Luroth's Theorem

This is a striking theorem about function fields in one variable. Nothing like it is true in two or more variables. The key ingredients are a previous homework problem, and Gauss Lemma on primitive polynomials over a u.f.d. The use of two variables is inevitable, since one must stand for an element of a field, and the other must play the role of the variable in a minimal polynomial.

Theorem (Luroth). *Let F be a field and x a transcendental over F. Let $F \subsetneq E \subset F(x)$ be a field between F and $F(x)$. Then $E = F(y)$ for some element $y \in F(x)$, and $F(x)$ is finite-dimensional over E.*

By a homework problem, $F(x)/E$ is finite-dimensional. Let $p(t)$ be the minimal polynomial of x over E. We multiply by an element $a \in F[x]$ so that $f = ap(t)$ is primitive in $F[x][t]$ (since p to begin with had coefficients in $F(x)[t]$). Write

$$f = a_0(x) + a_1(x)t + \cdots + a_n(x)t^n$$

in $F[x][t]$, where $n = \deg_t(f) = \deg(p) = [F(x) : E]$. ($\deg_t(f)$ is the degree of f in t.) Since p is monic, we must have $a = a_n(x)$, and all $a_i(x)/a_n(x)$ lie in E. Since x is transcendental over F, we cannot have all $a_i(x)/a_n(x)$ in F. Say $u = a_i(x)/a_n(x) \in E$ but not in F. Write

$$u = \frac{g(x)}{h(x)} \quad g, h \in F[t], \text{ and relatively prime}$$

Let $r = \max\{\deg(g), \deg(h)\}$, taking the maximum over all the ratios $a_i(x)/a_n(x)$. For this maximum r, we have, by a previous homework problem $[F(x) : F(u)] = r$.

Let $d = g(x)h(t) - h(x)g(t) \in F[x,t]$. The fact that g and h are relatively prime says that $d \neq 0$ in the u.f.d. $F[x,t]$.

Now $h(x)^{-1}d \in E[t]$ has x as a root, so $p(t) \mid h(x)^{-1}d$ in $E[t]$, and so $f \mid h(x)^{-1}d$ in $F(x)[t]$. But f is a primitive element in $F[x][t]$ so it follows from Gauss' Lemma that f divides d in $F[x,t]$. Then $d = f\alpha$, $\alpha \in F[x,t]$. We have

$$\deg_x(d) \leq r, \quad \deg_x(f) \geq \max\{\deg(a_i)\} = r$$

Thus $f = d\alpha$ means $\deg_x(d) = \deg_x(f) = r$, $\deg_x(\alpha) = 0$. Then $\alpha \in F[t]$, and in particular α is primitive in $F[x][t]$. Since f is also primitive, it follows that d is primitive in $F[x][t]$. As d is skew-symmetric, it follows that d is primitive in $F[t][x]$. But $\alpha \in F[t]$ and $\alpha \mid d$, so α is a unit in $F[t]$, i.e. $\alpha \in F$.

Now

$$n = \deg_t(f) = \deg_t(d) = \deg_x(d) = \deg_x(f) = r$$

so $E = F(u)$ as desired. (The fun part comes if one tries to make Luroth's theorem effective; it is, as usual, a classic existence theorem)