The second exam will be on Wednesday, March 24, 2010. The syllabus for Exam II is Chapter 6 Section 3–5 and Chapter 8 Sections 1 and 2. While the material in Sections 6.1 and 6.2 was on the last exam, it is worth pointing out that this material is central to all of Chapters 6 and 8. Some of the main examples and facts from this material (including Sections 6.1 and 6.2) are listed below. You should be sure to know precise definition of the terms we have used, and you should know precise statements (including all relevant hypotheses) for the main theorems proved.

- If $E$ is a field containing $F$ as a subfield, and $\alpha \in E$, then there is a substitution homomorphism $\phi_\alpha : F[x] \to E$ given by $\phi(p(X)) = p(\alpha)$.
- Know the definition of algebraic and transcendental elements over a field $F$.
- If $\alpha$ in a field $E$ containing $F$ as a subfield is algebraic over $F$, then the minimal polynomial $p(X)$ is the monic polynomial in $F[X]$ of smallest degree with $p(\alpha) = 0$.
- If $p(X)$ is the minimal polynomial of $\alpha$ and $f(X) \in F[X]$, then $f(\alpha) = 0$ if and only if $p(X)$ divides $f(X)$ in $F[X]$.
- If $p(X)$ is any polynomial in $F[X]$, know the concept of congruence modulo $p(X)$ and how to do arithmetic of congruence classes in the quotient ring $F[X]/\langle p(X) \rangle$. In particular, multiplication of congruence classes is described by $[f(X)][g(X)] = [r(X)]$ where $r(X)$ is the remainder upon division of $f(X)g(X)$ by $p(X)$.
- The units of $F[X]/\langle p(X) \rangle$ are the congruence classes $[f(X)]$ with $\gcd(f(X), p(X)) = 1$. When $[f(X)]$ is a unit, know how to use the Euclidean algorithm to find the inverse: Write $u(X)f(X) + g(X)p(X) = 1$. Then $[f(X)]^{-1} = [u(X)]$.
- $F[X]/\langle p(X) \rangle$ is a field if and only if $p(X)$ is irreducible over $F$.
- Kronecker’s Theorem: If $p(X)$ is irreducible over $F$, then $E = F[X]/\langle p(X) \rangle$ is a field containing $F$ as a subfield and $\theta = [X]$ is a root of $p(X)$ in $E$.
- Know the definition of the adjunction of elements $\theta_1, \theta_2, \ldots, \theta_k$ to a field $F$, and the description of the elements of $F(\theta_1, \ldots, \theta_k)$.
- If $p(X)$ is the minimal polynomial of an element $\theta$ which is algebraic over $F$, then
  $$F(\theta) = \{a_0 + a_1 \theta + \cdots + a_{n-1} \theta^{n-1} : a_0, \ldots, a_{n-1} \in F\}$$
  where $n$ is the degree of $p(X)$. Thus, every element of $F(\theta)$ can be represented as a polynomial in $\theta$ with coefficients in $F$ and of degree less than $n$. Moreover, this representation is unique. Hence $F(\theta)$ is a vector space over $F$ of dimension $n = \deg p(X)$.
- If $\theta$ is algebraic over $F$ with minimal polynomial $p(X)$, then $F(\theta)$ is isomorphic to the congruence ring $F[X]/\langle p(X) \rangle$.
- If $\theta_1$ and $\theta_2$ are roots of the same irreducible polynomial in $F[X]$, then $F(\theta_1)$ is isomorphic (over $F$) to $F(\theta_2)$. (See Lemma 6.4.3 Page 291)
- $[E : F] = \dim_F E$ = the dimension of $E$ as a vector space over $F$.
- $[F(u) : F] = \deg p(x)$, the degree of the minimal polynomial $p(X)$ of $u$ over $F$. 

---

Exam II Review Sheet

Math 4201
• If $E$ is a finite extension of $K$ and $F$ is a finite extension of $E$, then $F$ is a finite extension of $K$ and
\[ [F : K] = [F : E][E : K]. \]
(Tower Theorem, i.e., Theorem 6.2.5, Page 278.)

• A real number $\alpha$ is **constructible** if it is possible to construct a line segment of length $|\alpha|$ by using only a straightedge and compass.

• A real number $u$ is constructible if and only if $u$ is included in a subfield $F$ of $\mathbb{R}$ obtained from $\mathbb{Q}$ by successively adjoining square roots. (Theorem 6.3.6, Page 286.)

• If $u$ is a constructible real number, then $u$ is algebraic over $\mathbb{Q}$ and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2. (Corollary 6.3.7, Page 286.)

• $E$ is a **splitting field** for $f(X) \in F[X]$ if $E = F(\mu_1, \ldots, \mu_n)$ and
\[ f(X) = c(X - \mu_1) \cdots (X - \mu_n) \in E[X]. \]

• Every $f(X) \in F[X]$ has a splitting field $E$ and any two splitting fields $E$ and $E'$ are isomorphic over $F$, i.e., there is a field isomorphism $\sigma : E \to E'$ with $\sigma(a) = a$ for all $a \in F$. (Theorem 6.4.5, Page 293.)

• If $|F| < \infty$ then $|F| = p^n$ where $p$ is prime. The prime $p$ is also the characteristic of the field $F$.

• If $|F| = p^n$, then the map $\sigma : F \to F$ defined by $\sigma(a) = a^p$ is a field automorphism which fixes the subfield $\mathbb{Z}_p$.

• If $|F| = p^n$ then $F$ is the splitting field of $f(X) = X^{p^n} - X$ over $\mathbb{Z}_p$.

• Any two finite fields of the same order are isomorphic. The unique field of order $p^n$ is known as the **Galois Field of order** $p^n$ and is denoted $\text{GF}(p^n)$.

• $\text{GF}(p^m) \subseteq \text{GF}(p^n)$ if and only if $m$ divides $n$. Know how to use this fact to draw the lattice of subfields of a given finite field.

• Any finite subgroup of the multiplicative group of a field is cyclic. In particular, $F^*$ is a cyclic group if $|F| < \infty$. (Theorem 6.5.10, Page 298.)

• A finite field $K$ is a simple extension of any subfield $F$ (Theorem 6.5.11, Page 299).

• There is an irreducible polynomial of every degree $n$ over $\mathbb{Z}_p$. (Corollary 6.5.12, Page 300.)

• If $F$ is an extension field of a field $K$, then the Galois group of $F$ over $K$, denoted $\text{Gal}(F/K)$ is the group, under composition, of field automorphism of $F$ which fix $K$, i.e. $\sigma \in \text{Gal}(F/K)$ if $\sigma : F \to F$ is a field isomorphism and $\sigma(a) = a$ for all $a \in K$.

• The Galois group of a polynomial $f(X) \in K[X]$ is the Galois group of $E$ over $K$ where $E$ is a splitting field for $f(X)$ over $K$.

• If $F$ is an extension field of $K$, $f(X) \in K[X]$, $u \in F$, and $\sigma \in \text{Gal}(F/K)$, then $\sigma(f(u)) = f(\sigma(u))$. In particular, if $u$ is a root of $f(X)$, then $\sigma(u)$ is also a root.
As a consequence of the previous item, if $F$ is the splitting field of $f(X) \in K[X]$, then the Galois group of $F$ over $K$ is isomorphic to a subgroup of the group of permutations of the roots of $f(X)$. In particular, if $\deg f(X) = n$ then $\text{Gal}(F/K)$ is isomorphic to a subgroup of the symmetric group $S_n$. (Proposition 8.1.4, Page 367.)

Let $K$ be a field, let $f(x)$ be a polynomial of positive degree in $K[x]$, and let $F$ be a splitting field for $f(x)$ over $K$. If no irreducible factor of $f(x)$ has repeated roots in $F$, then $\lvert \text{Gal}(F/K) \rvert = \lceil F \rceil : K \rceil$.

(Theorem 8.1.6, Page 369.)

If $F$ is a finite field with $\text{char}(F) = p$, the map $\phi : F \to F$ defined by $\phi(x) = x^p$, for all $x \in F$, is an automorphism of $F$ called the Frobenius automorphism of $F$.

Let $K$ be a finite field with $\lvert K \rvert = p^r$, where $p = \text{char}(K)$. Let $F$ be an extension field of $K$ with $[F : K] = m$, and let $\phi$ be the Frobenius automorphism of $F$. The $\text{Gal}(F/K)$ is a cyclic group of order $m$, generated by $\phi^r$.

A polynomial $f(x) \in K[x]$ has no multiple roots if and only if $\gcd(f(x), f'(x)) = 1$.

A polynomial $f(x) \in K[x]$ is separable if its irreducible factors have only simple roots.

An algebraic extension $F$ of $K$ is called separable if the minimal polynomial of each element of $F$ is separable.

A field $F$ is called perfect if every polynomial over $F$ is separable.

Any field of characteristic 0 is perfect. A field of characteristic $p > 0$ is perfect if and only if each of its elements has a $p$-th root.

Any finite field is perfect. (Corollary 8.2.7, Page 374.)

If $F$ is a finite separable extension of $K$, then $F$ is a simple extension, i.e. $F = K(u)$ for some $u \in F$.

Review Exercises

Be sure that you know how to do all assigned homework exercises. The following are supplemental exercises similar to those already assigned as homework. These exercises are listed randomly. That is, there is no attempt to give the exercises in the order of presentation of material in the text, and there is no claim that a representative of every assigned exercise is included.

1. Show that the polynomial $X^3 + X + 1$ is irreducible over $\mathbb{Z}_2$. Then $E = \mathbb{Z}_2[X]/(X^3 + X + 1)$ is a field. Let $\alpha = [X]$ and let $\beta = \alpha + 1$. Find the irreducible polynomial of $\beta$ over $\mathbb{Z}_2$ and show that $\mathbb{Z}_2(\beta) = E$.

2. Show that $u = \sqrt[3]{5} - \sqrt{2}$ is constructible.

3. Suppose that $\alpha \in \mathbb{R}$ is a root of the polynomial $x^3 + 5x - 1$. Show that $\alpha$ is not constructible.

4. Find a monic polynomial in $\mathbb{R}[X]$ with $1 - i$ and $i$ as roots. Is there such a polynomial of degree 3?
5. Construct a field of order 25.

6. Let \( g(x) = x^4 - \sqrt{5}x^3 + \sqrt{2}x - 1 \) and let \( \beta \) be a complex number with \( g(\beta) = 0 \). Show that \( [\mathbb{Q}(\beta) : \mathbb{Q}] \leq 16 \).

7. Find the splitting field \( E \) of \( f(X) \) over \( \mathbb{Q} \) and the degree \( [E : \mathbb{Q}] \) for each of the following polynomials \( f(X) \in \mathbb{Q}[X] \).
   (a) \( f(X) = X^4 - 2 \)
   (b) \( f(X) = X^4 + X^2 + 1 \)
   (c) \( f(X) = X^6 - 4 \)

8. Find all of the subfields of the field \( GF(p^{20}) \) and give the inclusion relations among these subfields.

9. Let \( f(x) = x^3 + 5 \in \mathbb{Q}[x] \). Show that the splitting field of \( f(x) \) is \( F = \mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{5}) \) and compute \( [F : \mathbb{Q}] \).

10. Let \( f(x) = x^4 - 25 \in \mathbb{Q}[x] \).
    (a) Find the factorization of \( f(x) \) as a product of irreducible polynomials in \( \mathbb{Q}[x] \).
    (b) Find all the roots of \( f(x) \) in the complex numbers \( \mathbb{C} \).
    (c) Find the splitting field \( K \) of \( f(x) \) over \( \mathbb{Q} \).
    (d) Find \( [K : \mathbb{Q}] \). Justify your answer.

11. Let \( F = \mathbb{Z}_3 \) be the finite field with 3 elements and let \( f(x) = x^2 + x + 2 \in F[x] \). Let \( u \) be a root of \( f(x) \) in some extension field of \( F \) and let \( L = F(u) \).
    (a) Show that \( f(x) \) is irreducible in \( F[x] \).
    (b) How many elements does \( L \) have?
    (c) Write \( f(x) \) as a product of irreducible polynomials in \( L[x] \).
    (d) Is \( g(x) = x^2 + 2x + 2 \) irreducible in \( F[x] \)? Justify your answer.
    (e) Is \( g(x) = x^2 + 2x + 2 \) irreducible in \( L[x] \)? Justify your answer.

12. Let \( K \) be an extension field of a field \( F \) and let \( f(x) \in F[x] \) be a polynomial with coefficients in \( F \). Define each of the following terms:
    (a) An automorphism of \( K \) over \( F \).
    (b) The Galois group \( \text{Gal}(K/F) \) of \( K \) over \( F \).
    (c) The Galois group of the polynomial \( f(x) \).

13. Let \( w = \sqrt[4]{2} \) and \( K = \mathbb{Q}(w, i) \). Then \( K \) is a splitting field over \( \mathbb{Q} \) of the polynomial \( f(x) = x^4 - 2 \), since the roots of \( f(x) \) are \( w, -w, wi, \) and \( -wi \). Let \( G = \text{Gal}(K/\mathbb{Q}) \) be the Galois group of \( K \) over \( \mathbb{Q} \).
    (a) If \( \sigma \in G \) explain why \( \sigma(w) \in \{w, -w, wi, -wi\} \) and \( \sigma(i) \in \{i, -i\} \). Just quote the appropriate theorem.
    (b) How can you compute \( \sigma(i) \) if you know \( \sigma(w) = \alpha \) and \( \sigma(wi) = \beta \)? That is, give a formula for \( \sigma(i) \) in terms of \( \alpha \) and \( \beta \).
(c) As proved in class any $\sigma \in G$ determines a permutation of the set $\{w, -w, wi, -wi\}$ by the rule:

$$
\left( \begin{array}{cccc}
w & -w & wi & -wi \\
\sigma(w) & \sigma(-w) & \sigma(wi) & \sigma(-wi)
\end{array} \right).
$$

Show that the following permutation is not induced by any $\sigma \in G$:

$$
\left( \begin{array}{cccc}
w & -w & wi & -wi \\
wi & w & -wi & -w
\end{array} \right).
$$