Here is the proof of the theorem that I was in the process of proving at the end of class.

**Theorem.** If $\sigma_1, \ldots, \sigma_n$ is a group of automorphisms of $E$, and if $F$ is the fixed field, then $[E : F] = n$. In particular, $E/F$ is Galois.

**Proof.** We use linear algebra again. Suppose $[E : F] \geq n + 1$. Say $\sigma_1$ is the identity. Then let $\alpha_1, \ldots, \alpha_n, \alpha_{n+1}$ be elements of $E$ that are linearly independent with respect to $F$. By linear algebra, there is a nontrivial solution $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ in $E$ to the system of equations

$$
\begin{align*}
 x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \cdots + x_{n+1}\sigma_1(\alpha_{n+1}) &= 0 \\
 x_1\sigma_2(\alpha_1) + x_2\sigma_2(\alpha_2) + \cdots + x_{n+1}\sigma_2(\alpha_{n+1}) &= 0 \\
 &\vdots \\
 x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \cdots + x_{n+1}\sigma_n(\alpha_{n+1}) &= 0.
\end{align*}
$$

The solution can’t lie in $F$ (i.e. all $x_i$ can’t lie in $F$) or else the first equation would be a dependence over $F$.

Among all nontrivial solutions $(x_1, \ldots, x_n)$, we choose one with the least number of nonzero elements. We’ll get a contradiction out of this. We may suppose this solution is $(a_1, \ldots, a_r, 0, \ldots, 0)$, where the first $r$ are non-zero. Also, dividing by $a_r$, we may assume $a_r = 1$. So we have:

$$
\begin{align*}
 a_1\sigma_1(\alpha_1) + a_2\sigma_1(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\
 a_1\sigma_2(\alpha_1) + a_2\sigma_2(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\
 &\vdots \\
 a_1\sigma_n(\alpha_1) + a_2\sigma_n(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0.
\end{align*}
$$

Note that $r \neq 1$. We may also assume $a_1$ is in $E$, but not in $F$ (as not all $a_i$ can lie in $F$, as observed above). Thus there is an automorphism $\sigma_k$ for which $\sigma_k(a_1) \neq a_1$. Apply $\sigma_k$ to
(1) to get
\[
\begin{align*}
\sigma_k(a_1)\sigma_k(\alpha_1) + \sigma_k(a_2)\sigma_k(\alpha_2) + \cdots + \sigma_k(\alpha_r) &= 0 \\
\sigma_k(a_1)\sigma_k(\alpha_1) + \sigma_k(a_2)\sigma_k(\alpha_2) + \cdots + \sigma_k(\alpha_r) &= 0 \\
& \vdots \\
\sigma_k(a_1)\sigma_k(n(\alpha_1) + \sigma_k(a_2)\sigma_k(n(\alpha_2) + \cdots + \sigma_k(\alpha_r) &= 0.
\end{align*}
\]

Using the fact that \(\sigma_1, \ldots, \sigma_n\) form a group (this is where we use the hypothesis!), we see that \(\sigma_k \cdot \sigma_1, \ldots, \sigma_k \cdot \sigma_2, \ldots, \sigma_k \cdot \sigma_n\) is a permutation of \(\sigma_1, \ldots, \sigma_k\). Thus we can rearrange the rows to get
\[
\sigma_k(a_1)\sigma_1(\alpha_1) + \sigma_k(a_2)\sigma_1(\alpha_2) + \cdots + \sigma_k(\alpha_r) = 0 \\
\sigma_k(a_1)\sigma_2(\alpha_1) + \sigma_k(a_2)\sigma_2(\alpha_2) + \cdots + \sigma_1(\alpha_r) = 0 \\
& \vdots \\
\sigma_k(a_1)\sigma_n(\alpha_1) + \sigma_k(a_2)\sigma_n(\alpha_2) + \cdots + \sigma_1(\alpha_r) = 0.
\]

Subtracting these from (1), we get
\[
\begin{align*}
(a_1 - \sigma_k(a_1))\sigma_1(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_1(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0 \\
(a_1 - \sigma_k(a_1))\sigma_2(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_2(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0 \\
& \vdots \\
(a_1 - \sigma_k(a_1))\sigma_n(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_n(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0.
\end{align*}
\]

Thus we have a solution with a fewer number of nonzero entries. Contradiction! \(\square\)

E-mail address: vakil@math.stanford.edu