The second exam will be on Friday, March 22, 2013. The syllabus for Exam II is Chapter 6 Section 1–5. 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 $\phi(p) = p(\alpha)$.
- Know the definition of algebraic and transcendental elements over a field F.
- If α in a field E containing F as a subfield is algebraic over F, then the *minimal polynomial* p is the monic polynomial in $F[x]$ of smallest degree with $p(\alpha) = 0$.
- If p is the minimal polynomial of α and $f \in F[x]$, then $f(\alpha) = 0$ if and only if p divides f in $F[x]$.
- If p is any polynomial in $F[x]$, know the concept of congruence modulo p and how to do arithmetic of congruence classes in the quotient ring $F[x]/\langle p\rangle$. In particular, multiplication of congruence classes is described by $[f][g] = [r]$ where r is the remainder upon division of fg by p.
- The units of $F[x]/\langle p\rangle$ are the congruence classes $[f]$ with $\gcd(f, p) = 1$. When $[f]$ is a unit, know how to use the Euclidean algorithm to find the inverse: Write $uf + gp = 1$. Then $[f]^{-1} = [u]$.
- $F[x]/\langle p\rangle$ is a field if and only if p is irreducible over F.
- *Kroneckers Theorem:* If p is irreducible over F, then $E = F[x]/\langle p\rangle$ is a field containing F as a subfield and $\theta = [x]$ is a root of p 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 is the minimal polynomial of an element θ which is algebraic over F, then

  $$F(\theta) = \left\{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} : a_1, \ldots, a_{n-1} \in F\right\}$$

  where n is the degree of p. Thus, every element of $F(\theta)$ can be represented as a polynomial in θ 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 $n = \deg p$.
- If θ is algebraic over F with minimal polynomial p, then $F(\theta)$ is isomorphic to the congruence class ring $F[x]/\langle p\rangle$.
- If θ_1 and θ_2 are roots of the same irreducible polynomial in $F[x]$, then $F(\theta_1)$ is isomorphic (over F) to $F(\theta_2)$.
- $[E : F] = \dim_F E =$ the dimension of E as a vector space over F.
- $[F(u) : F] = \deg p$, the degree of the minimal polynomial p of u over F.
- 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 or Multiplication Theorem, i.e., Theorem 5, Page 287.)

- E is a *splitting field* for $f \in F[x]$ if $E = F(\theta_1, \ldots, \theta_n)$ and

$$f = c(x - \theta_1) \cdots (x - \theta_n) \in E[x].$$

- Every $f \in F[x]$ 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 4, Page 294.)
- 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 $f = x^{p^n} - x$ 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 $\mathrm{GF}(p^n)$.
- $\mathrm{GF}(p^m) \subseteq \mathrm{GF}(p^n)$ if and only if m divides n. Know how to use this fact to draw the lattice of subfields of a give 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 7, Page 302.)
- Know the definition and existence of primitive elements of $\mathrm{GF}(p^n)$.
- A finite field K is a simple extension of any subfield F (Corollary 1, Page 302).
- There is an irreducible polynomial of every degree n over $\mathbb{Z}_p$. (Corollary 2, Page 303.)

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 $x^2 + x + 1$ is the only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$.
2. Let $\beta = 1 + \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$. Find expressions for β^2, β^3, and β^{-1} in terms of the standard basis 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2 = \sqrt[3]{4}$ for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.
3. Show that the polynomial $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$. Then $E = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ is a field. Let $t = x + \langle x^3 + x + 1\rangle$ and let $\beta = t + 1$. Find the irreducible polynomial of β over $\mathbb{Z}_2$ and show that $\mathbb{Z}_2(\beta) = E$.
4. Let $a = 2^{\frac{1}{p}}$ where p is prime. Prove that $[\mathbb{Q}(a) : \mathbb{Q}] = p$ and that $\mathbb{Q}(a)$ has only two subfields (the obvious ones).
5. Let a be a root of $x^6 - 4x + 2 \in \mathbb{Q}[x]$. Prove that $\mathbb{Q}(a) : \mathbb{Q}] = 6$.
6. Let $a = \sqrt{3} - \sqrt[3]{2}$. Show that $[\mathbb{Q}(a) : \mathbb{Q}] = 6$ and find the minimal polynomial of a over $\mathbb{Q}$.

7. Compute [GF(729) : GF(9)] and [GF(64) : GF(8)].

8. Construct a field of order 25.

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

10. Find the splitting field E of f over $\mathbb{Q}$ and the degree $[E : \mathbb{Q}]$ for each of the following polynomials $f \in \mathbb{Q}[x]$.

    (a) $f = x^4 - 2$

    (b) $f = x^4 + x^2 + 1$

    (c) $f = x^6 - 4$

11. Find the splitting field for $x^4 - x^2 - 2$ over $\mathbb{Z}_3$.

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

13. Let $f = x^4 - 25 \in \mathbb{Q}[x]$.

    (a) Find the factorization of f as a product of irreducible polynomials in $\mathbb{Q}[x]$.

    (b) Find all the roots of f in the complex numbers $\mathbb{C}$.

    (c) Find the splitting field K of f over $\mathbb{Q}$.

    (d) Find $[K : \mathbb{Q}]$. Justify your answer.

14. Let $F = \mathbb{Z}_3$ be the finite field with 3 elements and let $f = x^2 + x + 2 \in F[x]$. Let u be a root of f in some extension field of F and let $L = F(u)$.

    (a) Show that f is irreducible in $F[x]$.

    (b) How many elements does L have?

    (c) Write f as a product of irreducible polynomials in $L[x]$.

    (d) Is $g = x^2 + 2x + 2$ irreducible in $F[x]$? Justify your answer.

    (e) Is $g = x^2 + 2x + 2$ irreducible in $L[x]$? Justify your answer.

15. Show that $x^{21} + 2x^8 + 1$ does not have multiple roots in any extension of $\mathbb{Z}_3$.

16. Show that $x^{21} + 2x^9 + 1$ has multiple roots in some extension of $\mathbb{Z}_3$.

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

18. Find elements of order 3, 5, and 15 in the multiplicative group of GF(16).

19. If g is irreducible over $\mathrm{GF}(p)$ and g divides $x^{p^n} - x$, prove that $\deg g$ divides n.