I. Détermination de $Rac(A)$ dans quelques exemples.

1. Les sous espaces propres $E_{\lambda_i}(A)$ sont de dimension ≥ 1 et en somme directe. Leur somme a donc une dimension au moins égale à n. Comme elle est incluse dans $\mathbb{R}^n$, sa dimension est en réalité égale à n et chaque $E_{\lambda_i}(A)$ a une dimension égale à 1. Notons (f_i) une base de $E_{\lambda_i}(A)$. La famille $(f_1, \dots, f_n)$ est une base de $\mathbb{R}^n$. Si P est la matrice de la base canonique de $\mathbb{R}^n$ aux f_i alors $P^{-1}AP$ est la matrice dans la base (f_i) de l'endomorphisme canoniquement associé à A. Par choix des f_i, cette matrice est $diag(\lambda_1, \dots, \lambda_n)$ et on a donc

$$A = PDP^{-1} \text{ avec } D = diag(\lambda_1, \dots, \lambda_n)$$

Soit $R \in M_n(\mathbb{R})$ et $S = P^{-1}RP$. On a $R^2 = A$ si et seulement si $P^{-1}R^2P = D$ (il y a équivalence car on revient en arrière en multipliant par P à gauche et P^{-1} à droite) c'est à dire $S^2 = D$. On peut donc écrire

$$Rac(A) = P.Rac(D).P^{-1}$$

2. a. On a $SD = S^3 = DS$.

   b. On fait le produit matriciel pour obtenir

$$\forall i, j,\ S_{i,j}\lambda_j = \sum_{k=1}^{n} S_{i,k}D_{k,j} = \sum_{k=1}^{n} D_{i,k}S_{k,j} = \lambda_i S_{i,j}$$

   Les λ_k étant deux à deux distincts, on a donc

$$\forall i \neq j,\ S_{i,j} = 0$$

   et S est diagonale.

   c. On a alors $S^2 = diag(s_1^2, \dots, s_n^2)$. Comme $S^2 = D$, on a donc

$$\forall i,\ s_i^2 = \lambda_i$$

   d. Si il existe un i tel que $\lambda_i < 0$, les relations précédentes sont impossible et donc

$$Rac(A) = \emptyset$$

   e. Si tous les λ_i sont positifs, on vient de voir que

$$Rac(D) \subset \{diag(\varepsilon_1\sqrt{\lambda_1}, \dots, \varepsilon_n\sqrt{\lambda_n}) /\ \forall i,\ \varepsilon_i = \pm 1\}$$

   Réciproquement, si $S = diag(\varepsilon_1\sqrt{\lambda_1}, \dots, \varepsilon_n\sqrt{\lambda_n})$ (où $\varepsilon_i = \pm 1$) alors $S^2 = D$. L'inclusion ci-dessus est une égalité.

3. L'application $M \mapsto P^{-1}MP$ est une bijection de $Rac(A)$ dans $Rac(D)$.

   - Si $\lambda_1 < 0$, on a vu en $2.d$ que $Rac(A) = \emptyset$. Il n'y a donc pas de racine carrée pour A.
   - Si $\lambda_1 \geq 0$ alors une racine carrée de D est connue par le choix des ε_i et

$$Rac(A) = \{P.diag(\varepsilon_1\sqrt{\lambda_1}, \dots, \varepsilon_n\sqrt{\lambda_n}).P^{-1} /\ \forall i,\ \varepsilon_i = \pm 1\}$$

   Deux choix différents des ε_i donneront deux racines carrées distinctes de D sauf dans le cas où $\lambda_1 = 0$. On a donc

$$Card(Rac(A)) = 2^{n-1} \text{ si } \lambda_1 = 0$$

$$Card(Rac(A)) = 2^n \text{ si } \lambda_1 > 0$$

4. $(0,1,1)$ est vecteur propre associé à la valeur propre 0. $(1,1,-1)$ est vecteur propre associé à la valeur propre 1. Avec la trace, on voit que la dernière valeur propre est 16. Une résolution de système montre que $(2,-1,1)$ est vecteur propre associé. On pose donc

$$P = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

On a alors $P^{-1}AP = diag(0,1,16)$. A admet quatre racines carrées qui sont

$$P.diag(0,1,4).P^{-1},\ P.diag(0,-1,4).P^{-1},\ P.diag(0,1,-4).P^{-1},\ P.diag(0,-1,-4).P^{-1}$$

ou encore

$$\begin{pmatrix} 3 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 7/3 & -5/3 & 5/3 \\ -5/3 & 1/3 & -1/3 \\ 5/3 & -1/3 & 1/3 \end{pmatrix}, \begin{pmatrix} -7/3 & 5/3 & -5/3 \\ 5/3 & -1/3 & 1/3 \\ -5/3 & 1/3 & -1/3 \end{pmatrix}, \begin{pmatrix} -3 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & -1 \end{pmatrix}$$

On remarque bien sûr que les matrices sont deux à deux opposées.

5. a. $R^2 = 0$ se traduit par $f \circ f = 0$ et donc par

$$Im(f) \subset Ker(f)$$

Or, le théorème du rang indique que $r + dim(Ker(f)) = n$. Comme $dim(Ker(f)) \geq r$, on a donc

$$r \leq \frac{n}{2}$$

b. La famille $\mathcal{B}$ ayant n éléments, il suffit de montrer qu'elle est libre ou génératrice pour conclure que c'est une base de $\mathbb{R}^n$. Supposons donc que

$$(*)\ :\ \sum_{i=1}^{n-r} \alpha_i e_i + \sum_{i=1}^{r} \beta_i u_i = 0$$

Avec les notations de l'énoncé, ceci s'écrit

$$\sum_{i=1}^{r} \alpha_i f(u_i) + \sum_{i=r+1}^{n-r} e_i + \sum_{i=1}^{r} \beta_i u_i = 0$$

En composant par f, on obtient (avec $f^2 = 0$ et $f(e_i) = 0$ si $i \in \{r+1, \dots, n-r\}$)

$$\sum_{i=1}^{r} \beta_i e_i = \sum_{i=1}^{r} \beta_i f(u_i) = 0$$

Comme $(e_1, \dots, e_r)$ est libre, les β_i sont nuls. En reportant dans $(*)$ et comme $(e_1, \dots, e_{n-r})$ est libre, les α_i sont aussi nul. Ainsi, $\mathcal{B}$ est libre et c'est une base de $\mathbb{R}^n$.
Par choix des vecteurs de $\mathcal{B}$, on a (définition par blocs)

$$M_r = Mat(f, \mathcal{B}) = \begin{pmatrix} 0 & I_r \\ 0 & 0 \end{pmatrix}$$

6. a. Si $R \in Rac(A)$ alors soit $R = 0$ soit il existe une matrice inversible P et un entier $r \in [1..n/2]$ telle que $R = PM_rP^{-1}$.
Réciproquement, la matrice nulle est une racine carrée de 0 et si $r \leq n/2$, un produit par blocs montre que $M_r^2 = 0$ et donc $(PM_rP^{-1})^2 = PM_r^2P^{-1} = 0$. Ainsi,

$$Rac(0) = \{PM_rP^{-1} /\ P \in GL_n(\mathbb{R}),\ r \in [1, n/2]\} \cup \{0\}$$

b. Dans le cas $n = 4$, les racines carrées de 0 sont 0 et les matrices semblables à l'une des deux matrices

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

7. a. $R^2 = I_n$ donne $det(R)^2 = 1$ et donc $det(R) \neq 0$. R est donc inversible.
   b. $X^2 - 1$ est un polynôme qui annule R. Comme il est scindé à racines simples, R est diagonalisable. En outre, les valeurs propres de R sont racines de $X^2 - 1$ et ne peuvent valoir que 1 ou -1. Ainsi, R est semblable à une matrice diagonale où les coefficients diagonaux valent 1 ou -1.
8. Ce qui précède montre que

$$Rac(I_n) \subset \left\{P.diag(\varepsilon_1, \dots, \varepsilon_n).P^{-1} / \ P \in GL_n(\mathbb{R}), \ \forall i, \ \varepsilon_i \in \{-1, +1\}\right\}$$

Réciproquement $D = diag(\varepsilon_1, \dots, \varepsilon_n)$ verifie $D^2 = I_n$ quand les ε_k valent 1 ou -1 et $(PDP^{-1})^2 = PD^2P^{-1} = I_n$. L'inclusion précédente est donc une égalité.
9. $diag(-1, -2, \dots, -n)$ est une matrice symétrique réelle qui, d'après l'exemple 1, n'admet pas de racine carrée.
10. Soit $A \in S_n^+(\mathbb{R})$. Le théorème spectrale donne l'existence d'une matrice orthogonale P et d'une matrice diagonale D telles que $P^{-1}AP = D$. Les coefficients diagonaux d_i de D sont valeurs propres pour A. Si X_i est vecteur propre associé alors

$$0 \leq {}^tX_iAX_i = {}^tX_i(d_iX_i) = d_i\|X_i\|^2$$

où $\|.\|$ est le norme euclidienne. Comme $\|X_i\|^2 > 0$ (X_i est non nul puisque c'est un vecteur propre), on a $d_i \geq 0$. On peut alors poser

$$R = P.diag(\sqrt{d_1}, \dots, \sqrt{d_n}).P^{-1} = P\Delta P^{-1}$$

P étant orthogonale on a $P^{-1} = {}^tP$ et R est symétrique. Par ailleurs, $R^2 = PDP^{-1} = A$ et R est racine carrée de A. Enfin, R est positive :

$$\forall X \ {}^tXRX = {}^tXP\Delta{}^tPX = \sum_{i=1}^{n} \sqrt{d_i}y_i^2 \ \text{ avec } \ Y = {}^tPX$$

et cette quantité est bien positive. On a finalement montré que

$$Rac(A) \cap S_n^+(\mathbb{R}) \neq \emptyset$$

II. Etude topologique de $Rac(A)$.

$M_n(\mathbb{R})$ étant de dimension finie, toutes les normes y sont équivalentes. On pourra choisir la norme N de l'énoncé ou toute autre norme. Cela ne change rien du point de vue topologique.

11. Par théorèmes généraux, $R \mapsto R^2$ est continue sur $M_n(\mathbb{R})$ (chaque fonction coordonnée l'est comme fonction polynomiale des coefficients de R). Ainsi, si (R_k) est une suite convergente d'éléments de limite R alors $R_k^2 \to R^2$.
Ainsi, si (R_k) est une suite convergente d'éléments de $Rac(A)$, la limite est dans $Rac(A)$. Ce dernier ensemble est donc fermé.
12. a. On a $S_q^2 = I_2$. Comme $N(S_q) = \max(|q|, 1) \to +\infty$ quand $q \to +\infty$, $Rac(I_2)$ n'est pas borné.

b. Définissons par blocs la matrice $M_q = \begin{pmatrix} S_q & 0 \\ 0 & I_{n-q} \end{pmatrix}$. On a alors $M_q^2 = I_n$ (calcul par blocs) et $N(M_q) \to +\infty$ quand $q \to +\infty$. Ainsi, $Rac(I_n)$ n'est pas borné pour $n \geq 3$.

c. On vient de voir que l'on peut trouver une suite (R_k) de racines carrées de I_n telles que (R_k) n'est pas bornée. Si, par l'absurde, il existait une norme surmultiplicative $\|.\|$ alors on aurait

$$\forall k,\ \|R_k\|^2 \leq \|R_k^2\| = \|I_2\|$$

Le membre de droite est constant et celui de gauche de limite infinie (voir remarque préliminaire en début de partie). On obtient une contradiction ce qui prouve la non existence d'une norme surmultiplicative.

Partie III. Intérieur de $Rac(A)$.

13. a. On a

$$B_\infty(a,r) = \prod_{i=1}^{p}]a_i - r, a_i + r[$$

b. Soit $a \in F \cap G$. Si, par l'absurde, il existait $r > 0$ tel que $B_\infty(a,r) \subset F \cap G$ alors on aurait a fortiori $B_\infty(a,r) \subset F$ et donc a serait intérieur à F ce qui est exclus (et donne une contradiction). $F \cap G$ n'a donc pas de point dintérieur.
Remarque : pour arriver à cette conclusion, il suffit que F OU G soit d'intrieur vide.

14. a. Le seul polynôme admettant une infinité de racines est le polynôme nul. Pour le voir, on peut, par exemple, prouver par récurrence q'un polynôme non nul de degré n admet au plus n racines.
   - Si P est constant non nul il n'admet pas de racine.
   - Supposons le résultat vrai jusqu'au rang n. Soit P de degré $n+1$. Entre deux racines de P, il y a une racine de P' (théorème de Rolle). Comme P' admet au plus n racines ($deg(P') = deg(P) - 1 = n$), P en admet au plus $n+1$.

   On peut aussi prouver le résultat (et on n'utilise alors plus la structure ordonnée de $\mathbb{R}$) en montrant que si $P(a) = 0$ alors $(X - a)$ divise P et en raisonnant par degré.

b. Dans le plan $(0, x_1, x_2)$, $2x_1 - x_2 = 1$ est l'équation d'une droite. $Z(P)$ est donc infini. $x_1^2 - x_2 = 0$ est l'équation d'une parabole et $Z(Q)$ est aussi infini.

15. a. Le résultat pour $p = 1$ a été justifié en question 14.a.
Supposons le résultat vrai jusqu'à un rang $p \geq 1$. Soient alors P une fonction polynomiale qui s'annule sur $I_1 \times \cdots \times I_{p+1}$ où chaque I_k est une partie infinie de $\mathbb{R}$. En ordonnant les puissances de x_{p+1}, on peut écrire

$$P(x_1, \dots, x_{p+1}) = \sum_{i=0}^{N} P_i(x_1, \dots, x_p) x_{p+1}^i$$

où chaque P_i est dans Γ_p.
Fixons $x_1, \dots, x_p$ avec $x_i \in I_i$ et considérons l'expression précédente comme fonction de x_{p+1}. C'est une fonction polynomiale qui s'annule en une infinité de points. D'après l'initialisation, c'est le polynôme nul. On a donc

$$\forall i \in \{1, .., N\},\ \forall (x_1, \dots, x_p) \in I_1 \times \cdots \times I_p,\ P_i(x_1, \dots, x_p) = 0$$

L'hypothèse de récurrence donne la nullité des P_i et donc celle de P. On a ainsi prouvé le résultat au rang $p+1$ et complété la récurrence.

b. D'après la question 13.a, toute partie d'intérieur non vide contient une sous-partie $\prod I_k$ où chaque I_k est infini (intervalle de longueur $2r > 0$). Si P s'annule sur une partie d'intérieur non vide, P est alrs nul avec la question précédente.

c. En contraposant le résultat de la question précédente, si $P \neq 0$ alors $Z(P)$ est d'intérieur vide.

16. a. R^2 est une matrice dont le coefficient générique est

$$\sum_{k=1}^{n} R_{i,k} R_{k,j}$$

Considérons alors

$$Q_{i,j} = \left(\sum_{k=1}^{n} x_{i,k} x_{k,j} \right) - a_{i,j} \in \Gamma_{n^2}$$

Par définition de $Rac(A)$, on a

$$Rac(A) = \bigcap_{1 \leq i,j \leq n} Z(Q_{i,j})$$

ce qui fait apparaître $Rac(A)$ comme sous-ensemble de $\mathbb{R}^{n^2}$.

b. Comme intersection de parties d'intérieur vide, $Rac(A)$ est d'intérieur vide avec la question 13.b.