Math 622 Q2 Prep: These will help a lot with your preparations on Test 2. I'll have extra hours this coming Weds afternoon. Let me know if you'd like to come by to ask questions about these problems, or other preparation on Quiz 2, and give me a time. Thanks.

1. Very important: Let $t(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Let S/F be a splitting field of $t(x)$. Show that $n! \geq [S : F]$. (Suggestion: Do it by induction on $deg(t(x))$.

2. Here are two major facts we've proved. I would expect you could prove each.

   (a) Let $t(x) \in F[x]$ be a polynomial, and let K/F be a splitting field of $t(x)$. Let $R = \{r_1, \ldots, r_k\}$ be the roots of $t(x)$—so $R \subseteq K$, and $K = F(r_1, \ldots, r_k)$. You've proven that $Aut(K/F)$ acts on R—-it maps elements of R to elements of R. You've proven also that that $Aut(K/F)$ acts **faithfully** on R—that is, if $\sigma \in Aut(K/F)$, and $\sigma(r) = r$ for all $r \in R$, then $\sigma = id_K$. That is, $Aut(K/F)$ can be embedded in S_R, the permutations of R.

   (b) In class, we proved that Proposition 5, page 562, which states (in part) that if K/F is a splitting field of a separable polynomial $t(x) \in F[x]$, then $|Aut(K/F)| = [K : F]$.

   Use the two facts above to prove the following:

   A. Give a two-line proof of this: Let K be the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. So $K = \mathbb{Q}(2^{1/3}, \omega)$, and $[K : \mathbb{Q}] = 6$. Show that $Aut(K/\mathbb{Q}) \cong S_3$.

   B. (This was an exercise in the last homework.) Let $n \in \mathbb{N}$, and let $\Phi_n(x)$ be the n-th cyclotomic polynomial. We've shown that $\Phi_n(x) \in \mathbb{Q}$ is irreducible and separable, and $deg(\Phi_n(x)) = \phi(n)$, the Euler number of n, and with $\psi = e^{2\pi i/n}$, a primitive n-th root of unity, we have $K = \mathbb{Q}(\psi)$ is the splitting field of $\Phi_n(x)$.

      i. Show that if $\sigma \in Aut(K/\mathbb{Q})$, then $\sigma(\psi) = \psi^k$, where $n > k \geq 1$, and $(n, k) = 1$. (Easy - use the "roots to roots" propery that we've proven.)

      ii. Show that $\sigma(\psi) = \psi^k$ completely determines σ. Notation: if $\sigma(\psi) = \psi^k$, let $\sigma := \sigma_k$.

      iii. Show that $Aut(K/\mathbb{Q})$ is Abelian.

      iv. Show that $Aut(K/\mathbb{Q}) \cong U_n$, where U_n is the group of units of $\mathbb{Z}_n$.

3. Two basic, somewhat boring, exercises follow. Be sure to try them:

   (a) $\{A_i : i \in I\}$ is a non-empty collection of fields such that for each $i \in I$, F is contained in A_i and A_i is contained in K. So $F \leq A_i \leq K$, for all $i \in I$.

   Prove that $\cap_{i \in I} A_i$ is a subfield of K, a subfield that contains F. (This is not difficult, but is a necessary exercise.)

   (b) Let F be a field contained in a larger field K. Let A and B be fields with $F \leq A \leq K$ and $F \leq B \leq K$. Use the exercise above to show show that there exists a least subfield in K that contains A and B. (Look at the set of all subfields of K that contain both A and B—that set is non-empty. Use the above exercise.) NOTATION: "AB" is the notation used for the least subfield containing A and B.

4. pg. 545: 6. This is an important (and not difficult) exercise. Be sure to do it.

5. pg. 545: 4.

6. pg. 530: 3, 4,5. These are basic, important exercise—everyone in the class should be able to do these. Give them a try.

7. pg. 530: 7. Nice exercise–basic, classic type of problem.

8. pg. 530: 14. Very nice classic exercise. I've seen this problem on Qualifying Exams, and in many textbooks.

9. pg. 530: 16: If K/F is an algebraic extension (of fields), and R is a *ring* contained in K and containing F. Then R is a field. (Comment: We've seen this kind of phenomenon—what is given as a ring turns out, surprisingly, to be a field. That K/F is algebraic is critical. Let $\gamma \in R - F$. It's algebraic. Consider the minimal polynomial $m_{\gamma,F}(x) \in F[x]$. Of course $B = \{t(\gamma) : t(x) \in F[x]\}$ is contained in the ring R. Now show that B is a field: If $\alpha \in B - \{0\}$, use gcd arguments to show α has an inverse in B.)

10. pg. 552: 8. Let p be a prime number. Use the following three facts to prove pg 552, number 8.

    (a) We've shown that if p is a prime and $p > m > 0$, then $p | \binom{p}{m}$.

(b) One consequence of the above is that if K is a field of characteristic p, then for all $a, b \in F$, we have $(a+b)^p = a^p + b^p$ (the "Freshman's Dream").

(c) We also known that if $u \in F_p$ (the field with p elements, also known as $\mathbb{Z}_p$), then $u^p = u$. (Be sure you can explain this—the multiplicative group on $F_p - \{0\}$ has $p-1$ elements. So if $u \in F_p - \{0\}$, $u^{p-1} = 1$ (by a corollary of Lagrange), so $u^p = u$; lastly, if $u = 0$, it's obvious $0^p = 0$.)

11. page 555, number 5. Not a bad little exercise.