Source : Oraux X-ENS – Francinou, Gianella, Nicolas

1. Idéaux maximaux et premiers

Énoncé

Soit A un anneau commutatif et I un idéal de A distinct de A.

1. Montrer que I est maximal pour l'inclusion parmi les idéaux de A distincts de A si, et seulement si, pour tout $a \in A \setminus I$, on a $I + aA = A$.

On dit qu'un idéal I est premier si $A \setminus I$ est stable pour le produit.

2. Montrer que tout idéal maximal est premier.
3. Donner un exemple d'idéal premier.
4. Soit A l'anneau des fonctions de classe $\mathscr{C}^\infty$ de $\mathbb{R}$ dans $\mathbb{R}$ et I l'idéal des fonctions de A s'annulant en 0. L'idéal I est-il principal ? premier ? maximal ?
5. Soit J l'ensemble des fonctions de A telles que $f^{(k)}(0) = 0$ pour tout $k \in \mathbb{N}$. L'ensemble J est-il un idéal ? Si oui, est-il principal ? premier ? maximal ?

Solution

1. Soit I un idéal de A, distinct de A. On note que $I + aA$ est encore un idéal. C'est le plus petit idéal de A contenant I et a.
   Supposons que I soit maximal. Pour tout $a \in A \setminus I$, l'ensemble $I + aA$ est un idéal de A contenant I et distinct de I, car $a = 0 + a \cdot 1$ appartient à $I + aA$. On a donc $I + aA = A$.
   Supposons réciproquement que cette propriété soit vérifiée. Si J est un idéal de A qui contient I et est distinct de I, on considère $a \in J \setminus I$. Alors J contient $I + aA = A$, donc $J = A$ et I est maximal.
2. Soit I un idéal maximal, a et b deux éléments qui ne sont pas dans I. Comme $I + aA = A$, il existe $c \in A$ et $i \in I$ tels que $1 = i + ac$. On en déduit que $b = bi + abc$. Si $ab \in I$, alors $abc \in I$ et comme $bi \in I$, $b \in I$. C'est faux, donc $ab \notin I$ et I est premier.
3. Si $A = \mathbb{Z}$, les idéaux $p\mathbb{Z}$, avec p premier, sont premiers. En effet, si a et b sont deux entiers tels que p divise ab, alors p divise a ou b. Ce sont les seuls idéaux premiers non nuls, car si n est un entier naturel non premier, il existe des entiers n_1 et n_2 strictement supérieurs à 1 tels que $n = n_1 n_2$. Alors n_1 et n_2 n'appartiennent pas à $n\mathbb{Z}$ et $n_1 n_2 \in n\mathbb{Z}$, donc $n\mathbb{Z}$ n'est pas premier.
   Notons que les idéaux $p\mathbb{Z}$, avec p premier, sont aussi maximaux. En effet, si $a \notin p\mathbb{Z}$, alors a est premier avec p, donc $a\mathbb{Z} + p\mathbb{Z} = (a \wedge p)\mathbb{Z} = \mathbb{Z}$.
4. - La fonction $\mathrm{id}_\mathbb{R}$ appartient à I. Montrons que I est principal, engendré par $\mathrm{id}_\mathbb{R}$. Si f est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$, et s'annule en 0, la fonction g définie par $g(x) = \dfrac{f(x)}{x}$ pour $x \neq 0$ et $g(0) = f'(0)$ est de classe $\mathscr{C}^\infty$ (théorème de division). Rappelons-en rapidement une démonstration.
     Pour $x \neq 0$, le changement de variable $t = ux$ donne
     $$f(x) = \int_0^x f'(t)\,dt = x \int_0^1 f'(ux)\,\mathrm{d}u \quad \text{et donc} \quad g(x) = \int_0^1 f'(ux)\,\mathrm{d}u,$$
     formule qui reste vraie pour $x = 0$. La fonction $h : (x,u) \mapsto f'(xu)$ est de classe $\mathscr{C}^\infty$ par rapport à x et les dérivées partielles $\dfrac{\partial^k h}{\partial x^k} : (x,u) \mapsto u^k f^{(k+1)}(xu)$ sont continues sur $\mathbb{R} \times [0,1]$; chaque dérivée partielle est donc bornée par une constante sur les compacts $[a,b] \times [0,1]$ et les constantes étant intégrables sur $[0,1]$, on en déduit que g est de classe $\mathscr{C}^\infty$.
     Enfin, $f = g\,\mathrm{id}_\mathbb{R}$ et $I = \mathrm{id}_\mathbb{R} A$.
   - L'idéal I est maximal car si f appartient à $A \setminus I$ et $g \in A$, on a $f(0) \neq 0$, donc on peut écrire
     $$g = \left(g - \frac{g(0)}{f(0)} f\right) + \frac{g(0)}{f(0)} f ;$$
     ainsi g appartient à $I + fA$.
   - D'après la question 2, I est a fortiori premier.
5. - Il est clair que J est un sous-groupe additif de A. Si $f \in J$ et $g \in A$, la formule de Leibniz montre que fg a toutes ses dérivées nulles en 0. Elle est donc dans J : c'est un idéal de A.
   - Montrons que J n'est pas principal en raisonnant par l'absurde. Soit $f \in J$ tel que $J = fA$. Comme $f(0) = 0$, il existe g dans A telle que $f = \mathrm{id}_\mathbb{R}\, g$. La démonstration de la question 4 montre que $g(x) = \int_0^1 f'(ux)\,\mathrm{d}u$, pour tout réel x et donc que
     $$g^{(k)}(x) = \int_0^1 u^k f^{(k+1)}(ux)\,\mathrm{d}u,$$

pour tout (k,x) de $\mathbb{N}\times\mathbb{R}$. On a en particulier,

$$g^{(k)}(0)=\int_0^1 u^k f^{(k+1)}(0)\,\mathrm{d}u=0.$$

Ainsi $g\in J$ et il existe $h\in A$ telle que $g=fh=\mathrm{id}_{\mathbb{R}}\,gh$. Montrons que g ne s'annule qu'en 0. Il est classique que la fonction φ définie sur $\mathbb{R}$ par

$$\varphi(x)=\begin{cases}\mathrm{e}^{-\frac{1}{x^2}} & \text{si } x\neq 0\\ 0 & \text{si } x=0\end{cases}$$

appartient à J. Comme $\varphi\in fA$ et ne s'annule qu'en 0, il en est de même de f et donc de g. On obtient donc $1=xh(x)$ pour tout $x\neq 0$. En faisant tendre x vers 0, on obtient une contradiction. Donc J n'est pas principal.

- L'idéal J n'est pas maximal car il est contenu strictement dans I.
- Montrons que J est premier. Soit f et g deux éléments de $A\setminus J$. Notons $n=\inf\{k\in\mathbb{N}, f^{(k)}(0)\neq 0\}$ et $p=\inf\{k\in\mathbb{N}, g^{(k)}(0)\neq 0\}$. D'après la formule de Leibniz, on a

$$(fg)^{(n+p)}(0)=\sum_{k=0}^{n+p}\binom{n+p}{k}f^{(k)}(0)g^{(n+p-k)}(0)=\binom{n+p}{n}f^{(n)}(0)g^{(p)}(0)\neq 0,$$

car si $k<n$, $f^{(k)}(0)=0$ et si $k>n$, $n+p-k<p$ et $g^{(n+p-k)}(0)=0$. Ainsi fg n'appartient pas à J.

2. Les anneaux $A[X]$ principaux

Énoncé

1. L'anneau $\mathbb{Z}[X]$ est-il principal ?
2. Soit A un anneau commutatif. À quelle condition $A[X]$ est-il principal ?

Solution

1. Pour montrer la non-principalité, il suffit d'exhiber un idéal non principal.
   C'est le cas de l'idéal I engendré par 2 et X. En effet, supposons qu'il existe $P\in\mathbb{Z}[X]$ tel que $I=(P)$.
   Comme $2\in I$, le polynôme P doit être constant et diviser 2. Donc $P=\pm 1$ ou $P=\pm 2$.
   Mais, comme 2 ne divise pas X dans $\mathbb{Z}[X]$, on a $P=\pm 1$.
   L'idéal $I=(2)+(X)$ contient alors 1, et il existe U et V dans $\mathbb{Z}[X]$ tels que $1=2U+XV$.
   On obtient, en considérant les valeurs en 0 des polynômes, $1=2U(0)$, ce qui est absurde, puisque $U(0)\in\mathbb{Z}$.
2. Nous savons que si A est un corps, $A[X]$ est principal. Montrons que c'est une condition nécessaire.
   On suppose donc que $A[X]$ est principal.
   Alors A est intègre, car sinon $A[X]$ ne serait pas intègre (il existerait deux polynômes constants non nuls dont le produit est nul) donc ne serait pas principal.
   Les propriétés du degré dans $A[X]$ sont par conséquent les mêmes que dans $K[X]$ où K est un corps.
   Soit $a\in A$, non nul. Considérons l'idéal I engendré par X et a.
   On trouve comme dans la première question qu'il est engendré par un polynôme constant c.
   Comme c divise X, il existe $Q\in K[X]$ tel que $cQ=X$.
   Le polynôme Q est nécessairement de la forme dX et $cd=1$.
   Donc $1\in I$ et il existe des polynômes U et V tels que $1=aU+XV$.
   En évaluant en 0, on trouve $1=aU(0)$ donc a est inversible.
   On peut conclure que $A[X]$ est un anneau principal si et seulement si A est un corps.

3. L'anneau $\mathbb{D}$ est principal

Énoncé

Soit $\mathbb{D}$ l'anneau des nombres décimaux :

$$\mathbb{D}=\{x\in\mathbb{Q},\ \exists n\in\mathbb{Z},\ x\cdot 10^n\in\mathbb{Z}\}.$$

Montrer que $\mathbb{D}$ est un anneau principal.

Solution

C'est facilement un sous-anneau de $(\mathbb{Q},+,\times)$, ce qui assure en particulier son intégrité. Ses éléments s'écrivent de manière unique $2^\alpha 5^\beta p$ avec $p\in\mathbb{Z}$ premier avec 10 et $\alpha,\beta\in\mathbb{Z}$.

Comme dans $\mathbb{Z}$, soit I un idéal non réduit à 0 de $\mathbb{D}$ et $x=2^\alpha 5^\beta p$ un élément non nul de I.

Alors $p=2^{-\alpha}5^{-\beta}x\in I$ car $2^{-\alpha}5^{-\beta}\in\mathbb{D}$. Ainsi $|p|\in\mathbb{N}^*\cap I$, partie non vide de N qui possède un min noté a.

On a déjà $a\mathbb{D}\subset I$.

Si, réciproquement, $x=2^\alpha 5^\beta p\in I$, alors $p\in I$ et par division euclidienne, $p=aq+r$ avec $r\in I\cap\mathbb{N}$ et $r<a$ donc $r=0$: $p=aq$ et $x=aq2^\alpha 5^\beta$: $I\subset a\mathbb{D}$.

On montre de la même manière que tout sous-anneau de $\mathbb{Q}$ est principal.