Lecture Notes for Math 627B
Modern Algebra
Groups, Fields, and Galois Theory

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
www-rohan.sdsu.edu/ ˜ mosulliv

April 21, 2012

10 Field Extensions: Algebraic and Transcendental

Definition 10.1. Field subfield extension field

Observation that if $F \leq K$ then K is a vector space over F. $[K : F]$ is the dimension.

Proposition 10.2 (Dimension)**.** $[K : E][E : F] = [K : F]$

Proof. □

Intersection of fields is a field. Intersection of rings is a ring.

Definition 10.3. $F[\alpha]$, the intersection of all rings containing F and α. $F(\alpha)$ as intersection of all fields containing F and α. $F[S]$ and $F(S)$

Proposition 10.4. *$F[\alpha]$ is all polynomials in α. $F(\alpha)$ is all rational polynomials in α*

Proof. □

Proposition 10.5. *The universal property of $F[x]$.*

Proof. □

Definition 10.6. algebraic, transcendental, minimum polynomial

Corollary 10.7. *If K contains some transcendental element then $[K : F]$ is infinite.*

Proof. □

Corollary 10.8. *For β algebraic $F[x]/m_\beta(x) \cong F[\beta] = F(\beta)$*

Proof. □

Use $F[\beta]$ to emphasize polynomials, even though it is a field.

Proposition 10.9. *Let $F \leq D \leq E$ and $\beta \in E$. Let $m(x)$ be the min poly of β over F and $p(x) \in D[x]$ the min poly over D. Then $p(x) \mid m(x)$.*

Proof. □

Proposition 10.10. *If $[E : F] = n$ then each $\beta \in E$ is algebraic of some degree d dividing n.*

Proof. □

How to find the minimum polynomial.

Proposition 10.11 (Transitivity of algebraic extensions)**.** *If $F \leq D$ and $D \leq E$ are both algebraic extensions then so is $F \leq E$. Conversely if $F \leq E$ is algebraic, so are the extensions $F \leq D$ and $D \leq E$.*

Proof. □

11 Splitting Fields

Definition 11.1. $f(x)$ splits over F.

Adjoining a root.

Example 11.2. $x^3 - 3x + 1$. Factor, after adjoining a root.

Example 11.3. $x^3 - 2$. Factor, after adjoining a root. Factor the remaining irreducible factor.

Subtle issue: suppose $F \cong \tilde{F}$ with irreducible $f(x)$ corresponding to $\tilde{f}(x)$. Then $F[x]/f(x) \cong \tilde{F}[x]/\tilde{f}(x)$. So if α is a root of $f(x)$ in $E \geq F$, $\tilde{\alpha}$ a root of $\tilde{f}(x)$ in $\tilde{E} \geq \tilde{F}$ $F[\alpha] \cong \tilde{F}[\tilde{\alpha}]$.

Definition 11.4. Splitting field of a polynomial.

Theorem 11.5 (Splitting Field)**.**

Proof. □

Corollary 11.6. *The splitting field for $f(x) \in F[x]$ of degree n has dimension at most $n!$ over F.*

Proof. □

Example 11.7. Splitting field of $x^3 - 2$.

Compare with cubic formula.

12 Algebraic Closure

Proposition 12.1. *For a field C the following are equivalent.*

(1) Each $f(x) \in C[x]$ has a root.

(2) Each $f(x) \in C[x]$ splits in $C[x]$

(3) *Each irreducible* $f(x) \in C[x]$ *is linear.*

(4) C *has no proper algebraic extensions.*

Proof. □

Definition 12.2. A field satisfying the properties of the proposition is called *algebraically closed*

Theorem 12.3 (Algebraic Closure)**.** *Existence and uniqueness.*

Proof. □

We will show that the complex field $\mathbb{C}$ is algebraically closed in Theorem **??**.

13 Separable Extensions

A polynomial $f(x) \in \mathbb{Q}[x]$ has repeated roots iff $\gcd(f, f') = 1$.

Proof. □

Extend to arbitrary fields.

Definition 13.1. An irreducible polynomial $f(x)$ of degree d in $F[x]$ that has d distinct roots in its splitting field is called *separable*. An arbitrary polynomial is separable when each of its irreducible factors is.

Definition 13.2. Derivative of f

Example 13.3. Over finite field.

Proposition 13.4 (Properties of the derivative)**.**

Proof. □

The repeated roots theorem is valid for any field.

Theorem 13.5. *A polynomial* $f(x) \in F[x]$ *has repeated roots iff* $\gcd(f, f') = 1$.

Proposition 13.6. *For* $f(x)$ *irreducible:* $f(x)$ *is separable iff* $f' \neq 0$.

Proof. □

Corollary 13.7. *Every polynomial over a field of characteristic 0 is separable.*

Proof. □

Corollary 13.8. *Every polynomial in $\mathbb{F}_q[x]$ is separable.*

Proof. $\square$

Definition 13.9. separable extension, perfect,

The classic example of an inseparable polynomial.

Example 13.10.

Discussion: Suppose that $\varphi : F \longrightarrow E$ is an embedding of F into C, the algebraic closure of E. Then there is an extension of φ to an embedding of E into C. In particular for $E = F[\alpha]$ we may (and must!) take α to a root of $m_\alpha(x)$, the minimal polynomial of α in $F[x]$.

Theorem 13.11. *Let E/F be an extension of dimension n and let C be an algebraic closure of F. There are at most n distinct embeddings of E into C and there are exactly n embeddings iff E is separable over F.*

Proof. $\square$

14 Normal Field Extensions

Definition 14.1. A field extension $F \leq E$ satisfying the equivalent conditions in the following theorem is called *normal*.

Theorem 14.2 (Normal)**.** *Let $F \leq E \leq C$ be field extensions with E algebraic over F and C the algebraic closure of E. The following are equivalent.*

(1) Each irreducible $m(x) \in F[x]$ that has a root in E splits in E.

(2) E is the splitting field of some set of polynomials.

(3) Every embedding of E into C that fixes F has image E, and is therefore an automorphism of E.

Proof. We prove the theorem just for the case where $[E : F]$ is finite. The infinite dimensional case requires some modification of this proof, esentially reducing to the case of a finite dimensional extension.

(3) $\Longrightarrow$ (1). Let $m(x)$ be an irreducible in $F[x]$ having a root α in E. Let $\beta \in C$ be another root of $m(x)$; we will show $\beta \in E$. Since β is arbitrary, $m(x)$ splits in E.

We know $F[\alpha] \cong F[\beta]$, because both are isomorphic to $F[x]/m(x)$. Since E is an algebraic extension of F this isomorphism extends to an embedding of E in

C. By assumption, the image is E, so in particular $\beta \in E$. (This proof works for infinite extensions.)

(1) $\Longrightarrow$ (2). Let $\alpha_1, \dots \alpha_r$ be such that $E = F[\alpha_1, \dots, \alpha_r]$. (Here we use finiteness.) Let $m_i(x)$ be the minimal polynomial of α_i over F. By assumption, $m_i(x)$ splits in E, so E contains the splitting field of $m(x) = \prod_{i=1}^{r} m_i(x)$. On the other hand the splitting field of $m(x)$ contains all the α_i, so it contains the field generated by them, $F[\alpha_1, \dots, \alpha_r] = E$. Thus E is the splitting field of $m(x)$. (Thus in the finite dimensional case, E is the splitting field of a single polynomial.)

(2) $\Longrightarrow$ (3) (Assuming finite). Suppose that E is the splitting field of $m(x)$, and let $\alpha_1, \dots, \alpha_r$ be the roots of $m(x)$. Let $\tau : E \longrightarrow C$ be an embedding of E into C that fixes F. We have seen that τ must take roots of $m(x)$ to roots of $m(x)$. The roots generate E, so $\tau(E) \subseteq E$. Since τ is an isomorphism onto its image the dimension of $\tau(E)$ over F is equal to $[E : F]$. Thus $\tau(E) = E$. □

Corollary 14.3. *Let $[E : F] = n$. E/F is normal and separable over F iff $|\mathrm{Aut}(E/F)| = n$*

Proof. $\Longrightarrow$ By separability, there are exactly n embeddings of E into C fixing F. By normality, these must all be automorphisms of E. Thus $|\mathrm{Aut}(E/F)| = n$.

$\Longleftarrow$ By the the theorem on separability, there are at most n embeddings of E into C that fix F, and the number of embeddings is n iff E is separable over F. Consequently, if $|\mathrm{Aut}(E/F)| = n$, then E must be separable and the automorphisms of E fixing F account for all the embeddings of E into C fixing F. Thus E is normal. □

Definition 14.4. When E is normal and separable over F, the extension E/F is called *Galois*. In this case, it is common to call the automorphism group $\mathrm{Aut}(E/F)$ the *Galois group* and write $\mathrm{Gal}(E/F)$. (Some authors use $\mathrm{Gal}(E/F)$ for arbitrary algebraic extensions.)

Recall that we showed that for separable extensions we have transitivity. In fact, for $F \leq D \leq E$, E/F is separable iff each of E/D and D/F is separable. Neither implication is true for normality, but we do have the following weaker property.

Proposition 14.5. *If E/F is normal then E/D is normal for any $F \leq D \leq E$.*

Proof. Suppose E/F is normal. By the normality theorem, there is some set of polynomials, $P \subseteq F[x]$, for which E is the smallest field containing F in the polynomials in P all split. Since $P \subseteq D[x]$, E is the also the smallest field containing D in which the polynomials in P split. So E is normal over D. □

Here is an immediate consequence.

Corollary 14.6. *Let E/F be Galois. Then E is Galois over any intermediate extension.*

15 Galois main theorem

Let E/F be an algebraic field extension and let $G = \mathrm{Aut}(E/F)$. We now consider the relationship between subfields of E containing F and subgroups of G. Define the *fixed field* functor $\mathcal{F}$ and the *fixing group* functor $\mathcal{G}$ by

$$\mathcal{F}(H) = \{x \in E : \sigma(x) = x \,\forall\, \sigma \in H\}$$
$$\mathcal{G}(D) = \{\sigma \in G : \sigma(x) = x \,\forall\, x \in D\}$$

Please verify that for D a field with $F \leq D \leq E$, $\mathcal{G}(D)$, which we call the fixing group of D, is a subgroup of G (it is closed under the operation of composition and taking inverses). Similarly, $\mathcal{F}(H)$, which we call the fixed field of H, is indeed a field (closure for both addition and multiplication, and both additive and multiplicative inversion). The following proposition characterizes these functors and their relationship to each other.

Theorem 15.1. *Let E/F be an algebraic extension and $\mathcal{F}$ and $\mathcal{G}$ the operations defined above.*

(1) $\mathcal{G}$ and $\mathcal{F}$ are inclusion reversing.

(2) $\mathcal{F}\mathcal{G}$ and $\mathcal{G}\mathcal{F}$ are increasing.

(3) $\mathcal{F}\mathcal{G}\mathcal{F} = \mathcal{F}$ and $\mathcal{G}\mathcal{F}\mathcal{G} = \mathcal{G}$.

Proof. Let $F \leq D \leq D' \leq E$. Any $\sigma \in \mathcal{G}(D')$ fixes everything in D', so it must fix each element of D. Thus $\mathcal{G}(D) \geq \mathcal{G}(D')$. Similarly one shows that for $H \leq H' \leq G$, $\mathcal{F}(H) \geq \mathcal{F}(H')$.

Next we want to show that $\mathcal{F}\mathcal{G}(D) \geq D$. This is clear: since everything in $\mathcal{G}(D)$ fixes D, the fixed field of $\mathcal{G}(D)$ contains D. The analogous result for $\mathcal{G}\mathcal{F}$ is similar.

Applying $\mathcal{G}$ to the result of the previous paragraph, and using item (1), $\mathcal{G}(\mathcal{F}\mathcal{G}(D)) \leq \mathcal{G}(D)$. On the other hand, since $\mathcal{G}\mathcal{F}$ is increasing, when it is applied to $\mathcal{G}(D)$ we get $\mathcal{G}\mathcal{F}(\mathcal{G}(D)) \geq \mathcal{G}(D)$. Thus $\mathcal{G}\mathcal{F}\mathcal{G} = \mathcal{G}$, and by analogous argument $\mathcal{F}\mathcal{G}\mathcal{F} = \mathcal{F}$. $\square$

The most useful approach to studying the relationship between subfields and subgroups of field automorphisms is to restrict to Galois extensions. In fact, this is not a restrictive restriction. If one wants to study the arbitrary extension E/F, one can first tease apart E/F into a separable part E_s/F and purely inseparable part E_i/F. The purely inseparable part has a trivial automorphism group and $\mathrm{Aut}(E/F) \cong \mathrm{Aut}(E_s/F)$. Thus we reduce to separable extensions. Now, assuming E/F is separable, one can form the normal closure E' of E and get information about $\mathrm{Aut}(E/F)$ from $\mathrm{Aut}(E'/F)$. The details may be found in many standard graduate algebra texts.

We will focus on E/F Galois, but first, here is the key result used in establishing the main theorem of Galois theory. I found this proof in Lang's *Algebra* and he atributes it to Artin.

Proposition 15.2. *Let E be any field and let G be a subgroup of* $\mathrm{Aut}(E)$. *Let* $F = \{x \in E : \sigma(x) = x \,\forall\, \sigma \in G\}$.

(1) E/F *is Galois.*

(2) $\mathrm{Gal}(E/F) = G$.

(3) $[E : F] = |\mathrm{Gal}(E/F)| = |G|$.

Proof. Let $\alpha \in E$ and let $m(x)$ be the minimal polynomial for α. We will show $m(x)$ factors completely over E with distinct roots. Since α is arbitrary, E/F is Galois.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be the orbit of α under G, so each $\alpha_i \in E$. Let $\sigma_i \in G$ be such that $\sigma_i(\alpha) = \alpha_i$. Each $\sigma \in G$ fixes F, so $\sigma(m(x)) = m(x)$. (Here we are implicitly extending σ to an automorphism of $E[x]$ by applying σ to each coefficient.) Furthermore, we have

$$0 = \sigma(m(\alpha)) = m(\sigma(\alpha))$$

so each α_i is a root of $m(x)$. Consequently, $\prod_{i=1}^r (x - \alpha_i)$ divides $m(x)$.

On the other hand, each $\sigma \in G$ permutes the α_i: because $\sigma(\alpha_i) = \sigma(\sigma_i(\alpha)) \in \mathrm{orb}(\alpha) = \{\alpha_1, \ldots, \alpha_r\}$. (Of course $\sigma(\alpha_i) = \sigma(\alpha_j)$ is only true for $i = j$ since σ is injective.) Now we have

$$\sigma\Big(\prod_{i=1}^r (x - \alpha_i)\Big) = \prod_{i=1}^r \sigma(x - \alpha_i) = \prod_{i=1}^r (x - \sigma(\alpha_i)) = \prod_{i=1}^r (x - \alpha_i)$$

This shows that $\prod_{i=1}^r (x-\alpha_i)$ is fixed under σ for all $\sigma \in G$ and therefore $\prod_{i=1}^r (x-\alpha_i) \in F[x]$. Since $m(x)$ is the minimal polynomial of α it must divide $\prod_{i=1}^r (x-\alpha_i)$. This shows that $m(x) = \prod_{i=1}^r (x - \alpha_i)$ and therefore $m(x)$ has distinct roots and that it splits over E.

Since E/F is separable, the primitive element theorem says that $E = F[\alpha]$ for some α. For this α, and the notation of the previous paragraph,

$$[E : F] = \deg m_\alpha(x) = \deg \prod_{i=1}^r (x - \alpha_i) \le |G|$$

On the other hand, since E/F is separable, $[E : F] = |\mathrm{Gal}(E/F)| \leq G$. The latter inequality is because each $\sigma \in G$ is, by assumption, an automorphism of E and it fixes F by definition of F. Thus we must have $[E : F] = |G|$ and $G = \mathrm{Gal}(E/F)$. $\square$

Now we come to the climax of the theoretical work in this course.

Theorem 15.3 (Galois)**.** *Let E/F be a Galois extension and set $G = \mathrm{Gal}(E/F)$. Let $\mathcal{F}$ and $\mathcal{G}$ be the fixed field and fixing group functors for this extension.*

(1) $\mathcal{F}$ and $\mathcal{G}$ are inverses of each other.

(2) For $H \leq G$, $[E : \mathcal{F}(H)] = |H|$, or equivalently, $[\mathcal{F}(H) : F] = [G : H]$.

(3) $\mathcal{F}$ and $\mathcal{G}$ respect conjugation. For $\sigma \in G$, and $H \leq G$,

$$\mathcal{F}(\sigma H \sigma^{-1}) = \sigma \mathcal{F}(H)$$

(4) $\mathcal{F}$ and $\mathcal{G}$ respect normality in the following sense:

$$H \text{ is normal in } G \iff \mathcal{F}(H)/F \text{ is a normal extension}$$

Furthermore, if H is normal, $\mathrm{Gal}(\mathcal{F}(H)/F) \cong G/H$.

For items (2)-(4) in the proof, I've expressed the result using $\mathcal{F}$. As a quick exercise, find the corresponding result for $\mathcal{G}$, and obtain it directly from the result for $\mathcal{F}$ using item (1).

Proof. Let $H \leq G$. By the proposition, $E/\mathcal{F}(H)$ is Galois, $\mathrm{Gal}(E/\mathcal{F}(H)) = H$, and $[E : \mathcal{F}(H)] = |H|$. This shows that $\mathcal{G}\mathcal{F}$ is the identity. It also establishes item (2). We derive $[\mathcal{F}(H) : F] = [G : H]$ from

$$[E : \mathcal{F}(H)][\mathcal{F}(H) : F] = [E : F] = |G| = |H|[G : H]$$

Now let $F \leq D \leq E$. By Corollary 14.6, E is Galois over both D and $\mathcal{F}(\mathcal{G}(D))$ and by the proposition,

$$[E : D] = |\mathrm{Gal}(E/D)| = |\mathcal{G}(D)|$$
$$[E : \mathcal{F}\mathcal{G}(D)] = |\mathrm{Gal}(E/\mathcal{F}\mathcal{G}(D))| = |\mathcal{G}\mathcal{F}\mathcal{G}(D)|$$

Since $\mathcal{G}\mathcal{F}\mathcal{G} = \mathcal{G}$ and $D \leq \mathcal{F}\mathcal{G}(D)$, we get $D = \mathcal{F}\mathcal{G}(D)$. Thus $\mathcal{F}$ and $\mathcal{G}$ are inverses of each other.

Now we consider conjugation by $\sigma \in G$. Let $H \leq G$ and let θ be an arbitrary element of H. An element of $\sigma\mathcal{F}(H)$ may be written $\sigma(x)$ with $x \in \mathcal{F}(H)$. We have

$$\sigma\theta\sigma^{-1}(\sigma(x)) = \sigma(x) \in \mathcal{F}(H)$$

So $\sigma\mathcal{F}(H) \subseteq \mathcal{F}(\sigma H\sigma^{-1})$. Applying this result again we have

$$\mathcal{F}(\sigma H\sigma^{-1}) = \sigma(\sigma^{-1}\mathcal{F}(\sigma H\sigma^{-1})) = \sigma(\mathcal{F}(\sigma^{-1}\sigma H\sigma^{-1}\sigma)) = \sigma\mathcal{F}(H)$$

This establishes item (3).

If H is normal, item (3) gives $\sigma\mathcal{F}(H) = \mathcal{F}(H)$ for all $\sigma \in G$. Any embedding of $\mathcal{F}(H)$ into the algebraic closure of E that fixes F can be extended to E. Since E/F is normal, the only embedddings of E fixing F are automorphisms of F. Consequently, the only embeddings of $\mathcal{F}(H)$ are restrictions of elements of G to $\mathcal{F}(H)$. We have just shown that these all have image $\mathcal{F}(H)$, so $\mathcal{F}(H)$ must be normal.

Conversely, if $\mathcal{F}(H)/F$ is normal, then every embedding of $\mathcal{F}(H)$ into its algebraic closure has image $\mathcal{F}(H)$. Thus for any $\sigma \in G$, $\mathcal{F}(\sigma H\sigma^{-1}) = \sigma\mathcal{F}(H) = \mathcal{F}(H)$. Now apply $\mathcal{G}$, to get $\sigma H\sigma^{-1} = H$.

For any field $D \leq E$ we get a homomorphism $G \longrightarrow \mathrm{Aut}(D/F)$ just by restricting the domain of $\sigma \in G$ to D. For the field $\mathcal{F}(H)$ with H normal the previous result shows that H is in the kernel of $G \longrightarrow \mathrm{Aut}(\mathcal{F}(H)/F) = \mathrm{Gal}(\mathcal{F}(H)/F)$. By the factor theorem we have $G/H \longrightarrow \mathrm{Gal}(\mathcal{F}(H)/F)$. By item (2), and Proposition 15.2,

$$|\mathrm{Gal}(\mathcal{F}(H)/F)| = [\mathcal{F}(H) : F] = [G : H] = |G/H|$$

so in fact $G/H \cong \mathrm{Gal}(\mathcal{F}(H)/F)$.

□