1 Énoncé

Tous les anneaux considérés sont commutatifs et unitaires. On notera 0 l'élément neutre pour la loi additive et 1 l'élément neutre pour la loi multiplicative d'un tel anneau.

Une partie non vide S d'un anneau A est dit multiplicative si le produit de deux éléments de S est encore dans S.

Si A est un anneau et n un entier naturel non nul, on note $\Sigma_n(A)$ l'ensemble des éléments a de A qui peuvent s'écrire $a = \sum_{k=1}^{n} a_k^2$, où les a_k pour k compris entre 1 et n sont des éléments de A.

Si $\mathbb{K}$ est un corps commutatif, on note $\mathbb{K}[X]$ [resp. $\mathbb{K}(X)$] l'anneau [resp. le corps] des polynômes [resp. des fractions rationnelles] à coefficients dans $\mathbb{K}$ en une indéterminée X.

Enfin $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ désignent les ensembles de nombres habituels.

Pour tout entier naturel non nul p, on note $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

– I – Exemples

1. Soit A un sous-anneau de $\mathbb{R}$. Montrer que $\Sigma_2(A)$ est multiplicatif.
2. Montrer que pour tout anneau A (commutatif et unitaire) $\Sigma_2(A)$ est multiplicatif.
3. Déterminer $\Sigma_n(\mathbb{Z}_8)$ pour $n = 1, 2$ et 3.
4. Montrer que $\Sigma_3(\mathbb{Z})$ n'est pas multiplicatif.
5. Soit (a_1, a_2, a_3, a_4) dans $\mathbb{Z}^4$. Montrer que si $\sum_{k=1}^{4} a_k^2$ est divisible par 8, alors tous les entiers a_k sont pairs.
6. Soit n un entier relatif congru à -1 modulo 8. Montrer que n n'appartient ni à $\Sigma_3(\mathbb{Z})$ ni à $\Sigma_3(\mathbb{Q})$.
7. L'ensemble $\Sigma_3(\mathbb{Q})$ est-il multiplicatif ?
8. Montrer qu'un polynôme $P \in \mathbb{R}[X]$ est dans $\Sigma_2(\mathbb{R}[X])$ si, et seulement si, $P(x) \geq 0$ pour tout réel x.
9. Montrer que $\Sigma_n(\mathbb{R}[X]) = \Sigma_2(\mathbb{R}[X])$ pour tout entier $n \geq 3$.
10. A-t-on $\Sigma_n(\mathbb{R}(X)) = \Sigma_2(\mathbb{R}(X))$ pour tout entier $n \geq 3$?

– II – Produits de sommes de n carrés dans un corps

Pour cette partie $\mathbb{K}$ est un corps commutatif de caractéristique nulle.

Pour tout couple (i, j) d'entiers naturels, on note $\delta_{i,j}$ le symbole de Kronecker ($\delta_{ii} = 1$ et $\delta_{i,j} = 0$ pour $i \neq j$).

On note $\mathcal{M}_n(\mathbb{K})$ l'anneau des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ d'unité I_n.

Pour toute matrice M, carrée ou rectangulaire, on note ${}^tM$ la transposée de M et $\Delta(M)$ la somme des carrés des éléments de la première ligne de M.

Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est dite semi-orthogonale si l'on a :

$$A \cdot {}^tA = {}^tA \cdot A = \Delta(A)\, I_n.$$

Si n est un entier naturel supérieur ou égal à 2, on désigne par $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, 2, \cdots, n\}$ et par $\mathcal{B} = (e_1, \cdots, e_n)$ la base canonique de $\mathbb{K}^n$.

Si $\sigma \in \mathfrak{S}_n$, on appelle matrice de permutation associée à σ, la matrice de passage P_σ de la base canonique de $\mathbb{K}^n$ à la base $\mathcal{B}_\sigma = \left(e_{\sigma(1)}, \cdots, e_{\sigma(n)}\right)$, soit :

$$P_\sigma = \left(\left(\delta_{i,\sigma(j)}\right)\right)_{1 \leq i,j \leq n}.$$

1. Soient $A \in \mathcal{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$ tels que $A \cdot {}^tA = \lambda I_n$.
   (a) Montrer que $\lambda = \Delta(A)$.
   (b) Montrer que si $\lambda \neq 0$, A est semi-orthogonale.
2. Soient A, B semi-orthogonales dans $\mathcal{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$. Montrer que les matrices λA, ${}^tA$ et AB sont semi-orthogonales et calculer $\Delta(\lambda A)$, $\Delta({}^tA)$ et $\Delta(AB)$.
3. Montrer qu'une permutation quelconque des lignes ou des colonnes n'affecte pas la semi-orthogonalité d'une matrice.
4. Soit $L = (\ell_1, \cdots, \ell_n)$ une matrice ligne à coefficients dans $\mathbb{K}$ telle que $\Delta(L) = 0$.
   (a) Montrer que la matrice ${}^tL \cdot L$ est semi-orthogonale et déterminer sa i-ème ligne pour $1 \leq i \leq n$.
   (b) En déduire qu'on peut trouver dans $\mathcal{M}_n(\mathbb{K})$ une matrice semi-orthogonale dont L soit la première ligne.
5. Soient A et B semi-orthogonales dans $\mathcal{M}_n(\mathbb{K})$. On suppose que $\Delta(A) \neq 0$ et $\Delta(A) + \Delta(B) \neq 0$. On pose $C = -\dfrac{1}{\Delta(A)}\, {}^tA\, {}^tBA$. Démontrer que la matrice $\begin{pmatrix} A & B \\ C & {}^tA \end{pmatrix}$ est semi-orthogonale dans $\mathcal{M}_{2n}(\mathbb{K})$.
6. Soient $x_1, \cdots, x_n$ dans $\mathbb{K}$. Montrer qu'il existe dans $\mathcal{M}_n(\mathbb{K})$ une matrice semi-orthogonale dont la première ligne est $(x_1, \cdots, x_n)$ dans chacun des cas suivants :
   (a) $\mathbb{K} = \mathbb{R}$;
   (b) $\mathbb{K}$ quelconque et n puissance de 2.
7. Montrer que, si n est une puissance de 2, un élément a de $\mathbb{K}$ appartient à l'ensemble $\Sigma_n(\mathbb{K})$ si, et seulement si, il existe une matrice semi-orthogonale A dans $\mathcal{M}_n(\mathbb{K})$ telle que $\Delta(A) = a$.
8. Montrer que, si n est une puissance de 2, alors $\Sigma_n(\mathbb{K}) \setminus \{0\}$ est un groupe multiplicatif (et donc $\Sigma_n(\mathbb{K})$ est un ensemble multiplicatif).
9. Montrer que si le cône isotrope de la forme quadratique Q définie sur $\mathbb{K}^n$ par $Q(x) = \sum_{k=1}^{n} x_k^2$ n'est pas réduit à $\{0\}$, alors $\Sigma_n(\mathbb{K}) = \mathbb{K}$ (c'est-à-dire que tout élément de $\mathbb{K}$ est somme de n carrés).

– III – -1 comme sommes de carrés dans un corps

Pour cette partie $\mathbb{K}$ est un corps commutatif de caractéristique quelconque.
Le niveau de $\mathbb{K}$ est défini par :
– $\nu(\mathbb{K}) = +\infty$ si -1 ne peut pas s'écrire comme somme de carrés ;
– $\nu(\mathbb{K})$ est le plus petit entier naturel non nul n tel que $-1 \in \Sigma_n(\mathbb{K})$ dans le cas contraire.

1. Calculer le niveau des corps $\mathbb{R}$ et $\mathbb{C}$.
2. Quel le niveau d'un corps de caractéristique 2 ? d'un corps de caractéristique 5 ?
3. Soit p un nombre premier impair.
   (a) Quel est le noyau du morphisme $x \mapsto x^2$ du groupe commutatif $\mathbb{Z}_p^*$ dans lui même ?

(b) Quel le cardinal de l'image E de ce morphisme ?

(c) T désignant l'ensemble des éléments de $\mathbb{Z}_p$ de la forme $-1-y$ avec $y \in \Sigma_1(\mathbb{Z}_p) = E \cup \{0\}$, démontrer que l'intersection $T \cap \Sigma_1(\mathbb{Z}_p)$ n'est pas vide.

(d) En déduire que $\nu(\mathbb{Z}_p) \leq 2$.

4. Démontrer que, si le corps $\mathbb{K}$ (fini ou infini) est de caractéristique non nulle, alors $\nu(\mathbb{K}) \leq 2$.

5. On suppose, dans cette question, que le corps $\mathbb{K}$ est de caractéristique nulle et de niveau $\nu = \nu(\mathbb{K}) \neq +\infty$. Il existe donc $x_1, \cdots, x_\nu$ dans $\mathbb{K}$ tels que $-1 = \sum_{k=1}^{\nu} x_k^2$. Soit n la plus grande puissance de 2 telle que $n \leq \nu$ et $x = \sum_{k=1}^{n} x_k^2$.

Montrer que $x \neq 0$, puis successivement que $-x$, $-x^2$ et -1 sont dans $\Sigma_n(\mathbb{K})$.

6. Montrer que le niveau d'un corps commutatif est égal à $+\infty$ ou à une puissance de 2.

– IV – Sommes de carrés dans $\mathbb{K}[X]$

Pour cette partie $\mathbb{K}$ est un corps de caractéristique nulle.

1. Montrer que $\Sigma_1(\mathbb{K}[X]) = \mathbb{K}[X] \cap \Sigma_1(\mathbb{K}(X))$.

2. Soient $f_1, \cdots, f_{n-1}, f$ dans $\mathbb{K}(X)$ avec $n \geq 2$. Simplifier l'expression :

$$(f+1)^2 + \sum_{k=1}^{n-1} (f_k(f-1))^2$$

lorsque $\sum_{k=1}^{n-1} f_k^2 = -1$.

3. En déduire que, s'il existe $n \geq 2$ tel que $-1 \in \Sigma_{n-1}(\mathbb{K})$, alors $\Sigma_n(\mathbb{K}) = \mathbb{K}$, $\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X]$ et $\Sigma_n(\mathbb{K}(X)) = \mathbb{K}(X)$.

4. Pour quels entiers $n \geq 1$, les ensembles $\Sigma_n(\mathbb{C}(X))$ sont-ils multiplicatifs ?

5. Soit n un entier supérieur ou égal à 2 tel que $-1 \notin \Sigma_{n-1}(\mathbb{K})$ et soient $P_1, \cdots, P_n$ des polynômes dans $\mathbb{K}[X]$. Démontrer que si $\sum_{k=1}^{n} P_k^2 = aX$, avec $a \in \mathbb{K}$, alors tous les polynômes P_k sont nuls.

6. Soient $P, Q, P_1, \cdots, P_n, Q_1, \cdots, Q_n$ des polynômes dans $\mathbb{K}[X]$ avec $n \geq 2$. On pose

$$\begin{cases} R = P - \sum_{k=1}^{n} Q_k^2, \\ S = PQ - \sum_{k=1}^{n} P_k Q_k, \\ T = 2S - QR \\ T_k = 2Q_k S - P_k R \ (1 \leq k \leq n) \end{cases}$$

(a) Montrer que, si l'on a l'égalité :

$$Q^2 P = \sum_{k=1}^{n} P_k^2 \tag{1}$$

alors, on a aussi les deux égalités :

$$T^2 P = \sum_{k=1}^{n} T_k^2 \text{ et } QT = \sum_{k=1}^{n} (P_k - QQ_k)^2.$$

(b) On suppose, outre l'égalité (1), que $-1 \notin \Sigma_{n-1}(\mathbb{K})$, que $Q \neq 0$ et que $T = 0$. Montrer que :

$$P = \sum_{k=1}^{n} Q_k^2$$

7. Soit $n \geq 2$ tel que $-1 \notin \Sigma_{n-1}(\mathbb{K})$ et soient $P, Q, P_1, \cdots, P_n$ dans $\mathbb{K}[X]$ vérifiant l'égalité (1) et les conditions :

$$PQ \neq 0 \text{ et } \deg(Q) \geq 1.$$

Montrer qu'on peut trouver $U, U_1, \cdots, U_n$ dans $\mathbb{K}[X]$ vérifiant :

$$U^2 P = \sum_{k=1}^{n} U_k^2$$

et :

$$PU \neq 0,\ \deg(U) < \deg(Q).$$

8. Démonter que $\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X))$ pour tout $n \geq 1$.
9.

(a) Montrer que les corps $\mathbb{K}$ et $\mathbb{K}(X)$ ont même niveau.

(b) Montrer que si n est une puissance de 2, alors l'ensemble $\Sigma_n(\mathbb{K}[X])$ est multiplicatif.

2 Corrigé

– I – Exemples

1. Soient $n = a^2 + b^2$ et $m = c^2 + d^2$ où a, b, c, d sont dans l'anneau A. En écrivant que $n = |u|^2$ et $m = |v|^2$ où, $u = a + ib$ et $v = c + id$ dans $\mathbb{C}$, on a :

$$\begin{aligned} nm = |uv|^2 &= |(ac - bd) + (ad + bc)\, i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \in \Sigma_2(A). \end{aligned}$$

L'ensemble $\Sigma_2(A)$ est donc bien multiplicatif.
Prenant $A = \mathbb{Z}$, ce résultat peut se traduire par :

$$\forall x = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4,\ P(x) = 0$$

où P est le polynôme de $\mathbb{R}[X_1, X_2X_3, X_4]$ défini par :

$$P(X_1, X_2X_3, X_4) = \left(X_1^2 + X_2^2\right)\left(X_3^2 + X_4^2\right) - (X_1X_3 - X_2X_4)^2 + (X_1X_4 + X_2X_3)^2$$

Comme $\mathbb{Z}$ est un anneau intègre infini, on en déduit que P est le polynôme nul.

2. Le morphisme d'anneaux $\varphi : \mathbb{Z} \to A$ défini par $\varphi(k) = k \cdot 1$ pour tout $k \in \mathbb{Z}$, se prolonge en un morphisme d'anneaux $\psi : \mathbb{Z}[X] \to A[X]$ en posant, pour tout polynôme $Q = \sum_{k=0}^{n} a_k X^k$ dans $\mathbb{Z}[X]$, $\psi(Q) = \sum_{k=0}^{n} \varphi(a_k) X^k$. Par ce morphisme on a $\psi(P) = 0$ où P est le polynôme défini à la question précédente et en conséquence $\psi(P)(x)$ pour tout $x \in A^4$, ce qui signifie que pour tout $x = (x_1, x_2, x_3, x_4)$ dans A^4, on a :

$$\left(x_1^2 + x_2^2\right)\left(x_3^2 + x_4^2\right) = (x_1x_3 - x_2x_4)^2 + (x_1x_4 + x_2x_3)^2$$

et $\Sigma_2(A)$ est multiplicatif.

3. On a $\mathbb{Z}_8 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\right\}$ et :
$$\Sigma_1(\mathbb{Z}_8) = \mathbb{Z}_8^2 = \left\{\overline{0}, \overline{1}, \overline{4}\right\}$$
$$\Sigma_2(\mathbb{Z}_8) = \mathbb{Z}_8^2 + \mathbb{Z}_8^2 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{4}, \overline{5}\right\}$$
$$\Sigma_3(\mathbb{Z}_8) = \mathbb{Z}_8^2 + \mathbb{Z}_8^2 + \mathbb{Z}_8^2 = \Sigma_2(\mathbb{Z}_8) + \Sigma_1(\mathbb{Z}_8) = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\right\}$$

4. Les entiers $3 = 1^2 + 1^2 + 1^2$ et $5 = 0^2 + 1^2 + 2^2$ sont dans $\Sigma_3(\mathbb{Z})$ mais pas leur produit 15. En effet si $n \in \Sigma_3(\mathbb{Z})$, alors $\overline{n} \in \Sigma_3(\mathbb{Z}_8)$ et $\overline{15} = \overline{7} \notin \Sigma_3(\mathbb{Z}_8)$.

5. Si $\sum_{k=1}^{4} a_k^2$ est divisible par 8, alors $\sum_{k=1}^{4} \overline{a_k}^2 = \overline{0}$ dans $\mathbb{Z}_8$ et $-\overline{a_4}^2 = \sum_{k=1}^{3} \overline{a_k}^2$ est dans l'intersection de $-\Sigma_1(\mathbb{Z}_8) = \left\{-\overline{0}, -\overline{1}, -\overline{4}\right\} = \left\{\overline{0}, \overline{7}, \overline{4}\right\}$ et $\Sigma_3(\mathbb{Z}_8)$, donc $-\overline{a_4}^2$ vaut $\overline{0}$ ou $\overline{4}$, ce qui équivaut à dire que $\overline{a_4}^2$ vaut $\overline{0}$ ou $\overline{4}$ et dans les deux cas a_4 est pair.
Comme les entiers a_k, pour k compris entre 1 et 4 jouent des rôles symétriques, on montre ainsi que tous ces entiers sont pairs (et même multiples de 4).

6. Si $n \in \Sigma_3(\mathbb{Z})$, alors $\overline{n} \in \Sigma_3(\mathbb{Z}_8)$ et $\overline{n} \neq \overline{7} = -\overline{1}$. Donc un entier congru à -1 modulo 8 n'est pas somme de 3 carrés d'entiers.
Un entier non nul n dans $\Sigma_3(\mathbb{Q})$ s'écrit $n = \dfrac{a^2+b^2+c^2}{d^2}$ où les entiers a, b, c, d sont premiers entre eux dans leur ensemble. Si n est congru à -1 modulo 8, on a alors :
$$-\overline{d^2} = \overline{nd^2} = \overline{a^2+b^2+c^2}$$
dans $\mathbb{Z}_8$, ou encore $\overline{a^2+b^2+c^2+d^2} = \overline{0}$ et $a^2+b^2+c^2+d^2$ est divisible par 8, ce qui impose que tous les entiers a, b, c, d sont pairs, en contradiction avec le fait qu'ils sont premiers entre eux dans leur ensemble. Donc $n \notin \Sigma_3(\mathbb{Q})$, c'est-à-dire un entier congru à -1 modulo 8 n'est pas somme de 3 carrés de nombres rationnels.

7. Les entiers 3 et 5 sont dans $\Sigma_3(\mathbb{Z}) \subset \Sigma_3(\mathbb{Q})$ et leur produit 15 qui est congru à -1 modulo 8 n'est pas dans $\Sigma_3(\mathbb{Q})$. Donc $\Sigma_3(\mathbb{Q})$ n'est pas multiplicatif.

8. Si $P = U^2 + V^2$ dans $\mathbb{R}[X]$, on a alors $P(x) = U^2(x) + V^2(x) \geq 0$ pour tout réel x.
Réciproquement soit $P \in \mathbb{R}[X]$ tel que $P(x) \geq 0$ pour tout réel x.
Si P est le polynôme constant égal à λ, on a nécessairement $\lambda \in \mathbb{R}^+$ et $P = U^2 + V^2$, où U est le polynôme constant égal à $\sqrt{\lambda}$ et V le polynôme nul.
Si P est non constant de degré $n \geq 1$, il s'écrit $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$. Comme $P(x)$ est équivalent à $a_n x^n$ en $+\infty$, on a nécessairement $a_n > 0$.
Si x_0 est une racine réelle de P de multiplicité m, on a $P(x) = (x - x_0)^m Q(x)$ avec $Q(x_0) \neq 0$ et $P(x)$ est équivalent à $(x - x_0)^m Q(x_0)$ dans un voisinage ouvert de x_0, ce qui impose m pair (et $Q(x_0) > 0$). Les racines réelles de P sont donc toutes de multiplicité paire.
La décomposition en facteurs irréductibles de P dans $\mathbb{R}[X]$ est donc de la forme :
$$P = a_n \prod_{k=1}^{r} (x - x_k)^{2p_k} \prod_{k=1}^{s} \left(x^2 + b_k x + c_k\right)^{q_k}$$
avec $r \geq 0$, $s \geq 0$ (dans le cas où r ou s est nul, le produit correspondant vaut 1) et $b_k^2 - 4c_k < 0$ pour tout k compris entre 1 et s (si $s \geq 1$). Chaque terme de ces produit étant dans $\Sigma_2(\mathbb{R}[X])$ (c'est évident pour les $\left((x - x_k)^{p_k}\right)^2$ et :
$$x^2 + b_k x + c_k = \left(x + \frac{b_k}{2}\right)^2 + \left(\frac{\sqrt{4c_k - b_k^2}}{2}\right)^2$$
pour k compris entre 1 et s) avec $\Sigma_2(\mathbb{R}[X])$ qui est multiplicatif (question **I.2.**), on en déduit que P est dans $\Sigma_2(\mathbb{R}[X])$.

9. On a de manière évidente $\Sigma_2(\mathbb{R}[X]) \subset \Sigma_n(\mathbb{R}[X])$.
Réciproquement un polynôme P dans $\Sigma_n(\mathbb{R}[X])$ étant à valeurs positives est dans $\Sigma_2(\mathbb{R}[X])$ d'après la question précédente.

10. Là encore $\Sigma_2(\mathbb{R}(X)) \subset \Sigma_n(\mathbb{R}(X))$ est évident.2
Réciproquement, toute fonction rationnelle f non nulle (le cas de $f = 0$ est évident) dans $\Sigma_n(\mathbb{R}(X))$ s'écrit $f = \sum_{k=0}^{n} \frac{P_k^2}{Q_k^2}$ où les P_k et Q_k sont des polynômes et en réduisant au même dénominateur, on a $f = \frac{1}{D^2} \sum_{k=0}^{n} U_k^2$ où D et les U_k sont des polynômes. Le polynôme $\sum_{k=0}^{n} U_k^2$ étant à valeurs positives est dans $\Sigma_2(\mathbb{R}[X])$ et en conséquence s'écrit $A^2 + B^2$, où A, B sont de polynômes, ce qui donne $f = \left(\frac{A}{D}\right)^2 + \left(\frac{B}{D}\right)^2 \in \Sigma_2(\mathbb{R}(X))$.
On a donc $\Sigma_n(\mathbb{R}(X)) = \Sigma_2(\mathbb{R}(X))$ pour tout entier $n \geq 3$.

– II – Produits de sommes de n carrés dans un corps

1.

(a) Si $A \cdot {}^tA = \lambda I_n$, on a en particulier :

$$\lambda = \left(A \cdot {}^tA\right)_{11} = \sum_{k=1}^{n} a_{1k}a_{1k} = \sum_{k=1}^{n} a_{1k}^2 = \Delta(A).$$

(b) Il s'agit de montrer que A et ${}^tA$ commutent si $\lambda \neq 0$. L'égalité $A \cdot {}^tA = \lambda I_n$ peut aussi s'écrire, pour $\lambda \neq 0$:

$$A \cdot \left(\frac{1}{\lambda}\, {}^tA\right) = I_n$$

encore équivalent à dire que la matrice A est inversible d'inverse $\frac{1}{\lambda}\, {}^tA$. Comme A commute à son inverse, elle commute aussi à ${}^tA = \lambda A^{-1}$.

2. Si $A \cdot {}^tA = {}^tA \cdot A = \Delta(A) I_n$, on a alors pour tout $\lambda \in \mathbb{K}$:

$$\begin{aligned}(\lambda A)\ {}^t(\lambda A) &= \lambda^2 \left(A \cdot {}^tA\right) = \lambda^2 \left({}^tA \cdot A\right) \\ &= {}^t(\lambda A)(\lambda A) = \lambda^2 \Delta(A) I_n\end{aligned}$$

ce qui prouvent que λA est semi-orthogonale avec $\Delta(\lambda A) = \lambda^2 \Delta(A)$.
De même, on a :

$$\begin{aligned}\left({}^tA\right)\ {}^t\left({}^tA\right) &= {}^tA \cdot A = A \cdot {}^tA \\ &= {}^t\left({}^tA\right)\left({}^tA\right) = \Delta(A) I_n\end{aligned}$$

ce qui prouvent que ${}^tA$ est semi-orthogonale avec $\Delta\left({}^tA\right) = \Delta(A)$.
Pour B semi-orthogonale, on a :

$$\begin{aligned}(AB)\ {}^t(AB) &= A\left(B\, {}^tB\right)\ {}^tA = A\left(\Delta(B) I_n\right)\ {}^tA \\ &= \Delta(B) A \cdot {}^tA = \Delta(A)\Delta(B) I_n\end{aligned}$$

donc $\Delta(AB) = \Delta(A)\Delta(B)$ et avec

$$\begin{aligned}{}^t(AB)(AB) &= {}^tB\left({}^tAA\right)B = \Delta(A)\ {}^tBB \\ &= \Delta(A)\Delta(B) I_n = (AB)\ {}^t(AB)\end{aligned}$$

on déduit que AB est semi-orthogonale.

3. Effectuer une permutation des lignes sur une matrice A revient à multiplier à gauche la matrice A par une matrice de permutation et une permutation des colonnes revient à multiplier à droite la matrice A par une matrice de permutation. Il nous suffit donc de montrer qu'une matrice de permutation est semi-orthogonale, ce qui se déduit du fait qu'une matrice de permutation est orthogonale et une matrice orthogonale est en particulier semi-orthogonale. En effet une matrice orthogonale vérifiant $A\cdot\ {}^tA = I_n$ est semi-orthogonale (question **II.2.** avec $\lambda = 1$). Et pour toute matrice de permutation $P_\sigma = \left(\left(\delta_{i,\sigma(j)}\right)\right)_{1\leq i,j\leq n}$, on a :

$$P_\sigma\cdot\ {}^tP_\sigma = \left(\left(a_{ij}\right)\right)_{1\leq i,j\leq n}$$

avec :

$$a_{ij} = \sum_{k=1}^{n}\delta_{i,\sigma(k)}\delta_{j,\sigma(k)} = \delta_{j,\sigma(\sigma^{-1}(i))} = \delta_{j,i}$$

ce qui signifie que $P_\sigma\cdot\ {}^tP_\sigma = I_n$ et P_σ est orthogonale.

4.

(a) On a :

$$A = {}^tL\cdot L = \begin{pmatrix}\ell_1\\ \vdots\\ \ell_n\end{pmatrix}(\ell_1,\cdots,\ell_n) = \left(\left(\ell_i\ell_j\right)\right)_{1\leq i,j\leq n}$$

et la i-ème ligne de A est $\ell_i L$.
Cette matrice est symétrique et :

$$A\cdot\ {}^tA = {}^tA\cdot A = A^2 = \left(\left(b_{ij}\right)\right)_{1\leq i,j\leq n}$$

avec :

$$b_{ij} = \sum_{k=1}^{n}a_{ik}a_{kj} = \ell_i\ell_j\sum_{k=1}^{n}\ell_k^2 = \ell_i\ell_j\Delta(L) = 0.$$

La matrice A est donc semi-orthogonale avec $\Delta(A) = 0$.

(b) Si $L = 0$, la matrice $A = 0$ est semi-orthogonale de première ligne L.
Si $L \neq 0$, il existe un indice i tel que $\ell_i \neq 0$ et en notant $\theta_{1,i}$ la transposition $(1,i)$ si $i \neq 1$ ou l'identité si $i = 1$, la matrice $P_{\theta_{1,i}}A$ déduite de la matrice semi-orthogonale $A = {}^tL\cdot L$ en permutant les lignes 1 et i est aussi semi orthogonale de première ligne $\ell_i L$. La matrice $\dfrac{1}{\ell_i}P_{\theta_{1,i}}A$ est alors semi orthogonale de première ligne L.

5. Soit $M = \begin{pmatrix}A & B\\ C & {}^tA\end{pmatrix}$ dans $\mathcal{M}_{2n}(\mathbb{K})$. On a :

$$\begin{aligned}M\cdot\ {}^tM &= \begin{pmatrix}A & B\\ C & {}^tA\end{pmatrix}\begin{pmatrix}{}^tA & {}^tC\\ {}^tB & A\end{pmatrix}\\ &= \begin{pmatrix}A\cdot\ {}^tA + B\cdot\ {}^tB & A\cdot\ {}^tC + BA\\ C\cdot\ {}^tA + {}^tA\cdot\ {}^tB & C\cdot\ {}^tC + {}^tA\cdot A\end{pmatrix}\\ &= \begin{pmatrix}\left(\Delta(A)+\Delta(B)\right)I_n & A\cdot\ {}^tC + BA\\ C\cdot\ {}^tA + {}^tA\cdot\ {}^tB & C\cdot\ {}^tC + \Delta(A)I_n\end{pmatrix}\end{aligned}$$

et tenant compte de $C = -\dfrac{1}{\Delta(A)}\ {}^tA\ {}^tBA$, on a :

$$\begin{cases}A\cdot\ {}^tC + BA = -\dfrac{1}{\Delta(A)}\left(A\ {}^tA\right)BA + BA = 0\\ C\cdot\ {}^tA + {}^tA\cdot\ {}^tB = -\dfrac{1}{\Delta(A)}\ {}^tA\ {}^tB\left(A\ {}^tA\right) + {}^tA\cdot\ {}^tB = 0\\ C\cdot\ {}^tC + \Delta(A)I_n = \dfrac{1}{\Delta(A)^2}\ {}^tA\ {}^tB\left(A\ {}^tA\right)BA + \Delta(A)I_n = \left(\Delta(B)+\Delta(A)\right)I_n\end{cases}$$

et :

$$M \cdot {}^tM = (\Delta(A) + \Delta(B))\, I_{2n}$$

avec $\Delta(A) + \Delta(B) \neq 0$, ce qui signifie que est semi-orthogonale dans $\mathcal{M}_{2n}(\mathbb{K})$ avec $\Delta(M) = \Delta(A) + \Delta(B)$.

6. Si $\Delta(L) = 0$, la question **II.4.** nous dit qu'il existe une matrice A semi-orthogonale dans $\mathcal{M}_n(\mathbb{K})$ de première ligne $L = {}^tx = (x_1, \cdots, x_n)$ que n soit une puissance de 2 ou pas, le corps $\mathbb{K}$ étant quelconque (commutatif et de caractéristique nulle).
On suppose donc que $\Delta(L) \neq 0$.

   (a) Si $\mathbb{K} = \mathbb{R}$, on munit alors l'espace vectoriel $\mathbb{R}^n$ de sa structure euclidienne usuelle. À partir du vecteur $\varepsilon_1 = \dfrac{1}{\|x\|}x$ ($\|x\| = \sqrt{\Delta(L)} \neq 0$) on construit une base orthonormée $\mathcal{B}' = (\varepsilon_1, \cdots, \varepsilon_n)$ de $\mathbb{R}^n$ et la matrice de passage P de la base canonique de $\mathbb{R}^n$ à $\mathcal{B}'$ est orthogonale, donc semi-orthogonale. La matrice $A = \|x\|\ {}^tP$ est alors semi-orthogonale de première ligne ${}^tx$.

   (b) Ici $n = 2^p$ avec $p \geq 1$.
   On raisonne par récurrence sur $p \geq 1$.
   Pour $p = 1$, la matrice $A = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$ dans $\mathcal{M}_2(\mathbb{K})$ est telle que :

$$A \cdot {}^tA = {}^tA \cdot A = \left(x_1^2 + x_2^2\right) I_2$$

   donc semi-orthogonale et sa première ligne est (x_1, x_2).
   Supposons le résultat acquis pour $p \geq 1$ et soit :

$$L = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$$

   avec $n = 2^p$. L'hypothèse de récurrence nous dit qu'il existe deux matrices semi-orthogonales A, B dans $\mathcal{M}_n(\mathbb{K})$ telles $L_1 = (x_1, \cdots, x_n)$ soit la première ligne de A et $L_2 = (x_{n+1}, \cdots, x_{2n})$ la première ligne de B. On a alors $\Delta(A) = \Delta(L_1)$, $\Delta(B) = \Delta(L_2)$ et $\Delta(A) + \Delta(B) = \Delta(L_1) + \Delta(L_2) = \Delta(L) \neq 0$.
   Si $\Delta(A) \neq 0$, la matrice $M = \begin{pmatrix} A & B \\ C & {}^tA \end{pmatrix}$ construite en **II.5.** convient.
   Si $\Delta(A) = 0$, on a alors $\Delta(B) = \Delta(L) \neq 0$ et la question **II.5.** nous dit que la matrice $M = \begin{pmatrix} B & A \\ D & {}^tB \end{pmatrix}$ où $D = -\dfrac{1}{\Delta(B)}\ {}^tB\ {}^tAB$ est semi-orthogonale dans $\mathcal{M}_{2n}(\mathbb{K})$ de première ligne (L_2, L_1). En désignant par σ la permutation :

$$\begin{pmatrix} 1 & 2 & \cdots & n & n+1 & \cdots & 2n \\ n+1 & n+2 & & 2n & 1 & \cdots & n \end{pmatrix}$$

   la matrice MP_σ déduite de M en faisant agir σ sur ses colonnes est semi-orthogonale dans $\mathcal{M}_{2n}(\mathbb{K})$ de première ligne $(L_1, L_2) = L$.

7. Si $\Delta(A) = a$, alors a est dans $\Sigma_n(\mathbb{K})$ que A soit semi-orthogonale ou pas et que n soit une puissance de 2 ou pas.
   Réciproquement soit $a = \sum_{k=1}^{n} a_k^2 \in \Sigma_n(\mathbb{K})$ avec $n = 2^p$. On sait qu'il existe une matrice semi-orthogonale A dans $\mathcal{M}_n(\mathbb{K})$ de première ligne $L = (a_1, \cdots, a_n)$ et on a $\Delta(A) = \Delta(L) = a$.

8. Ici $n = 2^p$ avec $p \geq 1$.
   L'ensemble $\Sigma_n(\mathbb{K}) \setminus \{0\}$ est non vide puisqu'il contient 1.
   Comme n est une puissance de 2, pour a, b dans $\Sigma_n(\mathbb{K}) \setminus \{0\}$, on peut trouver deux matrices

semi-orthogonales A et B dans $\mathcal{M}_n(\mathbb{K})$ telles que $a = \Delta(A)$ et $b = \Delta(B)$. La matrice AB est aussi semi-orthogonale avec $\Delta(AB) = \Delta(A)\Delta(B) = ab$, ce qui implique que ab est aussi dans $\Sigma_n(\mathbb{K}) \setminus \{0\}$.

En écrivant que $\dfrac{a}{b} = \dfrac{ab}{b^2}$ avec ab et $\dfrac{1}{b^2} = \left(\dfrac{1}{b}\right)^2$ dans $\Sigma_n(\mathbb{K}) \setminus \{0\}$, on déduit que $\dfrac{a}{b}$ est aussi dans $\Sigma_n(\mathbb{K}) \setminus \{0\}$.

En définitive $\Sigma_n(\mathbb{K}) \setminus \{0\}$ est un sous-groupe de $\mathbb{K}^*$.

9. On a toujours $\Sigma_n(\mathbb{K}) \subset \mathbb{K}$ et $0 \in \Sigma_n(\mathbb{K})$.

   Si le cône isotrope de la forme quadratique $Q(x) = \sum_{k=1}^{n} x_k^2$ n'est pas réduit à $\{0\}$, on peut trouver un vecteur x dans $\mathbb{K}^n$ tel que $Q(x) = 0$. Soit i un indice compris entre 1 et n te que $x_i \neq 0$. Pour $\lambda \in \mathbb{K}^*$, on note $\mu = \dfrac{\lambda}{4x_i^2}$ et y est le vecteur de $\mathbb{K}^n$ défini par :

$$x_k = \begin{cases} (1+\mu)\, x_i \text{ si } k = i \\ (1-\mu)\, x_k \text{ si } k \neq i \end{cases}$$

   On a alors :

$$\begin{aligned} Q(y) &= (1+\mu)^2 x_i^2 + (1-\mu)^2 \sum_{\substack{k=1 \\ k\neq i}}^{n} x_k^2 \\ &= (1+\mu)^2 x_i^2 + (1-\mu)^2 \left(Q(x) - x_i^2\right) \\ &= (1+\mu)^2 x_i^2 - (1-\mu)^2 x_i^2 = 4\mu x_i^2 = \lambda \end{aligned}$$

   c'est-à-dire que $\lambda = Q(y) \in \Sigma_n(\mathbb{K})$. On a donc bien $\Sigma_n(\mathbb{K}) = \mathbb{K}$.

– III – -1 comme sommes de carrés dans un corps

1. Comme $-1 \in \mathbb{R}^{-,*}$ et pour tout entier $n \geq 1$, on a $\Sigma_n(\mathbb{R}) \subset \mathbb{R}^+$, on déduit que $\nu(\mathbb{R}) = +\infty$.
   Comme $-1 = i^2 \in \Sigma_1(\mathbb{C})$, on a $\nu(\mathbb{C}) = 1$.
2. Si $\mathbb{K}$ est de caractéristique 2, on a alors $2 \cdot 1 = 0$ dans $\mathbb{K}$ et $-1 = 1^2 \in \Sigma_1(\mathbb{K})$, donc $\nu(\mathbb{K}) = 1$.
   Si $\mathbb{K}$ est de caractéristique 5, on a alors $5 \cdot 1 = 1 + 2^2 = 0$ dans $\mathbb{K}$ et $-1 = 2^2 \in \Sigma_1(\mathbb{K})$, donc $\nu(\mathbb{K}) = 1$.
3. (a) Dans $\mathbb{Z}_p^*$, l'égalité $x^2 = 1$ équivaut à $(x-1)(x+1) = 0$ encore équivalent à $x = 1$ ou $x = -1$. Le noyau du morphisme $\varphi : x \mapsto x^2$ est donc $\ker(\varphi) = \{-1, 1\}$ et ce noyau a deux éléments puisque $-1 \neq 1$ dans $\mathbb{Z}_p^*$ pour p premier impair.

   (b) Le morphisme φ qui est surjectif de $\mathbb{Z}_p^*$ sur $E = \mathrm{Im}(\varphi)$ réalise un isomorphisme du groupe quotient $\dfrac{\mathbb{Z}_p^*}{\ker(\varphi)}$ sur E. On a donc :

$$\mathrm{card}(E) = \mathrm{card}\left(\frac{\mathbb{Z}_p^*}{\ker(\varphi)}\right) = \frac{\mathrm{card}\left(\mathbb{Z}_p^*\right)}{\mathrm{card}(\ker(\varphi))} = \frac{p-1}{2}.$$

   (c) L'ensemble T étant en bijection avec $\Sigma_1(\mathbb{Z}_p)$, on a :

$$\mathrm{card}(T) = \mathrm{card}(\Sigma_1(\mathbb{Z}_p)) = \mathrm{card}(E) + 1 = \frac{p+1}{2}$$

   et nécessairement $T \cap \Sigma_1(\mathbb{Z}_p) \neq \emptyset$ (sinon $\mathrm{card}(T \cup \Sigma_1(\mathbb{Z}_p)) = p + 1 > p$, ce qui est incompatible avec $T \cup \Sigma_1(\mathbb{Z}_p)$ contenu dans $\mathbb{Z}_p$ de cardinal p).

(d) Il existe donc x dans $T \cap \Sigma_1(\mathbb{Z}_p)$ et un tel x s'écrit $x = a^2 = -1 - b^2$ avec a, b dans $\mathbb{Z}_p$, ce qui donne $-1 = a^2 + b^2 \in \Sigma_2(\mathbb{Z}_p)$ et $\nu(\mathbb{Z}_p) \leq 2$.
En fait, on sait que, pour p premier impair, -1 est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4. On a donc :

$$\nu(\mathbb{Z}_p) = \begin{cases} 1 \text{ si } p = 2 \text{ ou } p \equiv 1 \ (4) \\ 2 \text{ si } p \equiv 3 \ (4) \end{cases}$$

4. On rappelle que la caractéristique de $\mathbb{K}$ est l'entier naturel p qui vérifie $\ker(\varphi) = p\mathbb{Z}$, où φ est le morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$ défini par $\varphi(k) = k \cdot 1$ pour tout $k \in \mathbb{Z}$. Le morphisme φ induit alors par passage au quotient un morphisme du corps $\mathbb{Z}_p$ dans $\mathbb{K}$ et $\varphi(\mathbb{Z}_p)$ est un sous corps de $\mathbb{K}$. On a donc :
$$1 \leq \nu(\mathbb{K}) \leq \nu(\mathbb{Z}_p) \leq 2.$$
Pour p congru à 1 modulo 4, on a $\nu(\mathbb{K}) = 1$.

5. De $-1 = \sum_{k=1}^{\nu} x_k^2$ avec $\nu = \nu(\mathbb{K})$, on déduit que tous les x_k, pour k compris entre 1 et ν, sont non nuls (caractère minimal de ν).
Si $x = 0$, on a alors $-x_n^2 = \sum_{k=1}^{n-1} x_k^2$ et :
$$-1 = \sum_{k=1}^{n-1} \left(\frac{x_k}{x_n}\right)^2 = \sum_{k=1}^{n-1} y_k^2 \in \Sigma_{n-1}(\mathbb{K})$$
avec $n - 1 \leq \nu - 1 < \nu$, en contradiction avec le caractère minimal de ν. On a donc $x \neq 0$.
En écrivant que :
$$-1 = \sum_{k=1}^{\nu} x_k^2 = \sum_{k=1}^{n} x_k^2 + \sum_{k=n+1}^{\nu} x_k^2 = x + \sum_{k=n+1}^{\nu} x_k^2$$
et :
$$-x = 1^2 + \sum_{k=n+1}^{\nu} x_k^2 \in \Sigma_{\nu-n+1}(\mathbb{K})$$
avec $n = 2^p \leq \nu < 2^{p+1} = 2n$, soit $0 \leq \nu - n < n$ et $\nu - n + 1 \leq n$. Donc $-x \in \Sigma_n(\mathbb{K})$.
Comme n est une puissance de 2, $\Sigma_n(\mathbb{K})$ est multiplicatif (question **II.8.**) et $-x^2 = x(-x) \in \Sigma_n(\mathbb{K})$.
Enfin de $-x^2 = \sum_{k=1}^{n} z_k^2$ avec $x \neq 0$, on déduit que $-1 = \sum_{k=1}^{n} \left(\frac{z_k}{x}\right)^2 = \sum_{k=1}^{n} t_k^2 \in \Sigma_n(\mathbb{K})$ avec $n \leq \nu$, ce qui impose $n = \nu$ et ν est une puissance de 2.

6. On a vu que si $\mathbb{K}$ est de caractéristique non nulle, alors $\nu(\mathbb{K}) = 1 = 2^0$ ou $\nu(\mathbb{K}) = 2 = 2^1$ (question **III.4.**) et si $\mathbb{K}$ est de caractéristique nulle, alors son niveau est $+\infty$ ou une puissance de 2 (question **III.5.**).

– IV – Sommes de carrés dans $\mathbb{K}[X]$

1. Pour $n \geq 1$, on a toujours l'inclusion $\Sigma_n(\mathbb{K}[X]) \subset \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X))$.
Si $P \in \mathbb{K}[X] \cap \Sigma_1(\mathbb{K}(X))$, on a alors $P = \frac{A^2}{B^2}$ avec A, B dans $\mathbb{K}[X]$ premiers entre eux et de $A^2 = PB^2$, on déduit que B divise A^2, donc A (théorème de Gauss) et B est nécessairement constant non nul. On a alors $P = \left(\frac{A}{B}\right)^2 = (B^{-1}A)^2 \in \Sigma_1(\mathbb{K}[X])$. On a donc bien $\Sigma_1(\mathbb{K}[X]) = \mathbb{K}[X] \cap \Sigma_1(\mathbb{K}(X))$.

2. Si $\sum_{k=1}^{n-1} f_k^2 = -1$, on a alors :

$$\begin{aligned}(f+1)^2 + \sum_{k=1}^{n-1} \left(f_k\left(f-1\right)\right)^2 &= (f+1)^2 + (f-1)^2 \sum_{k=1}^{n-1} f_k^2 \\ &= (f+1)^2 - (f-1)^2 = 4f.\end{aligned}$$

3. Si $-1 \in \Sigma_{n-1}(\mathbb{K})$, il existe alors $f_1, \cdots, f_{n-1}$ dans $\mathbb{K}$ tels que $-1 = \sum_{k=1}^{n-1} f_k^2$. Pour tout $\lambda \in \mathbb{K}$, en prenant $f = \dfrac{\lambda}{4}$ dans l'identité obtenue à la question précédente, on a :

$$\lambda = 4f = (f+1)^2 + \sum_{k=1}^{n-1} \left(f_k\left(f-1\right)\right)^2 \in \Sigma_n(\mathbb{K}).$$

On a donc $\mathbb{K} = \Sigma_n(\mathbb{K})$.
Dire que $-1 \in \Sigma_{n-1}(\mathbb{K})$ entraîne que -1 est dans $\Sigma_n(\mathbb{K}[X])$ et dans $\Sigma_n(\mathbb{K}(X))$ et le raisonnement précédent nous montre que $\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X]$ et $\Sigma_n(\mathbb{K}(X)) = \mathbb{K}(X)$.

4. De $-1 = i^2 \in \Sigma_1(\mathbb{C}) \subset \Sigma_{n-1}(\mathbb{C})$ pour tout $n \geq 2$, on déduit de la question précédente que $\Sigma_n(\mathbb{C}(X)) = \mathbb{C}(X)$ est multiplicatif. Pour $n = 1$, $\Sigma_1(\mathbb{C}(X))$ est de manière évidente multiplicatif (mais $\Sigma_1(\mathbb{C}(X)) \subsetneq \mathbb{C}(X)$ – par exemple $\dfrac{1}{X} \notin \Sigma_1(\mathbb{C}(X))$, puisque $\dfrac{1}{X} = \dfrac{A^2}{B^2}$ donne $A^2 = XB^2$ de degré pair et impair, ce qui est impossible –).

5. Si $P = \sum_{k=1}^{n} P_k^2 = aX$, on a alors $P(0) = \sum_{k=1}^{n} P_k^2(0) = 0$. Si l'un des $P_k(0)$ est non nul, on a $-P_k^2(0) = \sum_{\substack{j=1 \\ j\neq k}}^{n} P_j^2(0)$ et $-1 = \sum_{\substack{j=1 \\ j\neq k}}^{n} a_j^2$ où on a noté $a_j = \dfrac{P_j(0)}{P_k(0)}$ dans $\mathbb{K}$, mais alors $-1 \in \Sigma_{n-1}(\mathbb{K})$, ce qui contredit l'hypothèse de départ. On a donc $P_k(0)$ pour tout k compris entre 1 et n, ce qui revient à dire que $P_k = XQ_k$ et $P = X^2 \sum_{k=1}^{n} Q_k^2 = aX$, soit $a = X \sum_{k=1}^{n} Q_k^2$ et l'évaluation en 0 donne $a = 0$. On a donc $P = \sum_{k=1}^{n} P_k^2 = 0$. Si les P_k ne sont pas tous nuls, en désignant par $m \geq 1$ la valuation minimale des P_k non nuls, on a $P_k = X^m R_k$ dans $\mathbb{K}[X]$ pour tout k compris entre 1 et m ($R_k = 0$ si $P_k = 0$ et $R_k(0) \neq 0$ pour certains indices k) et $X^{2m} \sum_{k=1}^{n} R_k^2 = 0$, donc $\sum_{k=1}^{n} R_k^2 = 0$ et $\sum_{k=1}^{n} R_k^2(0) = 0$ dans $\mathbb{K}$, certains des $R_k^2(0)$ étant non nuls (par définition de m), ce qui contredit $-1 \notin \Sigma_{n-1}(\mathbb{K})$. Les P_k sont donc tous nuls.

6.

(a) On a :

$$\begin{aligned}T^2P = (2S - QR)^2 P &= \left(4S^2 - 4SQR + Q^2R^2\right) P \\ &= \left(4S^2 - 4SQR\right) P + R^2 \sum_{k=1}^{n} P_k^2\end{aligned}$$

et :

$$\sum_{k=1}^{n} T_k^2 = \sum_{k=1}^{n} \left(2Q_kS - P_kR\right)^2$$
$$= 4S^2 \sum_{k=1}^{n} Q_k^2 - 4SR \sum_{k=1}^{n} P_kQ_k + R^2 \sum_{k=1}^{n} P_k^2$$
$$= 4S^2 \left(P - R\right) - 4SR \left(PQ - S\right) + R^2 \sum_{k=1}^{n} P_k^2$$
$$= \left(4S^2 - 4SQR\right) P + R^2 \sum_{k=1}^{n} P_k^2 = T^2P.$$

On a aussi :

$$QT = Q\left(2S - QR\right) = Q\left(2S - Q\left(P - \sum_{k=1}^{n} Q_k^2\right)\right)$$
$$= 2QS - PQ^2 + \sum_{k=1}^{n} \left(QQ_k\right)^2$$
$$= 2Q\left(PQ - \sum_{k=1}^{n} P_kQ_k\right) - PQ^2 + \sum_{k=1}^{n} \left(QQ_k\right)^2$$
$$= PQ^2 - 2Q \sum_{k=1}^{n} P_kQ_k + \sum_{k=1}^{n} \left(QQ_k\right)^2$$

et tenant compte de $Q^2P = \sum_{k=1}^{n} P_k^2$, on obtient :

$$QT = \sum_{k=1}^{n} P_k^2 - 2Q \sum_{k=1}^{n} P_kQ_k + \sum_{k=1}^{n} \left(QQ_k\right)^2$$
$$= \sum_{k=1}^{n} \left(P_k^2 - 2QP_kQ_k + \left(QQ_k\right)^2\right) = \sum_{k=1}^{n} \left(P_k - QQ_k\right)^2.$$

(b) Si $T = 0$, on a alors $\sum_{k=1}^{n} T_k^2 = T^2P = 0$ et tous les $T_k = 2Q_kS - P_kR$ sont nuls si $-1 \notin \Sigma_{n-1}\left(\mathbb{K}\right)$ (question **IV.5.**). On a alors $P_kT_k = 2P_kQ_kS - P_k^2R = 0$ pour tout k compris entre 1 et n et :

$$2S \sum_{k=1}^{n} P_kQ_k - R \sum_{k=1}^{n} P_k^2 = 0 \tag{2}$$

avec $\sum_{k=1}^{n} P_kQ_k = PQ - S$, $\sum_{k=1}^{n} P_k^2 = Q^2P$ et $T = 2S - QR = 0$, ce qui donne :

$$0 = 2S\left(PQ - S\right) - RQ^2P = PQ\left(2S - QR\right) - 2S^2 = -2S^2$$

et $S = 0$. De plus $T = 2S - QR = 0$ et $S = 0$ donnent $QR = 0$ avec $Q \neq 0$, donc $R = 0$ et $P = \sum_{k=1}^{n} Q_k^2$ par définition de R.

7. En effectuant, pour k compris entre 1 et n, la division euclidienne de P_k par Q (on a $\deg(Q) \geq 1$), on définit deux polynômes Q_k et R_k tels que :

$$P_k = QQ_k + R_k$$

avec R_k nul ou de degré strictement inférieur à celui de Q. En associant aux polynômes P, P_k, Q et Q_k les polynômes R, S, T et T_k de la question **IV.6.** et tenant compte de l'égalité $Q^2P = \sum_{k=1}^{n} P_k^2$, on a les égalités :

$$T^2P = \sum_{k=1}^{n} T_k^2 \text{ et } QT = \sum_{k=1}^{n} (P_k - QQ_k)^2 = \sum_{k=1}^{n} R_k^2.$$

Si $T \neq 0$, on pose $U = T$, $U_k = T_k$ pour k compris entre 1 et n et on a $PU \neq 0$ ($PQ \neq 0$) et :

$$\deg(Q) + \deg(U) = \deg(QU) = \deg(QT)$$
$$= \deg\left(\sum_{k=1}^{n} R_k^2\right) \leq \max_{1\leq k\leq n} \deg\left(R_k^2\right) < \deg\left(Q^2\right) = 2\deg(Q)$$

(les R_k ne sont pas tous nuls puisque $QT \neq 0$), donc $\deg(U) < \deg(Q)$.

Si $T = 0$, comme $Q \neq 0$ et $-1 \notin \Sigma_{n-1}(\mathbb{K})$, on a $P = \sum_{k=1}^{n} Q_k^2$ (question **IV.6.b.**). On pose alors $U = 1$ et $U_k = Q_k$ pour k compris entre 1 et n. On a bien $PU = P \neq 0$ et $\deg(U) = 0 < \deg(Q)$.

8. Pour $n = 1$, on a déjà montré en **IV.1.** que $\Sigma_1(\mathbb{K}[X]) = \mathbb{K}[X] \cap \Sigma_1(\mathbb{K}(X))$.
On suppose donc que $n \geq 2$. L'inclusion $\Sigma_n(\mathbb{K}[X]) \subset \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X))$ est évidente.
Si $-1 \in \Sigma_{n-1}(\mathbb{K})$, en **IV.3.** que $\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X]$ et $\Sigma_n(\mathbb{K}(X)) = \mathbb{K}(X)$, donc :

$$\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X] \cap \mathbb{K}(X) = \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X)).$$

Supposons que $-1 \notin \Sigma_{n-1}(\mathbb{K})$ et soit $P \in \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X))$. Si $P = 0$, il est bien dans $\Sigma_n(\mathbb{K}[X])$. On suppose donc que P est non nul. Comme il est dans $\Sigma_n(\mathbb{K}(X))$, il existe des polynômes A_k et B_k tels que $P = \sum_{k=1}^{n} \frac{A_k^2}{B_k^2}$ et en réduisant au même dénominateur, on dispose de polynômes P_k et Q tels que $Q^2P = \sum_{k=1}^{n} P_k^2$ avec $Q \neq 0$. Si le polynôme Q est constant, il est alors dans $\mathbb{K}^*$ et P est dans $\Sigma_n(\mathbb{K}[X])$. Sinon, $\deg(Q) \geq 1$ et la question précédente nous dit que qu'on dispose de polynômes $U, U_1, \cdots, U_n$ tels que $U^2P = \sum_{k=1}^{n} U_k^2$ avec $PU \neq 0$ et $\deg(U) < \deg(Q)$. En réitérant ce raisonnement, on aboutit au bout d'un nombre fini d'étapes à un polynôme constant non nul U et des polynômes U_k tel que $U^2P = \sum_{k=1}^{n} U_k^2$, ce qui implique que $P \in \Sigma_n(\mathbb{K}[X])$. On a donc l'inclusion $\mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X)) \subset \Sigma_n(\mathbb{K}[X])$ et l'égalité pour tout $n \geq 1$.

9.

(a) De $\mathbb{K} \subset \mathbb{K}(X)$, on déduit que $\nu(\mathbb{K}(X)) \leq \nu(\mathbb{K})$.
Si $\nu(\mathbb{K}(X)) = +\infty$, on a aussi $\nu(\mathbb{K}) = +\infty$ et $\nu(\mathbb{K}(X)) = \nu(\mathbb{K})$.
Si $\nu(\mathbb{K}(X)) = \nu < +\infty$, on dispose de fonctions rationnelles f_k telles que $-1 = \sum_{k=1}^{\nu} f_k^2$ dans $\mathbb{K}(X)$ et l'évaluation en 0 donne $-1 = \sum_{k=1}^{\nu} f_k^2(0)$ dans $\mathbb{K}$, ce qui entraîne $\nu(\mathbb{K}) \leq \nu = \nu(\mathbb{K}(X))$ et $\nu(\mathbb{K}(X)) = \nu(\mathbb{K})$.

(b) Si n est une puissance de 2, le résultat de la question **II.8.** appliqué au corps $\mathbb{K}(X)$ nous dit que $\Sigma_n(\mathbb{K}[X])$ est multiplicatif. Il en résulte que $\Sigma_n(\mathbb{K}[X]) = \mathbb{K}[X] \cap \Sigma_n(\mathbb{K}(X))$ est multiplicatif comme produit de deux ensembles multiplicatifs.