MATH 250A LECTURE RECAPS (FIELDS)

PATRICK OARE

Let L/K be a field extension unless otherwise specified.

1. 10/31 (Field Extensions, Algebraic Closure)

- **Fields**: A **field** is a commutative division ring. We say that L/K, or $K \leq L$, is a **field extension** if K is a subfield of L. The **degree** of a field extension is denoted:

$$[L : K]$$

  and is the dimension of L as a K-vector space. An extension L/K is **finite** if $[L : K]$ is finite.
- **Algebraic Extensions**: An element $\alpha \in L$ is called **algebraic** over K if it is the root of a nontrivial polynomial over K, i.e. if $\exists p(x) \in K[X] \setminus \{0\}$ with $p(\alpha) = 0$. L/K is called an **algebraic** extension if every element in L is algebraic over K. Every finite extension is algebraic, as if $\alpha \in L/K$ is in a finite extension, $\{1, \alpha, \alpha^2, ...\}$ is K-linearly dependent and terminates, giving a nontrivial relation among the powers of α with coefficients in K.
- **Tower Law**: Let L/K and K/F be field extensions. Then:

$$[L : F] = [L : K][K : F]$$

  Take bases $\{u_i\}_{i=1}^n$ and $\{v_j\}_{j=1}^m$ of L over K and of K over F. Then $\{u_i v_j\}_{i,j=1,1}^{n,m}$ is a basis of L as an F-vector space.
- **Splitting Fields**: Given a polynomial in $f \in K[X]$, we can construct a field extension L/K such that p has a root in L. Indeed, if $p|f$ is an irreducible polynomial, then $L := K[X]/(p)$ is a field as irreducible elements generate maximal ideals, and $p(x)$ has a root in L, namely $x \mod (p)$. If $p \in K[X]$, we call L a **splitting field** of p if:
  (1) p splits into linear factors over L.
  (2) L is generated over K by the roots of p.

  To construct the splitting field L of p, we keep extending K with more roots of p until we have all of them. If $deg(p) = n$, then $[L : K] \leq n!$ (I believe it actually divides $n!$). **The splitting field L is unique** up to an isomorphism fixing K.
- **Finite Fields**: The finite field $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. For each prime power p^n, there is a unique finite field $\mathbb{F}_{p^n}$, which we may construct as the splitting field of $x^{p^n} - x$ over $F_p[x]$. The derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = -1$, which is coprime to $x^{p^n} - x$, and so the polynomial is separable and has p^n roots. The roots

are closed under $+, -, \cdot$ and division, and so form a field of order p^n. It is unique, as it is the splitting field of the polynomial.

- **Algebraic Closure**: We call L the **algebraic closure** of K if:
  (1) Any element of L is algebraic over K.
  (2) Any polynomial in $L[X]$ has a root in L.

  Any field K is contained in an algebraic closure L. Furthermore, L is unique up to isomorphism.

2. 11/7 (Normal, Separable, Galois Extensions)

- **Normal Extensions**: An algebraic extension L/K is **normal** if whenever an irreducible polynomial $p \in K[X]$ has a root in L, it splits into linear factors in $L[X]$.

  For an algebraic extension L/K, TFAE:
  (1) L/K is normal.
  (2) L is the splitting field of a family of polynomials in $K[X]$.

Proof. Suppose ii, and that $p \in K[X]$ is irreducible and has a root in $\alpha \in L$. Let M be the algebraic closure of L. We may extend any homomorphism $\phi : K(\alpha) \to M$ to a homomorphism $\psi : L \to M$ because M is algebraically closed. But, we have $im(\psi) = L$ because L is the uniquely determined splitting field of a family of polynomials, and this implies $\alpha \in L$ (this part makes no sense). □

For example, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, as it is the splitting field of $x^2 - 2$. But, $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ is not normal; $x^3 - 2$ has one root in the field, but the other roots are not in the field.

- **Separable Extensions**: A polynomial is called **separable** if it has no multiple roots, i.e. p and p' are coprime. If L/K is a field extension, an element $\alpha \in L$ is **separable** if its minimal polynomial over K is separable. An extension is called separable if every element is separable over the base field.

Theorem 2.1. If $char(K) = 0$, then L/K is a separable extension.

This follows because if $p(x)$ is the minimal polynomial of α over K, then because $deg(p') < deg(p) \implies$ these can have no common factors since p is irreducible unless $p' = 0$, and $p' = 0 \implies p$ is constant and has no multiple roots. If $char(p) \neq 0$, then the derivative of p can be 0 while p is not constant, so this proof only holds in $char$ 0.

Furthermore, **any extension $\mathbb{F}_q/\mathbb{F}_p$ of finite fields is separable**. This follows because if $q = p^n$, any element x of $\mathbb{F}_q$ satisfies $x^q - x = 0$, and this has derivative -1 and so is separable.

Ex of a non-separable extension: Take t transcendental over $\mathbb{F}_p$. Then the extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is degree p as the minimal poly of t over $\mathbb{F}_p(t^p)$ is $x^p - t^p$. However, this polynomial factors over $\mathbb{F}_p(t)$ as $(x-t)^p$, so this polynomial is not separable and this is not a separable extension.

- **Extending field homomorphisms**:

  Lemma 2.2. Suppose L/K is a field extension of degree n. Then if M/K is any field extension, there are at most n ways to define a field homomorphism $L \to M$ which fixes K.

  Proof. Let σ be such a homomorphism. Suppose first that $L = K(\alpha)$. Then α is a root of some $f \in K[X]$ of degree $\leq n$, and so σ must map α to another root of f as it fixes K, so as σ is completely determined by its action on α, we have $\leq n$ possibilities for σ. Now, suppose $L = K(\alpha_1, ..., \alpha_n)$. The tower of primitive extensions $K \leq K(\alpha_1) \leq ... \leq K(\alpha_1, \alpha_n) = L$ has number of extensions of each previous map $\leq$ its degree, and so if we combine them, we reproduce the tower law and have $\leq [L : K]$ ways to define σ.

  $\square$

  Lemma 2.3. Let L/K be an algebraic extension, and let $f : K \to \Omega$ be a homomorphism into an algebraically closed field Ω. Then, we may extend f to a homomorphism $F : L \to \Omega$ with $F|_K = f$.

  Check out this link for a proof of this: https://math.stackexchange.com/questions/897660/extending homomorphism-into-algebraically-closed-field