43) (10 points). 1) $\Rightarrow$ 2) Let $f(x) \in F[X]$ be an irreducible polynomial having a root $\alpha \in E$. Let $\beta \in \bar{F}$ be another root of $F$. The isomorphism $F(\alpha) \to F(\beta)$ extends to an isomorphism $\sigma \in \text{Aut}(\bar{F}/F)$. By the property $\sigma(E) = E$ stated in 1), we get $\beta \in E$. Thus every irreducible polynomial $f(x) \in F[X]$ which has a root in $E$ splits completely in $E$, which is statement 2).

2) $\Rightarrow$ 1) : Let $\sigma$ be any element of Aut($\bar{F}/F$), and let $\alpha$ be any element of $E$. Let $f(X)$ be the irreducible polynomial of $\alpha$ over $F$. Then $\sigma$ sends $\alpha$ to some root $\beta \in \bar{F}$ of $f(X)$. However by the property stated in 2), that that $f(X)$ splits completely in $E$, we get that $\beta \in E$. This shows that $\sigma(E) = E$ for all $\sigma \in \text{Aut}(\bar{F}/F)$, which is statement 1).

44) (10 points). Prove that a finite extension $E/F$ is normal if and only if $E$ is the splitting field of some $f \in F[X]$.

For a finite extension $E/F$, statement 2) of the previous problem is equivalent to the statement that $E$ is the splitting field of a polynomial $f(X) \in F[X]$ (We showed this as Problem 28, HW7). Thus the equivalence of the statements 1) and 2), implies the equivalence of statement 1) (that the finite extension $E/F$ is normal) with the statement that $E$ is the splitting field of a polynomial $f(X) \in F[X]$.

46 [D-F], 14.2 #21 (5 points). Use the linear independence of characters to show that for any Galois extension $K/F$, there is an element $\alpha \in K$ with $\text{Tr}_{K/F}(\alpha) \neq 0$

Let $G = \text{Gal}(K/F)$. To say that there is no $\alpha$ meeting the requirement stated in the problem is to say that $\sum_{\sigma \in G} \sigma = 0$ as a linear combination of characters of $K^\times$ with values $K$. But we know that the $\sigma \in G$ being distinct are linearly independent over $K$. This shows that there exists an element $\alpha \in K$ with $\text{Tr}_{K/F}(\alpha) \neq 0$

46 [D-F], 14.4 #3 (10 points). Let $F$ be a field contained in the ring of $n \times n$ matrices over $\mathbb{Q}$. Prove that $|F : \mathbb{Q}| \leq n$. 

Solutions to Homework 10
Math 601, Spring 2008
Clearly $F/\mathbb{Q}$ is finite dimensional, and by the primitive element theorem, we may write $F = \mathbb{Q}(\alpha)$. The minimal polynomial of the matrix $\alpha$ is the irreducible polynomial for $\alpha$ over $\mathbb{Q}$. The minimal polynomial has degree $\leq n$ (because it divides the characteristic polynomial). Thus $[F : \mathbb{Q}] \leq n$.

46 [D-F], 14.2 #17, 18, 19 (15 points). Let $F \subset K \subset L$ with $L/F$ Galois. Let $G = \text{Gal}(L/F)$ and $H < G$ be the subgroup such that $L^H = K$. For $\alpha \in K$ define $N_{K/F}(\alpha) = \prod_{\sigma \in G/H} \sigma(\alpha)$ and $\text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in G/H} \sigma(\alpha)$.

We will prove Problems 17 d) and Problem 14.2.31 [D-F]. The latter problem states the following: multiplication by $\alpha$ is an $F$-linear map from $K$ to itself defines a linear transformation $T_\alpha$. Then

\[ N_{K/F}(\alpha) = \det(T_\alpha) \quad \text{and} \quad \text{Tr}_{K/F}(\alpha) = \text{Trace}(T_\alpha) \]

We will also prove that the minimal polynomial of $\alpha$ over $F$, $m_\alpha(X) \in F[X]$ is related to $\text{char}(T_\alpha) \in F[X]$ by $\text{char}(T) = m_\alpha(X))^{[K:F(\alpha)]}$. The answers to Problems 17 a), b), c), and Problems 18), 19), 20 and even 22) of [14.2 D-F] can be read off from these observations.

17d): In a Galois extension $L/F$, every irreducible polynomial $f(X) \in F[X]$ of degree $d$ having a root in $\alpha \in L$ is separable and splits completely in $L$ as $f(X) = \prod_{i=1}^{d} (X - \alpha_i)$, with $\alpha_1, \ldots, \alpha_d$ being the distinct Galois conjugates of $\alpha$ in $L$. (for proof see the proof of Thm 14.2.13 [D-F]). Let $G = \text{Gal}(L/F)$, let $\alpha \in L$ and let $H' < G$ be the subgroup defined by $F(\alpha) = L^{H'}$. Then $\alpha_i = g_i(\alpha)$ where the $g_i H'$ are the cosets of $H'$ in $G$ (again, see proof of Thm 14.2.13 [D-F]). If $H$ is a subgroup of $H'$ and $h_j H$ are the cosets of $H$ in $H'$, then clearly $g_i h_j H$ are the cosets of $H$ in $G$. So if $K \subset L$ is a subfield defined by $K = L^H$, then we immediately get that

\[ N_{K/F}(\alpha) = \prod_{\sigma \in G/H} \sigma(\alpha) = \left( \prod_{g \in G/H'} g(\alpha) \right)^{[H':H]} \]

Let $n := [K : F]$ and $d := [F(\alpha) : F]$ and $m_\alpha(X) := X^d + a_{d-1}X^{d-1} + \cdots + a_0$. As observed above $m_\alpha(X)$ has $d$ distinct roots namely $g(\alpha)$ for $g \in G/H'$. Thus we obtain $\prod_{g \in G/H'} g(\alpha) = (-1)^d a_0$. The integer $[H' : H] = [K : F(\alpha)]$ works out to be $n/d$ so that $d|n$, and we can rewrite the above equation as

\[ N_{K/F}(\alpha) = \prod_{\sigma \in G/H} \sigma(\alpha) = \left( \prod_{g \in G/H'} g(\alpha) \right)^{[H':H]} = (-1)^d a_0^{n/d} \]
This completes 17d). We also note in passing that \( \text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in G/H} \sigma(\alpha) \) simplifies to \( n/d(-a_{d-1}) \) thus answering 18d).

**Problem 14.2.31 [D-F]**: Clearly for \( f \in F[X] \), we have \( f(T_a) = 0 \) (in \( \text{End}_F(K) \)) \( \iff \) \( f(\alpha) = 0 \) (in \( K \)). Thus \( \text{min}(T) = m_\alpha(X) \). Let \( g(X) \) be an irreducible factor of \( \text{char}(T_a) \). Since every root of \( \text{char}(T_a) \) is a root of \( m_\alpha(X) \), namely some \( g_i(\alpha) \), we see that \( g(X) \) is irreducible and has a root in \( L \), whence it is separable and splits completely in \( L \). In other words \( g(X) = \prod_{i'} (X - g_{i'}(\alpha)) \) for some subset \( \{i'\} \subset \{i\} \). Therefore \( g(X) \) divides \( m_\alpha(X) \), and this is possible only if \( g(X) = m_\alpha(X) \). It follows that \( \text{char}(T) = (m_\alpha(X))^{n/d} \). Thus the trace and determinant of the linear transformation \( T \) are exactly \( \text{Tr}_{K/F}(\alpha) \) and \( N_{K/F}(\alpha) \) respectively.