Your exam is Monday May 2 in 6402 AP&M. The room is booked from 12pm-3pm. You get one hour and 50 minutes, so come either from 12-1:50pm or from 1-2:50pm. The exam covers Chapter 6, sections 6.1-6.6, and homeworks 1-4. Please bring a blue book.

Some of the problems on the exam will be similar in style to homework problems. I will also ask you to reproduce the proofs of a sample of key theorems we proved. These will be chosen from among the results I list below. (Note that you are not going to be asked to prove all of these on the test, just a few of them.) So you should study the results below, and also study homeworks 1-4.

1. Prove that if $K \subseteq F$ is a field extension and $u \in F$ is an algebraic element, then $K(u) \cong K[x]/\langle f(x) \rangle$ as rings, where $f(x)$ is the minimal polynomial of $u$ over $K$.

2. Prove Kronecker’s theorem: if $K$ is a field and $f(x) \in K[x]$, then there is a field extension $K \subseteq F$ such that $f(u) = 0$ for some $u \in F$.

3. Prove that if $K \subseteq F$ is a field extension, then the set $E = \{a \in F | a \text{ is algebraic over } K\}$ is a subfield of $F$.

4. Prove that if $K \subseteq E \subseteq F$ and $K \subseteq E$ and $E \subseteq F$ are algebraic extensions, then $K \subseteq F$ is an algebraic extension.

Date: April 27, 2016.
5. Recall the theorem that a real number \( u \) is constructible if and only if there is a sequence of real numbers \( u_1, \ldots, u_n \), such that \( u \in \mathbb{Q}(u_1, \ldots, u_n) \) with \( u_i^2 \in \mathbb{Q}(u_1, \ldots, u_{i-1}) \) for all \( 1 \leq i \leq n \) (when \( i = 1 \) this is interpreted as \( u_1^2 \in \mathbb{Q} \)).

Prove using this theorem that if \( u \) is a constructible number, then \([\mathbb{Q}(u) : \mathbb{Q}]\) is a power of 2.

6. Prove that if \( K \) is a field and \( f(x) \in K[x] \), then there exists a splitting field \( F \) for \( f(x) \) over \( K \).

7. Prove that if \( F \) is a field of characteristic \( p \) and \( n \geq 1 \), then \( E = \{ a \in F | a^{p^n} = a \} \) is a subfield of \( F \).

8. Prove that for any \( n \geq 1 \) and prime number \( p \), the splitting field of \( x^{p^n} - x \) over \( \mathbb{Z}_p \) is a field \( F \) with \( p^n \) elements, and that in fact \( F \) is precisely the set of roots of \( x^{p^n} - x \) in \( F \).

9. Prove that if \( F \) is a field with \( p^n \) elements, where \( p \) is prime, then \( F \) is the splitting field over its prime subfield \( \mathbb{Z}_p \) of the polynomial \( x^{p^n} - x \). Conclude that there is only one field with \( p^n \) elements up to isomorphism.