

DM 52 : Corrigé.

Il s'agit d'un problème posé pour l'agrégation interne de 1993, avec quelques aménagements.

Partie I

1°) Soit $(\alpha, \beta) \in S_2(B)^2$.

Il existe $(x, y, z, t) \in B^4$ tel que $\alpha = x^2 + y^2$ et $\beta = z^2 + t^2$.

$$\begin{aligned}\alpha\beta &= (x^2 + y^2)(z^2 + t^2) = |x + iy|^2 |z + it|^2 \\ &= |(x + iy)(z + it)|^2 = |(xz - yt) + i(yz + xt)|^2 \\ &= (xz - yt)^2 + (yz + xt)^2,\end{aligned}$$

or B étant un anneau, $xz - yt$ et $yz + xt$ sont des éléments de B , donc $\alpha\beta \in S_2(B)$, ce qui prouve que $S_2(B)$ est multiplicatif.

2°)

- D'après la résolution de la question précédente, dans l'anneau B ,

$$(*) \iff (x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (yz + xt)^2.$$

Démontrons que cette identité reste valable dans un anneau commutatif A quelconque.

Soit $(x, y, z, t) \in A^4$. $(xz - yt)^2 + (yz + xt)^2 = x^2z^2 + y^2t^2 - 2xzyt + y^2z^2 + x^2t^2 + 2yzxt$, car A est commutatif, donc

$$(xz - yt)^2 + (yz + xt)^2 = x^2z^2 + y^2t^2 + y^2z^2 + x^2t^2 = (x^2 + y^2)(z^2 + t^2).$$

- Soit $(\alpha, \beta) \in S_2(A)^2$.

Il existe $(x, y, z, t) \in A^4$ tel que $\alpha = x^2 + y^2$ et $\beta = z^2 + t^2$.

$$\alpha\beta = (x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (yz + xt)^2 \in S_2(A),$$

donc $S_2(A)$ est multiplicatif.

3°)

a) Soit $n \in \mathbb{Z}$.

Si n est pair, il existe $h \in \mathbb{Z}$ tel que $n = 2h$, donc $n^2 \equiv 4h^2 \equiv 0 \pmod{4}$.

Si n est impair, il existe $h \in \mathbb{Z}$ tel que $n = 2h + 1$, donc $n^2 \equiv 4h^2 + 4h + 1 \equiv 1 \pmod{4}$.

Ainsi n^2 est congru à 0 ou à 1 modulo 4.

b) Pour tout $i \in \{1, 2, 3\}$, x_i^2 est congru à 0 ou à 1 modulo 4. Ainsi, si l'un des x_i au moins est pair, $x_1^2 + x_2^2 + x_3^2$ est congru à 0, 1 ou 2 modulo 4, ce qui est faux car $x_1^2 + x_2^2 + x_3^2 = 15 \equiv 3 \pmod{4}$. On a donc montré que x_1, x_2 et x_3 sont impairs.

c) Quitte à remplacer x_i par $-x_i$ et à intervertir l'ordre de x_1, x_2 et x_3 , on peut supposer que $0 \leq x_1 \leq x_2 \leq x_3$.

De plus, $x_3^2 \leq x_1^2 + x_2^2 + x_3^2 = 15$, donc $x_3 \leq \sqrt{15} < \sqrt{16} = 4$. Ainsi, $x_3 \in \{1, 3\}$.

Etudions tous les cas possibles.

- ◊ Si $x_1 = 3$, alors $x_1 = x_2 = x_3 = 3$, donc $15 = x_1^2 + x_2^2 + x_3^2 = 27$, ce qui est faux.
- ◊ Si $x_1 = 1$ et $x_2 = 3$, alors $x_3 = 3$ et $15 = x_1^2 + x_2^2 + x_3^2 = 19$, ce qui est faux.
- ◊ Si $x_1 = 1, x_2 = 1$ et $x_3 = 3$, alors $15 = x_1^2 + x_2^2 + x_3^2 = 11$, ce qui est faux.
- ◊ Enfin, si $x_1 = 1, x_2 = 1$ et $x_3 = 1$, alors $15 = x_1^2 + x_2^2 + x_3^2 = 3$, ce qui est encore faux.

On en déduit qu'il n'existe aucun triplet $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tel que $15 = x_1^2 + x_2^2 + x_3^2$, c'est-à-dire que $15 \notin S_3(\mathbb{Z})$.

• $3 = 1^2 + 1^2 + 1^2 \in S_3(\mathbb{Z})$ et $5 = 0^2 + 1^2 + 2^2 \in S_3(\mathbb{Z})$, mais $3 \times 5 = 15 \notin S_3(\mathbb{Z})$, donc $S_3(\mathbb{Z})$ n'est pas multiplicatif.

4°)

$$\begin{aligned} S_1(E) &= \{x^2/x \in \mathbb{Z}/8\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{4}\}. \\ S_2(E) &= S_1(E) + S_1(E) = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}\}. \\ S_3(E) &= S_2(E) + S_1(E) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = (\mathbb{Z}/8\mathbb{Z}) \setminus \{\bar{7}\}. \end{aligned}$$

5°) Supposons que l'un de ces nombres est impair.

Quitte à réordonner a, b, c et d , on peut supposer qu'il s'agit de a .

$\bar{a}^2 \in S_1(E)$ et a^2 est impair, donc $\bar{a}^2 = \bar{1}$.

Ainsi, $b^2 + c^2 + d^2 \equiv 7 \pmod{8}$, donc, dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{7} = \bar{b}^2 + \bar{c}^2 + \bar{d}^2 \in S_3(E)$, ce qui est faux.

Ainsi, les quatre nombres a, b, c et d sont pairs.

6°) Soit n un entier relatif congru à -1 modulo 8.

• Supposons que $n \in S_3(\mathbb{Z})$. Il existe $(a, b, c) \in \mathbb{Z}^3$ tel que $n = a^2 + b^2 + c^2$, donc $a^2 + b^2 + c^2 \equiv -1 \equiv 7 \pmod{8}$. Ainsi, $\bar{7} \in S_3(E)$, ce qui est faux. On a donc montré que $n \notin S_3(\mathbb{Z})$.

• Supposons que $n \in S_3(\mathbb{Q})$. Il existe $(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}) \in \mathbb{Q}^3$ tel que $n = \frac{a_1^2}{b_1^2} + \frac{a_2^2}{b_2^2} + \frac{a_3^2}{b_3^2}$.

En multipliant par $(b_1 b_2 b_3)^2$, on obtient : $n(b_1 b_2 b_3)^2 = a_1^2 b_2^2 b_3^2 + a_2^2 b_1^2 b_3^2 + a_3^2 b_1^2 b_2^2$, donc il existe $(a, b, c, d) \in \mathbb{Z}^4$ tel que $d \neq 0$ et $nd^2 = a^2 + b^2 + c^2$.

En divisant cette égalité par une puissance convenable de 2, on peut supposer que l'un des nombres a, b, c ou d est impair.

Or $a^2 + b^2 + c^2 \equiv -d^2 \pmod{8}$. C'est impossible d'après la question 5. On a donc montré que $n \notin S_3(\mathbb{Q})$.

7°) $15 \equiv -1 \pmod{8}$, donc $15 \notin S_3(\mathbb{Q})$, or $3 \in S_3(\mathbb{Z}) \subset S_3(\mathbb{Q})$ et $5 \in S_3(\mathbb{Q})$, donc

$$\boxed{S_3(\mathbb{Q}) \text{ n'est pas multiplicatif.}}$$

8°)

a) On suppose que f est de degré 2, donc il existe $(a, b, c) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}$ tel que $f(X) = aX^2 + bX + c$.

Au voisinage de $+\infty$, $f(t) \sim at^2$ et $f(t) \geq 0$, donc $a > 0$. De plus f possède au plus une racine réelle, donc $\Delta = b^2 - 4ac \leq 0$.

Ainsi, $f(X) = \left(\sqrt{a}X + \frac{b}{2\sqrt{a}}\right)^2 + c - \frac{b^2}{4a} = \left(\sqrt{a}X + \frac{b}{2\sqrt{a}}\right)^2 + \left(\frac{\sqrt{-\Delta}}{2\sqrt{a}}\right)^2 \in S_2(\mathbb{R}[X])$.

b) Soit α une racine réelle de f . Notons m sa multiplicité.

Il existe $P \in \mathbb{R}[X]$ tel que $f(X) = (X - \alpha)^m P(X)$ avec $P(\alpha) \neq 0$.

Au voisinage de α , $f(x) \sim P(\alpha)(x - \alpha)^m$, or le signe de f est constant, donc m est nécessairement pair.

c) La décomposition de f en facteurs irréductibles est donc de la forme :

$$f(X) = a \prod_{i=1}^k (X - \alpha_i)^{2m_i} \prod_{j=1}^h (X^2 + b_j X + c_j)^{n_j}, \text{ où } a > 0, (k, h) \in \mathbb{N}^{*2}, \text{ pour tout } i \in \mathbb{N}_k,$$

$\alpha_i \in \mathbb{R}$ et $m_i \in \mathbb{N}^*$, et pour tout $j \in \mathbb{N}_h$, $n_j \in \mathbb{N}^*$ et $X^2 + b_j X + c_j$ est un polynôme de $\mathbb{R}[X]$ de discriminant strictement négatif.

- ◇ $a = \sqrt{a^2} \in S_1(\mathbb{R}[X]) \subset S_2(\mathbb{R}[X])$,
- ◇ pour tout $i \in \mathbb{N}_k$, $(X - \alpha_i)^2 \in S_1(\mathbb{R}[X]) \subset S_2(\mathbb{R}[X])$,
- ◇ et, pour tout $j \in \mathbb{N}_h$, d'après le début de cette question, $X^2 + b_j X + c_j \in S_2(\mathbb{R}[X])$.

Or, d'après la question 2, $S_2(\mathbb{R}[X])$ est multiplicatif, donc $f \in S_2(\mathbb{R}[X])$.

• On a donc montré que $\{g \in \mathbb{R}[X] / \forall x \in \mathbb{R} \ g(x) \geq 0\} \subset S_2(\mathbb{R}[X])$.

Réciproquement, si $g \in S_2(\mathbb{R}[X])$, il existe $(P, Q) \in \mathbb{R}[X]^2$ tel que $g(X) = P(X)^2 + Q(X)^2$, donc, pour tout $x \in \mathbb{R}$, $g(x) \geq 0$.

Ainsi, $\{g \in \mathbb{R}[X] / \forall x \in \mathbb{R} \ g(x) \geq 0\} = S_2(\mathbb{R}[X])$.

9°)

• Soit $n \in \mathbb{N}$ avec $n \geq 3$.

Si $f \in S_2(\mathbb{R}[X])$, il existe $(P, Q) \in \mathbb{R}[X]^2$ tel que $f(X) = P(X)^2 + Q(X)^2$,

donc $f(X) = P(X)^2 + Q(X)^2 + \sum_{h=3}^n 0^2 \in S_n(\mathbb{R}[X])$.

Réciproquement, si $f \in S_n(\mathbb{R}[X])$, pour tout $x \in \mathbb{R}$, $f(x) \geq 0$, donc, d'après la question précédente, $f \in S_2(\mathbb{R}[X])$.

On a ainsi montré que $S_2(\mathbb{R}[X]) = S_n(\mathbb{R}[X])$.

• Soit $f \in S_2(\mathbb{R}(X))$. Il existe $(P, Q) \in \mathbb{R}(X)^2$ tel que $f(X) = P(X)^2 + Q(X)^2$, donc

$f(X) = P(X)^2 + Q(X)^2 + \sum_{h=3}^n 0^2 \in S_n(\mathbb{R}(X))$, ce qui montre que $S_2(\mathbb{R}(X)) \subset S_n(\mathbb{R}(X))$.

Réciproquement, soit $F \in S_n(\mathbb{R}(X))$.

Il existe $(P_i)_{1 \leq i \leq n} \in \mathbb{R}[X]^n$ et $(Q_i)_{1 \leq i \leq n} \in (\mathbb{R}[X] \setminus \{0\})^n$ tels que $F = \sum_{i=1}^n \frac{P_i^2}{Q_i^2}$.

Ainsi, $\left(\prod_{i=1}^n Q_i\right)^2 F \in S_n(\mathbb{R}[X]) = S_2(\mathbb{R}[X])$, donc il existe $(P, Q) \in \mathbb{R}[X]^2$ tel que

$$\left(\prod_{i=1}^n Q_i\right)^2 F = P^2 + Q^2.$$

$$\text{Ainsi, } F = \left(\frac{P}{\prod_{i=1}^n Q_i}\right)^2 + \left(\frac{Q}{\prod_{i=1}^n Q_i}\right)^2 \in S_2(\mathbb{R}(X)).$$

On a donc montré que $\boxed{S_n(\mathbb{R}(X)) = S_2(\mathbb{R}(X))}$.

Partie II

1°)

- Dans \mathbb{R} ou \mathbb{C} , pour tout $n \geq 1$, $n.1 = n \neq 0$, donc $\text{car}(\mathbb{R}) = \text{car}(\mathbb{C}) = 0$.
- Soit $n \in \mathbb{N}^*$. Pour tout $x \in S_n(\mathbb{R})$, $x \geq 0$, donc $-1 \notin S_n(\mathbb{R})$. Ainsi, $\boxed{s(\mathbb{R}) = +\infty}$.
- $-1 = i^2 \in S_1(\mathbb{C})$, donc $\boxed{s(\mathbb{C}) = 1}$.

2°)

a) Dans $\mathbb{Z}/p\mathbb{Z}$, pour tout $n \in \mathbb{N}^*$, $n.1 = 0 \iff \bar{n} = \bar{0} \iff n \in p\mathbb{Z}$, donc $\text{car}(\mathbb{Z}/p\mathbb{Z}) = p$.

b)

- Soit k un corps de caractéristique 2. $1_k + 1_k = 0_k$, donc $-1_k = 1_k = 1_k^2 \in S_1(k)$, donc $\boxed{s(k) = 1}$.
- Soit k un corps de caractéristique 5. $1_k + 4.1_k = 0_k$, donc $-1_k = (2.1_k)^2 \in S_1(k)$, donc $\boxed{s(k) = 1}$.

3°) a) Notons $\varphi : \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{array}$. Il s'agit d'un endomorphisme de groupes.

$x \in \text{Ker}(\varphi) \iff x^2 = 1 \iff (x-1)(x+1) = 0 \iff x \in \{1, -1\}$, car \mathbb{F}_p est un corps. Ainsi, $\boxed{\text{Ker}(\varphi) = \{-1, 1\}}$.

3°) b)

- $-A = \{\overline{-1}, \overline{-2}, \dots, \overline{\left(\frac{1-p}{2}\right)}\}$, donc

$$-A = \{\overline{p-1}, \overline{p-2}, \dots, \overline{p + \frac{1-p}{2}}\} = \left\{\overline{\left(\frac{p+1}{2}\right)}, \dots, \overline{p-2}, \overline{p-1}\right\}.$$

Ainsi, $A \cup (-A) = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\} = \mathbb{F}_p^*$.

De plus, A et $-A$ sont non vides et $A \cap (-A) = \emptyset$, donc A et $-A$ constituent une partition de \mathbb{F}_p^* .

- Notons $u : \begin{array}{ccc} A & \longrightarrow & E \\ x & \longmapsto & x^2 \end{array}$.

Soit $x \in E$. Il existe $y \in \mathbb{F}_p^*$ tel que $y^2 = x$.

Si $y \in A$, alors $x = \varphi(y) = u(y)$.

Sinon, $y \in (-A)$, donc $x = (-y)^2 = u(-y)$.

Ainsi, dans tous les cas, x possède au moins un antécédent par u , ce qui prouve que u est surjective.

Soit $(x, y) \in A^2$ tel que $u(x) = u(y)$. Ainsi, $x^2 = y^2$, donc $(x - y)(x + y) = 0$.

\mathbb{F}_p étant un corps, on en déduit que $x = y$ ou bien que $x = -y$.

Si $x = -y$, alors $x \in A \cap (-A) = \emptyset$, ce qui est impossible, donc $x = y$. On a ainsi prouvé l'injectivité de u .

u est donc une bijection de A dans E .

3°) c) L'application
$$\begin{array}{ccc} S_1(\mathbb{F}_p) & \longrightarrow & T \\ y & \longmapsto & -1 - y \end{array}$$
 est surjective par définition de T et elle est injective, car, pour tout $(y, z) \in S_1(\mathbb{F}_p)^2$, $-1 - y = -1 - z \implies y = z$.

On en déduit que $\text{card}(T) = \text{card}(S_1(\mathbb{F}_p))$.

Supposons que $T \cap S_1(\mathbb{F}_p) = \emptyset$. Alors, $p = \text{card}(\mathbb{F}_p) \geq \text{card}(T \cup S_1(\mathbb{F}_p)) = 2\text{card}(S_1(\mathbb{F}_p))$.

Or $S_1(\mathbb{F}_p) = \{x^2/x \in \mathbb{F}_p\} = E \cup \{0\}$,

donc $\text{card}(S_1(\mathbb{F}_p)) = 1 + \text{card}(E) = 1 + \text{card}(A) = 1 + \frac{p-1}{2} = \frac{p+1}{2}$.

Ainsi, si $T \cap S_1(\mathbb{F}_p) = \emptyset$, $p \geq p+1$, ce qui est faux.

On a donc montré que $T \cap S_1(\mathbb{F}_p)$ est non vide.

3°) d) Il existe $x \in T \cap S_1(\mathbb{F}_p)$.

$x \in S_1(\mathbb{F}_p)$, donc il existe $x_1 \in \mathbb{F}_p$ tel que $x = x_1^2$.

$x \in T$, donc il existe $y \in S_1(\mathbb{F}_p)$ tel que $x = -1 - y$. De plus, $y \in S_1(\mathbb{F}_p)$, donc il existe $x_2 \in \mathbb{F}_p$ tel que $y = x_2^2$.

Ainsi, $x_1^2 = -1 - x_2^2$, ce qui prouve que $-1 = x_1^2 + x_2^2 \in S_2(\mathbb{F}_p)$.

On en déduit que $s(\mathbb{F}_p) \leq 2$.

4°) a) \diamond Posons
$$\begin{array}{ccc} f & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \bar{h} & \longmapsto & h.1 \end{array}$$
 et montrons d'abord que f est correctement défini,

c'est-à-dire que si $h, \ell \in \mathbb{Z}$ vérifient $\bar{h} = \bar{\ell}$, alors $h.1 = \ell.1$: en effet, il existe $\alpha \in \mathbb{Z}$ tel que $h = \ell + \alpha n$, donc $h.1 = \ell.1 + \alpha n.1$, mais par définition de la caractéristique de k , $n.1 = 0$, donc $h.1 = \ell.1$.

\diamond On a clairement $f(\bar{1}) = 1.1 = 1$, $f(\bar{h} + \bar{\ell}) = f(\bar{h}) + f(\bar{\ell})$ et $f(\bar{h}.\bar{\ell}) = f(\bar{h}).f(\bar{\ell})$, donc f est un morphisme d'anneaux.

\diamond Si $f(\bar{h}) = 0$, alors $h.1 = 0$. Ecrivons la division euclidienne de h par n : $h = nq + r$ où $0 \leq r < n$. On a $r.1 = h.1 - nq.1 = h.1 = 0$, mais $r < n$, donc par définition de la caractéristique de k , $r = 0$. Ainsi $h = nq$ puis $\bar{h} = 0$. On a montré que $\text{Ker}(f) = \{0\}$, donc f est un morphisme injectif.

b) Soit $h, \ell \in \mathbb{Z}$ tel que, dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{h}.\bar{\ell} = 0$. Alors $0 = f(0) = f(\bar{h}.\bar{\ell}) = f(\bar{h}).f(\bar{\ell})$, mais k étant un corps, il est intègre, et $f(\bar{h}), f(\bar{\ell}) \in k$, donc $f(\bar{h}) = 0$ ou bien $f(\bar{\ell}) = 0$, or f est injectif, donc $\bar{h} = 0$ ou bien $\bar{\ell} = 0$. Ainsi $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre, donc d'après le cours, n est un nombre premier.

c) Si $n = 2$, d'après la question II.2, $s(k) = 1 \leq 2$.

Supposons que $n \geq 3$. n est premier, donc d'après la question II.3.d,

il existe $(x_1, x_2) \in \mathbb{F}_n^2$ tel que $-\bar{1} = x_1^2 + x_2^2$.

L'image par f de cette égalité donne : $-1_k = -f(\bar{1}) = f(-\bar{1}) = f(x_1)^2 + f(x_2)^2$, donc $s(k) \leq 2$.

5°)

• Supposons que $x = 0$. Alors, $-1 = x + \sum_{h=n+1}^s x_h^2 = \sum_{h=n+1}^s x_h^2$, donc $-1 \in S_{s-n}(k)$, ce qui implique que $s \leq s - n$, donc que $n = 0$. Or $s \geq 1 = 2^0$, donc $n \geq 1$. Ainsi, $x \neq 0$.

• $-1 = x + \sum_{i=n+1}^s x_i^2$, donc $-x = 1^2 + \sum_{i=n+1}^s x_i^2 \in S_{s-n+1}(k)$.

Or, par définition de n , $2n > s$, donc $s - n < n$. On en déduit que $s - n + 1 \leq n$, puis que $-x \in S_n(k)$.

• $x = \sum_{i=1}^n x_i^2 \in S_n(k)$ et $-x \in S_n(k)$, or, n étant une puissance de 2 et k étant de caractéristique nulle, d'après un résultat admis par l'énoncé à la fin de la première partie, $S_n(k)$ est multiplicatif. On en déduit que $-x^2 = (-x)x \in S_n(k)$.

• Il existe donc $(y_1, \dots, y_n) \in k^n$ tel que $-x^2 = \sum_{i=1}^n y_i^2$.

De plus, $x \neq 0$, donc $-1 = \sum_{i=1}^n \left(\frac{y_i}{x}\right)^2 \in S_n(k)$.

• On en déduit que $s \leq n$, or $n \leq s$. Ainsi $s = n$, ce qui prouve que s est une puissance de 2.

6°) Soit k un corps commutatif de niveau $s \neq +\infty$.

Premier cas. Supposons que k est de caractéristique non nulle. Alors, d'après la question II.4, $s(k) \in \{1, 2\}$, donc $s(k)$ est une puissance de 2.

Deuxième cas. Supposons que k est de caractéristique nulle. Alors, d'après la question II.5, $s(k)$ est une puissance de 2.

Partie III

1°)

• Soit $P \in S_1(A)$. Il existe $Q \in A$ tel que $P = Q^2$.

$A \subset K$, donc $Q \in K$ et $P = Q^2 \in S_1(K)$. Ainsi, $P \in A \cap S_1(K)$.

On a donc prouvé que $S_1(A) \subset A \cap S_1(K)$.

• Réciproquement, soit $P \in A \cap S_1(K)$.

Il existe $F \in K$ tel que $P = F^2$,

et il existe $(Q, Q') \in A^2$ tel que $F = \frac{Q}{Q'}$, Q et Q' étant premiers entre eux.

$Q'^2 P = Q^2$, donc Q' est un diviseur commun de Q' et de Q^2 , or Q' et Q^2 sont premiers entre eux, donc $Q' \in k \setminus \{0\}$.

Ainsi, $F = \frac{1}{Q'} Q \in A$ et $P = F^2 \in S_1(A)$.

On a donc prouvé que $A \cap S_1(K) \subset S_1(A)$.

2°)

$$\begin{aligned} (b+1)^2 + \sum_{i=1}^{n-1} (a_i(b-1))^2 &= (b+1)^2 + (b-1)^2 \sum_{i=1}^{n-1} a_i^2 \\ &= (b+1)^2 - (b-1)^2 = 4b. \end{aligned}$$

On a donc montré que $\boxed{(b+1)^2 + \sum_{i=1}^{n-1} (a_i(b-1))^2 = 4b}$.

3°) Supposons qu'il existe $n \geq 2$ tel que $-1 \in S_{n-1}(k)$.

Il existe donc $(a_1, \dots, a_{n-1}) \in k^{n-1}$ tel que $-1 = \sum_{i=1}^{n-1} a_i^2$.

Soit $b \in K$. k est un sous-corps de \mathbb{C} , donc $4.1_k \neq 0$. Ainsi,

$$\begin{aligned} b = \frac{1}{4.1_k}(4b) &= \frac{1}{4.1_k} \left[(b+1)^2 + \sum_{i=1}^{n-1} (a_i(b-1))^2 \right] \\ &= \left(\frac{b+1}{2.1_k} \right)^2 + \sum_{i=1}^{n-1} \left(\frac{a_i(b-1)}{2.1_k} \right)^2. \end{aligned}$$

La relation précédente montre que,

- ◇ si $b \in k$, alors $b \in S_n(k)$,
- ◇ si $b \in A$, alors $b \in S_n(A)$
- ◇ et si $b \in K$, alors $b \in S_n(K)$.

Ainsi, $k \subset S_n(k)$, $A \subset S_n(A)$ et $K \subset S_n(K)$.

Les inclusions réciproques sont claires.

4°) Pour $n = 1$, $S_n(\mathbb{C}(X)) = \{F^2/F \in \mathbb{C}(X)\}$, donc $S_n(\mathbb{C}(X))$ est multiplicatif. Pour $n \geq 2$, $-1 \in S_1(\mathbb{C}) \subset S_{n-1}(\mathbb{C})$, donc $S_n(\mathbb{C}(X)) = \mathbb{C}(X)$ est aussi multiplicatif.

5°) Soient $a \in k$ et $(R_1, \dots, R_n) \in A^n$ tels que $aX = \sum_{i=1}^n R_i^2$.

Supposons qu'il existe $i_0 \in \mathbb{N}_n$ tel que $R_{i_0} \neq 0$.

Pour tout $i \in \mathbb{N}_n$, notons $R_i = \sum_{j \in \mathbb{N}} a_{i,j} X^j$ et posons $J = \{j \in \mathbb{N} / \exists i \in \mathbb{N}_n \ a_{i,j} \neq 0\}$.

J est non vide car $R_{i_0} \neq 0$, et J est une partie de \mathbb{N} , donc J admet un minimum, que l'on notera h . Par définition de h , il existe $i_1 \in \mathbb{N}_n$ tel que $a_{i_1,h} \neq 0$,

et, pour tout $j \in \{0, \dots, h-1\}$, pour tout $i \in \mathbb{N}_n$, $a_{i,j} = 0$.

Ainsi, pour tout $i \in \mathbb{N}_n$, il existe $Q_i \in A$ tel que $R_i = a_{i,h} X^h + Q_i X^{h+1}$.

$$aX = \sum_{i=1}^n R_i^2 = X^{2h} \sum_{i=1}^n a_{i,h}^2 + 2X^{2h+1} \sum_{i=1}^n a_{i,h} Q_i + X^{2h+2} \sum_{i=1}^n Q_i^2.$$

Ainsi, le coefficient de degré $2h$ de aX vaut $\sum_{i=1}^n a_{i,h}^2$. On a donc : $\sum_{i=1}^n a_{i,h}^2 = 0$.

Or $a_{i_1,h} \neq 0$, donc $-1 = \sum_{\substack{1 \leq i \leq n \\ i \neq i_1}} \left(\frac{a_{i,h}}{a_{i_1,h}} \right)^2 \in S_{n-1}(k)$, ce qui est faux.

On en déduit que, pour tout $i \in \mathbb{N}_n$, $R_i = 0$.

6°) a) On suppose que la relation (1) est vérifiée.

$$\begin{aligned} \sum_{i=1}^n P_i'^2 &= \sum_{i=1}^n (4Q_i^2 T^2 + P_i^2 S^2 - 4Q_i T P_i S) \\ &= 4T^2 \sum_{i=1}^n Q_i^2 + S^2 \sum_{i=1}^n P_i^2 - 4TS \sum_{i=1}^n P_i Q_i \\ &= 4T^2(P - S) + S^2 P Q^2 - 4TS(PQ - T) \\ &= 4T^2 P + S^2 Q^2 P - 4TSQP \\ &= (2T - SQ)^2 P = Q'^2 P, \end{aligned}$$

ce qui démontre la relation (2).

$$\begin{aligned} \sum_{i=1}^n (P_i - QQ_i)^2 &= \sum_{i=1}^n (P_i^2 + Q^2 Q_i^2 - 2QP_i Q_i) \\ &= Q^2 P + Q^2(P - S) - 2Q(PQ - T) \\ &= -Q^2 S + 2QT \\ &= Q(2T - QS) = QQ', \end{aligned}$$

ce qui démontre la relation (3).

6°) b) $\sum_{i=1}^n (P_i - QQ_i)^2 = QQ' = 0$, donc, si l'on pose $a = 0$, $\sum_{i=1}^n (P_i - QQ_i)^2 = aX$.

D'après la question III.5, pour tout $i \in \mathbb{N}_n$, $P_i = QQ_i$.

Ainsi, $Q^2 P = \sum_{i=1}^n P_i^2 = \sum_{i=1}^n Q^2 Q_i^2 = Q^2 \sum_{i=1}^n Q_i^2$, or $Q \neq 0$, donc $P = \sum_{i=1}^n Q_i^2$.

7°) Pour tout $i \in \mathbb{N}_n$, notons Q_i et R_i le quotient et le reste de la division euclidienne de P_i par Q . Ainsi, $P_i = Q_i Q + R_i$ et $\deg(R_i) < \deg(Q)$.

En reprenant les notations introduites par l'énoncé à la question III.6,

on obtient : $Q'^2 P = \sum_{i=1}^n P_i'^2$.

De plus, $QQ' = \sum_{i=1}^n (P_i - QQ_i)^2 = \sum_{i=1}^n R_i^2$, donc $\deg(QQ') \leq \max_{1 \leq i \leq n} \deg(R_i^2) < 2\deg(Q)$,

ce qui prouve que $\deg(Q') < \deg(Q)$.

Si $Q' \neq 0$, on a bien : $Q'^2 P = \sum_{i=1}^n P_i'^2$, $PQ' \neq 0$ et $\deg(Q') < \deg(Q)$.

Si $Q' = 0$, d'après la question III.6.b, $P = \sum_{i=1}^n Q_i^2$. De plus, $P.1 \neq 0$ et $\deg(1) = 0 <$

$\deg(Q)$,

donc, en posant $Q'' = 1$ et, pour tout $i \in \mathbb{N}_n$, $P''_i = Q_i$, on obtient encore le résultat attendu.

8°) Le cas où $n = 1$ a déjà été prouvé à la question III.1. Supposons maintenant que $n \geq 2$.

L'inclusion $S_n(A) \subset (A \cap S_n(K))$ est claire.

Réciproquement, soit $P \in A \cap S_n(K)$.

Premier cas. Supposons que $P = 0$. Alors $P = \sum_{i=1}^n 0^2 \in S_n(A)$.

Deuxième cas. Supposons que $-1 \in S_{n-1}(k)$.

Alors, d'après la question III.3, $P \in A \cap K = A = S_n(A)$.

Troisième cas. Supposons que $-1 \notin S_{n-1}(k)$ et que $P \neq 0$.

Il existe $(F_1, \dots, F_n) \in K^2$ tel que $P = \sum_{i=1}^n F_i^2$. De plus, pour tout $i \in \mathbb{N}_n$, il existe

$(R_i, Q_i) \in A \times (A \setminus \{0\})$ tel que $F_i = \frac{R_i}{Q_i}$.

Ainsi, $\left(\prod_{i=1}^n Q_i\right)^2 P = \sum_{i=1}^n \left[\left(\prod_{\substack{1 \leq j \leq n \\ j \neq i}} Q_j\right) R_i \right]^2$.

Posons $Q = \prod_{i=1}^n Q_i \in A$ et, pour tout $i \in \mathbb{N}_n$, $P_i = \left(\prod_{\substack{1 \leq j \leq n \\ j \neq i}} Q_j\right) R_i \in A$.

Ainsi, $Q^2 P = \sum_{i=1}^n P_i^2$, avec $PQ \neq 0$ et $\deg(Q) \geq 0$.

Soit $h \in \mathbb{N}$. Notons $R(h)$ l'assertion suivante : il existe $(P_{i,h})_{1 \leq i \leq n} \in A^n$ et $Q'_h \in A$ tels que $Q'_h{}^2 P = \sum_{i=1}^n P_{i,h}^2$, avec $PQ'_h \neq 0$ et $\deg(Q'_h) \leq h$.

$R(\deg(Q))$ est vérifiée et, d'après la question III.7, pour tout $h \in \mathbb{N}^*$, $R(h) \implies R(h-1)$.

Le principe de la récurrence descendante prouve ainsi $R(0)$.

Or $Q'_0 \in k \setminus \{0\}$ et $P = \sum_{i=1}^n \left(\frac{P_{i,0}}{Q'_0}\right)^2 \in S_n(A)$.

Ainsi, dans chacun des trois cas, on a montré que $P \in S_n(A)$.

On a bien prouvé que $S_n(A) = (A \cap S_n(K))$.

9°) a) Soit $n \in \mathbb{N}^*$ tel que $-1 \in S_n(K)$.

$-1 \in A \cap S_n(K) = S_n(A)$, donc il existe $(R_1, \dots, R_n) \in A^n$ tel que $-1 = \sum_{i=1}^n R_i^2$.

En particulier, $-1 = \sum_{i=1}^n R_i(0)^2$ et pour tout i , $R_i(0) \in k$, donc $-1 \in S_n(k)$.

Réciproquement, si $-1 \in S_n(k)$, k étant inclus dans K , $-1 \in S_n(K)$.

On a donc montré que, pour tout $n \in \mathbb{N}^*$, $-1 \in S_n(k) \iff -1 \in S_n(K)$.

Ainsi, $\{n \in \mathbb{N}^* / -1 \in S_n(k)\} = \{n \in \mathbb{N}^* / -1 \in S_n(K)\}$, ce qui prouve que k et K ont le même niveau.

9°) b) Supposons que $S_s(K) = S_{s+1}(K)$.

$-1 \in S_s(K)$, donc, d'après la question III.3, $S_{s+1}(K) = K$. Ainsi, $S_s(K) = K$.

Si $s = 1$, ceci signifie que $K = \{F^2/F \in K\}$. En particulier, toute fraction rationnelle est de degré pair, ce qui est faux.

Si $s \geq 2$, $X \in K = S_s(K)$, donc il existe $(R_1, \dots, R_s) \in A^s$ tel que $X = R_1^2 + \dots + R_s^2$.

Or, par définition de s , $-1 \notin S_{s-1}(K)$, donc, d'après la question III.5, $R_1 = \dots = R_s = 0$. Ceci entraîne que $X = 0$, ce qui est faux.

Ainsi, dans tous les cas, $S_s(K) \neq S_{s+1}(K)$.

10°) Soit $(P, Q) \in S_n(A)^2$. P et Q sont dans $S_n(K)$, or, K étant un corps de caractéristique nulle, d'après une propriété admise par l'énoncé à la fin de la première partie, $S_n(K)$ est multiplicatif. On en déduit que $PQ \in S_n(K)$.

Donc $PQ \in (A \cap S_n(K)) = S_n(A)$, ce qui prouve que $S_n(A)$ est multiplicatif.