

Solutions – Semaine 1

Exercice 1.

Soit R un anneau. Parmi les sous-ensembles suivants, lesquels sont-ils des sous-anneaux ?

1. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i > j\} \subset M_n(R)$.
2. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \leq j\} \subset M_n(R)$.
3. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \neq j\} \subset M_n(R)$.
4. $\{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
5. $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$.
6. $\left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \subset M_2(\mathbb{Z})$.
7. $\left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}/2\mathbb{Z} \right\} \subset M_2(\mathbb{Z}/2\mathbb{Z})$.

Corrigé. Puisque nous considérons des sous-ensembles d'anneaux, les propriétés de compatibilité et de distributivité sont automatiquement vérifiées. Il s'agit seulement de vérifier si le sous-ensemble est stable par addition et multiplication, et s'il contient l'élément neutre et le zéro. Nous indiquons les réponses.

1. Les matrices triangulaires supérieures forment un sous-anneau.
2. Ce sous-ensemble ne contient pas la matrice identité.
3. Les matrices diagonales forment un sous-anneau.
4. Cet ensemble (il s'agit de $\mathbb{Z}[i]$) est un sous-anneau.
5. Cet ensemble (il s'agit de $\mathbb{Z}[\sqrt{3}]$) est un sous-anneau.
6. Ce sous-ensemble ne contient pas l'identité.
7. On vérifie par calcul direct que cet ensemble est un sous-anneau.

□

Exercice 2.

Dans chacun des cas suivants, déterminez l'ensemble des homomorphismes d'anneaux $A \rightarrow B$.

1. $A = \mathbb{Z}$ et $B = \mathbb{Z}$.
2. $A = \mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$.
3. $A = \mathbb{Z}/n\mathbb{Z}$ et $B = \mathbb{Z}$ où $n \in \mathbb{N}$.
4. $A = \mathbb{Z}/m\mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $m, n \in \mathbb{N}$.
5. $A = \mathbb{Q}$ et $B = \mathbb{R}$.
6. $A = \mathbb{R}$ et $B = \mathbb{R}$.
7. $A = \mathbb{R}$ et $B = \mathbb{Q}$.
8. $A = \mathbb{R}[t]$ et $B = \mathbb{R}$.
9. $A = \mathbb{R}$ et $B = \mathbb{R}[t]$.

Indication : Pour le point 6, montrez qu'un homomorphisme $f: \mathbb{R} \rightarrow \mathbb{R}$ envoie les réels positifs vers les réels positifs, et déduisez que f préserve l'ordre usuel sur les réels.

Corrigé. 1. Si $f: \mathbb{Z} \rightarrow \mathbb{Z}$ est un homomorphisme, alors

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ fois}}) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ fois}} = \underbrace{1 + \cdots + 1}_{n \text{ fois}} = n$$

donc $f = \text{Id}_{\mathbb{Z}}$.

2. Le même raisonnement qu'au point précédent donne que, s'il existe un homomorphisme, alors il est donné par $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, s \mapsto [s]_n$. On vérifie sans peine qu'il s'agit bien d'un homomorphisme.
3. Si $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$ est un homomorphisme, alors $n \cdot f([1]) = f([n]) = f([0]) = 0$ d'une part, et $n \cdot f([1]) = n \cdot 1 = n \neq 0$ d'autre part, ce qui est une contradiction. Donc il n'existe pas d'homomorphisme $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$.

4. Le même raisonnement qu'au second point donne que, s'il existe un homomorphisme, alors il est donné par $f: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, [s]_m \mapsto [s]_n$. Cependant, cette fonction n'est pas toujours bien définie. Par exemple, si $n = 2$ et $m = 3$, alors on devrait avoir

$$[0]_2 = f([0]_3) = f([1]_3) + f([1]_3) + f([1]_3) = [1]_2 + [1]_2 + [1]_2 = [1]_2,$$

ce qui est absurde.

On prétend que f est bien définie si et seulement si n divise m . Il s'agit d'abord d'une condition nécessaire, puisque

$$[0]_n = f([0]_m) = f(m \cdot [1]_m) = m \cdot f([1]_m) = m \cdot [1]_n = [m]_n.$$

Inversément, supposons que $m = nk$. Alors f est une fonction bien définie, puisque

$$f([s + lm]_m) = [s + lm]_n = [s + lnk]_n = [s]_n = f([s]_m)$$

et l'on vérifie sans peine que f est bien un homomorphisme d'anneaux.

5. Soit $f: \mathbb{Q} \rightarrow \mathbb{R}$ un homomorphisme. Puisque $f(1) = 1$, on a $0 = f(0) = f(1 - 1) = 1 + f(-1)$ et donc $f(-1) = -1$. Par additivité on obtient que $f(n) = n$ pour tout $n \in \mathbb{Z}$. Pour $n \in \mathbb{Z}^*$ on a

$$1 = f(1) = f(n \cdot n^{-1}) = n \cdot f(n^{-1})$$

et donc $f(n^{-1}) = n^{-1}$. Par multiplicativité on obtient $f(x) = x$ pour tout $x \in \mathbb{Q}$. Donc f est l'homomorphisme d'inclusion.

6. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ un homomorphisme. Par le point précédent, la restriction $f|_{\mathbb{Q}}$ est l'inclusion. Nous allons montrer qu'en fait $f = \text{Id}_{\mathbb{R}}$.

Prenons un nombre réel $x > 0$. Alors il existe un nombre réel y tel que $y^2 = x$. Ainsi $f(x) = f(y^2) = f(y)^2 > 0$. En particulier si $a > b$, alors $f(a) - f(b) = f(a - b) > 0$. Donc f préserve l'ordre usuel sur les réels.

Prenons maintenant un nombre réel x , et choisissons deux suites de nombres rationnels (y_i) et (z_j) tels que $y_i < x < z_j$ pour tous i, j et $\lim_i y_i = x = \lim_j z_j$. Par les observations précédentes, on a

$$y_i = f(y_i) < f(x) < f(z_j) = z_j$$

pour tous i, j . Les conditions sur les limites nous assurent alors, par un simple argument d'analyse, que $f(x) = x$.

7. Il n'existe pas d'homomorphisme $f: \mathbb{R} \rightarrow \mathbb{Q}$. En effet, si un tel f existait, alors la composition

$$\mathbb{R} \xrightarrow{f} \mathbb{Q} \hookrightarrow \mathbb{R}$$

serait un homomorphisme d'anneaux non-surjectif, en particulier distinct de l'identité, ce qui contredit le point précédent.

8. Par la propriété universelle des anneaux polynomiaux, un homomorphisme $\mathbb{R}[t] \rightarrow \mathbb{R}$ est équivalent au choix d'un homomorphisme $\mathbb{R} \rightarrow \mathbb{R}$ et d'un élément $a \in \mathbb{R}$ (qui sera l'image de t). En vertu de ce qui précède, on obtient que

$$\mathbb{R} \xrightarrow{1:1} \text{Hom}(\mathbb{R}[t], \mathbb{R}), \quad a \mapsto [p(t) \mapsto p(a)].$$

9. De manière générale, un morphisme d'anneaux doit envoyer un élément inversible vers un élément inversible (la preuve en est aisée). Donc si $f: \mathbb{R} \rightarrow \mathbb{R}[t]$ est un homomorphisme, tout élément $x \in \mathbb{R}^*$ étant inversible, son image $f(x) \in \mathbb{R}[t]$ est inversible. Or les polynômes inversibles sont les constantes non-nulles. Ainsi f se co-restreint à un homomorphisme $f: \mathbb{R} \rightarrow \mathbb{R}$, qui est nécessairement l'identité par ce qui précède. Ceci établit que $f: \mathbb{R} \rightarrow \mathbb{R}[t]$ est l'homomorphisme d'inclusion. □

Exercice 3.

Dans chacun des cas suivants, déterminer si l'ensemble B est un sous-anneau, un idéal à gauche, un idéal à droite, un idéal bilatère de l'anneau A ou s'il ne possède aucune de ces propriétés:

- (a) $A = \mathbb{Z}$ et $B = 9\mathbb{Z}$;
- (b) $A = \mathbb{F}_{11}$ et $B = \{[0], [2], [4], [6], [8], [10]\}$;
- (c) $A = \mathbb{Z}[t]$ et $B = t^2 \cdot \mathbb{Z}[t^2]$;
- (d) $A = \mathbb{F}_2[t]$ et $B = t^2 \cdot \mathbb{F}_2[t]$;
- (e) $A = \mathbb{Q}$ et $B = \mathbb{Z}[\sqrt{5}]$;
- (f) $A = \mathbb{Z}/15\mathbb{Z}$ et $B = \{[0], [5], [10]\}$;
- (g) $A = M_n(\mathbb{R})$, $B = \{M \mid m_{ij} = 0 \text{ si } i < j\}$;
- (h) $A = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \text{ ne divise pas } b \right\}$ et $B = p^n \mathbb{Z}_{(p)}$, où p est un premier et $n \in \mathbb{N}$;
- (i) $A = M_3(\mathbb{R})$ et $B = \left\{ \begin{pmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$;

Corrigé. (a) $1 \notin B$, therefore B is not a subring of A . On the other hand, B is a bilateral ideal in A (Definition 1.4.4).

- (b) $[1] \notin B$, hence B is not a subring of A and, as A is a field, B is neither an ideal in A .
- (c) $1 \notin B$, therefore B is not a subring of A . For $t \in A$ and $t^2 \in B$ we have that $t \cdot t^2 = t^3 \notin B$, hence B is not a left ideal in A and moreover, as A is commutative, B is neither a right ideal.
- (d) $[1] \notin B$, therefore B is not a subring of A . Let $f(t) \in A$ and let $t^2 g(t) \in B$, for some $g(t) \in A$. Then $f(t) \cdot (t^2 g(t)) = t^2 (f(t)g(t)) \in B$ and thus B is a left ideal in A . Furthermore, as A is commutative, B is a bilateral ideal.
- (e) $B \not\subseteq A$.
- (f) $[1] \notin B$, therefore B is not a subring of A . Moreover, as $B = ([5])$, B is a bilateral ideal of A .
- (g) B is the set of lower triangular matrices in $M_n(\mathbb{R})$, hence it is a subring of A . If $n > 1$ then B is not an ideal of A . if $n = 1$ then $B = A$ and we conclude that B is a bilateral ideal in A .
- (h) If $n = 0$ then $A = B$ and thus B is both a subring and a bilateral ideal of A . If $n > 0$, then $1 \notin B$, hence B is not a subring of A , but, on the other hand, as $B = (p^n)$, we have that B is a bilateral ideal of A .
- (i) $I_3 \notin B$, hence B is not a subring of A . We check to see if B is a left ideal in A . For this let $A = (a_{ij}) \in A$ and we have

$$A \begin{pmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a + a_{12}b + a_{13}c & a_{11}a + a_{12}b + a_{13}c & 0 \\ a_{21}a + a_{22}b + a_{23}c & a_{21}a + a_{22}b + a_{23}c & 0 \\ a_{31}a + a_{32}b + a_{33}c & a_{31}a + a_{32}b + a_{33}c & 0 \end{pmatrix} \in B.$$

Therefore B is a left ideal of A . On the other hand, B is not a right ideal as

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 3 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix} \notin B.$$

□

Exercice 4.

Soit A un anneau commutatif. Montrer les isomorphismes suivants:

- (a) $A[t]/(t - a) \cong A$ pour $a \in A$.
- (b) $M_n(A)/M_n(I) \cong M_n(A/I)$ si I est un idéal bilatère de A .
- (c) Montrer que l'application

$$f: A[t] \rightarrow A[t], \quad p(t) \mapsto p(t + a)$$

est un isomorphisme d'anneaux.

Corrigé. 1. Par propriété universelle de l'anneau de polynôme $A[t]$ avec le morphisme identité $A \rightarrow A$ et envoyant t sur $a \in A$ on obtient le morphisme d'évaluation en a

$$A[t] \rightarrow A \quad p(t) \mapsto p(a).$$

Que $(t - a)$ soit dans le noyau est clair. Maintenant, pour montrer l'inclusion inverse, on prend un élément du noyau, on procède par induction sur le degré et par division Euclidienne par $t - a$. On commence par le degré zéro. Si $p = b \in A[t]$ est un polynôme constant de termes constant $b \in A$ et qu'il est envoyé sur zéro par le morphisme d'évaluation c'est que $b = 0$. Maintenant on procède au pas d'induction. Si $p(a) = 0$ pour $p(t) \in A[t]$ alors on considère la division euclidienne de $p(t)$ par $t - a$

$$p(t) = q(t)(t - a) + b.$$

On rappelle que la division euclidienne dans les anneaux de polynômes est possible par tout polynôme dont le coefficient dominant est inversible, donc dans ce cas on a l'existence (et l'unicité) de $q(t) \in A[t]$ et $b \in A$ qui satisfont à l'équation ci-dessus. Dès lors on a en évaluant en a que $b = 0$. Ainsi $p(t) \in (t - a)$ ce qui conclut.

- 2. Recall the quotient homomorphism $\xi : A \rightarrow A/I$ given by $a \xrightarrow{\xi} [a]$. This induces the surjective ring homomorphism $f : M_n(A) \rightarrow M_n(A/I)$ given by $(a_{ij}) \xrightarrow{f} ([a_{ij}])$. The kernel of f consists of those matrices in $M_n(A)$ whose coefficients are zero in A/I , hence $\ker(f) = M_n(I)$. We conclude that $M_n(A)/M_n(I) \cong M_n(A/I)$.
- 3. C'est un morphisme d'anneaux car cela peut se définir grâce à la propriété universelle de l'anneaux de polynômes comme l'évaluation en $t + a$. L'inverse est $p(t) \mapsto p(t - a)$ et aussi un morphisme pour la même raison.

□

Exercice 5.

Soit X, Y des ensembles et A, B des anneaux. On note $\text{Fun}(X, A)$ pour l'anneau des fonctions ensemblistes ou les lois d'anneaux sont prises ponctuellement.

1. Soit $f: X \rightarrow Y$ une fonction ensembliste. Montrez que

$$f^*: \text{Fun}(Y, A) \rightarrow \text{Fun}(X, A)$$

donné par la précomposition par f est un morphisme d'anneau.

2. Soit $\varphi: A \rightarrow B$ un morphisme d'anneau. Montrez que

$$\varphi_*: \text{Fun}(X, A) \rightarrow \text{Fun}(X, B)$$

donné par la postcomposition par φ est un morphisme d'anneau.

3. Soit maintenant X un espace topologique compact et $\mathbb{R}$ le corps des nombres réels. On considère $C^0(X, \mathbb{R})$ l'anneau des fonctions continues de X vers $\mathbb{R}$.

- (a) Montrez que si $x \in X$ alors

$$\{f \in C^0(X, \mathbb{R}) \mid f(x) = 0\}$$

est un idéal maximal.

- (b) Montrez que tout idéal maximal est de cette forme.

Corrigé. 3. Pour le premier point on le déduit car c'est par définition le noyau du morphisme surjectif (grâce aux applications constantes notamment) $C^0(X, \mathbb{R}) \rightarrow \mathbb{R}$ qui envoie $x \mapsto f(x)$. Pour le deuxième point, on montre que si I est un idéal tel que pour tout $x \in X$ il existe $f_x \in C^0(X, \mathbb{R})$ tel que $f_x(x) \neq 0$ alors $I = C^0(X, \mathbb{R})$.

En effet, considérons l'ouvert $U_x = f_x^{-1}(\mathbb{R} \setminus \{0\})$ qui contient x . Par compacité, on obtient un nombre fini d'ouverts $U_1, \dots, U_n$ et de fonctions $f_1, \dots, f_n \in I$ tels que f_i ne s'annule pas sur U_i . Quitte à considérer les carrés des f_i , on peut même supposer que f_i est strictement positive sur U_i pour chaque i . Maintenant considérons

$$f := f_1 + \dots + f_n \in I.$$

Notons que cette fonction est positive – de plus pour chaque $x \in X$, il existe un i avec $x \in U_i$. Dès lors, on déduit que f est en fait strictement positive comme dès lors $f_i(x) > 0$. Maintenant, comme f ne s'annule nulle part, la fonction $1/f$ composée des fonctions continues

$$X \xrightarrow{f} \mathbb{R} \setminus 0 \xrightarrow{1/(-)} \mathbb{R}$$

est bien définie et continue. Dès lors, on déduit que $1 = 1/f \cdot f \in I$ ce qui conclut que $I = C^0(X, \mathbb{R})$.

Maintenant si I est maximal, l'idéal est propre. Donc, forcément il existe un $x \in X$ avec

$$I \subset \{f \in C^0(X, \mathbb{R}) \mid f(x) = 0\}.$$

En tant qu'inclusion d'idéaux maximaux, on a alors une égalité, ce qui conclut. □

Exercice 6.

Soit K un corps et $M_n(K)$ l'anneau des matrices carrées de taille $n \times n$.

1. Soit $i, j \in \{1, \dots, n\}$ fixés. Soit I un idéal à gauche de $M_n(K)$ contenant la matrice e_{ij} . Montrer que I contient aussi toutes les matrices “concentrées dans la j -ème colonne”, i.e. (b_{rs}) avec $b_{rs} = 0$ si $s \neq j$.

2. Montrer que le sous-ensemble des matrices concentrées dans la j -ème colonne forme un idéal à gauche de $M_n(K)$.
3. Montrer que les seuls idéaux bilatères de $M_n(K)$ sont $\{0\}$ et $M_n(K)$.

Corrigé. 1. Let $A = (a_{ij}) \in M_n(K)$ be a matrix which is concentrated in the j^{th} column, i.e. $a_{rs} = 0$ for all $s \neq j$. For all $1 \leq r \leq n$ consider the matrix $B_r = a_{rj}e_{ri} \in M_n(K)$. Then $B_re_{ij} \in I$, where

$$(B_re_{ij})_{kl} = \sum_{m=1}^n (a_{rj}e_{ri})_{km} (e_{ij})_{ml} = a_{rj} \sum_{m=1}^n \delta_{rk} \delta_{im} \delta_{jl} = a_{rj} \delta_{rk} \delta_{jl} = \begin{cases} a_{rj}, & \text{if } k = r \text{ and } l = j \\ 0, & \text{otherwise} \end{cases}.$$

Lastly, as $A = \sum_{r=1}^n (B_re_{ij})$, we conclude that $A \in I$.

2. Let $S \subseteq M_n(K)$ be the subset of matrices which are concentrated in the j^{th} column. Clearly, S is an additive subgroup of $M_n(K)$. Now, let $A = (a_{rs}) \in M_n(K)$ and let $B = (b_{rs}) \in S$. As

$$(A \cdot B)_{rs} = \sum_{m=1}^n a_{rm} b_{ms},$$

it follows that $(A \cdot B)_{rs} = 0$ for all $s \neq j$, and we deduce that $A \cdot B \in S$. Therefore, S is a left ideal in $M_n(K)$.

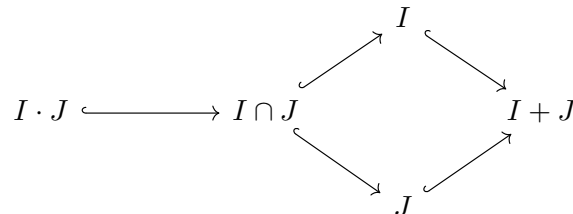
3. Let $\{0\} \neq I$ be a bilateral ideal in $M_n(K)$. Let A be a non-zero matrix in I . Then A admits a non-zero coefficient a_{ij} . As I is an ideal and K is a field we have that $\frac{1}{a_{ij}} \mathbf{I}_n \cdot A \in I$ and so, we can assume without loss of generality that $a_{ij} = 1$. Since I is a bilateral ideal, it follows that for all $1 \leq r, s \leq n$, the product $e_{ri} A e_{js} \in I$. We compute

$$\begin{aligned} (e_{ri} A e_{js})_{kl} &= \sum_{q=1}^n (e_{ri} A)_{kq} (e_{js})_{ql} = \sum_{q=1}^n \left[\sum_{p=1}^n (e_{ri})_{kp} a_{pq} \right] \delta_{jq} \delta_{sl} = \sum_{p=1}^n \delta_{rk} \delta_{ip} a_{pj} \delta_{sl} \\ &= \delta_{rk} a_{ij} \delta_{sl} = \delta_{rk} \delta_{sl} = (e_{rs})_{kl} \end{aligned}$$

and it follows that $e_{rs} \in I$ for all $1 \leq r, s \leq n$. Lastly, as I is an additive subgroup of $M_n(K)$, we conclude that $I = M_n(K)$. □

Exercice 7.

Considérons $\mathbb{Q}[x, y]$ et soient $I = (xy)$ et $J = (y^2)$. Montrer que chacune des inclusions dans le diagramme suivant sont strictes.



Corrigé. Calculons des générateurs de chaque idéal. Par la remarque 2.4.30, on a que $I \cdot J = (xy^3)$ et que $I + J = (xy, y^2)$. Montrons que $I \cap J = (xy^2)$. Tout d'abord, $xy^2 \in I \cap J$, donc $(xy^2) \subseteq I \cap J$. Pour l'autre inclusion, soit $f \in I \cap J$. On peut alors écrire $f = xyg$ et $f(x, y) = y^2h$ pour certains $g, h \in \mathbb{Q}[x, y]$. En particulier,

$$xyg = y^2h,$$

et donc

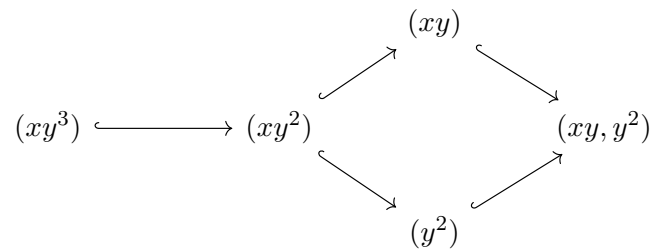
$$y(xg - yh) = 0.$$

Comme $\mathbb{Q}[x, y]$ est intègre, on en déduit que $xg = yh$. En particulier, y divise xg . Un calcul explicite montre alors que y divise en fait g , et donc on peut écrire $g = yg'$ pour un certain $g' \in \mathbb{Q}[x, y]$. Ainsi,

$$f = xyg = xy^2g' \in (xy^2),$$

et donc on a bien montré que $I \cap J = (xy^2)$.

Il faut donc montrer que chaque inclusion



est stricte. Faisons juste un exemple, car c'est à chaque fois le même argument. On a que $xy^2 \in (xy^2) \setminus (xy^3)$, car sinon $xy^2 = qxy^3$ pour un certain $q \in \mathbb{Q}[x, y]$. Or, le premier polynôme a degré 2 en y , alors que cela ne peut pas être le cas du deuxième (il est soit en moins 3, soit ce polynôme lui-même est zéro si $q = 0$).

□