On considère deux éléments a et b de l'anneau $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$.
L'élément d est un pgcd de a et b si, et seulement si, il existe deux éléments α et β premiers entre eux de A tel que

$$a = d\alpha \qquad \textit{et} \qquad b = d\beta.$$

Si d est un pgcd de a et b, alors

$$aA + bA = dA \tag{1}$$

donc $aA \subset dA$ et $bA \subset dA$. Ainsi, d divise a et b, donc il existe deux éléments α et β de A tels que

$$a = d\alpha \qquad \text{et} \qquad b = d\beta.$$

Mais on déduit aussi de (1) qu'il existe deux éléments u et v de A tels que

$$d = au + bv = d(\alpha u + \beta v).$$

► Si $d \neq 0$, alors on peut simplifier par d et en déduire que

$$\alpha u + \beta v = 1.$$

D'après le Théorème de Bézout, les éléments α et β sont premiers entre eux.

✍ *Dans un anneau intègre (comme $\mathbb{Z}$ ou comme $\mathbb{K}[X]$), on peut simplifier par tout facteur non nul – qu'il soit inversible ou non.*

► Si $d = 0$, alors $a = b = 0$ et on peut choisir $\alpha = \beta = 1$.

✍ *Ce second cas est sans aucun intérêt mathématique, mais ce n'est pas une raison pour l'ignorer.*

❧ Réciproquement, supposons qu'il existe deux éléments α et β de A, premiers entre eux, tels que $a = d\alpha$ et $b = d\beta$. Il est alors clair que d divise a et b, donc

$$aA \subset dA \qquad \text{et} \qquad bA \subset dA.$$

Ainsi, dA est un idéal qui contient les deux idéaux aA et bA, donc

$$aA + bA \subset dA.$$

✍ *Si I et J sont deux idéaux de A, alors $I + J$ est le plus petit idéal de A (pour la relation d'ordre partiel $\subset$) qui contienne à la fois I et J.*

Par ailleurs, d'après le Théorème de Bézout, il existe deux éléments u et v de A tels que

$$\alpha u + \beta v = 1.$$

On en déduit que

$$d = d(\alpha u + \beta v) = au + bv \in aA + bA$$

et donc que

$$dA \subset aA + bA.$$

✍ *L'idéal dA engendré par d est le plus petit idéal (pour la relation $\subset$) qui contienne d. Il est donc contenu dans $aA + bA$, qui est un idéal qui contient d.*

On a ainsi démontré que $dA = aA + bA$ et donc que d était un pgcd de a et b.