

Math 547, Exam 3 Information.

4/16/10, LC 303B, 10:10 - 11:00.

Exam 3 will be based on:

Homework and textbook sections covered by lectures 3/15 - 4/12.
(see <http://www.math.sc.edu/~boylan/SCCourses/547Sp10/547.html>)

At minimum, you need to understand how to do the homework problems.

Topic List (not necessarily comprehensive):

You will need to know: theorems, results, and definitions from class.

1. Root multiplicities and the formal derivative.

Definition. Let F be a field, let $c \in F$, and let $f(x) \in F[x]$. Then c is a root of multiplicity $m \geq 1$ if and only if $(x - c)^m \mid f(x)$, but $(x - c)^{m+1} \nmid f(x)$.

(a) c is a simple root if and only if $m = 1$.

(b) c is a multiple root if and only if $m > 1$.

Definition. Let F be a field. The formal derivative of $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ is

$$f'(x) = \sum_{i=1}^n n a_i x^{i-1} \in F[x].$$

Remark. The formal derivative satisfies all the familiar rules from basic calculus.

Theorem. Let F be a field, let $f(x) \in F[x]$, and let $c \in F$. Then c is a multiple root if and only if $f(c) = 0$ and $f'(c) = 0$.

Theorem. Let F be a field, and let $f(x) \in F[x]$ be non-constant. Then we have $\gcd(f(x), f'(x)) = 1$ if and only if $f(x)$ has no multiple roots in F .

Theorem. Let F be a field, let $f(x) \in F[x]$ be non-constant, and suppose that $\gcd(f(x), f'(x)) \neq 1$. Then $f(x)$ has an irreducible factor of multiplicity ≥ 2 .

2. Polynomial rings in several variables.

Proposition. Let R be a commutative ring, and let x_1, \dots, x_n be indeterminates.

(a) If R is an integral domain, then so is $R[x_1, \dots, x_n]$. The units in $R[x_1, \dots, x_n]$ are R^\times .

(b) If R is a UFD, then $R[x_1, \dots, x_n]$ is a UFD.

(c) If R is an integral domain, but not a field, then $R[x_1, \dots, x_n]$ is not a PID.

(d) If R is a field, then $R[x_1, \dots, x_n]$ is a PID if and only if $n = 1$, in which case $R[x_1]$ is actually Euclidean.

3. Basic facts on fields.

Definition. Let $F \subseteq K$ be fields. Then we have

- (a) An element $u \in F$ is algebraic over K if and only if there exists $f(x) \neq 0$ in $K[x]$ with $f(u) = 0$.
- (b) An element $u \in F$ is transcendental over K if and only if no $f(x) \neq 0$ in $K[x]$ exists with $f(u) = 0$.

Definition. Let K be a field, and let x be an indeterminate. Then the field of rational functions in x over K is

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

Definition. Let $F \supseteq K$ and let $u \in F$. Then the extension field of K generated by u (or the extension field of K obtained by adjoining u) is $K(u)$, the smallest subfield of F containing both K and u . (We read: “ K adjoin u ”.)

Theorem. Let $F \supseteq K$ be fields, let x be an indeterminate, and let $u \in F$ be transcendental over K . Then we have $K(u) \cong K(x)$.

Definition. Let $F \supseteq K$ be fields, and let $u \in F$ be algebraic over K . Then $f(x)$ is the minimal polynomial of u over K if and only if $f(x)$ is the unique monic irreducible polynomial in $K[x]$ which has u as a root. (Such a polynomial exists and is unique, and we denote it by $f_u(x)$ or by $f_{K,u}(x)$).

Proposition. Let $F \supseteq K$ be fields, let $u \in F$ be algebraic over K , and let $f(x) \in K[x]$. The following statements are equivalent.

- (a) The polynomial $f(x)$ is the minimal polynomial of u over K . (I.e., it is a monic irreducible in $K[x]$ which has u as a root.)
- (b) The polynomial $f(x)$ is the monic polynomial of least degree in $K[x]$ which has u as a root.
- (c) The polynomial $f(x)$ has the property that if $g(x) \in K[x]$ satisfies $g(u) = 0$, then $f(x) \mid g(x)$.
- (d) The polynomial $f(x)$ is the monic generator for the kernel of the evaluation homomorphism $\phi_u : K[x] \rightarrow F$. I.e., we have $\ker \phi_u = (f(x))$.

Proposition. Let $F \supseteq K$ be fields. Then F is a K -vector space (a vector space over K).

Definition. Let $F \supseteq K$ be fields.

- (a) The degree of F over K is $[F : K] = \dim_K F$.
- (b) Let $u \in F$ be algebraic over K . Then the degree of u over K is $[K(u) : K] = \dim_K K(u)$.

Theorem. Let $F \supseteq K$ be fields, and let $u \in F$ be algebraic over K with minimal polynomial $f_{K,u}(x)$ of degree n . Then we have

$$(a) \quad K(u) = \{a_{n-1}u^{n-1} + \cdots + a_1u + a_0 : a_i \in K\}.$$

(b) $\frac{K[x]}{(f_{K,u}(x))} \cong K(u).$

(c) $K(u)$ is a K -vector space of dimension $[K(u) : K] = \deg(f_{K,u}(x)) = n$ with basis $\{1, u, \dots, u^{n-1}\}.$

Theorem. Suppose that $F \supseteq E \supseteq K.$ Then we have $[F : K] = [F : E] \cdot [E : K].$

Corollary. Let $F \supseteq K$ be fields, let $u \in F,$ and suppose that $[F : K]$ is finite. Then

- (a) The element u is algebraic.
- (b) $\deg f_{K,u}(x) = [K(u) : K] \mid [F : K].$

Corollary. Let $F \supseteq K$ be fields, and let $u_1, \dots, u_n \in F$ be algebraic over $K.$ Then we have

$$[K(u_1, \dots, u_n) : K] \leq [K(u_n) : K] \cdots [K(u_1) : K].$$

Corollary. Let $F \supseteq K.$ Then the set of all elements in F algebraic over K form a field.

Definition. Let $F \supseteq K$ be fields. Then F is an algebraic extension of K (or F is algebraic over K) if and only if every $u \in F$ is algebraic over $K.$

Proposition. Let $F \supseteq K.$

- (a) An element $u \in F$ is algebraic over K if and only if $[K(u) : K]$ is finite.
- (b) Suppose that $[F : K]$ is finite. Then F is algebraic over $K.$

Remark. The converse of part (b) of the proposition is false:

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

is an algebraic extension over \mathbb{Q} of infinite degree.

Theorem. Let $F \supseteq E \supseteq K,$ and suppose that F is algebraic over E and that E is algebraic over $K.$ Then F is algebraic over $K.$ I.e., algebraicity is transitive in towers of fields.

4. Splitting fields.

Definition. Let K be a field, and let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ have $\deg(f(x)) = n.$ Then a field $F \supseteq K$ is a splitting field for $f(x)$ over K if and only if there exists $r_1, \dots, r_n \in F$ such that

- (a) $f(x) = a_n(x - r_1) \cdots (x - r_n).$ (We say that $f(x)$ splits over $F.$)
- (b) $F = K(r_1, \dots, r_n).$

Example. Suppose that $d \in \mathbb{Z}$ is square-free. Then a splitting field of $x^2 - d$ over \mathbb{Q} is $\mathbb{Q}(\sqrt{d}).$

Example. A splitting field of $x^3 - 2$ over \mathbb{Q} is $\mathbb{Q}(\zeta_3, \sqrt[3]{2}),$ and $[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}] = 6.$

Example. Let p be prime. A splitting field of $x^p - 1$ over \mathbb{Q} is $\mathbb{Q}(\zeta_p = e^{\frac{2\pi i}{p}}).$

Theorem (Kronecker). Let K be a field, and let $f(x) \in K[x]$ be non-constant. Then there exists a field $F \supseteq K$ and an element $u \in F$ for which $f(u) = 0.$ I.e., every polynomial in $K[x]$ has a root in some extension of $K.$

Theorem. Let K be a field, and let $f(x) \in K[x]$ have $\deg(f(x)) = n \geq 1$. Then there exists a splitting field $F \supseteq K$ for $f(x)$ over K , and $[F : K] \leq n!$. I.e., splitting fields exist.

Theorem. Let K be a field, and let $f(x) \in K[x]$ have $\deg(f(x)) = n \geq 1$. Suppose that $F, E \supseteq K$ are splitting fields for $f(x)$ over K . Then there exists an isomorphism $\phi : F \rightarrow E$ such that $\forall k \in K$, we have $\phi(k) = k$. I.e., a splitting field for $f(x)$ over K is unique up to an isomorphism which fixes K .

5. Introduction to Galois Theory.

Definition. Let $F \supseteq K$ be fields. Then $\phi : F \rightarrow F$ is a K -automorphism if and only if

- (a) ϕ is an automorphism of F .
- (b) ϕ fixes K pointwise: for all $k \in K$, we have $\phi(k) = k$.

Proposition. Let $F \supseteq K$ be fields. The set of all K -automorphisms of F is a subgroup of the set of all automorphisms of F .

Definition. Let $F \supseteq K$ be fields.

- (a) The Galois group of F over K is $\text{Gal}(F/K) = \{\phi : \phi \text{ is a } K\text{-automorphism of } F\}$.
- (b) Let $f(x) \in K[x]$, and suppose that F is a splitting field of $f(x)$ over K . Then the Galois group of $f(x)$ over K is $\text{Gal}(F/K)$.

Proposition. Let $F \supseteq K$ be fields, let $f(x) \in K[x]$, and let $\sigma \in \text{Gal}(F/K)$. Then we have

- (a) Let $v \in F$. Then $\sigma(f(v)) = f(\sigma(v))$.
- (b) Let $u \in F$ be a root of $f(x)$. Then $\sigma(u)$ is also a root of $f(x)$.
- (c) The K -automorphism σ permutes the roots of $f(x)$ which lie in F .

Proposition. Let $F \supseteq K$ be fields, and let $u \in F$ be algebraic. Then $\sigma \in \text{Gal}(K(u)/K)$ is completely determined by $\sigma(u)$.

Corollary. Let $F \supseteq K$, and let $u \in F$ be algebraic with $[K(u) : K] = \deg(f_{K,u}(x)) = n$. Suppose that $f_{K,u}(x)$ has $m \leq n$ distinct roots in $K(u)$. Then we have $|\text{Gal}(K(u)/K)| \leq m \leq n$.

Example. $\text{Gal}(\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}) = \langle 1 \rangle$; but the Galois group of $x^3 - 7$ over \mathbb{Q} is $\text{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{7})/\mathbb{Q}) \cong S_3$.

Example. Let $d \in \mathbb{Z}$ be square-free. Then we have $\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle \sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d} \rangle \cong \mathbb{Z}_2$.

Example. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then we have $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ with generators $(1, \sigma)$ and $(\tau, 1)$, where $\sigma : \sqrt{3} \mapsto -\sqrt{3}$ and $\tau : \sqrt{5} \mapsto -\sqrt{5}$.

Example. Let $m \geq 3$ in \mathbb{Z} . Then we have $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathbb{Z}_m^\times$.