Solutions to Homework 11

49. (Dummit-Foote, 14.4, #2) Let $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. Then α is fixed by no element of $G = \mathrm{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbf{Q})$, hence the subgroup of G fixing the field $\mathbf{Q}(\alpha)$ is the trivial subgroup. Hence $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ by the Galois correspondence.

50. (Dummit-Foote, 14.5, #12) For all $x \in \mathbf{F}_{p^n}$, we have $x^{p^n} - x = 0$. Therefore σ_p satisfies the polynomial $X^n - 1$ and since this polynomial is of degree n, it must be the characteristic polynomial. The linear transformation σ_p is diagonalizable over $\mathbf{F}_p$ if and only if $X^n - 1$ splits into linear factors in $\mathbf{F}_p$, which happens if and only if $\mathbf{F}_p$ contains the all of the n^{th} roots of unity. But this happens if and only if $\mathbf{F}_p^\times$ contains a cyclic subgroup of order n, which happens if and only if $n || \mathbf{F}_p^\times | = p - 1$ because the group $\mathbf{F}_p^\times$ is cyclic.

The linear transformation σ_p will be diagonalizable over $\overline{\mathbf{F}_p}$ if and only if $X^n - 1$ is separable. But $X^n - 1$ is separable if and only if it is relatively prime to its derivative nX^{n-1}, which happens if and only if this latter polynomial is non-zero. Clearly $nX^{n-1} = 0$ if and only if $p|n$.

51. (Dummit-Foote, 14.6, #11) Let $E/\mathbf{Q}$ be the Galois closure of F. We can write $F = \mathbf{Q}(\alpha)$ for some $\alpha \in F$, and then E is the splitting field of the minimal polynomial of α. Because this polynomial has degree 4, the group $G = \mathrm{Gal}(E/\mathbf{Q})$ must be a subgroup of S_4. As E contains a subfield which is quartic over $\mathbf{Q}$, G must contain a subgroup of index 4. Clearly $|G| > 4$ because F is not Galois over $\mathbf{Q}$, so $|G| = 8, 12, 24$. If the order of G is 24, then $G = S_4$. If the order of G is 12 then $G = A_4$, the only index 2 subgroup of S_4. If $|G| = 8$ then $G = D_8$, which is the only group of order 8 containing a non-normal subgroup (which corresponds to the non-Galois subextension F of E).

The field F contains a quadratic extension of $\mathbf{Q}$ if and only if given a subgroup of G of index 4, there is a subgroup of index 2 containing it. Neither S_4 nor A_4 satisfy this (A_4 has no subgroups of index 2, and the only subgroup of index 2 in S_4 is A_4). However, every element of D_8 of order 2 is contained in a subgroup of order 4.

52. (Dummit-Foote, 14.7, #12) Let p divide the order of $G = \mathrm{Gal}(L/\mathbf{Q})$. By Cauchy's Theorem, G has a subgroup H which corresponds to some subfield F' of L with $[L : F'] = p$. Suppose that for all $\sigma \in G$, we had $\sigma(\alpha) \in F'$. Then $F' = L$, which is absurd. Hence there exists some $\sigma \in G$ such that $\sigma(\alpha) \notin F'$. By the tower law and the fact that p is prime, we have $F'(\sigma(\alpha)) = L$. Setting $F = \sigma^{-1}(F')$, we have $F(\alpha) = L$ and $[L : F] = p$.

53. (Dummit-Foote, 14.8, #3) The discriminant of $f(X) = X^5 + 20X + 16$ is a square in $\mathbf{Q}$, hence the Galois group is contained in A_5. Modulo 3, $f(X)$ factors into two linear factors and one cubic factor, thus the Galois group of f contains a 3-cycle. Modulo 7 it is irreducible, proving that the Galois group contains a 5-cycle. But a 3-cycle and a 5-cycle will generate all of A_5.

(Dummit-Foote, 14.8, #4) Let $\zeta = \zeta_{11}$. Note that $\zeta^{-1} = \bar{\zeta}$, hence $\mathbf{Q}(\zeta + \zeta^{-1})$ is totally real and thus strictly contained in $\mathbf{Q}(\zeta)$. However, ζ satisfies the polynomial $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbf{Q}(\zeta + \zeta^{-1})[X]$, which proves that $[\mathbf{Q}(\zeta) : \mathbf{Q}(\zeta + \zeta^{-1})] = 2$. Since $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{Z}/10\mathbf{Z}$, we have

$\mathrm{Gal}(\mathbf{Q}(\zeta+\zeta^{-1})/\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$. Now, the given polynomial is of degree 5 and is satisfied by $\zeta+\zeta^{-1}$, which proves the result.