M622, Quiz 2, Mar. 30. 28 minutes.

1. (3 points) Suppose S is a splitting field of the polynomial $t(x) \in F[x]$ over F, and J is a subfield of S that contains F (i.e., $F \leq J \leq S$). Show in a couple of sentences that S is also a splitting field of $t(x) \in J[x]$ over J.

   Explanation. Observe that $t(x) \in J[x]$, and since K is an s.f. for $t(x)$ over F, $K = F(r_1, \ldots, r_n)$, where $\{r_1, \ldots, r_n\}$ are the roots of $t(x)$. Since $r_1, \ldots, r_n$ are all roots of $t(x)$, and $F \subseteq J \subseteq K$, it follows that S splits $t(x) \in J[x]$. If E is an intermediate field, $J \subseteq E \subseteq S$, then E splits $t(x) \in J[x]$ only if $r_1, \ldots, r_n$ are all contained in E. Since E contains F, and $r_1, \ldots, r_n$, E must be S. It follows that no proper subfield S over J splits $t(x) \in J[x]$, so S is an s.f. of $t(x) \in J[x]$.

2. (7 points) Suppose $t(x) \in F[x]$ is a monic polynomial of degree $n \geq 1$ over F and S is a splitting field of $t(x)$. Show that $n! \geq [S : F]$. Use induction on $\deg(t(x))$, and also the problem above (Problem 1).

   Proof. The proof is by induction on $\deg(t(x))$. If $\deg(t(x)) = 1$, then $F = S$, and $[F : F] = 1 = 1!$, completing the base step. Assume deg(t(x))= n, and the statement holds for all polynomial in $F[x]$ having degree less than n.

   Now consider $t(x)$ of degree n. If all roots of $t(x)$ are in F, then $S = F$, and $[S : F] = 1 \leq n!$. So suppose γ is a root of $t(x)$ not in F. Then γ is a root of an irreducible factor $p(x)$ of $t(x)$. As we've shown, $[F(\gamma) : F] = deg(p(x)) \leq deg(t(x)) = n$.

   As showed above, S is a s.f. of $t(x)$ over $F(\gamma)$. We have $t(x) = (x-\gamma)q(x)$, for some $q(x) \in F(\gamma)[x]$. Notice that S is a s.f. of $q(x)$ over $F(\gamma)$. Of course $deg(q(x)) = n - 1 < n$. By the induction hypothesis, $[S : F(\gamma)] \neq deg(q(x))! = (n-1)!$.

   Now by the Double Extension Lemma, we have $[S : F] = [S : F(\gamma)][F(\gamma) : F] \leq (n-1)!n = n!$, completing the induction proof.

3. (3 points) Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. (Suggestion: Use that the inverse of $\sqrt{2} + \sqrt{3}$ is in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.)

   Solution. $\sqrt{3} - \sqrt{2} = (\sqrt{2} + \sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. It follows easily that $\sqrt{2}, \sqrt{3}$ are both in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

4. (8 points) Let $x^4 - 2 = p(x) \in \mathbb{Q}[x]$. Let S be the splitting field of $p(x)$.

   (a) Show that $p(x)$ is irreducible—this is a one-line proof. REASON: Eisenstein.

   (b) List the roots of $p(x)$ below. ROOTS: $\{2^{1/4}, -2^{1/4}, i2^{1/4}, -i2^{1/4}\}$.

(c) Determine $[S:\mathbb{Q}]$—**Explain.** DMENSION, EXPLANATION: Since S is closed under multiplication and inverses, using the roots, it follows readily that $i \in S$. Now $S = \mathbb{Q}(2^{1/4}, i)$. We have $[\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 4 = deg(x^4 - 2)$, the latter an irreducible polynomial. Observe that $i \notin \mathbb{Q}(2^{1/4})$, the latter a subfield of $\mathbb{R}$; thus $x^2 + 1\ in \mathbb{Q}(2^{1/4})[x]$ is irreducible. Now we have $[S:\mathbb{Q}] = [S:\mathbb{Q}(2^{1/4}][Q(\mathbb{Q}(2^{1/4}):\mathbb{Q}] = 4(2) = 8$.

(d) Since $Aut(S/\mathbb{Q})$ acts faithfully on the four roots of $p(x)$ in S, $Aut(S/\mathbb{Q})$ is embedded in S_4. Based on your answers to first three parts ((a), (b), and (c)), briefly explain why there is no element $\sigma \in Aut(S/\mathbb{Q})$ such that σ fixes exactly one root of $p(x)$.

ANSWER: Fixing one root means the other three move. In S_4, this can be done only by a three-cycle. But our group $Aut(S/\mathbb{Q})$ has order 8, and by Lagrange, has no element of order 3.

(e) **+1 EC.** Based on your answers to the first three parts, determine a subgroup H of S_4 satisfying $H \cong Aut(S/\mathbb{Q})$. Briefly explain your answer: EXPLANATION.

Any 8-element subgroup of S_4 is a Sylow-2 subgroup. The Sylow 2-subgroups are pairwise isomorphic. One of those Sylow-2 subgroups is isomorphic to D_8, an 8-element subgroup of S_4. So our group is isomorphic to D_8.

5. (7 points max—2 points each.) True or false? If false, provide a specific counterexample.

(a) For any prime p, the group $F_p^{\times}$ is cyclic. (Here the group $F_p^{\times}$ is the group of units of F_p.) TRUE

(b) For any positive integer $n > 1$, if ψ is a primitive nth root of unity, then $\mathbb{Q}(\psi)$ is a splitting field for $\Phi_n(x)$ over $\mathbb{Q}$. TRUE

(c) Let p be a prime, and let $n \in \mathbb{N}$. Consider F_{p^n}, the finite field having p^n elements.

If $k \in \mathbb{N}$, and $k|p^n$, then F_{p^n} contains a subfield containing p^k elements.

FALSE. F_4 is not a subfield of F_8 since 2 doesn't divide 3.

(d) If K/F is a field extension with $\beta \in K - F$, and $[F(\beta) : F]$ is finite, then $[F(\beta) : F] = |Aut(F(\beta)/F)|$. FALSE: $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois, as we've mentioned.