(1) Recall from last lecture that $K = E(t_1, \ldots, t_n)$, $k = \text{Fix}(S_n)$, $S_n = \Gamma(K/k)$, $[K : k] = n!$. We saw that
(a) $k = E(s_1, \ldots, s_n)$ where the $s_i$ are the elementary symmetric polynomials.
(b) $K/k$ is a splitting field for $f_n$.
(c) For each $i$, $t_i$ has degree $i$ over $k(t_n, \ldots, t_{i+1})$ and $f_i$ is the minimal polynomial.
(d) The coefficients of $f_i$ are polynomials (not just rational functions) in $s_1, \ldots, s_n, t_{n}, \ldots, t_{i+1}$ with coefficients from $E$.

(2) Multiplying bases as in the proof that degrees of extensions are multiplicative, we find a basis $M$ for $K/k$ consisting of all the $n!$ monomials $t_{a_1}^{a_1} \cdot \ldots \cdot t_{a_n}^{a_n}$ where $0 \leq a_j < j$.

Since $f_j$ is monic, the equation $f_j(t_j) = 0$ and an easy induction permit us to express $t_{j}^{a_j}$ for $0 \leq a < j$, where each coefficient is a polynomial in $s_1, s_2, \ldots, s_n, t_{n}, \ldots, t_{i+1}$ with coefficients in $E$.

Accordingly, any polynomial in $E[t_1, \ldots, t_n]$ can be expressed as a linear combination of elements of $M$, where each coefficient is a polynomial in $s_1, s_2, \ldots, s_n$ with coefficients in $E$. Since $M$ is a basis for $K$ as VS over $k$, this expression is unique!

(3) Suppose now that $f \in E[t_1, \ldots, t_n]$ is symmetric and express it in the form described above; that is $f = \sum a_{\bar{a}} P_{\bar{a}} m_{\bar{a}}$ where $\bar{a} = (a_1, \ldots, a_n)$, $a_j < j$, $P_{\bar{a}}$ is a polynomial in the $s_i$, and $m_{\bar{a}} = t_{a_1}^{a_1} \cdot \ldots \cdot t_{a_n}^{a_n}$. It is easy to see that only the coefficient associated with $\bar{0}$ is nonzero.

(4) Conclusion: any symmetric polynomial in the $t_i$ is a polynomial in the $t_i$. In particular any symmetric polynomial in the roots of the polynomial $f$ can be expressed as a polynomial in the $t_i$ in the coefficients of $f$.

(5) Now we sketch how find the general solution of the cubic, leaving the messy formulae to the handout (which was made using computer algebra).

Suppose that $E$ has characteristic zero and contains $\zeta$ a primitive cube root of 1. As above let $k = E(s_1, s_2, s_3)$ and $K = E(t_1, t_2, t_3)$. Our task is obtain formulae for the $t_i$ in terms of the $s_i$; this amounts to finding the general formula for solving the cubic.

Consider the intermediate field $l = \text{Fix}(A_3)$. On general grounds we know that $[l : k] = 2$, so that $l$ should be obtained by adjoining to $k$ a square root. Let $\Delta = (t_1 - t_2)(t_2 - t_3)(t_3 - t_1)$, then easily $\Delta \in \text{Fix}(A_3) = l$ but $\Delta \notin \text{Fix}(S_3) = k$. So $l = k(\Delta)$. What is more $\Delta^2 \in \text{Fix}(S_3) = k$, and $\Delta^2$ is symmetric so can be written as a polynomial in $s_1, s_2, s_3$.

Cultural note: the expression $\Delta$ is called the discriminant of the cubic, and we have more to say about discriminants next week.
(6) Of course \( \Gamma(K/l) = A_3 \), which is cyclic. We note that there are exactly three characters \( \sigma_0, \sigma_1, \sigma_2 \) of \( A_3 \) in \( l \), obtained by mapping the generating element \((123)\) to \( 1, \zeta, \zeta^2 \) respectively.

Now we use an idea from the general analysis of cyclic Galois extensions, which we did using such characters. The linear combination \( \rho = 1e + \zeta(123) + \zeta^2(132) \) is not zero, and if we can find an element \( b \) on which it does not take the value zero then various good things happen: notably if \( a = \rho(b) \) then \( K = l(a), \ a^3 \in l \).

But easily \( \rho(t_1) = t_1 + \zeta t_2 + \zeta^2 t_3 \), so if we let \( a_1 = t_1 + \zeta t_2 + \zeta^2 t_3 \) then \( a_1^3 \in l \) (not astonishing when we consider that \((123)\) maps \( a_1 \) to \( \zeta^2 a_1 \)). So \( a_1^3 \) can be expressed in terms of \( s_1, s_2, s_3, \Delta \). A similar argument holds for \( a_2 = t_1 + \zeta^2 t_2 + \zeta t_3 \), and of course \( a_0 = t_1 + t_2 + t_3 = s_1 \).

This gives us three linearly independent expressions (again this is no surprise, characters form an independent set) so we can solve for \( t_1, t_2, t_3 \) by linear algebra.