M622 Test 2 prep probs.

1. Let K be a finite field with p^n elements. So p is a prime, $n \in \mathbb{N}$. So the prime subfield of K is of course $\mathbb{F}_p$, K is referred to as $\mathbb{F}_{p^n}$.
   (a) Explain why the map $\phi : K \to K$ given by $\phi(x) = x^p$ is an automorphism of K, and that ϕ fixes each element of the base field $\mathbb{F}_p$.
   (b) IMPORTANT: Explain why F above is the splitting field of $t(x) = x^{p^n} - x$.
   (c) Carefully go over the discussion, proof of (1) in solution set to M622.HWSolnsEtc.pdf, a problem that involves the subfields of a finite field. Be sure you understand why if A is a subfield of the finite field $\mathbb{F}_{p^n}$ and $|A| = p^k$, then $k|n$. (For example, a finite field with 8 elements has no subfield of order 4.) I'm attaching M622.HWSolnsEtc.pdf.

2. This problem involves the field $K = \mathbb{Q}(\sqrt{5} + \sqrt{7})$.
   (a) Show that $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
   (b) Determine $[K : \mathbb{Q}]$.
   (c) Find a polynomial $t(x) \in \mathbb{Q}[x]$ such that K is the splitting field for $t(x)$ over $\mathbb{Q}$.
   (d) Determine G up to isomorphism, providing clear and concise arguments to support your answer.
   (e) Question: Does G act transitively on the roots of $t(x)$? Explain.
   (f) The Fundamental Theorem of Galois Theory states in part that if K/F is there is an (order-reversing) bijection between the subgroups of $Aut(K/F)$ and the intermediate fields between F and K. In the example above, the group $Aut(K/\mathbb{Q})$ is small, and you can determine its subgroups. Use that information, and the theorem, to determine all intermediate fields between $\mathbb{Q}$ and K.

3. Let a, b be positive integers. Show that $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ contains $\sqrt{a - \sqrt{b}}$.

4. Suppose that $K/\mathbb{Q}$ is Galois, and $[K : \mathbb{Q}] = 4$. Is it possible that the only subfields of K are K and $\mathbb{Q}$? Explain.

5. Nice little problem: Suppose $K/\mathbb{Q}$ is the splitting field of a cubic polynomial $c(x) \in \mathbb{Q}[x]$. Prove that if $[K : \mathbb{Q}] = 3$, then $K \subseteq \mathbb{R}$.

6. This problem involves the polynomial $a(x) = x^4 - 2$.

   (a) Easy: Show that $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ is not Galois. (Show $Aut(mathbbQ(2^{1/4})/\mathbb{Q})$ is trivial group, and go from there. Explain things concisely and clearly.)

   (b) Easy: Show that $\mathbb{Q}(2^{1/2})/\mathbb{Q}$ is Galois.

   (c) Easy: Show $\mathbb{Q}(2^{1/4})/\mathbb{Q}(2^{1/2})$ is Galois.

   The point: E is Galois over F and D is Galois over E does not imply that D is Galois over F.

7. Determine the dimension of the splitting field S for $p(x) = x^5 - 3$ over $\mathbb{Q}$. Without explicitly determining $G = Aut(S/\mathbb{Q})$, do the following:

   (a) Explain why G has a unique subgroup N of order 5, and that N is normal in G. (Hints: Think Sylow subgroups, the Sylow Theorem.)

   (b) Since N is normal, the Fund. Thm of Galois Theory guarantees that (i.) the fixed field of N—which we'll call J—is Galois over $\mathbb{Q}$, and (ii.) $4 = [G : N] = [J : \mathbb{Q}]$. What must J be? (Hint: Think "roots of unity".)