1) (a) Si $F(X)=G(X)H(X)$ avec $G(X),H(X)\in\mathbb{Z}[X]$, alors le produit des coefficients dominants de G et de H vaut 1.

Ces coefficients sont donc tous deux égaux à 1 ou à -1.

Quitte à changer $G(X)$ par $-G(X)$ et $H(X)$ par $-H(X)$, on peut alors supposer que G et H sont unitaires.

Comme $F(\alpha)=0$, on a, par exemple, $G(\alpha)=0$.

Or $\deg G\leq\deg F$ et par l'hypothèse de minimalité de $\deg F$, on a $\deg G=\deg F$ donc $G=F$ et F est irréductible dans $\mathbb{Z}[X]$.

(b) On a $Cont(F)=1$ car F est unitaire donc $F(X)$ est irréductible dans $\mathbb{Q}[X]$.

Ainsi, $F(X)$ est un polynôme unitaire irréductible de $\mathbb{Q}[X]$ qui s'annule en α. Il est donc égal à $Irr(\alpha,\mathbb{Q},X)$.

2) On vient de voir que si α est entier sur $\mathbb{Z}$, alors $Irr(\alpha,\mathbb{Q},X)\in\mathbb{Z}[X]$.

Inversement, si un nombre complexe α est tel que $Irr(\alpha,\mathbb{Q},X)\in\mathbb{Z}[X]$, alors α est zéro du polynôme unitaire $Irr(\alpha,\mathbb{Q},X)$ à coefficients dans $\mathbb{Z}$, donc α est entier sur $\mathbb{Z}$ par définition.

3) Si d n'est pas un carré parfait, alors $\sqrt{d}\notin\mathbb{Q}$ donc $\alpha\notin\mathbb{Q}$.

Aussi, on a $\alpha^2=\dfrac{1+2\sqrt{d}+d}{4}=\alpha+\dfrac{(d-1)}{4}$.

α est donc racine du polynôme $f(X)=X^2-X+\dfrac{(1-d)}{4}$. Le polynôme minimal de α sur $\mathbb{Q}$ est de degré ≥ 2 (puisque $\alpha\notin\mathbb{Q}$ et divise $f(X)$). Il est donc égal à $f(X)$.

Par 2), α est entier sur $\mathbb{Z}$ si et seulement si $\dfrac{(1-d)}{4}\in\mathbb{Z}$, ce qui équivaut à dire que $d\equiv 1[4]$.