DS n°7

Pour le 26 janvier

Ne pas rédiger les questions avec une étoile *.

Le but de ce problème est l'étude d'ensembles de polynômes prenant sur certaines parties des valeurs particulières

NOTATIONS.

Si A et B désignent 2 ensembles, B étant inclus dans A, on note

$$A \setminus B = \{x \in A; x \notin B\}.$$

On désigne par $\mathbf{P}$ l'ensemble des nombres premiers.

Pour tout nombre premier p, on note $Z_{(p)}$ l'ensemble des rationnels dont une représentation irréductible a un dénominateur non divisible par p.

Pour tout réel x, on appelle partie entière de x et on note $\lfloor x \rfloor$ l'unique entier k vérifiant $k \leq x < k+1$.

On note :

$\mathbf{Q}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients rationnels,

$\mathbf{R}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients réels et, pour tout entier naturel n, $\mathbf{R}_n[X]$ le sous-ensemble de $\mathbf{R}[X]$ formé des polynômes de degré inférieur ou égal à n.

Pour tous sous-ensembles E et F de $\mathbf{R}$, on note :

$$\mathcal{P}(E,F) = \{P \in \mathbf{R}[X]; P(E) \subset F\},$$

à savoir, l'ensemble des éléments de $\mathbf{R}[X]$ dont la valeur en chaque élément de E appartient à F.

A - Exemples élémentaires : $\mathcal{P}(\mathbf{Q},\mathbf{Q})$, $\mathcal{P}(\mathbf{R},\mathbf{R}_+)$, $\mathcal{P}(\mathbf{Q},\mathbf{Q}_+)$.

A - I. *Caractérisation de $\mathcal{P}(\mathbf{Q},\mathbf{Q})$ à l'aide des polynômes de Lagrange.*

Soit m un entier naturel. Pour tous les entiers i et j compris entre 0 et m, on note δ_i^j le symbole de Kronecker défini par : $\delta_i^j = 0$ si $i \neq j$ et $\delta_i^i = 1$.

Soient q_0, q_1, $\ldots q_m$, $m+1$ réels distincts.

A - I. 1. * Expliciter, pour $j = 0, 1, \ldots, m$, le polynôme L_j de $\mathbf{R}_m[X]$ vérifiant :

$$L_j(q_i) = \delta_i^j \text{ pour } i = 0, 1, \ldots, m.$$

A - I. 2. *Montrer que la famille $(L_j)_{0\leq j\leq m}$ forme une base de l'espace vectoriel réel $\mathbf{R}_m[X]$.

A - I. 3. *Pour tout polynôme P de $\mathbf{R}_m[X]$, exprimer P dans la base $(L_j)_{0\leq j\leq m}$ en fonction des réels $(P(q_j))_{0\leq j\leq m}$.

A - I. 4. Comparer l'ensemble $\mathcal{P}(\mathbf{Q},\mathbf{Q})$ avec l'ensemble $\mathbf{Q}[X]$.

A - II. *Caractérisation de l'ensemble $\mathcal{P}(\mathbf{R},\mathbf{R}_+)$.*

A - II. 1. Soit P un élément non nul de $\mathcal{P}(\mathbf{R}, \mathbf{R}_+)$.

A - II. 1. i Soit z_0 un élément de $\mathbf{C} \setminus \mathbf{R}$. Montrer que z_0 est racine de P de multiplicité β si et seulement si $\bar{z_0}$ est racine de P de multiplicité β.

A - II. 1. ii Soit x_0 un réel. Montrer que si x_0 est racine de P de mulltiplicité (non nulle) α, alors α est pair.

A - II. 1. iii Montrer que le coefficient dominant c de P est strictement positif.

A - II. 1. iv Soit Q un élément de $\mathbf{C}[X]$. On note respectivement Q_1 et Q_2 la partie réelle et la partie imaginaire de Q, c'est-à-dire que Q_1 et Q_2 sont éléments de $\mathbf{R}[X]$ et $Q = Q_1 + iQ_2$. Calculer $Q\bar{Q}$ en fonction de Q_1 et Q_2.

A - II. 1. v En décomposant P dans $\mathbf{C}[X]$, déduire des questions précédentes que P est la somme des carrés de deux polynômes de $\mathbf{R}[X]$.

A - II. 1. vi Donner une caractérisation de l'ensemble $\mathcal{P}(\mathbf{R}, \mathbf{R}_+)$.

A - III. *La caractérisation précédente n'est pas valable pour $\mathcal{P}(\mathbf{Q}, \mathbf{Q}_+)$.*

A - III. 1. Montrer que $\mathcal{P}(\mathbf{Q}, \mathbf{Q}_+)$ est contenu dans $\mathcal{P}(\mathbf{R}, \mathbf{R}_+)$.

A - III. 2. i Donner deux décompositions du polynôme $2X^2 + 4$ en la somme des carrés de deux polynômes de $\mathbf{R}[X]$.

A - III. 2. ii Soient a, b, c, d des réels tels que l'on ait :

$$2X^2 + 4 = (aX + b)^2 + (cX + d)^2.$$

Montrer que la matrice

$$\begin{pmatrix} \frac{a}{\sqrt{2}} & \frac{b}{2} \\ \frac{c}{\sqrt{2}} & \frac{d}{2} \end{pmatrix}$$

possède une propriété remarquable à préciser. En déduire que les réels a, b, c, d ne peuvent pas tous être dans $\mathbf{Q}$.

A - III. 2. iii Le polynôme $2X^2 + 4$ peut-il être la somme des carrés de deux éléments de $\mathbf{Q}[X]$?

B - Étude de $\mathcal{P}(E, \mathbf{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier fixé.

B - I. 1. * Montrer que, pour tout rationnel non nul x, il existe un unique entier relatif k tel que x s'écrive sous la forme $p^k \frac{a}{b}$ où a et b sont des entiers non multiples de p. Cet entier k est noté $v_p(x)$. On pose de plus $v_p(0) = +\infty$. On définit ainsi une application v_p de $\mathbf{Q}$ dans $\mathbf{Z} \cup \{+\infty\}$. On adopte les conventions usuelles :
$k + (+\infty) = (+\infty) + k = +\infty$ et $k \leq +\infty$ pour tout k de $\mathbf{Z} \cup \{+\infty\}$.

B - I. 2. Montrer que :
(i) L'application v_p est surjective,
(ii) Pour tous x, y de $\mathbf{Q}$, $v_p(xy) = v_p(x) + v_p(y)$,
(iii) Pour tous x, y de $\mathbf{Q}$, $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

B - I. 3. Que vaut $v_p(1)$? Que vaut $v_p(-1)$? Pour tout (x, y) de $\mathbf{Q} \times \mathbf{Q}^*$, exprimer $v_p\left(\frac{x}{y}\right)$ en fonction de $v_p(x)$ et $v_p(y)$.

B - I. 4. Vérifier que $\mathbf{Z}_{(p)} = \{x \in \mathbf{Q} \mid v_p(x) \geq 0\}$ et $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$. Caractériser les éléments inversibles de $\mathbf{Z}_{(p)}$ à l'aide de v_p.

B - I. 5. i Montrer que, pour tout (k, n) élément de $\mathbf{N}^* \times \mathbf{N}^*$,

$$|\{j \in \mathbf{N} \mid 1 \leq j \leq n, v_p(j) = k\}| = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.$$

B - I. 5. ii Justifier la formule suivante due à Legendre : pour tout entier naturel n,

$$v_p(n!) = \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Facultatif (conseillé pour les 5/2 et élèves en liste $\star$)

Dans la suite de cette partie, E désigne une partie infinie de $\mathbf{Z}$.

B - II. 1. Montrer que

$$\mathbf{Z} = \bigcap_{l \in \mathbf{P}} \mathbf{Z}_{(l)}$$

B - II. 2. Vérifier que

$$\mathcal{P}(E, \mathbf{Z}) = \bigcap_{l \in \mathbf{P}} \mathcal{P}(E, \mathbf{Z}_{(l)}).$$

B - III. *On dit qu'une suite $(u_n)_{n\in\mathbf{N}}$ d'éléments distincts de E est p-ordonnée dans E si elle vérifie :*

$$\forall n \in \mathbf{N}^* \quad v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \min_{x\in E} v_p\left(\prod_{k=0}^{n-1}(x - u_k)\right).$$

B - III. 1. Dans cette question uniquement, on suppose que $p = 3$, $E = \{1\} \cup \{3k \mid k \in \mathbf{N}\}$ et $(u_n)_{n\in\mathbf{N}}$ est une suite 3-ordonnée de E où $u_0 = 0$.
Quelles sont les valeurs possibles pour u_1 et u_2 ?

B - III. 2. Montrer que si $E = \mathbf{Z}$, la suite $(n)_{n\in\mathbf{N}}$ est p-ordonnée.

B - III. 3. Montrer par récurrence que, pour tout a dans E, il existe au moins une suite $(u_n)_{n\in\mathbf{N}}$, p-ordonnée dans E et vérifiant $u_0 = a$. Y a-t-il en général unicité d'une telle suite ?

B - IV. *Dans cette question, on considère une suite $(u_n)_{n\in\mathbf{N}}$ p-ordonnée dans E.* On lui associe la suite de polynômes $(P_n)_{n\in\mathbf{N}}$ définie par :

$$P_0(X) = 1 \quad \text{et, pour } n \geq 1, \quad P_n(X) = \prod_{k=0}^{n-1} \frac{X - u_k}{u_n - u_k}.$$

B - IV. 1. i Montrer que les polynômes P_n appartiennent à $\mathcal{P}(E, \mathbf{Z}_{(p)})$.

B - IV. 1. ii Montrer que, pour tout entier naturel m, la famille $(P_n)_{0\leq n\leq m}$ est une base de l'espace vectoriel réel $\mathbf{R}_m[X]$.

B - IV. 1. iii Préciser les valeurs $P_n(u_k)$ pour n dans $\mathbf{N}$ et $0 \leq k \leq n$.

Dans la suite de cette partie, m désigne un entier naturel et P un élément de $\mathbf{R}_m[X]$.

Ecrivons :

$$P(X) = \sum_{n=0}^{m} c_n P_n(X) \text{ avec } c_0, c_1, \ldots, c_m \in \mathbf{R}.$$

B - IV. 2. Montrer que les assertions suivantes sont équivalentes :
(i) $P \in \mathcal{P}(E, \mathbf{Z}_{(p)})$,
(ii) $c_0, c_1, \ldots, c_m \in \mathbf{Z}_{(p)}$,
(iii) $P(u_0), P(u_1), \ldots, P(u_m) \in \mathbf{Z}_{(p)}$.

B - IV. 3. On pose $\omega(0) = 0$ et, pour tout élément n de $\mathbf{N}^*$, on note $\omega(n)$ l'entier $v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right)$.

Montrer que si P appartient à $\mathcal{P}(E, \mathbf{Z}_{(p)})$, alors les coefficients de $p^{\omega(m)}P$ appartiennent à $\mathbf{Z}_{(p)}$. Vérifier que $\mathcal{P}(E, \mathbf{Z}_{(p)})$ est un sous-anneau de $\mathbf{Q}[X]$.

Correction du DM n°7

A - Exemples élémentaires : $\mathcal{P}(\mathbf{Q},\mathbf{Q})$, $\mathcal{P}(\mathbf{R},\mathbf{R}_+)$, $\mathcal{P}(\mathbf{Q},\mathbf{Q}_+)$.

A - I. *Caractérisation de $\mathcal{P}(\mathbf{Q},\mathbf{Q})$ à l'aide des polynômes de Lagrange.*

A - I. 1. Soit $j \in \{0,1,\dots,m\}$, L_j, dont le texte admet l'existence et l'unicité, s'annule en les m points distincts $q_0,\dots,q_{j-1},q_{j+1},\dots,q_m$, de degré m, il est donc de la forme

$$L_j = c\prod_{i=1\dots n,\, i\neq j}(X-q_j),$$

avec c réel. L'égalité $L_j(q_j)=1$ assure que nécessairement L_j est le polynôme :

$$L_j = \frac{\prod\limits_{i=1\dots n,\, i\neq j}(X-q_j)}{\prod\limits_{i=1\dots n,\, i\neq j}(q_i-q_j)}.$$

$$L_j(q_i)=\delta_i^j \text{ pour } i=0,1,\dots,m.$$

A - I. 2. La famille $(L_j)_{0\leq j\leq m}$ est de cardinal $m+1$ qui est aussi la dimension de $\mathbf{R}_m[X]$, pour que cette famille soit une base il suffit donc qu'elle soit libre. Ce qu'elle puisque si $a_0,a_1,\dots a_m$ sont des réels tels que : $0=\sum\limits_{j=0}^{m}a_jL_j$, alors

$$0=\sum_{j=0}^{m}a_jL_j(q_i)=a_i\times 1,$$

pour $i=0,1,\dots,m$.
La famille $(L_j)_{0\leq j\leq m}$ est une base de $\mathbf{R}_m[X]$.

A - I. 3. Pour tout polynôme P élément de $\mathbf{R}_m[X]$, se décompose dans la base $(L_j)_{0\leq j\leq m}$ en :

$$P=\sum_{j=0}^{m}x_jL_j,$$

où $x_0,x_1,\dots,x_m$ sont des réels. Donc pour $i=0,\dots,m$, $P(q_i)=\sum\limits_{j=0}^{m}x_jL_j(q_i)=x_i\times 1$ et finalement :
$P=\sum\limits_{j=0}^{m}P(q_j)L_j$.

Remarque : on en déduit par exemple en appliquant ce résultat aux polynômes X^0 et X que $\sum\limits_{j=0}^{m}L_j=1$ et $\sum\limits_{j=0}^{m}jL_j=X$.

A - I. 4. • $\mathbf{Q}$ étant un anneau, on a clairement $\mathbf{Q}[X]\subset\mathcal{P}(\mathbf{Q},\mathbf{Q})$.

- Soit réciproquement P un élément de $\mathcal{P}(\mathbf{Q},\mathbf{Q})$. Choisisons pour $j=0,1,\ldots,m$, $q_j=j$ de sorte que $L_j\in\mathbf{Q}[X]$. Comme $P(0),P(1),\ldots,P(m)$ sont rationnels, $P=\sum_{j=0}^{m}P(j)L_j\in\mathbf{Q}[X]$ et donc $\mathcal{P}(\mathbf{Q},\mathbf{Q})\subset\mathbf{Q}[X]$.

Au total, $\underline{\mathcal{P}(\mathbf{Q},\mathbf{Q})=\mathbf{Q}[X]}$.

A - II. *Caractérisation de l'ensemble $\mathcal{P}(\mathbf{R},\mathbf{R}_+)$.*

A - II. 1. Soit P un élément non nul de $\mathcal{P}(\mathbf{R},\mathbf{R}_+)$.

A - II. 1. i Supposons que z_0 soit racine d'ordre β de P. P se laisse décomposer dans la base canonique en $P=\sum_{j=0}^{d}a_iX^i$, avec $a_0,a_1,\ldots,a_d$ réels.

$$P(\bar{z}_0)=\sum_{j=0}^{d}a_i\overline{z_0^i}=\sum_{j=0}^{d}\bar{a}_i\overline{z_0}^i=\overline{\sum_{j=0}^{d}a_iz_0{}^i}=\bar{0}=0.$$

De même $P^{(1)}(\bar{z}_0)=P^{(2)}(\bar{z}_0)=\cdots=P^{(\beta-1)}(\bar{z}_0)$ et donc $\bar{z}_0$ est racine de P d'ordre supérieur à β, disons β'. Mais ce qui vient d'être prouvé dit que $z_0=\bar{\bar{z}}_0$ est racine de P d'ordre supérieur ou égal à β', et donc $\beta=\beta'$. Donc $\bar{z}_0$ est racine de P d'ordre β.

A - II. 1. ii Le polynôme P s'écrit $P=(x-x_0)^\alpha\times Q$ avec Q un élément de $\mathbf{R}[X]$, tel que $Q(x_0)\neq 0$. Or P admet un nombre fini de racines, donc il existe un voisinage de x_0 de la forme $]x_0-h,x_0+h[$ sur lequel Q n'admet pas de racine. La continuité de Q vue comme fonction polynomiale assure que Q y garde un signe constant, si α était impaire pour tout élément x de $]x_0,x_0+h[$, $P(x)$ serait du signe de Q et sur $]x_0-h,x_0[$ du signe opposé, contredisant sa positivité.

Donc $\underline{\alpha \text{ est pair}}$.

A - II. 1. iii Notons d le degré de P, après avoir exclu le cas où P est constant et où évidement son coefficient dominant qui est sa valeur est strictement positif ($P\neq 0$), remarquons que

$$P(x)\sim cx^d,\ (x\to+\infty)$$

Donc si c était strictement négatif la limite en $+\infty$ de P serait $-\infty$ ce qui contredit sa positivité.

Donc $\boxed{c>0}$

.

A - II. 1. iv Après calcul :

$$\boxed{Q\bar{Q}=Q_1^2+Q_2^2}$$

A - II. 1. v La décomposition de P dans $\mathbf{C}[X]$ s'écrit d'après les précédente questions :

$$\omega^2\prod_{i=1}^{p}(x-x_i)^{2\gamma_i}\prod_{j=1}^{q}(x-z_j)^{\beta_j}(x-\bar{z}_j)^{\beta_j},$$

où $\omega=\sqrt{c}$ (cf iii.), $x_1,x_2,\ldots,x_p$ sont les racines réelles deux à deux distinctes de P et $z_1\bar{z}_1,\ldots,z_q,\bar{z}_q$ les racines complexes non réelles deux à deux distinctes

de P, $2\gamma_i$ la multiplicité de x_i (cf. ii.), β_j celle de z_j et $\bar{z}_j$ (cf i.) Posons $Q = \prod_{j=1}^{q} (x - z_j)^{\beta_j}$, alors $\bar{Q} = \prod_{j=1}^{q} (x - \bar{z}_j)^{\beta_j}$ et donc

$$\prod_{j=1}^{q} (x - z_j)^{\beta_j} (x - \bar{z}_j)^{\beta_j} = Q_1^2 + Q_2^2,$$

Q_1 étant la partie réelle de Q et Q_2 la partie imaginaire.

Finalement : $P = P_1^2 + P_2^2$, avec $P_1 = \omega \prod_{i=1}^{p} (x - x_i)^{\gamma_i} Q_1$ et $P_2 = \omega \prod_{i=1}^{p} (x - x_i)^{\gamma_i} Q_2$.

P est bien la somme des carrés de deux polynômes réels.

A - II. 1. vi D'après la question précédente :

tout élément de $\mathcal{P}(\mathbf{R}, \mathbf{R}_+)$ est la somme des carrés de deux polynômes réels.

La réciproque est évidente.

A - III. *La caractérisation précédente n'est pas valable pour* $\mathcal{P}(\mathbf{Q}, \mathbf{Q}_+)$.

A - III. 1. Soit P un élément de $\mathcal{P}(\mathbf{Q}, \mathbf{Q}_+)$. Soit x un élément $\mathbf{R}$. Considérons $(q_n)_{n \in \mathbf{N}}$ une suite de rationnels qui converge vers x (densité de $\mathbf{Q}$ dans $\mathbf{R}$). Pour tout $n \in \mathbf{N}$, $P(q_n) \geq 0$ et donc par continuité de P, $P(x) \geq 0$. Donc $P \in \mathcal{P}(\mathbf{R}, \mathbf{R}_+)$.

On a prouvé : $\mathcal{P}(\mathbf{Q}, \mathbf{Q}_+) \subset \mathcal{P}(\mathbf{R}, \mathbf{R}_+)$

A - III. 2. i On a par exemple

$$2X^2 + 4 = (\sqrt{2}X)^2 + 2^2,$$
$$2X^2 + 4 = (X + \sqrt{2})^2 + (X - \sqrt{2})^2.$$

A - III. 2. ii Dans l'égalité $2X^2 + 4 = (aX + b)^2 + (cX + d)^2$, l'égalité des termes de degré 2,0 puis 1 assure que :

— $a^2 + c^2 = 2$,
— $b^2 + d^2 = 4$,
— $ab + dc = 0$.

Ces trois égalités donnent successivement que la première colonne de la matrice est normée, que la second l'est aussi, et que les deux colonnes sont orthogonales, autrement dit que la matrice est orthogonale. Donc le déterminant de cette matrice vaut ± 1 soit :

$$\frac{1}{2}(ad - bc) = \pm\sqrt{2}.$$

Si a, b, c, d étaient des rationnels alors il en serait de même pour $\sqrt{2}$ ce qui est notoirement faux.

Les réels a, b, c, d ne peuvent pas tous être éléments de $\mathbf{Q}$.

A - III. 2. iii Si le polynôme $2X^2+4$ étaient la somme des carrés de deux éléments de $\mathbf{Q}[X]$, chacun de ces éléments serait de degré inférieur ou égal à 1, ce qui d'après la question précédente est impossible.

B - Étude de $\mathcal{P}(E, \mathbf{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier fixé.

B - I. 1. • Existence — Soit x un rationnel non nul. Il s'écrit par définition sous la forme $x = \frac{c}{d}$ avec $c \in \mathbf{Z}$ et $d \in \mathbf{N}^*$. Soit α l'exposant (possiblement nul) du facteur premier p dans la décomposition en facteur premiers de c, c s'écrit alors

$c = p^\alpha a$, où a est un entier non divisible par p. De même d s'écrit $d = p^\beta b$, avec b un entier non divisible par p et donc en posant $k = \alpha - \beta$,

$$x = p^k \frac{a}{b}$$

et a et b sont des entiers non multiples de p.

- UNICITÉ — Supposons qu'il existe des entiers k' a' et b' tels que p ne divise ni a ni b et

$$x = p^{k'} \frac{a'}{b'}.$$

Alors $ab'p^{k-k'} = a'b$. Donc $p^{k-k'} | a'b$. Mais p étant *premier* et ne divisant ni a' ni b' il ne saurait diviser leurs produit [1]. Donc $k - k' = 0$.

B - I. 2. Montrer que :

(i) Soit $k \in \mathbf{Z}$, $v_(p^k) = k$ et $v_p(0) = +\infty$, donc L'application v_p est donc surjective.

(ii) Soient x, y éléments de $\mathbf{Q}$ non nuls, il existe des entiers a, a', b, et b' non divisible par p tels que

$$x = p^{v_p(x)} \frac{a}{b},\ y = p^{v_p(y)} \frac{a'}{b'}.$$

Donc $xy = p^{v_p(x)+v_p(y)} \frac{aa'}{bb'}$. Comme p ne divise ni a ni a' et qu'il est premier il ne divise pas aa' et pour des raisons similaires il ne divise pas d'avantage bb', si bien que :

$$\boxed{v_p(xy) = v_p(x) + v_p(y)}$$

Cette égalité se trivialise si l'un des entiers x ou y venait à être nul, du fait des règle de calcul dans $\bar{\mathbf{R}}$.

(iii) Gardons les notations du ii), et sans porter atteinte à la généralité, puisque x et y tiennent des rôles symétriques, supposons que $\min\{v_p(x), v_p(y)\} = v_p(x)$. Alors

$$x + y = p^{v_p(x)} \left(\frac{a}{b} + p^{v_p(x')-v_p(x)} \frac{a'}{b'} \right) = p^{v_p(x)} \left(\frac{ab' + a'p^{v_p(x')-v_p(x)} b}{bb'} \right).$$

Comme p ne divise pas bb',

$$v_p \left(\frac{ab' + a'p^{v_p(x')-v_p(x)}}{bb'} \right) \geq 0$$

et donc d'après ii)

$$v_p(x+y) = v_p(p^{v_p(x)}) + v_p \left(\frac{ab' + a'p^{v_p(x')-v_p(x)} b}{bb'} \right) \geq v_p(p^{v_p(x)}) = v_p(x).$$

Donc

$$\boxed{v_p(x+y) \geq \min\{v_p(x), v_p(y)\}}$$

Cette égalité se trivialise si x ou y ou $x + y$ s'annulent.

1. En effet p n'apparaît ni dans la décomposition en facteurs premiers de a' ni dans celle de b, donc pas d'avantage dans celle de $a'b$, ou, si l'on préfère, p ne divisant pas a' et étant premier, il est premier avec a' donc d'après Gauss s'il divisait $a'b$ alors il diviserait b ce qui n'est pas.

B - I. 3. $v_p(1) = v_p(-1) = 0$.

Soit un élément (x, y) de $\mathbf{Q}\times\mathbf{Q}^*$. $v_p\left(\frac{x}{y}\right) = v_p(x)+v_p\left(\frac{1}{y}\right)$, d'après (ii). Par ailleurs toujours d'après (ii), $0 = v_p(1) = v_p\left(y\frac{1}{y}\right) = v_p(y)+v_p\left(\frac{1}{y}\right)$, donc $v_p\left(\frac{1}{y}\right) = -v_p(y)$ et finalement

$$\boxed{v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y).}$$

B - I. 4.

- $0 = \frac{0}{1}$ est élément de $\mathbf{Z}_{(p)}$ et sa valuation, $+\infty$, est positive.
  Soit y un élément de $\mathbf{Z}_{(p)}$ non nul. Il existe des entiers a et b avec $b \neq 0$, $a \wedge b = 1$ et b non divisibles par p, tels que $x = \frac{a}{b}$. En notant k la puissance de p (éventuellement nulle) dans la décomposition de a en facteurs premiers et a' l'entier $\frac{a}{p^k}$ on obtient : $y = p^k\frac{a'}{b}$. comme ni a' ni b ne sont divisible par p, $v_p(y) = k \geq 0$. Nous avons prouvé :
  $$\mathbf{Z}_{(p)} \subset \{x \in \mathbf{Q} \mid v_p(x) \geq 0\}.$$
- Soit z élément de valuation positive. Si z est nul, alors il est, on la vu, dans $\mathbf{Z}_{(p)}$ sinon il existe $a \in \mathbf{Z}$ et $b \in \mathbf{N}^*$ entiers non divisibles par p tels que $z = p^{v_p(z)}\frac{a}{b}$ quitte à diviser a et b par le PGCD de a et b on peut supposer que $\frac{a}{b}$ est irréductible. Comme p ne divise pas b, $\frac{p^{v_p(z)}a}{b}$ est une fraction irréductible dont le dénominateur n'est pas de divisibles par p, et donc $z \in \mathbf{Z}_{(p)}$. Donc
  $$\{x \in \mathbf{Q} \mid v_p(x) \geq 0\} \subset \mathbf{Z}_{(p)}.$$

Finalement $\boxed{\mathbf{Z}_{(p)} = \{x \in \mathbf{Q} \mid v_p(x) \geq 0\}}$

$\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$, en effet :

- $1 \in \mathbf{Z}_{(p)}$ d'après le point précédent puisque, $v_p(1) = 0 \geq 0)$;
  Soient x et y des éléments de $\mathbf{Z}_{(p)}$
- $x - y \in \mathbf{Z}_{(p)}$, puisque
  $$v_p(x - y) \geq \min\{v_p(x), v_p(-y)\} = \min\{v_p(x), v_p(-y)\} \geq 0\,;$$
- $xy \in \mathbf{Z}_{(p)}$ puisque $v_p(xy) = v_p(x) + v_p(y) \geq 0$.

Soit x un élément de $\mathbf{Z}_{(p)}$ non nul. $v_p(x) \geq 0$. $v_p\left(\frac{1}{x}\right) = -v_p(x)$ donc $\frac{1}{x}$ est dans $\mathbf{Z}_{(p)}$ si et seulement si $v_p(x) = 0$. Par ailleurs $v_p(0) \neq 0$ et 0 n'est pas un inversible de $\mathbf{Z}_{(p)}$. Finalement :
les éléments inversibles de $\mathbf{Z}_{(p)}$ sont les rationnels de valuation nulle.

B - I. 5. i

$$\{j \in \mathbf{N} \mid 1 \leq j \leq n, v_p(j) \geq k\} = \{p^k, 2p^k, 3p^k, \ldots, qp^k\},$$

où $q = \left\lfloor \frac{n}{p^k} \right\rfloor$.

$$\{j \in \mathbf{N} \mid 1 \leq j \leq n, v_p(j) \geq k+1\} = \{p^{k+1}, 2p^{k+1}, \ldots, q'p^{k+1}\},$$

où $q' = \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$. Donc

$$\{j \in \mathbf{N} \mid 1 \leq j \leq n, v_p(j) = k\} = \{p^k, 2p^k, 3p^k, \ldots, qp^k\}\backslash\{p^{k+1}, 2p^{k+1}, \ldots, q'p^{k+1}\},$$

et donc

$$\underline{\operatorname{card}\left(\{j \in \mathbf{N} \mid 1 \leq j \leq n, v_p(j) = k\}\right) = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.}$$

B - I. 5. ii D'après B.I.2. (ii) $v_p(n!) = \sum_{i=1}^{n} v_p(i)$ Soit en regroupant dans la somme les termes de même valuation :

$$v_p(n!) = \sum_{k=1}^{+\infty} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right)$$

Notons que dans cette dernière somme (comme dans les suivantes), seul un nombre fini de termes est non nul, ceux pour lesquels $p^k \leq n$.

$$\begin{aligned} v_p(n!) =& \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \\ =& \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{h=2}^{+\infty} (h-1) \left\lfloor \frac{n}{p^h} \right\rfloor \\ =& 1 \times \left\lfloor \frac{n}{p^1} \right\rfloor + \sum_{k=2}^{+\infty} (k-(k-1)) \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

Donc finalement :

$$\underline{v_p(n!) = \sum_{k=0}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .}$$