Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

COURS À DISTANCE – SEMAINE 3 – ANNEAUX : MORPHISMES ET IDÉAUX – CORRIGÉ TD2

Exercice 1. *Soit A un anneau commutatif. Montrer que l'ensemble $\mathcal{N}(A) := \{a \in A \mid \exists n \in \mathbb{N}^*, a^n = 0_A\}$ des éléments nilpotents est un idéal de A.*

Montrons qu'il satisfait tous les axiomes d'un idéal.

- Il est non vide car il contient 0_A.
- Soit $a_1, a_2 \in \mathcal{N}(A)$, alors il existe $n_1, n_2 \in \mathbb{N}^*$ tels que $a_1^{n_1} = a_2^{n_2} = 0_A$. Mais alors, par le binôme de Newton, on a

$$\begin{aligned}
(a_1 - a_2)^{n_1+n_2} &= \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} a_1^k.(-a_2)^{n_1+n_2-k} \\
&= \sum_{k=0}^{n_1} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} a_1^k.a_2^{n_1+n_2-k} + \sum_{k=n_1+1}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} a_1^k.a_2^{n_1+n_2-k} \\
&= \sum_{k=0}^{n_1} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} a_1^k.a_2^{n_2}.a_2^{n_1-k} + \sum_{k=n_1+1}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} a_1^{n_1}.a_1^{k-n_1} a_2^{n_1+n_2-k} \\
&= \sum_{k=0}^{n_1} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} a_1^k.0_A.a_2^{n_1-k} + \sum_{k=n_1+1}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} 0_A.a_1^{k-n_1} a_2^{n_1+n_2-k} \\
&= 0_A,
\end{aligned}$$

  montrant que $a_1 - a_2 \in \mathcal{N}(A)$.
- Soit $a \in \mathcal{N}(A)$, alors il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$. Mais alors, pour tout $b \in A$, puisque A est commutatif, on a $(a.b)^n = a^n.b^n = 0_A.b^n = 0_A$, montrant que $a.b \in \mathcal{N}(A)$.

Exercice 2. *Soit A un anneau unitaire et I un idéal de A. Montrer que les propositions suivantes sont équivalentes :*

i. *$I = A$;*
ii. *I est un sous-anneau unitaire de A ;*
iii. *$1_A \in I$;*
iv. *I contient un élément inversible.*

Procédons par implications cycliques.

i.⇒ii. : A est bien entendu un sous-anneau de lui-même, et il contient bien 1_A ;
ii.⇒iii. : c'est la définition du caractère unitaire d'un sous-anneau ;
iii.⇒iv. : l'élément $1_A \in I$ est inversible ;
iv.⇒i. : soit $a \in I$ un élément inversible, alors pour tout $b \in A$, on a $b = (b.a^{-1}).a \in I$ puisque I est un idéal. On a donc $A \subset I$, l'inclusion inverse étant claire puisque I est un idéal de A.

Exercice 3. *En considérant l'application*

$$f : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P(i) \end{array},$$

montrer que $\mathbb{C}$ est isomorphe, en tant qu'anneau, à $\mathbb{R}[X]/_{(X^2+1)}$.

Il s'agit ici d'utiliser le théorème d'isomorphisme pour les anneaux. L'application f est en effet un morphisme d'anneaux puisque, pour tous $P, Q \in \mathbb{R}[X]$, on a $f(P+Q) = P(i) - Q(i) = f(P) + f(Q)$ et $f(P.Q) = P(i).Q(i) = f(P).f(Q)$. De plus, f est surjective. En effet, pour tout $a + ib \in \mathbb{C}$ (avec donc $a, b \in \mathbb{R}$), $a + ib = P(i)$ en posant $P := a + bX \in \mathbb{R}[X]$, et donc $a + ib = f(P) \in \mathrm{Im}(f)$.

Déterminons maintenant le noyau de f. On a $f(X^2+1) = i^2-1 = 0$, donc $X^2+1 \in \mathrm{Ker}(f)$ et donc, puisque que le noyau d'un morphisme d'anneaux est toujours un idéal, $(X^2+1) \subset \mathrm{Ker}(f)$. Réciproquement, soit $P \in \mathrm{Ker}(f)$. Par division euclidienne de P par X^2+1 dans $\mathbb{R}[X]$, il existe $R, S \in \mathbb{R}[X]$ tels que $P(X) = (X^2+1)S(X) + R(X)$ avec $\deg(R) < \deg(X^2+1) = 2$. On a donc $R(X) = aX + b$ avec $a, b \in \mathbb{R}$. Mais alors $0 = P(i) = (i^2+1)S(i) + ai + b = ai + b$ dont on déduit que $a = b = 0$ car sinon on aurait $i \in \mathbb{R}$, ce qui est absurde. On a donc $P(X) = (X^2+1)S(X) \in (X^2+1)$. On a donc $\ker(f) = (X^2+1)$.

D'après le théorème d'isomorphisme, f induit un isomorphisme entre $\mathbb{C} = \mathrm{Im}(f)$ et $\mathbb{R}[X]/_{(X^2+1)} = \mathbb{R}[X]/_{\mathrm{Ker}(f)}$.

Exercice 4.

1. *Soit $n \in \mathbb{Z}$. Montrer que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ et qu'il est engendré par n.*

   On a $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$. Cet ensemble est clairement un sous-groupe additive de $\mathbb{Z}$, stable par multiplication par n'importe quel entier ; c'est donc un idéal de $\mathbb{Z}$. Il est par ailleurs clairement engendré par n puisqu'il ne contient que les multiples de n.
2. *Soit I un idéal de $\mathbb{Z}$ non réduit à* 0.
   (a) *Montrer que l'ensemble $I \cap \mathbb{N}^*$ admet un minimum. On le note n.*

   Puisque que $I \cap \mathbb{N}^*$ est un sous-ensemble de $\mathbb{N}$, il suffit de montrer qu'il est non vide pour montrer qu'il possède un plus petit élément. Or I n'est pas réduit à 0, il possède donc un élément non nul, ainsi que son carré puisque I est stable par produit ; ce carré est alors strictement positif, donc un élément dans $I \cap \mathbb{N}^*$.

   (b) *Montrer que $I = (n)$.*

   Puisque I est un idéal contenant n, on a $(n) \subset I$. Réciproquement, considérons $k \in I$. Par division euclidienne de k par n, on a $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$ tels que $k = qn + r$. Mais alors $qn \in (n) \subset I$ et donc $r = qn - r \in I$. Par minimalité de n, on a donc $r = 0$ et donc $k = qn \in (n)$. On en déduit que $I \subset (n)$ et donc que $I = (n)$.
3. *Soient $m, n \in \mathbb{Z}$. Déterminer $(m) \cap (n)$ et $(m) + (n)$.*

   Un élément de $(m) \cap (n)$ est simultanément un multiple de m et de n, c'est donc un multiple de $\mathrm{ppcm}(m, n)$. Mais réciproquement, un multiple de $\mathrm{ppcm}(m, n)$ est bien simultanément un multiple de m et n. On a donc $(m) \cap (n) = \big(\mathrm{ppcm}(m, n)\big)$.

   D'après le théorème de Bachet–Bézout, il existe $a, b \in \mathbb{Z}$ tels que $\mathrm{pgcd}(m, n) = am + bn$. Or $am + bn \in (m) + (n)$, on a donc $\mathrm{pgcd}(m, n) \in (m) + (n)$ et, puisqu'une somme d'idéaux est un idéal, $\big(\mathrm{pgcd}(m, n)\big) \subset (m) + (n)$. Réciproquement, puisque m et n sont tous les deux des multiples de $\mathrm{pgcd}(m, n)$, on a $(m) \subset \big(\mathrm{pgcd}(m, n)\big)$ et $(n) \subset \big(\mathrm{pgcd}(m, n)\big)$, et donc $(m) + (n) \subset \big(\mathrm{pgcd}(m, n)\big)$ puisqu'un idéal est stable par somme. Au final, on a donc $(m) + (n) = \big(\mathrm{pgcd}(m, n)\big)$

Exercice 5. *On considère $\ell(\mathbb{Q})$ l'ensemble des suites à valeurs dans $\mathbb{Q}$ et on note*

- $\ell_C(\mathbb{Q}) := \left\{(u_n)_{n \in \mathbb{N}} \in \ell(\mathbb{Q}) \mid \forall k \in \mathbb{N}^*, \exists N \in \mathbb{N}, \forall n_1, n_2 \in \mathbb{N}, n_1, n_2 \geq N \Rightarrow |u_{n_2} - u_{n_1}| < \frac{1}{k}\right\}$ *le sous-ensemble des suites* de Cauchy *;*
- $\ell_0(\mathbb{Q}) := \left\{(u_n)_{n \in \mathbb{N}} \in \ell(\mathbb{Q}) \mid \forall k \in \mathbb{N}^*, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq N \Rightarrow |u_n| < \frac{1}{k}\right\}$ *le sous-ensemble des suites* convergeant vers 0.

1. (a) *Montrer que tout élément de $\ell_C(\mathbb{Q})$ est une suite bornée.*

Soit $(u_n)_{n\in\mathbb{N}} \in \ell_C(\mathbb{Q})$. Par définition, appliquée en $k=1$, il existe $N_1 \in \mathbb{N}$ tel que, pour tout $n \geq N_1$, on a $|u_n - u_{N_1}| < 1$ et donc $|u_n| < 1 + |u_{N_1}|$. En posant

$$M = \max\left\{|u_0|, |u_1|, \ldots, |u_{N_1-1}|, 1 + |u_{N_1}|\right\},$$

on obtient bien un majorant pour tous les termes de la suite car, pour $k \in [\![0, N_1 - 1]\!]$, on a directement $|u_k| \leq M$ par définition du max, et pour $k \geq N_1$, on a la majoration d'après ce qui précède. La suite $(u_n)_{n\in\mathbb{N}}$ est donc bornée.

(b) *En déduire que $\ell_C(\mathbb{Q})$ est un sous-anneau de $\ell(\mathbb{Q})$.*

Vérifions les axiomes d'un sous-anneau.

- L'ensemble $\ell_C(\mathbb{Q})$ est non vide car il contient les suites constantes.
- Soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \ell_C(\mathbb{Q})$.
  - Pour tout $k \in \mathbb{N}^*$, on sait qu'il existe, par définition des suites de Cauchy appliquée en $k' = 2k$, $N_u, N_v \in \mathbb{N}$ tels que, pour tout $n_1, n_2 \geq N_u$, on a $|u_{n_1} - u_{n_2}| < \frac{1}{2k}$ et, pour tout $n_1, n_2 \geq N_v$, on a $|v_{n_1} - v_{n_2}| < \frac{1}{2k}$. Mais alors, en posant $N_0 = \max(N_u, N_v)$, on a, pour tout $n_1, n_2 \geq N_0$,

$$|(u_{n_1}-v_{n_1})-(u_{n_2}-v_{n_2})| = |(u_{n_1}-u_{n_2})+(v_{n_2}-v_{n_1})| \leq |(u_{n_1}-u_{n_2})|+|(v_{n_2}-v_{n_1})| < \frac{1}{2k}+\frac{1}{2k} = \frac{1}{k}.$$

    La suite $(u_n - v_n)_{n\in\mathbb{N}}$ est donc elle aussi de Cauchy, donc dans $\ell_C(\mathbb{Q})$.
  - D'après la question précédente, les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont bornées. Quitte à arrondir à l'entier supérieur, fixons un majorant $M \in \mathbb{N}^*$ commun à ces deux suites. Pour tout $k \in \mathbb{N}^*$, on sait qu'il existe, par définition des suites de Cauchy appliquée en $k' = 2Mk$, $N_u, N_v \in \mathbb{N}$ tels que, pour tout $n_1, n_2 \geq N_u$, on a $|u_{n_1} - u_{n_2}| < \frac{1}{2Mk}$ et, pour tout $n_1, n_2 \geq N_v$, on a $|v_{n_1} - v_{n_2}| < \frac{1}{2Mk}$. Mais alors, en posant $N_0 = \max(N_u, N_v)$, on a, pour tout $n_1, n_2 \geq N_0$,

$$\begin{aligned} |(u_{n_1}.v_{n_1}) - (u_{n_2}.v_{n_2})| &= |(u_{n_1} - u_{n_2})v_{n_1} + u_{n_2}(v_{n_2} - v_{n_1})| \\ &\leq |(u_{n_1} - u_{n_2})|.|v_{n_1}| + |(v_{n_2} - v_{n_1})|.|u_{n_2}| \\ &< \frac{1}{2Mk}.M + \frac{1}{2Mk}.M = \frac{1}{k}. \end{aligned}$$

    La suite $(u_n.v_n)_{n\in\mathbb{N}}$ est donc elle aussi de Cauchy, donc dans $\ell_C(\mathbb{Q})$.

2. *Montrer que $\ell_0(\mathbb{Q})$ est un idéal de $\ell_C(\mathbb{Q})$.*

Commençons par montrer que $\ell_0(\mathbb{Q}) \subset \ell_C(\mathbb{Q})$. On considère pour cela $(u_n)_{n\in\mathbb{N}} \in \ell_0(\mathbb{Q})$ et on fixe $k \in \mathbb{N}^*$. Par définition, il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$, on a $|u_n| < \frac{1}{2k}$. Mais alors, pour tout $n_1, n_2 \geq N_0$, on a bien $|u_{n_1} - u_{n_2}| \leq |u_{n_1}| + |u_{n_2}| < \frac{1}{2k} + \frac{1}{2k} = \frac{1}{k}$, montrant que $(u_n)_{n\in\mathbb{N}} \in \ell_C(\mathbb{Q})$.

Pour le reste, il s'agit essentiellement de reprendre les raisonnements de la question précédente. Vérifions en effet les axiomes d'un idéal.

- L'ensemble $\ell_0(\mathbb{Q})$ est non vide car il contient la suite constante égale à 0.
- Soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \ell_0(\mathbb{Q})$. Pour tout $k \in \mathbb{N}^*$, on sait qu'il existe $N_u, N_v \in \mathbb{N}$ tels que, pour tout $n \geq N_u$, on a $|u_n| < \frac{1}{2k}$ et, pour tout $n \geq N_v$, on a $|v_n| < \frac{1}{2k}$. Mais alors, en posant $N_0 = \max(N_u, N_v)$, on a, pour tout $n \geq N_0$,

$$|u_n - v_n| \leq |u_n| + |u_n| < \frac{1}{2k} + \frac{1}{2k} = \frac{1}{k}.$$

  La suite $(u_n - v_n)_{n\in\mathbb{N}}$ est donc elle aussi dans $\ell_0(\mathbb{Q})$.
- Soient $(u_n)_{n\in\mathbb{N}} \in \ell_0(\mathbb{Q})$ et $(v_n)_{n\in\mathbb{N}} \in \ell_C(\mathbb{Q})$. D'après la question1., la suite $(v_n)_{n\in\mathbb{N}}$ est bornée. Quitte à arrondir à l'entier supérieur, fixons un majorant $M \in \mathbb{N}^*$ pour cette suite. Pour tout $k \in \mathbb{N}^*$, on sait qu'il existe $N_0 \in \mathbb{N}$ tel que, pour tout $n \geq N_0$, on a $|u_n| < \frac{1}{Mk}$. Mais alors, pour tout $n \geq N_0$, on a

$$|u_n.v_n| = |u_n|.|v_n| < \frac{1}{Mk}.M = \frac{1}{k}.$$

La suite $(u_n.v_n)_{n\in\mathbb{N}}$ est donc elle aussi dans $\ell_0(\mathbb{Q})$.

3. (a) *Montrer qu'une suite dans $\ell_C(\mathbb{Q})$ converge dans $\mathbb{R}$.*

   C'est un résultat classique d'analyse. Pour mémoire, voici les grandes lignes de la preuve (dont vous pourrez trouver les détails dans vos cours d'analyse). On considère une suite $(u_n)_{n\in\mathbb{N}} \in \ell_C(\mathbb{Q})$ et on pose, pour tout $n \in \mathbb{N}$, $\Omega_n := \{u_k \mid k \geq n\}$. D'après la question 1., ces ensembles sont tous bornés et on peut donc poser $a_n := \inf(\Omega_n)$ et $b_n := \sup(\Omega)$ (car c'est une propriété fondamentales de $\mathbb{R}$ que tout ensemble borné admet des bornes inférieures et supérieures). Puisque $\Omega_{n+1} \subset \Omega_n$, les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont respectivement croissantes et décroissantes. De plus, on a clairement $a_n \leq b_n$ et les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont donc respectivement majorée par b_0 et minorée par a_0. En tant que suite bornée monotone, les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ convergent donc vers des limites réelles l_a et l_b. Mais par définition des suites de Cauchy, pour tout $k \in \mathbb{N}^*$, il existe un rang à partir duquel le diamètre de Ω_n est majoré par $\frac{1}{k}$, c'est-à-dire un rang à partir duquel $|b_n - a_n| \leq \frac{1}{k}$. En passant à la limite, on a donc $|l_b - l_a| \leq \frac{1}{k}$ pour tout $k \in \mathbb{N}^*$, et donc $l_a = l_b$, que l'on peut donc noter l sans autre indice. Mais alors, pour tout $\varepsilon > 0$, il existe un rang à partir duquel tous les u_n sont entre $l-\varepsilon$ et $l+\varepsilon$ car a_n et b_n le sont. Cela signifie que la suite $(u_n)_{n\in\mathbb{N}}$ converge vers l.

   (b) *En considérant l'application*

$$\lambda\colon \begin{array}{ccc} \ell_C(\mathbb{Q}) & \longrightarrow & \mathbb{R} \\ (u_n)_{n\in\mathbb{N}} & \longmapsto & \lim\limits_{n\to\infty} u_n \end{array},$$

   montrer que $\ell_C(\mathbb{Q})/\ell_0(\mathbb{Q})$ est isomorphe, en tant qu'anneau, à $\mathbb{R}$.

   D'après les théorèmes de convergence des somme et produit de suites convergentes, l'application λ est un morphisme d'anneau. Ce morphisme est par ailleurs surjectif. En effet, pour tout $l \in \mathbb{R}$, on peut considérer la suite $(u_n)_{n\in\mathbb{N}}$ définie pour tout $n \in \mathbb{N}$ par $u_n = \frac{\lfloor (n+1)l \rfloor}{n+1}$, où $\lfloor\ .\ \rfloor$ est la fonction partie entière ; cette suite prend clairement ses valeurs dans $\mathbb{Q}$ et converge vers l, elle est donc en particulier de Cauchy. Enfin, le noyau de λ vaut $\ell_0(\mathbb{Q})$ par définition de $\ell_0(\mathbb{Q})$. On peut donc conclure par le théorème d'isomorphisme pour les anneaux.

C'est en fait une des constructions de $\mathbb{R}$ à partir de $\mathbb{Q}$. L'ensemble $\mathbb{R}$ est alors défini comme le quotient $\ell_C(\mathbb{Q})/\ell_0(\mathbb{Q})$, lequel est bien muni d'une structure d'anneau d'après la question 2.