❧ Par hypothèse, la matrice

$$B = A^2 - 2A = (A - I)^2 - I$$

est diagonalisable et par suite, la matrice $(A - I)^2$ est diagonalisable.

Il existe donc un polynôme $P_0 \in \mathbb{C}[X]$ scindé à racines simples

$$P_0 = \prod_{k=1}^{r} (X - \lambda_k)$$

tel que

$$P_0\big((A - I)^2\big) = 0.$$

❧ Comme $1 \notin \mathrm{Sp}(A)$, alors la matrice $(A - I)$ est inversible.

Si l'un des λ_k était nul, alors P_0 admettrait 0 pour racine et il existerait un polynôme $Q_0 \in \mathbb{C}[X]$ tel que

$$P_0 = XQ_0.$$

On aurait alors

$$0 = P_0\big((A - I)^2\big) = \underbrace{(A - I)^2}_{\text{inversible}} \cdot Q_0\big((A - I)^2\big)$$

et par conséquent, Q_0 serait un polynôme annulateur de $(A - I)^2$.

Le polynôme Q_0 est lui aussi scindé à racines simples et 0 n'est pas racine de Q_0.

Ainsi, quitte à remplacer P_0 par Q_0, on peut supposer que $(A - I)^2$ admet un polynôme annulateur P_0, scindé à racines simples et n'admettant que des racines *non nulles* $\lambda_1, \ldots, \lambda_r$.

❧ Comme P_0 est un polynôme annulateur de $(A - I)^2$, alors le polynôme

$$P_1 = P\big((X - 1)^2\big) = \prod_{k=1}^{r} \big((X - 1)^2 - \lambda_k\big)$$

est un polynôme annulateur de A.

Comme les λ_k sont *complexes*, il existe des complexes μ_k tels que $\mu_k^2 = \lambda_k$ et le polynôme annulateur

$$P_1 = \prod_{k=1}^{r} \big[(X - 1 - \mu_k)(X - 1 + \mu_k)\big]$$

est donc scindé.

❧ Il reste à vérifier que les racines de P_1 sont simples.

S'il existe deux indices i et j tels que $1 \pm \mu_i = 1 \pm \mu_j$, alors

$$\lambda_i = \mu_i^2 = \mu_j^2 = \lambda_j$$

et comme les λ_k sont deux à deux distincts, on en déduit que $i = j$.

Si $1 + \mu_i = 1 - \mu_i$, alors $\lambda_i = \mu_i^2 = 0$: c'est impossible car 0 n'est pas racine de P_0.

Par conséquent, les $2r$ racines de P_1 sont bien deux à deux distinctes et P_1 est un polynôme annulateur de A scindé à racines simples, donc la matrice A est bien diagonalisable.