A. Miller M542 An Example Spring 2000

Theorem. There exists a field F and α, β in some extension field of F such that $[F(\alpha,\beta) : F] < \infty$ but there is no $\gamma \in F[\alpha,\beta]$ such that $F(\alpha,\beta) = F(\gamma)$.

This is similar to the example on page 354 of Gallian's book. Let $F = \mathbb{Z}_2(s,t)$ where s, t are indeterminates, i.e., variables. F is the field of all quotients of polynomials in the two variables with coefficients 0 or 1.

By Kronecker's Theorem we know that in some extension field of F there exists α and β such that $\alpha^2 = s$ and $\beta^2 = t$.

Claim 1. $[F(\alpha,\beta) : F] = 4$.
Claim 2. For all $\gamma \in F(\alpha,\beta)$ we have that $\gamma^2 \in F$.

The Claims finish the proof because if $\gamma^2 = a \in F$, then γ is a root of the polynomial $f(x) = x^2 - a$ and therefore $[F(\gamma) : F] \leq 2$ and so $F(\alpha,\beta) \neq F(\gamma)$.

To prove Claim 1 note that it suffices to prove

$$\beta \notin F(\alpha).$$

This is because by symmetry $\alpha \notin F(\beta)$ and therefore $\alpha \notin F$. Now $[F(\alpha) : F]$ is either 1 or 2 because α is the root of a polynomial of degree 2. So $\alpha \notin F$ implies it is 2. Similarly for $[F(\alpha,\beta) : F(\alpha)]$. Hence

$$[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\alpha)][F(\alpha) : F] = 2 \times 2 = 4$$

SubClaim. $\beta \notin F(\alpha)$.

$F(\alpha) = \{a + b\alpha : a, b \in F\}$. In any field of characteristic 2 we have that $(a+b)^2 = a^2 + b^2$. Hence if $\beta \in F(\alpha)$ there would have to be $a, b \in F$ such that $\beta = a + b\alpha$ and so

$$t = \beta^2 = a^2 + b^2\alpha^2 = a^2 + b^2 s$$

The elements a and b are rational functions in the two variables, but by clearing the denominators we can find polynomials $a, b, c \in Z_2[s,t]$ such that (c nontrivial)

$$c^2 t = a^2 + b^2 s$$

If we think of the two sides as polynomials in t then the degree of poly on the left is odd. On the right the degree in t is even unless a and b have the same degree and the highest coefficient cancels. Say the highest coefficient of a is $a_n t^n$ and for b it is $b_n t^n$ where a_n and b_n are polynomials in the variable s. Then the term with the highest coefficient of a^2+b^2s is $(a_n^2+b_n^2s)t^{2n}$. For this coefficient to cancel means that $a_n^2+b_n^2s=0$. But a_n^2 has even degree (as a polynomial in s) and b_n^2s has odd degree, contradiction. Thus the SubClaim is proved and so is Claim 1.

To prove Claim 2 note that

$$F(\alpha) = \{a + b\alpha : a, b \in F\}$$

$$F(\alpha, \beta) = \{c + d\beta : c, d \in F(\alpha)\}$$

and therefor

$$F(\alpha, \beta) = \{a + b\alpha + c\beta + d\alpha\beta : a, b, c, d \in F\}$$

But if $\gamma = a + b\alpha + c\beta + d\alpha\beta$ then

$$\gamma^2 = a^2 + b^2\alpha^2 + c^2\beta^2 + d^2\alpha^2\beta^2 = a^2 + b^2s + c^2t + d^2st \in F$$