Math 622 Test 1 prep.
To prepare for Test 2,

1. Go over all homework problems.
2. Review all the quiz 1 like problems.
3. Go over Quiz 1.
4. Do the problems below.

Test 1 prep probs.

1. Read the notes M622.Notesfor02.21.pdf through and including *Exercise 2*. (So be sure to do Exercise 1 and Exercise 2 in those notes.)

2. Suppose that L/K is a finite-dimensional extension of L over K with basis $\{l_1, \ldots, l_m\}$, and let K/F be a finite-dimensional extension of F with basis $\{k_1, \ldots, k_j\}$. Show that $\{l_p k_q : 1 \leq p \leq m, 1 \leq q \leq j\}$ spans K over F. (This is one-half of the proof of the Double-Extension Lemma which states that $[L : K][K : F] = [L : F]$. The other half is showing the above set is linearly-independent over F.)

3. Use the Double-Extension Lemma for vector spaces to show that if K/F is a field extension and $[K : F] = p$ where p is a prime number, then for any $b \in K - F$, $F(b) = K$.

4. Prove that if K/F is a finite dimensional field extension, then every element of K is algebraic over F.

5. This problem involves $p(x) = x^4 + x + 1$.

   (a) Show that $x^4 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible: (Suggestion: First show that $x^2 + x + 1 \in\in \mathbb{Z}_2[x]$ is the only irreducible degree polynomial in that ring, and then observe that $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1$.) Provide a concise, clear argument.

   (b) So $K := \mathbb{Z}_2[x]/(x^4 + x + 1)$ is a field with $2^4 = 16$ elements. Let $\theta := x + (x^4 + x + 1)$, a root of $x^4 + x + 1$. Use the Euclidean algorithm and back-tracking to find $(\theta^2 + 1)^{-1}$. Show the work. (That is to say, find $s(x), t(x)$ in $\mathbb{Z}_2[x]$ such that $s(x)(x^2 + 1) + t(x)(x^4 + x + 1) = 1$. Having done so, $s(\theta)$ is then the inverse of $\theta^2 + 1$. Test your conjectured $(\theta^2 + 1)^{-1}$.)

6. Complete the following definitions, or provide a proof (as the case may be). K/F is a field extension.

   (a) $b \in K$ is **algebraic** over F if

   (b) Suppose $b \in K$ is algebraic over F. The minimal polynomial $m_{b,F}(x)$ is the monic polynomial...

   (c) With $b \in K$ algebraic over F, show that $m_{b,F}(x)$ is irreducible.

   (d) Show that if $p(x) \in F[x]$, and $p(b) = 0$, then $m_{b,F}(x)|p(x)$.

   (e) Let L/K be a field extension. (K/F is still assumed to be a field extension of F. So L/F is a field extension of F.) Suppose $c \in L$ is algebraic over F.

      i. Explain in one sentence why c would also be algebraic over K.

      ii. Show that $m_{c,K}(x)|m_{c,F}(x)$. Give an example to show that it could be that $m_{c,K}(x) \neq m_{c,F}(x)$.

7. Let K be a field, and let $Aut(K)$ be the field automorphisms of K. Of course $Aut(K)$ is a group (with operation function composition). Suppose K/F is a field extension. Let $Aut_F(K) = \{\phi \in Aut(K) : \forall b \in F \ \phi(b) = b\}$. These aren't difficult, but good for the purposes of review, and it serves our purposes to help you become comfortable with $Aut_F(K)$.

   (a) Show that $Aut_F(K)$ is a subgroup of $Aut(K)$, the automorphisms of the field K.

   (b) Let $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Show if $\phi \in Aut_{\mathbb{Q}}(K)$, then $\phi(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$.

   (c) Show that there is an element $\phi \in Aut_{\mathbb{Q}}(K)$ such that $\phi(\sqrt{2}) = -\sqrt{2}$. Define ϕ. Then show that ϕ is unique; that is, there is only one automorphism in $Aut_{\mathbb{Q}}(K)$ that carries $\sqrt{2}$ to $-\sqrt{2}$.

   (d) Show that if $\phi \in Aut_{\mathbb{Q}}(K)$, then ϕ is completely determined by $\phi(\sqrt{2})$. Conclude that $Aut_{\mathbb{Q}}(K)$ is a two-element group.

   (e) (Just a bit harder) Let $J = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $H = Aut_{\mathbb{Q}}(J)$. Show that there exists no $\phi \in H$ such that $\phi(\sqrt{2}) = \sqrt{3}$.