Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
Review sheet for final

Definitions:

- Let E/F be a field extension. We say $\alpha \in E$ is *algebraic* over F if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. We say $\alpha \in E$ is *transcendental* over F if α is not algebraic over F.
- Let E/F be a field extension and let $\alpha \in E$ be algebraic over F. The following are the two equivalent definitions of the minimum polynomial that I gave in class:
  - The *minimum polynomial* of α over F is the monic polynomial of smallest degree in $F[x]$ which has α as a zero.
  - The *minimum polynomial* of α over F is the monic generator of the ideal:

  $$I = \{f(x) \in F[x] \ : \ f(\alpha) = 0\}.$$

  We write $\mathrm{irr}(\alpha, F)$ for this polynomial.
- Let E/F be a field extension and let $\alpha \in E$. The *degree* of α over F is the degree of the minimum polynomial of α.
- A set of vectors $\{v_1, \ldots, v_n\}$ in a vector space V are *linearly independent* if whenever

  $$c_1 v_1 + \cdots + c_n v_n = 0$$

  for scalars $c_1, \ldots, c_n$, then $c_i = 0$ for all i.
- A *basis* of a vector space V is a set of vectors that are linearly independent and span V.
- An extension of fields E/F is an *algebraic extension* if every $\alpha \in E$ is algebraic over F.
- An extension of fields E/F is a *finite extension* if E is finite-dimensional as an F-vector space.
- The *degree* of a finite extension E/F of fields is the dimension of E as an F-vector space. We write this degree as $[E : F]$.
- A field F is *algebraically closed* if every non-constant polynomial $f(x) \in F[x]$ has a zero in F.
- For a field K, an *automorphism of* K is an isomorphism of K with itself, that is, a bijective ring homomorphism $\varphi : K \to K$.
- For K/F a field extension and $\varphi : K \to K$ an automophism, we say that φ fixes F is for every $\alpha \in F$, we have that $\varphi(\alpha) = \alpha$.
- A field E is an *algebraic closure* of a field F if (1) E/F is an algebraic extension and (2) E is algebraically closed.
- Let $\{f_i\}$ be a collection of polynomials in $F[x]$. Then the *splitting field* of the $\{f_i\}$ over F is the smallest subfield of $\overline{F}$ which contains F and every root of each f_i.
- Let $f(x) \in F[x]$. Then α is a zero of *multiplicity* e if $f(x) = (x - \alpha)^e g(x)$ with $g(\alpha) \neq 0$.
- Let K and L be fields. We say that $\sigma : K \to L$ is an *embedding* if σ is a non-zero ring homomorphism.
- Let K and L be fields each containing a subfield F. We say that $\sigma : K \to L$ is an *embedding over* F if σ is a non-zero ring homomorphism which fixes F (i.e. $\sigma(x) = x$ for all $x \in F$).
- An algebraic extension K/F is *normal* if any of the equivalent definitions hold: (you pick which one you want to answer with!)

1. K is a splitting field over F;
2. if $\tau : K \to \overline{F}$ is an embedding over F, then $\tau(K) \subseteq K$;
3. whenever $p(x)$ is a polynomial in $F[x]$ which has a zero in K, then $p(x)$ splits into linear factors in $K[x]$.

- An algebraic extension K/F is *separable* if for every $\alpha \in K$, we have $\operatorname{irr}(\alpha, F)$ has no multiple roots.
- A finite extension K/F is *Galois* if it is both normal and separable.

Theorems:

- Let E/F be an extension of fields and let $\alpha \in E$ be algebraic over F. Then the minimum polynomial $\text{irr}(\alpha, F)$ is irreducible.

  Proof: Assume $\text{irr}(\alpha, F) = f(x)g(x)$. Since α is a zero of $\text{irr}(\alpha, F)$, we have that $f(\alpha)g(\alpha) = 0$ and thus either $f(\alpha) = 0$ and $g(\alpha) = 0$. Without loss of generality, let's assume that $f(\alpha) = 0$. Then, by the definition of minimum polynomial, we have $\deg(f) \geq \deg(\text{irr}(\alpha, F))$. But this implies that $g(x)$ is a constant and hence $\text{irr}(\alpha, F)$ is irreducible.

- $F(\alpha) \cong F[x]/\langle \text{irr}(\alpha, F) \rangle$.

  Proof: Consider the ring homomorphism:

  $$\begin{aligned} \varphi : F[x] &\longrightarrow F(\alpha) \\ f(x) &\mapsto f(\alpha). \end{aligned}$$

  The kernel of this map equals

  $$\{f(x) \in F[x] \ : \ f(\alpha) = 0\}$$

  which by definition of minimum polynomial is simply $\langle \text{irr}(\alpha, F) \rangle$. Thus by the first isomorphism theorem (Theorem 26.17), we have an injective map

  $$\overline{\varphi} : F[x]/\langle \text{irr}(\alpha, F) \rangle \longrightarrow F(\alpha)$$

  which sends $x + \langle \text{irr}(\alpha, F) \rangle$ to α. Our job is to show that this map is surjective.

  So take any element $\beta \in F(\alpha)$. By definition of $F(\alpha)$, we know that

  $$\beta = \frac{a_0 + a_1\alpha + \dots a_n\alpha^n}{b_0 + b_1\alpha + \dots b_m\alpha^m}$$

  for $a_i, b_i \in F$ with non-zero denominator.

  Since $\text{irr}(\alpha, F)$ is irreducible, we know that $\langle \text{irr}(\alpha, F) \rangle$ is a maximal ideal and thus $F[x]/\langle \text{irr}(\alpha, F) \rangle$ is a field. Thus, we can form the element

  $$(a_0 + a_1x + \dots a_nx^n + \langle \text{irr}(\alpha, F) \rangle) \cdot (b_0 + b_1\alpha + \dots b_m\alpha^m + \langle \text{irr}(\alpha, F) \rangle)^{-1}$$

  in $F[x]/\langle \text{irr}(\alpha, F) \rangle$ and this element clearly maps to β under $\overline{\varphi}$. Hence φ is surjective and thus an isomorphism as desired.

- If E/F is a finite extension, then E/F is an algebraic extension.

  Proof: Let $\alpha \in E$ and consider $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ where $n = [E : F]$ which is finite by assumption. Since these are $n + 1$ elements of E which is an n-dimension vector space, we must have that these elements are linearly dependent. Thus, there exists $c_0, \dots, c_n \in F$ with at least 1 non-zero such that

  $$c_0 + c_1\alpha + \dots c_n\alpha^n = 0.$$

  Hence $c_0 + c_1x + \dots + c_nx^n$ is a non-zero polynomial in $F[x]$ with α as a zero. This proves that α is algebraic over F and thus E/F is an algebraic extension.

- Let $K/\mathbb{Q}$ be a field extension and φ an automorphism of K. Then φ fixes $\mathbb{Q}$.

  Proof: First note that $\varphi(1) = 1$ (as φ is surjective; Lemma from class). Then for $n \geq 0$, we have

  $$\begin{aligned} \varphi(n) &= \varphi(1 + \dots + 1) \quad \text{(n times)} \\ &= \varphi(1) + \dots + \varphi(1) \quad \text{(n times)} \\ &= 1 + \dots + 1 \quad \text{(n times)} \\ &= n. \end{aligned}$$

  Then for $n < 0$, we have $\varphi(n) = -\varphi(-n) = -(-n) = n$ as $-n > 0$. Thus, $\varphi(n) = n$ for all $n \in \mathbb{Z}$. Lastly, for any $r/s \in \mathbb{Q}$, we have $\varphi(r/s) = \varphi(r)/\varphi(s) = r/s$ as desired.

- Let K/F be an algebraic extension and let φ be an automorphism of K that fixes F. Then for every $\alpha \in K$, we have that $\varphi(\alpha)$ is a zero of $\operatorname{irr}(\alpha, F)$.

  Proof: Set
  $$\operatorname{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
  with each $a_i \in F$. Since α is a root of its own minimum polynomial, we have
  $$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$
  Applying φ to this equation gives
  $$\begin{aligned} 0 = \varphi(0) &= \varphi(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0) \\ &= \varphi(\alpha)^n + \varphi(a_{n-1})\varphi(\alpha)^{n-1} + \cdots + \varphi(a_1)\varphi(\alpha) + \varphi(a_0) \\ &= \varphi(\alpha)^n + a_{n-1}\varphi(\alpha)^{n-1} + \cdots + a_1\varphi(\alpha) + a_0. \end{aligned}$$
  Here we are using both the ring homomorphism properties of φ and the fact that φ fixes F. This last equation proves that $\varphi(\alpha)$ is a root of $\operatorname{irr}(\alpha, F)$ as desired.

- Let F be a field of characteristic 0. Let $f(x) \in F[x]$ and let α be a zero of $f(x)$ of multiplicity e. Then α is a zero of $f'(x)$ with multiplicity $e - 1$.

  Proof: Since $f(x) = (x - \alpha)^e g(x)$ with $g(\alpha) \neq 0$, differentiating gives
  $$f'(x) = e(x-\alpha)^{e-1}g(x) + (x-\alpha)^e g'(x) = (x-\alpha)^{e-1} \cdot (eg(x) + (x-\alpha)g'(x)).$$
  Note that setting $x = \alpha$ in $eg(x) + (x-\alpha)g'(x)$ gives $eg(\alpha) + (\alpha - \alpha)g'(\alpha) = eg(\alpha)$. By assumption $g(\alpha) \neq 0$ and since F has characteristic 0, $e \neq 0$. Thus $eg(x) + (x-\alpha)g'(x)$ does not vanish at α and hence α is a zero of $f'(x)$ with multiplicity $e - 1$.

- Let K be a splitting field over F. Then if $\tau : K \to \overline{F}$ is an embedding fixing F, we have $\tau(K) \subseteq K$.

  Proof: Let K be the splitting field of $\{f_j\}$ with each $f_j \in F[x]$. Set R equal to the collection of all zeroes of all of the f_j in $\overline{F}$. Then $K = F(\{\alpha\}_{\alpha \in R})$. To show that $\tau(K) \subseteq K$ we thus only need to check that $\tau(\alpha) \in K$ for each $\alpha \in R$ as τ fixes F. To this end, take α in R and write f_j for the polynomial in our collection for which α is a root. Then $\tau(\alpha)$ is again a zero of f_j as $f_j \in F[x]$ and τ fixes F. Hence $\tau(\alpha) \in R$ which implies $\tau(\alpha) \in K$. Thus $\tau(K) \subseteq K$.

- If $L/K/F$ is a tower of fields and L/F is separable, then L/K and K/F are separable.

  Proof: We first check that L/K is separable. To this end, let $\alpha \in L$ and we must check that $\operatorname{irr}(\alpha, K)$ has no repeated roots. But we know that
  $$\operatorname{irr}(\alpha, K) \text{ divides } \operatorname{irr}(\alpha, F)$$
  as $\operatorname{irr}(\alpha, F)$ has α as a root and has coefficients in K (and $\operatorname{irr}(\alpha, K)$ divides every polynomial in $K[x]$ which has α as a root). Since $\operatorname{irr}(\alpha, F)$ has no repeated roots, we deduce that $\operatorname{irr}(\alpha, K)$ has no repeated roots. Hence L/K is separable.

  Now we check K/F is separable. To this end, let $\alpha \in K$ and we must check that $\operatorname{irr}(\alpha, F)$ has no multiple roots. But since $K \subseteq L$ and L/F is separable, we deduce that $\operatorname{irr}(\alpha, F)$ has no multiple roots as desired. Thus, K/F is separable.

- Let K/F be Galois and let E be a subfield. Then $E = K^{\operatorname{Gal}(K/E)}$.

  Proof: See Theorem 2.4 in Galois theory notes.