

## Agrégation interne 1993, première épreuve d'admissibilité

### Sommes de $n$ carrés dans un corps et dans certains anneaux

Corrigé rédigé par C.Gille

Pour tout anneau  $A$  et tout entier  $n \geq 1$ ,  $S_n(A)$  désigne l'ensemble des sommes de  $n$  carrés d'éléments de  $A$ .

Remarque préliminaire : on a  $S_n(A) \subset S_{n+1}(A)$ .

#### PARTIE I. OÙ L'ON TRAITE QUELQUES EXEMPLES.

**I.1.** Soit  $B$  un sous-anneau de  $\mathbb{R}$ . Soit  $u$  et  $v$  deux éléments de  $S_2(B)$ . Ils s'écrivent  $u = x^2 + y^2$  et  $v = z^2 + t^2$  où  $x, y, z$  et  $t$  appartiennent à  $B$ . On a :

$$uv = (x^2 + y^2)(z^2 + t^2) = |x + iy|^2 |z + it|^2 = |(x + iy)(z + it)|^2 = |(xz - ty) + i(yz + tx)|^2 = (xz - ty)^2 + (yz + tx)^2.$$

Comme  $B$  est un anneau, on a bien que  $xz - ty \in B$  et  $yz + tx \in B$  donc  $uv \in S_2(B)$ .

On en déduit que  $S_2(B)$  est multiplicatif.

**I.2.** Soit  $A$  un anneau commutatif. Pour tout  $(x, y, z, t) \in A^4$ , on a :

$$(xz - ty)^2 + (yz + tx)^2 = x^2 z^2 - 2xyzt + t^2 z^2 + y^2 z^2 + 2xyzt + t^2 x^2 = x^2 z^2 + t^2 z^2 + y^2 z^2 + t^2 x^2 = (x^2 + y^2)(z^2 + t^2),$$

ce qui permet de montrer comme dans la question précédente que  $S_2(A)$  est multiplicatif.

**I.3.** Les carrés de  $\mathbb{Z}$  sont les éléments de  $S_1(\mathbb{Z}) = \{0, 1, 4, 9, 16, \dots\}$  (où on a écrit les éléments en ordre croissant). Les éléments de  $S_3(\mathbb{Z})$  sont exactement les sommes de trois éléments de  $S_1(\mathbb{Z})$  (non nécessairement distincts). Comme  $4 + 4 + 4 = 12$ , une décomposition de 15 en somme de trois carrés doit comporter au moins un terme égal à 9. Or  $15 - 9 = 6$  et il est clair que 6 n'est pas une somme de deux carrés. Ainsi  $15 \notin S_3(\mathbb{Z})$ . Par ailleurs,  $3 = 1 + 1 + 1$  et  $5 = 0 + 1 + 4$  appartiennent à  $S_3(\mathbb{Z})$  donc  $S_3(\mathbb{Z})$  n'est pas multiplicative.

**I.4.** Dans l'anneau  $E = \mathbb{Z}/8\mathbb{Z}$ , on a :  $S_1(E) = \{\bar{0}, \bar{1}, \bar{4}\}$ ,  $S_2(E) = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}\}$  et  $S_3(E) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ .

**I.5.** Commençons par une remarque : pour tout entier impair  $n$ , on a  $n^2 \equiv 1 \pmod{8}$ . On peut le montrer en utilisant que  $S_1(E) = \{\bar{0}, \bar{1}, \bar{4}\}$  ou alors directement : si  $n = 1 + 2k$  avec  $k \in \mathbb{Z}$  alors  $n^2 = 1 + 4k(k + 1)$ , or  $k(k + 1)$  est pair, d'où le résultat.

Soit maintenant  $a, b, c$  et  $d$  des entiers vérifiant  $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{8}$ . Si  $a$  était impair, alors on aurait  $a^2 \equiv 1 \pmod{8}$  et alors  $b^2 + c^2 + d^2 \equiv 7 \pmod{8}$  ce qui est impossible car  $7 \notin S_3(E)$ . Donc  $a$  est pair et de même  $b, c$  et  $d$  sont pairs.

**I.6.** Remarquons que pour tout  $n \in \mathbb{Z}$ , on a :  $(n \in S_3(\mathbb{Z}) \Rightarrow \bar{n} \in S_3(E))$ , 1.5 où  $\bar{n}$  est la classe de  $n$  dans  $E = \mathbb{Z}/8\mathbb{Z}$ . Soit maintenant  $n \in \mathbb{Z}$  tel que  $n \equiv -1 \pmod{8}$ . On a  $\bar{n} = \bar{-1} = \bar{7}$ , or d'après I.4.,  $\bar{7} \notin S_3(E)$ , donc  $n \notin S_3(\mathbb{Z})$ .

Montrons par l'absurde que  $n$  n'appartient pas non plus à  $S_3(\mathbb{Q})$ . Supposons que  $n$  est somme de carrés de trois rationnels : il existe des entiers  $p_1, q_1, p_2, q_2, p_3$  et  $q_3$  tels que  $n = (\frac{p_1}{q_1})^2 + (\frac{p_2}{q_2})^2 + (\frac{p_3}{q_3})^2$  et on peut supposer que les fractions sont réduites (c'est-à-dire que  $p_i \wedge q_i = 1$  pour  $i = 1, 2, 3$ ).

Posons  $m = \text{ppcm}(q_1, q_2, q_3)$ . On peut écrire  $m = q_i a_i$  pour  $i = 1, 2, 3$  où  $a_1, a_2$  et  $a_3$  sont des entiers premiers entre eux. On a alors  $nm^2 = (p_1 a_1)^2 + (p_2 a_2)^2 + (p_3 a_3)^2$  dans  $\mathbb{Z}$ , puis  $m^2 + (p_1 a_1)^2 + (p_2 a_2)^2 + (p_3 a_3)^2 \equiv 0 \pmod{8}$ .

On en déduit (d'après I.5.) que  $m, p_1 a_1, p_2 a_2$  et  $p_3 a_3$  sont pairs. Pour tout  $i \in \{1, 2, 3\}$ ,  $q_i a_i$  et  $p_i a_i$  sont pairs, mais  $p_i$  et  $q_i$  ne peuvent être simultanément pairs (car  $p_i \wedge q_i = 1$ ) donc  $a_i$  est pair. C'est impossible car les  $a_i$  sont premiers entre eux. On a donc montré que  $n \notin S_3(\mathbb{Q})$ .

Remarque : il est clair que  $S_3(\mathbb{Z}) \subset S_3(\mathbb{Q})$  donc la première partie de cette question peut être vue comme une conséquence de la deuxième.

**I.7.** On a  $15 \equiv -1 \pmod{8}$  donc  $15 \notin S_3(\mathbb{Q})$  d'après la question précédente. Or on a déjà vu en I.3. que 3 et 5 appartiennent à  $S_3(\mathbb{Z})$ , donc a fortiori ils appartiennent à  $S_3(\mathbb{Q})$ . On en déduit que  $S_3(\mathbb{Q})$  n'est pas multiplicative.

**I.8.** Il est clair que tout polynôme  $f$  appartenant à  $S_2(\mathbb{R}[X])$  est à valeurs positives ou nulles (c'est-à-dire qu'il vérifie :  $\forall x \in \mathbb{R}, f(x) \geq 0$ ). Montrons la réciproque. Soit  $f \in \mathbb{R}[X]$  à valeurs positives ou nulles.

• *Premier cas* :  $f$  est un polynôme constant. Dans ce cas,  $f$  est de la forme  $f = k$  avec  $k \in \mathbb{R}$  et nécessairement  $k \geq 0$ . On a donc  $f = (\sqrt{k})^2 + 0^2 \in S_2(\mathbb{R}[X])$ .

• *Deuxième cas* :  $f$  est unitaire de degré 2. Nécessairement son discriminant est négatif ou nul, et son coefficient dominant est 1.  $f$  est donc de la forme  $f = X^2 + bX + c$  avec  $b^2 - 4c \leq 0$ . On a donc :

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

• *Cas général*. On suppose  $f$  non constant et on le décompose en produit de facteurs irréductibles. Ainsi,  $f$  est le produit d'une constante  $k$ , de facteurs de la forme  $(X - a)^\alpha$  où  $a \in \mathbb{R}$  et  $\alpha \in \mathbb{N}^*$ , et de facteurs de la forme

$(X^2 + bX + c)^\beta$  où  $b, c \in \mathbb{R}$ ,  $b^2 - 4c < 0$  et  $\beta \in \mathbb{N}^*$ . D'après ce qui précède, les facteurs irréductibles de degré 2 sont éléments de  $S_2(\mathbb{R}[X])$ . De plus,  $k$  est le coefficient dominant de  $f$  donc  $\lim_{x \rightarrow +\infty} f(x) = \text{signe}(k)\infty$  et comme  $f$  est supposée à valeurs positives, on a  $k > 0$ . Ainsi  $k$  peut être vu comme un élément de  $S_2(\mathbb{R}[X])$ . Reste à traiter les facteurs de degré 1. Si un des coefficients  $\alpha$  est impair, alors  $f$  change de signe au voisinage de  $a$ , ce qui contredit l'hypothèse de positivité de  $f$ , donc tous les  $\alpha$  sont pairs. Ainsi le facteur correspondant à la racine  $a$  est de la forme  $(X - a)^\alpha = (X - a)^{2\gamma} = ((X - a)^\gamma)^2$  et c'est donc un élément de  $S_2(\mathbb{R}[X])$ . Finalement  $f$  est un produit d'éléments de  $S_2(\mathbb{R}[X])$ , or  $S_2(\mathbb{R}[X])$  est multiplicative (d'après I.1.), donc  $f \in S_2(\mathbb{R}[X])$ , ce qui achève la démonstration.

**I.9.** Soit  $n \geq 3$ .

- On sait déjà que  $S_2(\mathbb{R}[X]) \subset S_n(\mathbb{R}[X])$ . Montrons l'inclusion réciproque. Soit  $P \in S_n(\mathbb{R}[X])$ . Alors  $P$  est à valeurs positives ou nulles et donc d'après la question précédente,  $P \in S_2(\mathbb{R}[X])$ . On conclut que  $S_n(\mathbb{R}[X]) = S_2(\mathbb{R}[X])$ .
- On a aussi  $S_2(\mathbb{R}(X)) \subset S_n(\mathbb{R}(X))$ . Montrons l'inclusion réciproque. Soit  $F \in S_n(\mathbb{R}(X))$ . Alors  $F$  se décompose sous la forme  $F = \sum_{i=1}^n \left(\frac{P_i}{Q_i}\right)^2$  où  $P_1, \dots, P_n \in \mathbb{R}[X]$  et  $Q_1, \dots, Q_n \in \mathbb{R}[X] \setminus \{0\}$ .

On a alors  $(\prod_{i=1}^n Q_i)^2 F = \sum_{i=1}^n \left(P_i \prod_{j \neq i} Q_j\right)^2$  dans  $\mathbb{R}[X]$ , ce qui montre que  $(\prod_{i=1}^n Q_i)^2 F \in S_n(\mathbb{R}[X])$ .

Par ailleurs on a montré que  $S_n(\mathbb{R}[X]) = S_2(\mathbb{R}[X])$  donc il existe deux polynômes  $R$  et  $S$  dans  $\mathbb{R}[X]$  tels que  $(\prod_{i=1}^n Q_i)^2 F = R^2 + S^2$ . Finalement :

$$F = \left(\frac{R}{\prod_{i=1}^n Q_i}\right)^2 + \left(\frac{S}{\prod_{i=1}^n Q_i}\right)^2 \in S_2(\mathbb{R}[X])$$

On conclut qu'on a l'égalité  $S_n(\mathbb{R}(X)) = S_2(\mathbb{R}(X))$ .

## PARTIE II. OÙ L'ON ÉTUDIE LES PRODUITS DE SOMMES DE $n$ CARRÉS DANS UN CORPS.

Ici,  $k$  est un corps commutatif de caractéristique nulle. Si  $M$  est une matrice,  $\Delta(M)$  désigne la somme des carrés des éléments de sa première ligne. Une matrice  $A \in \mathcal{M}_n(k)$  est dite *semi-orthogonale* si l'on a :  ${}^tAA = A{}^tA = \Delta(A)I_n$ .

**II.1.** Soit  $A = (a_{ij}) \in \mathcal{M}_n(k)$  et  $a \in k$  tels que  $A{}^tA = aI_n$  ( $E$ ).

**II.1.a** On considère le terme en première ligne et première colonne dans l'égalité entre matrices ( $E$ ) et on obtient :  $a = \sum_{i=1}^n a_{1i}a_{1i} = \sum_{i=1}^n a_{1i}^2 = \Delta(A)$ .

**II.1.b** On suppose  $a \neq 0$ . Alors  $a^n \neq 0$  (car  $k$  est un corps) et comme  $\det(A{}^tA) = \det(A)\det({}^tA) = a^n$ ,  $A$  est inversible dans  $\mathcal{M}_n(k)$ . En multipliant l'égalité ( $E$ ) par  $A^{-1}$  à gauche et par  $A$  à droite on obtient  ${}^tAA = aI_n$ . Ainsi on a  $A{}^tA = {}^tAA = aI_n = \Delta(A)I_n$  et  $A$  est donc semi-orthogonale.

*Remarque* : dès lors qu'on a  ${}^tAA = A{}^tA = aI_n$ , cela prouve que  $\Delta(A) = a$  et aussi que  $A$  est semi-orthogonale (en revenant à la définition pour les cas  $a = 0$ ).

**II.2.** Soit  $A$  et  $B$  deux matrices semi-orthogonales dans  $\mathcal{M}_n(k)$  et  $e \in k$ .

- On a  $(eA)({}^teA) = e^2 A{}^tA = e^2 \Delta(A)I_n$  et de même  ${}^t(eA)(eA) = e^2 \Delta(A)I_n$  d'où  $eA$  est semi-orthogonale et  $\Delta(eA) = e^2 \Delta(A)$ .
- On a  $({}^tA)({}^t{}^tA) = {}^tAA = \Delta(A)I_n$  et de même  ${}^t({}^tA)({}^tA) = \Delta(A)I_n$  donc  ${}^tA$  est semi-orthogonale et  $\Delta({}^tA) = \Delta(A)$ .
- On a  $(AB)({}^tAB) = AB{}^tB{}^tA = \Delta(B)A{}^tA = \Delta(B)\Delta(A)I_n$  et de même  ${}^t(AB)(AB) = \Delta(A)\Delta(B)I_n$  donc  $AB$  est semi-orthogonale et  $\Delta(AB) = \Delta(A)\Delta(B)$ .

**II.3.** On pose  $\Omega_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  et pour  $n \geq 3$ ,  $\Omega_n = \begin{pmatrix} \Omega_2 & 0 \\ 0 & I_{n-2} \end{pmatrix}$ . Remarquons que  $\Omega_n$  est symétrique.

On a  $\Omega_2 {}^t\Omega_2 = \Omega_2^2 = I_2$  et il s'ensuit que pour  $n \geq 3$ ,  $\Omega_n {}^t\Omega_n = \Omega_n^2 = \begin{pmatrix} \Omega_2^2 & 0 \\ 0 & I_{n-2}^2 \end{pmatrix} = I_n$ .

On en déduit que  $\Omega_n$  est semi-orthogonale (et  $\Delta(\Omega_n) = 1$ ).

**II.4.** Soit  $n \geq 2$  et  $A$  semi-orthogonale dans  $\mathcal{M}_n(k)$ .

**II.4.a** La matrice obtenue à partir de  $A$  en échangeant les deux premières lignes est  $\Omega_n A$ , qui est semi-orthogonale comme produit de deux matrices semi-orthogonales (d'après II.2.).

**II.4.b** Soit pour toute paire  $\{i, j\}$  d'éléments de  $\{1, \dots, n\}$ ,  $P_{ij}$  la matrice obtenue à partir de  $I_n$  en échangeant

la  $i$ -ème ligne et la  $j$ -ème ligne. Rappelons que lorsqu'on multiplie une matrice à gauche par  $P_{ij}$ , on échange sa  $i$ -ème ligne et sa  $j$ -ème ligne. De plus  $P_{ij} {}^t P_{ij} = P_{ij}^2 = I_n$  donc  $P_{ij}$  est semi-orthogonale. On sait que le groupe symétrique  $\mathcal{S}_n$  est engendré par les transpositions. Par suite, toute matrice obtenue en permutant les lignes de  $A$  est de la forme  $PA$  où  $P$  est produit de matrices élémentaires de type  $P_{ij}$  et comme les  $P_{ij}$  sont semi-orthogonales il s'ensuit que  $PA$  l'est aussi. Le raisonnement est le même pour une permutation des colonnes (qui revient à multiplier  $A$  à droite par des matrices élémentaires de type  $P_{ij}$ ).

On peut donc conclure qu'une permutation quelconque des lignes ou des colonnes d'une matrice n'affecte pas la propriété de semi-orthogonalité.

**II.5.** Soit  $L = (l_1, \dots, l_n) \in \mathcal{M}_{1,n}(k)$  telle que  $\Delta(L) = 0$ .

**II.5.a.** Remarquons que  ${}^t LL$  est une matrice symétrique de  $\mathcal{M}_n(k)$  et que  $L {}^t L = \Delta(L) = 0$ .

On a  $({}^t LL) {}^t ({}^t LL) = {}^t LL {}^t LL = {}^t L (L {}^t L) L = 0 \cdot {}^t LL = 0_n$  (matrice nulle de  $\mathcal{M}_n(k)$ ) d'où  ${}^t LL$  est semi-orthogonale. De plus, sa  $i$ -ième ligne est  $l_i L = (l_i l_1, \dots, l_i l_n)$ .

**II.5.b.** Si  $L = (0, \dots, 0)$ , alors c'est la première ligne de la matrice nulle de  $\mathcal{M}_n(k)$ , qui est semi-orthogonale. Sinon, soit  $i \in \{1, \dots, n\}$  tel que  $l_i \neq 0$ . Alors  $l_i$  est inversible et la  $i$ -ième ligne de  $l_i^{-1} {}^t LL$  est  $L$ . De plus cette matrice est encore semi-orthogonale d'après II.2. Quitte à permuter ses lignes, ce qui n'affecte pas sa semi-orthogonalité, on obtient une matrice dont la première ligne est  $L$ .

**II.6.** Soit  $A$  et  $B$  deux matrices semi-orthogonales dans  $\mathcal{M}_n(k)$  telles que  $\Delta(A) \neq 0$  et  $\Delta(A) + \Delta(B) \neq 0$ .

Soit  $C = -(\Delta(A))^{-1} {}^t A {}^t B A$ . D'après II.2,  $C$  est semi-orthogonale et  $\Delta(C) = (\Delta(A))^{-2} \Delta(A) \Delta(B) \Delta(A) = \Delta(B)$ .

On pose  $M = \begin{pmatrix} A & B \\ C & {}^t A \end{pmatrix}$ . On a alors :  $M {}^t M = \begin{pmatrix} A {}^t A + B {}^t B & {}^t (C {}^t A + {}^t A {}^t B) \\ C {}^t A + {}^t A {}^t B & C {}^t C + {}^t A A \end{pmatrix}$ .

Par ailleurs  $C {}^t C = \Delta(C) I_n = \Delta(B) I_n$  et  $C {}^t A = -(\Delta(A))^{-1} {}^t A {}^t B A {}^t A = -{}^t A {}^t B$ ,

d'où :  $M {}^t M = \begin{pmatrix} (\Delta(A) + \Delta(B)) I_n & 0_n \\ 0_n & (\Delta(A) + \Delta(B)) I_n \end{pmatrix} = (\Delta(A) + \Delta(B)) I_{2n}$ .

Comme  $\Delta(A) + \Delta(B) \neq 0$ , on en déduit d'après II.1.b. que  $M$  est semi-orthogonale (et que  $\Delta(M) = \Delta(A) + \Delta(B)$ ).

**II.7.** Soit  $x_1, \dots, x_n$  des éléments de  $k$ . On va montrer que dans certains cas il existe une matrice semi-orthogonale dans  $\mathcal{M}_n(k)$  dont la première ligne est  $(x_1, \dots, x_n)$ .

**II.7.a.** Cas où  $k = \mathbb{R}$ .

Si  $\sum_{i=1}^n x_i^2 = 0$ , alors tous les  $x_i$  sont nuls et la matrice nulle convient. Si maintenant  $\sum_{i=1}^n x_i^2 \neq 0$ , on pose  $v_1 = (x_1, \dots, x_n)$  et on complète  $v_1$  en une base orthogonale  $(v_1, \dots, v_n)$  de  $\mathbb{R}^n$  (pour la structure euclidienne standard) où on normalise chaque  $v_i$  de telle sorte que  $\|v_i\|^2 = \sum_{i=1}^n x_i^2$ . Soit alors  $A$  la matrice de  $\mathcal{M}_n(\mathbb{R})$  où la  $i$ -ième ligne est  $v_i$  (pour  $i = 1, \dots, n$ ). On a  $A {}^t A = \sum_{i=1}^n x_i^2 I_n$  donc  $A$  est semi-orthogonale (d'après II.1.b.) et sa première ligne est  $v_1 = (x_1, \dots, x_n)$ .

**II.7.b.** Cas où  $k$  est quelconque et  $n$  est une puissance de 2.

Soit pour tout entier naturel  $p$  la propriété suivante :

$(H_p)$  : "Pour tout  $2^p$ -uplet  $(x_1, \dots, x_{2^p})$  de  $k^{2^p}$ , il existe une matrice semi-orthogonale dans  $\mathcal{M}_{2^p}(k)$  de première ligne  $(x_1, \dots, x_{2^p})$ ."

On va montrer par récurrence que  $(H_p)$  est vraie pour tout entier naturel  $p$ .

- $(H_0)$  est évident (toutes les matrices de  $\mathcal{M}_1(k)$  sont semi-orthogonales).
- On suppose  $(H_p)$  vérifiée pour  $p \in \mathbb{N}$ . Montrons  $(H_{p+1})$ . Soit  $(x_1, \dots, x_{2^{p+1}}) \in k^{2^{p+1}}$ . Remarquons que  $2^{p+1} = 2 \cdot 2^p$ . Si  $\sum_{i=1}^{2^{p+1}} x_i^2 = 0$  alors on applique II.5. et il existe une matrice semi-orthogonale dans  $\mathcal{M}_{2^{p+1}}(k)$  de première ligne  $(x_1, \dots, x_{2^{p+1}})$ . Sinon, alors soit  $\sum_{i=1}^{2^p} x_i^2 \neq 0$ , soit  $\sum_{i=2^p+1}^{2^{p+1}} x_i^2 \neq 0$ . D'après l'hypothèse de récurrence  $(H_p)$ , il existe une matrice semi-orthogonale  $\mathcal{M}_{2^p}(k)$  de première ligne  $(x_1, \dots, x_{2^p})$  et une autre de première ligne  $(x_{2^p+1}, \dots, x_{2^{p+1}})$ . Appelons  $A$  la première et  $B$  la seconde si  $\sum_{i=1}^{2^p} x_i^2 \neq 0$  (dans le cas contraire, on intervertit  $A$  et  $B$ ). Dans tous les cas on a  $\Delta(A) \neq 0$  et  $\Delta(A) + \Delta(B) \neq 0$ . On applique alors II.6. ce qui nous fournit une matrice semi-orthogonale dans  $\mathcal{M}_{2^{p+1}}(k)$  de première ligne  $(x_1, \dots, x_{2^{p+1}})$  ou  $(x_{2^p+1}, \dots, x_{2^{p+1}}, x_1, \dots, x_{2^p})$  suivant les cas. Quitte éventuellement à permuter les colonnes de cette matrice, on obtient bien une matrice semi-orthogonale dans  $\mathcal{M}_{2^{p+1}}(k)$  de première ligne  $(x_1, \dots, x_{2^{p+1}})$ , ce qui achève la récurrence.

**II.8.** On suppose que  $n$  est une puissance de 2. On fixe un élément  $a$  de  $k$ .

S'il existe une matrice semi-orthogonale  $A$  dans  $\mathcal{M}_n(k)$  tel que  $\Delta(A) = a$ , alors  $a$  est la somme des carrés des éléments de la première ligne de  $A$  donc  $a \in S_n(k)$  (ceci est toujours vrai, même si  $n$  n'est pas une puissance de 2). Montrons la réciproque. Supposons  $a \in S_n(k)$ . Alors il existe des éléments  $x_1, \dots, x_n$  de  $k$  tels que  $a = \sum_{i=1}^n x_i^2$ . D'après II.7.b. il existe donc une matrice  $A$  de  $\mathcal{M}_n(k)$  semi-orthogonale de première ligne  $(x_1, \dots, x_n)$ , et on a

alors  $\Delta(A) = \sum_{i=1}^n x_i^2 = a$ .

**II.9.** On suppose que  $n$  est une puissance de 2.

Soit  $a, b \in S_n(k)$ . Alors d'après II.8., il existe deux matrices semi-orthogonales  $A$  et  $B$  dans  $\mathcal{M}_n(k)$  telles que  $a = \Delta(A)$  et  $b = \Delta(B)$ . Alors d'après II.2,  $AB$  est semi-orthogonale et  $ab = \Delta(AB)$  donc, d'après II.8. de nouveau,  $ab \in S_n(k)$ . On conclut que  $S_n(k)$  est multiplicatif.

### PARTIE III. OÙ L'ON PRÉCISE LE NOMBRE DE CARRÉS NÉCESSAIRES POUR ÉCRIRE $-1$ .

Ici,  $k$  est un corps commutatif de caractéristique quelconque. Le niveau  $s(k)$  est le plus petit entier  $n \geq 1$  tel que  $-1 \in S_n(k)$ , si un tel entier existe ; sinon, on pose  $s(k) = +\infty$ .

**III.1.** Dans  $\mathbb{R}$ ,  $-1$ , étant strictement négatif, ne peut pas s'écrire comme somme de carrés, d'où  $s(\mathbb{R}) = +\infty$ . Dans  $\mathbb{C}$ ,  $-1 = i^2$  d'où  $s(\mathbb{C}) = 1$ .

**III.2.** Si  $k$  est de caractéristique 2, alors l'égalité  $-1 = 1 = 1^2$  dans  $k$  prouve que  $s(k) = 1$ . De même, si  $k$  est de caractéristique 5, alors on a  $-1 = 4 = 2^2$  dans  $k$ , d'où  $s(k) = 1$ .

**III.3.** On pose  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , où  $p$  est un nombre premier  $\geq 3$ .

**III.3.a.** Soit  $\varphi : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$  l'application qui à  $x$  associe  $x^2$ . Remarquons que pour tout  $x \in \mathbb{F}_p^*$ ,  $x^2 \in \mathbb{F}_p^*$  (car  $\mathbb{F}_p^*$  est un groupe pour la multiplication) donc  $\varphi$  est bien définie, et il est immédiat de vérifier que  $\varphi$  est multiplicatif, et donc un morphisme de groupes. Maintenant pour tout  $x \in \mathbb{F}_p^*$ , on a l'équivalence :  $x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0 \Leftrightarrow x = \pm 1$ , car  $\mathbb{F}_p$  est un corps. On en déduit que  $\text{Ker } \varphi = \{+1, -1\}$ . Remarque : comme  $p \geq 3$ ,  $1 \neq -1$  dans  $\mathbb{F}_p$ .

**III.3.b.** Soit  $E = \text{Im } \varphi$ .  $\varphi$  étant un morphisme de groupes, on a  $|E| = [\mathbb{F}_p^* : \text{Ker } \varphi] = |\mathbb{F}_p^*|/|\text{Ker } \varphi| = \frac{p-1}{2}$ . (Ici, si  $G$  est un groupe, on note  $|G|$  son cardinal).

**III.3.c.** On a  $S_1(\mathbb{F}_p) = S_1(\mathbb{F}_p^* \cup \{0\}) = E \cup \{0\}$  d'où  $\text{card}(S_1(\mathbb{F}_p)) = \frac{p-1}{2} + 1 = \frac{p+1}{2}$ .

L'ensemble  $T$  des éléments de  $\mathbb{F}_p$  de la forme  $-1 - y$  avec  $y \in S_1(\mathbb{F}_p)$  est en bijection avec  $S_1(\mathbb{F}_p)$ , donc également de cardinal  $\frac{p+1}{2}$ . Deux sous-ensembles de  $\mathbb{F}_p$  de cardinal  $\frac{p+1}{2}$  ont nécessairement au moins un élément en commun (car  $2 \cdot \frac{p+1}{2} = p+1 > p = \text{card}(\mathbb{F}_p)$ ), donc  $T \cap S_1(\mathbb{F}_p)$  est non vide.

**III.3.d.** On fixe  $x$  un élément de  $T \cap S_1(\mathbb{F}_p)$ . Il existe alors  $y \in S_1(\mathbb{F}_p)$  tel que  $-1 - y = x$  et on a donc  $-1 = x + y$  avec  $x$  et  $y$  deux carrés de  $\mathbb{F}_p$ . On en déduit que  $s(\mathbb{F}_p) \leq 2$ .

**III.4.** On suppose que  $k$  est de caractéristique non nulle. Alors sa caractéristique est un nombre premier  $p$  et  $k$  contient un sous-corps  $K_0$  isomorphe à  $\mathbb{F}_p$  (son sous-corps premier). D'après III.3, il existe  $x_1$  et  $x_2$  dans  $\mathbb{F}_p$  tels que  $-1 = x_1^2 + x_2^2$  dans  $\mathbb{F}_p$  et par isomorphisme on a le même type d'égalité dans  $K_0$  et donc dans  $k$ . On en déduit que  $s(k) \leq 2$ .

**III.5.** On suppose que  $k$  est de caractéristique nulle et de niveau fini  $s$ . Soit  $x_1, \dots, x_s$  dans  $k$  tels que  $-1 = x_1^2 + \dots + x_s^2$ . Soit  $n$  la plus grande puissance de 2 telle que  $n \leq s$ . On pose alors  $x = x_1^2 + \dots + x_n^2$ . Remarquons que  $1 \leq n \leq s < 2n$ . On peut donc écrire  $-1 = x + (x_{n+1}^2 + \dots + x_s^2)$ , la deuxième partie de la somme de droite étant vide si  $n = s$  (c'est-à-dire si  $s$  est une puissance de 2).

- On suppose  $x = 0$ . Alors dans le cas où  $n = s$  on a  $-1 = 0$  ce qui est impossible. Sinon on a  $-1 = x_{n+1}^2 + \dots + x_s^2$  ce qui contredit la définition de  $s$ . On en déduit que  $x$  est non nul.
- On a  $-x = 1 + x_{n+1}^2 + \dots + x_s^2$  donc  $-x$  est une somme de  $s - n + 1$  carrés. Or  $s - n + 1 < n + 1$  et ceci étant une égalité entre entiers, on a  $s - n + 1 \leq n$ . On en déduit que  $-x \in S_n(k)$ .
- Par définition on a  $x \in S_n(k)$ , d'après le point précédent on a  $-x \in S_n(k)$  et d'après II.9  $S_n(k)$  est multiplicatif (car  $k$  est de caractéristique nulle et  $n$  une puissance de 2) donc  $-x^2 \in S_n(k)$ .
- Enfin,  $(x^{-1})^2 \in S_n(k)$  donc en utilisant une nouvelle fois que  $S_n(k)$  est multiplicatif on a  $-1 = -x^2(x^{-1})^2 \in S_n(k)$ . On en déduit que  $n = s$  (par définition du niveau  $s$ ) et donc  $s$  est une puissance de 2.

**III.6.** Si  $k$  est de caractéristique non nulle alors d'après III.4.  $s(k)$  vaut 1 ou 2 et donc est une puissance de 2. Si  $k$  est de caractéristique nulle alors d'après III.5, soit  $s(k) = +\infty$  soit  $s(k)$  est une puissance de 2. Dans tous les cas, le niveau de  $k$  est soit  $+\infty$ , soit une puissance de 2.

## PARTIE IV. OÙ L'ON TRAITE LE CAS D'UN ANNEAU DE POLYNÔMES.

Ici,  $k$  est un corps commutatif de caractéristique nulle et on pose  $A = k[X]$  et  $K = k(X)$ .

**IV.1.** Par définition on a  $S_1(A) \subset A$  et comme  $A \subset K$  on a  $S_1(A) \subset S_1(K)$ , d'où l'inclusion  $S_1(A) \subset A \cap S_1(K)$ . Montrons l'inclusion réciproque. Soit un polynôme  $P \in A \cap S_1(K)$ . Alors il existe une fraction rationnelle dont on choisit une forme irréductible  $\frac{N}{D}$  telle que  $P = \left(\frac{N}{D}\right)^2$ . On a alors l'égalité  $PD^2 = N^2$  dans  $A$  qui est un anneau principal. Ainsi  $D$  divise  $N^2$ , or  $D$  et  $N$  sont premiers entre eux donc, d'après le lemme de Gauss,  $D$  divise  $N$ . Par suite,  $\frac{N}{D}$  est un polynôme et donc  $P \in S_1(A)$ . On conclut que  $S_1(A) = A \cap S_1(K)$ .

**IV.2.** Soit  $a_1, \dots, a_{n-1}, b$  des éléments de  $K$  tels que  $\sum_{i=1}^{n-1} a_i^2 = -1$ . Alors on a (dans le corps commutatif  $K$ ):  
 $(b+1)^2 + \sum_{i=1}^{n-1} (a_i(b-1))^2 = (b+1)^2 + \sum_{i=1}^{n-1} a_i^2(b-1)^2 = (b+1)^2 - (b-1)^2 = 4b$ .  
 Remarquons que ce calcul est valable dans tout sous-anneau de  $K$ , en particulier dans  $A$  et dans  $k$ .

**IV.3.** On suppose qu'il existe  $n \geq 2$  tel que  $-1 \in S_{n-1}(k)$ . Soit alors  $a_1, \dots, a_{n-1}$  des éléments de  $k$  tels que  $-1 = \sum_{i=1}^{n-1} a_i^2$ . Soit maintenant  $b \in k$ . Comme  $k$  est de caractéristique nulle, 2 est non nul et donc inversible dans  $k$ . En appliquant la formule établie en IV.2. on a :  $b = (2^{-1}(b+1))^2 + \sum_{i=1}^{n-1} (2^{-1}a_i(b-1))^2$ , ce qui prouve que  $b \in S_n(k)$ . On en déduit que tous les éléments de  $k$  sont des sommes de  $n$  carrés, c'est-à-dire que  $k = S_n(k)$ . 2 étant inversible dans  $k$ , il l'est a fortiori dans  $A$  et dans  $K$ , donc on montre exactement de la même façon que  $A = S_n(A)$  et  $K = S_n(K)$ .

**IV.4.** Il est clair que pour tout anneau commutatif  $A$ ,  $S_1(A)$  est multiplicatif, donc en particulier  $S_1(\mathbb{C}(X))$  l'est. De plus on a  $-1 \in S_1(\mathbb{C})$  donc, d'après IV.3,  $S_2(\mathbb{C}(X)) = \mathbb{C}(X)$ . Par suite pour tout  $n \geq 2$ , on a  $\mathbb{C}(X) = S_2(\mathbb{C}(X)) \subset S_n(\mathbb{C}(X)) \subset \mathbb{C}(X)$  d'où  $S_n(\mathbb{C}(X)) = \mathbb{C}(X)$ , et comme  $\mathbb{C}(X)$  est évidemment multiplicatif  $S_n(\mathbb{C}(X))$  l'est aussi. On conclut que pour tout  $n \geq 1$ ,  $S_n(\mathbb{C}(X))$  est multiplicatif.

**IV.5.** Soit un entier  $n \geq 2$  tel que  $-1 \notin S_{n-1}(k)$  et soit  $R_1, \dots, R_n$  des polynômes dans  $A$ . On suppose que  $R_1^2 + \dots + R_n^2 = aX$  ( $a \in k$ ). Montrons d'abord que  $a = 0$ . En évaluant l'égalité ci-dessus en 0, on obtient  $R_1^2(0) + \dots + R_n^2(0) = 0$  dans  $k$ . Supposons que l'un des  $R_i(0)$  soit non nul et, quitte à renuméroter, supposons que c'est  $R_n(0)$ . Alors  $R_n(0)$  est inversible dans  $k$  et on a alors  $(R_n(0)^{-1}R_1(0))^2 + \dots + (R_n(0)^{-1}R_{n-1}(0))^2 = -1$ , ce qui contredit l'hypothèse  $-1 \notin S_{n-1}(k)$ . Donc tous les  $R_i(0)$  sont nuls. Ainsi pour tout  $i = 1, \dots, n$ ,  $X$  divise  $R_i$  dans  $A$  et donc  $X^2$  divise  $R_i^2$ . Il s'ensuit que  $X^2$  divise  $aX$ , ce qui implique que  $a = 0$ .  
 On a maintenant l'égalité  $R_1^2 + \dots + R_n^2 = 0$  dans  $A$ . Soit  $x \in k$  fixé. Comme précédemment supposons que l'un des  $R_i(x)$  est non nul et, quitte à renuméroter, supposons que c'est  $R_n(x)$ . Alors on a  $(R_n(x)^{-1}R_1(x))^2 + \dots + (R_n(x)^{-1}R_{n-1}(x))^2 = -1$  d'où la même contradiction. Ainsi tous les  $R_i(x)$  sont nuls. Or ceci étant vrai pour tout  $x \in k$ , on en déduit que pour tout  $i = 1, \dots, n$  la fonction polynôme associée à  $R_i$  est nulle, ce qui implique que le polynôme  $R_i$  est nul (car  $k$  est de caractéristique nulle donc en particulier infini).

**IV.6.** Soit un entier  $n \geq 2$  et soit  $P, Q, P_1, \dots, P_n, Q_1, \dots, Q_n$  dans  $A$ .

On pose  $S = P - \sum_{i=1}^n Q_i^2$ ,  $T = PQ - \sum_{i=1}^n P_i Q_i$ ,  $Q' = 2T - QS$  et  $P'_i = 2Q_i T - P_i S$  pour  $i = 1, \dots, n$ .

**IV.6.a.** On suppose qu'on a l'égalité : (1)  $Q^2 P = \sum_{i=1}^n P_i^2$ .

Montrons qu'on a alors : (2)  $Q'^2 P = \sum_{i=1}^n P_i'^2$ , et (3)  $QQ' = \sum_{i=1}^n (P_i - QQ_i)^2$ .

On a :

$$\begin{aligned} \sum_{i=1}^n P_i'^2 &= \sum_{i=1}^n (2Q_i T - P_i S)^2 = 4 \left( \sum_{i=1}^n Q_i^2 \right) T^2 - 4 \left( \sum_{i=1}^n Q_i P_i \right) TS + \left( \sum_{i=1}^n P_i^2 \right) S^2 \\ &= 4(P - S)T^2 - 4(PQ - T)TS + Q^2 PS^2 = 4PT^2 - 4PQTS + Q^2 PS^2 = (2T - QS)^2 P = Q'^2 P \end{aligned}$$

d'où l'égalité (2).

Par ailleurs on a :

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

d'où l'égalité (3).

**IV.6.b.** On suppose qu'on a l'égalité (1), que  $-1 \notin S_{n-1}(k)$ , que  $Q \neq 0$ , et que  $Q' = 0$ . Alors, (3) devient  $\sum_{i=1}^n (P_i - QQ_i)^2 = 0$  et en utilisant IV.5., on en déduit que  $QQ_i = P_i$  pour tout  $i = 1, \dots, n$ . En élevant au carré et en sommant sur  $i$ , on obtient :  $Q^2 \sum_{i=1}^n Q_i^2 = \sum_{i=1}^n P_i^2 = Q^2 P$ . Comme  $Q$  est non nul (et que  $A$  est intègre),

on en déduit que  $P = \sum_{i=1}^n Q_i^2$ , c'est-à-dire l'égalité (4).

**IV.7.** Soit un entier  $n \geq 2$  tel que  $-1 \notin S_{n-1}(k)$  et soit  $P, Q, P_1, \dots, P_n$  dans  $A$  vérifiant (1) et tels que  $PQ \neq 0$  et  $\deg Q \geq 1$ .

- *1er cas* : pour tout  $i = 1, \dots, n$ ,  $Q$  divise  $P_i$  dans  $A$ .  
Soit alors pour tout  $i = 1, \dots, n$ ,  $P_i'' \in A$  tel que  $P_i = QP_i''$ . D'après (1) on a  $Q^2P = Q^2 \sum_{i=1}^n P_i''^2$  puis, comme  $Q \neq 0$ ,  $P = \sum_{i=1}^n P_i''^2$ . En posant  $Q'' = 1$ , on a bien  $Q''^2P = \sum_{i=1}^n P_i''^2$ ,  $PQ'' \neq 0$  et  $\deg Q'' < \deg Q$ .
- *2ème cas* : il existe  $i \in \{1, \dots, n\}$  tel que  $Q$  ne divise pas  $P_i$  dans  $A$ .  
Soit pour tout  $i = 1, \dots, n$ ,  $P_i = QQ_i + R_i$  la division euclidienne de  $P_i$  par  $Q$ . On applique alors la question IV.6. avec les mêmes notations. Si on avait  $Q' = 0$ , alors les hypothèses du point IV.6.b. seraient satisfaites, et on aurait  $QQ_i = P_i$  pour tout  $i = 1, \dots, n$ , ce qui contredit l'hypothèse de départ. Donc  $Q' \neq 0$ . De plus on a les égalités (2) et (3). Pour tout  $i = 1, \dots, n$ ,  $\deg R_i < \deg Q$  d'où  $\deg(\sum_{i=1}^n R_i^2) < 2 \deg Q$ . D'après (3) on a alors  $\deg Q + \deg Q' < 2 \deg Q$ , et donc  $\deg Q' < \deg Q$ . On pose alors  $Q'' = Q'$  et  $P_i'' = P_i'$  pour tout  $i = 1, \dots, n$ . On a bien  $Q''^2P = \sum_{i=1}^n P_i''^2$  (qui n'est autre que (2)),  $PQ'' \neq 0$  et  $\deg Q'' < \deg Q$ .

**IV.8.** D'après IV.1., on a déjà  $S_1(A) = A \cap S_1(K)$ . Soit maintenant un entier  $n \geq 2$ .

- *1er cas* :  $-1 \in S_{n-1}(k)$ .  
Alors, d'après IV.3.,  $S_n(A) = A$  et  $S_n(K) = K$ , d'où  $A \cap S_n(K) = A \cap K = A = S_n(A)$ .
- *2ème cas* :  $-1 \notin S_{n-1}(k)$ .  
De même qu'en IV.1., on a immédiatement l'inclusion  $S_n(A) \subset A \cap S_n(K)$ . Soit maintenant un polynôme  $P \in A \cap S_n(K)$ . On suppose  $P$  non nul (si  $P = 0$ , le résultat est immédiat).  $P$  est alors somme de  $n$  carrés de fractions non toutes nulles et donc, quitte à réduire ces fractions au même dénominateur, il existe  $Q, P_1, \dots, P_n$  dans  $A$  tels que  $Q \neq 0$  et  $P = \sum_{i=1}^n (\frac{P_i}{Q})^2$ .

On construit alors une suite de  $(n+1)$ -uplets de polynômes indexés par  $r \in \mathbb{N}$ ,  $(Q^{(r)}, P_1^{(r)}, \dots, P_n^{(r)})$  vérifiant  $Q^{(r)} \neq 0$  et  $(Q^{(r)})^2P = \sum_{i=1}^n (P_i^{(r)})^2$  de la manière suivante :

1. On pose  $Q^{(0)} = Q$  et  $P_i^{(0)} = P_i$  pour tout  $i = 1, \dots, n$ .
2. Soit  $r \in \mathbb{N}$ . On suppose  $Q^{(l)}, P_1^{(l)}, \dots, P_n^{(l)}$  construits pour  $l = 0, \dots, r$ . Si  $\deg Q^{(r)} = 0$  alors on arrête la construction. Si  $\deg Q^{(r)} \geq 1$ , alors  $P, Q^{(r)}, P_1^{(r)}, \dots, P_n^{(r)}$  vérifient les hypothèses de la question IV.7. On pose alors  $Q^{(r+1)} = Q''$  et  $P_i^{(r+1)} = P_i''$  pour tout  $i = 1, \dots, n$  (définis comme dans la question IV.7.). Alors on a  $\deg Q^{(r+1)} < \deg Q^{(r)}$  et  $P, Q^{(r+1)}, P_1^{(r+1)}, \dots, P_n^{(r+1)}$  vérifient les hypothèses de la question IV.7., sauf éventuellement la condition sur le degré de  $Q^{(r+1)}$ .

Comme le degré de  $Q^{(r)}$  est strictement décroissant en fonction de  $r$ , la construction s'arrête en un nombre fini d'étapes. Supposons qu'on ait  $\deg Q^{(r)} = 0$  à l'étape  $r$ . Alors  $Q^{(r)}$  est une constante non nulle  $q \in k^*$  et on a  $P = \sum_{i=1}^n (q^{-1}P_i^{(r)})^2$ . On en déduit que  $P \in S_n(A)$ .

On conclut que  $S_n(A) = A \cap S_n(K)$ .

**IV.9.a.** Soit un entier  $n \geq 1$ . On a  $k \subset K$ , donc on a l'implication :  $-1 \in S_n(k) \Rightarrow -1 \in S_n(K)$ .

Supposons maintenant que  $-1 \in S_n(K)$ . Alors il existe des polynômes  $N_i$  et  $D_i$  pour  $i = 1, \dots, n$  tels que  $-1 = \sum_{i=1}^n (\frac{N_i}{D_i})^2$ . Soit  $\alpha \in k$  qui n'est pôle d'aucun des dénominateurs  $D_i$ . Alors  $-1 = \sum_{i=1}^n (\frac{N_i(\alpha)}{D_i(\alpha)})^2$  ce qui montre que  $-1 \in S_n(k)$ . On a donc l'équivalence :  $-1 \in S_n(k) \Leftrightarrow -1 \in S_n(K)$ . On en déduit que  $k$  et  $K$  ont même niveau.

**IV.9.b.** On suppose que  $k$  et  $K$  sont de niveau  $s$  fini.

On a  $-1 \in S_s(k)$  donc d'après IV.3.,  $S_{s+1}(K) = K$ . Montrons par l'absurde que  $S_s(K) \neq K$ . Supposons  $S_s(K) = K$ . Alors le polynôme  $X$  de  $A$  est élément de  $S_s(K)$ . Or  $A \cap S_s(K) = S_s(A)$  d'après IV.8., donc il existe des polynômes  $R_1, \dots, R_s$  dans  $A$  tels que  $X = \sum_{i=1}^s R_i^2$ . De plus, par définition du niveau,  $-1 \notin S_{s-1}(k)$  donc d'après IV.5. les  $R_i$  sont tous nuls. Mais alors on aurait  $X = 0$  d'où une contradiction. On conclut que  $S_s(K) \neq K$  et donc que  $S_s(K) \neq S_{s+1}(K)$  (plus précisément on a  $S_s(K) \subsetneq S_{s+1}(K)$ ).

**IV.10.** Soit  $n$  une puissance de 2.  $k$  est de caractéristique nulle donc  $K$  également. Le résultat final de la partie II appliqué à  $K$  montre que  $S_n(K)$  est multiplicatif. L'anneau  $A$  est évidemment multiplicatif, donc on en déduit que  $S_n(A) = A \cap S_n(K)$  est multiplicatif.