A corollary of the Gauss Lemma

The point of this note is to prove the following commutative algebra lemma, which I have found that I will need twice:

Theorem 1. *Let A be an integrally closed domain. Let B be an A-algebra which is torsion-free and finitely generated as an A-module. Let $\theta \in B$ and map $A[t] \to B$ by $t \mapsto \theta$. The kernel of this map is a principal ideal $(g(t))$ in $A[t]$, and g is monic.*

Moreover, if we write $X = \mathrm{MaxSpec}(A)$ and $Y = \mathrm{MaxSpec}(B)$, then the corresponding map $Y \to Z(g) \subset X \times \mathbb{A}^1$ is surjective.

Recall that a polynomial is called ***monic*** if its leading coefficient is 1.

This result follows from Gauss's Lemma:

Theorem 2. *Let A be an integrally closed domain with fraction field K. Let $f(t)$ be a monic polynomial in $A[t]$ and suppose that $f(t)$ factors in $K[t]$ as $g(t)h(t)$ with g and h monic. Then g and h have coefficients in A.*

Gauss (1801) proved this when $A = \mathbb{Z}$. Note that the case where $A = \mathbb{Z}$ and $\deg g = 1$ is the rational root theorem (actually proving the rational root theorem in that manner would be circular though, since one usually uses the rational root theorem to show that $\mathbb{Z}$ is integrally closed).

Proof of Gauss's Lemma. Let L be a splitting field for f over K and let $f(t) = \prod_{i=1}^{r}(t - \alpha_i)$ in L. Let B be the integral closure of A in L, so the α_i are in B. Then $g(t)$ (and likewise $h(t)$) is of the form $\prod(t - \alpha_{i_j})$ for some subset $\{i_1, i_2, \ldots, i_s\}$ of $\{1, 2, \ldots, r\}$. Since B is a subring of L, this shows that the coefficients of $g(t)$ are in B.

So the coefficients of g are in $B \cap K$. Since A is algebraically closed, $B \cap K = A$. □

Proof of Theorem 1. Let $K = \mathrm{Frac}(A)$. First consider the map $K[t] \to B \otimes_A K$ by $t \mapsto \theta$. Since $K[t]$ is a PID, the kernel of this map is principal; call it $(g(t))$ with g a monic polynomial in $K[t]$. (This is the ***minimal polynomial*** of θ.)

Since B is integral over A, we also know that θ obeys some monic polynomial $f(t) \in A[t]$. So $g(t)|f(t)$ in $K[t]$ and, by Gauss's Lemma, we deduce that $g(t) \in A[t]$.

Now, $g(\theta)$ is *a prioiri* zero in $B \otimes_A K$. But, since B is torsion-free as an A-module, this shows that $g(\theta) = 0$ in B. Thus, $g(t)$ is in the kernel of $A[t] \to B$.

Suppose that $h \in A[t]$ with $h(\theta) = 0$. Then $g(t)|h(t)$ in $K[t]$, say $h(t) = g(t)p(t)$. Using Gauss's Lemma again (or just writing out the division algorithm), $p(t) \in A[t]$. So $g(t)|h(t)$ in $A[t]$.

We have now shown that $g(\theta) = 0$ and, if $h(\theta) = 0$ then $g(t)|h(t)$. So the kernel of $A[t] \to B$ is $(g(t))$.

We have now shown that there is a well defined injective map $A[t]/g(t) \to B$. Translating directly into geometry, we get a ***dominant*** map $Y \to Z(g)$. (Dominant means "has dense image".) But B is a finitely generated A-module, so it is also a finitely generated $A[t]$-module, and we thus know that the map $Y \to X \times \mathbb{A}^1$ has closed image. We conclude that $Z(g)$ is the image of Y. □