in \overline{E}$, F **n'est pas isomorphe** à S_y. Pour tout $x \in \overline{E}\backslash\{m\}$, posons

$$P(x) : \text{« } S_x \text{ est isomorphe à un segment initial de } F \text{ ».}$$

L'objectif des prochaines questions est de montrer que, pour tout $x \in \overline{E}$, $P(x)$ est vraie par récurrence transfinie.

2) Notons $s(m)$ le successeur de m dans $\overline{E}$. Prouver $P(s(m))$.

Supposons que $E \neq \{m\}$ (sinon on a déjà terminé la preuve). Soit $x \in \overline{E}\backslash\{m; s(m)\}$. On suppose que, pour tout $y \in S_x$, $P(y)$ est vraie, c'est-à-dire qu'il existe un segment initial T_y de F et un isomorphisme f_y de E dans T_y.

3) a) Montrer qu'il existe $x_0 \in \overline{E}$ tel que

$$\bigcup_{\substack{y \in \overline{E} \\ y<x}} S_y = S_{x_0}$$

et justifier que $S_{x_0} \subset S_x$.

b) Soit $t \in S_{x_0}$. Soient y et z dans $\overline{E}$ tels que $y < x$ et $z < x$, $t \in S_y$ et $t \in S_z$. Justifier que $f_y(t) = f_z(t)$.

Cela permet de définir une application f par : pour tout $t \in S_{x_0}$, $f(t) = f_y(t)$ avec y n'importe quel élément de $\overline{E}$ tel que $y < x$ et $t \in S_y$.

c) Montrer que f est un isomorphisme (d'ensembles bien ordonnés) de S_{x_0} sur $f(S_{x_0})$.

d) Justifier que $f(S_{x_0})$ est clos par minoration et différent de F.

On en déduit notamment que $f(S_{x_0})$ est un segment initial de F.

e) Montrer que $S_x = S_{x_0}$ ou bien $S_x = S_{x_0} \cup \{x_0\}$.
On a déjà vu plus haut que $S_x \subset S_{x_0}$. On pourra raisonner par l'absurde en supposant qu'il existe $a \in S_x\backslash(S_{x_0} \cup \{x_0\})$.

Si $S_{x_0} = S_x$, cela prouve $P(x)$. Si $S_x = S_{x_0} \cup \{x_0\}$, on considère a_0 le minimum de $F\backslash f(S_{x_0})$ (qui existe car sinon un segment initial de E serait isomorphe à $f(S_{x_0}) = F$). Dans ce cas, on prolonge f à x_0 en posant $f(x_0) = a_0$. On vérifie alors aisément (on ne demande pas de le faire) que f, ainsi prolongée, est strictement croissante sur S_x, bijective de S_x sur $f(S_x)$ et que $f(S_x)$ est un segment initial de Y. Ainsi, dans tous les cas, $P(x)$ est vraie.

Par principe de récurrence transfinie (cf. question C3), $P(x)$ est vraie pour tout $x \in \overline{E}$.

4) Conclure que E est isomorphe à un segment initial de F.

Nous venons donc de montrer[1] le théorème suivant : lorsque E et F sont deux espaces bien ordonnés,

- ou bien E et F sont isomorphes.
- ou bien F est isomorphe à un segment initial de E.
- ou bien E est isomorphe à un segment initial de F.

1. Les deux premiers points signifient qu'il existe $x \in \overline{E}$ tel que F est isomorphe à S_x (le premier point lorsque $x = \omega$, le deuxième point sinon) et nous avons donc entamé la preuve du troisième en supposant que les deux premiers n'étaient pas réalisés. Cela prouve donc bien que l'on est dans une des trois possibilités. On peut enfin remarquer que ces trois « ou bien » signifient que deux (quelconques) de ces trois points ne peuvent jamais arriver en même temps. C'est bien le cas car sinon on construirait (par composition) un isomorphisme entre deux segments initiaux d'un espace bien ordonné et on a vu en question D1b que cela n'était pas possible.