

Field and Galois Theory

Lectures by Uzi Vishne

Summary by Ari Feiglin (ari.feiglin@gmail.com)

Contents

1	Field Extensions and Minimal Polynomials	1
1.1	Dimensions of Field Extensions	1
1.2	Constructing Fields	1
1.3	Splitting Fields	4

1 Field Extensions and Minimal Polynomials

1.1 Dimensions of Field Extensions

1.1.1 Definition

Suppose F and K are fields such that $F \subseteq K$. Then the pair is called a **field extension** and is denoted K/F .

Notice that if K/F is a field extension, then K can be viewed as a F -linear space, and thus has a dimension. We denote this dimension $[K : F] := \dim_F K$, this is unsurprisingly called the *dimension* (or *degree* of the extension. An extension is called *finite* if its dimension is finite. Immediately we can prove a useful theorem about dimensions of extensions:

1.1.2 Theorem

Suppose K/F is a field extension and V a K -vector space. Then by viewing V as an F -linear space:

$$\dim_F V = \dim_K V \cdot [K : F]$$

Proof: let B_1 be a basis for V relative to K and B_2 be a basis for K relative to F . Then define $B = \{\alpha v \mid \alpha \in B_2, v \in B_1\} \subseteq V$, which we claim is a basis for V relative to F . Firstly, it is linearly independent: suppose $\alpha_1 v_1, \dots, \alpha_n v_n$ are in B and β_1, \dots, β_n are in F such that

$$\beta_1 \alpha_1 v_1 + \dots + \beta_n \alpha_n v_n = 0$$

Since B_1 is a basis for V , then $\beta_i \alpha_i = 0$ for all i , and since B_2 is a basis it has no zeroes, so $\beta_i = 0$ for all i , meaning B is linearly independent.

B spans V since if $v \in B$ then $v = \sum_{i=1}^n \alpha_i v_i$ for $v_i \in B_1$ and $\alpha_i \in K$, and so each α_i can be written as the linear combination of elements in B_2 . So all in all v can be written as the linear combination of elements in B . And so B is a basis of V , and $(\alpha, v) \mapsto \alpha v$ is a bijection from $B_1 \times B_2$ to B : it obviously is surjective and if $\alpha_1 v_1 = \alpha_2 v_2$ then $\alpha_1 = \alpha_2$ and $v_1 = v_2$ since B_1 is linearly independent. Thus V is a basis of cardinality $|B_1 \times B_2| = \dim_K V \cdot [K : F]$ as required. ■

In particular if $E/K/F$ are field extensions then

$$[E : F] = [E : K] \cdot [K : F]$$

this is called the *multiplicity of dimension*.

1.2 Constructing Fields

Recall the following methods of constructing fields:

- (1) If R is a commutative ring and $M \triangleleft R$ is a maximal ideal that R/M is a field. In particular if F is a field, $R = F[x]$, and p is an irreducible polynomial then (p) is maximal and so $F[x]/(p)$ is a field.
- (2) If F is a field, so is the field of rational functions:

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

- (3) If C is a chain of fields (meaning that for every $F, F' \in C$ either $F \subseteq F'$ or $F' \subseteq F$), then $\bigcup_{F \in C} F$ is also a field (the theory of fields is *inductive*). So for example $F(\lambda_1, \lambda_2, \dots)$ is a field, the union of the chain $F_n = F(\lambda_1, \dots, \lambda_n)$, the field of rational functions over F_{n-1} .
- (4) If C is a chain of fields, then $\bigcap_{F \in C} F$ is also a field.

1.2.1 Definition

Let K/F be a field extension and $a \in K$, then denote $F(a)$ the smallest subfield of K containing both F and a .

It is not hard to see that

$$F(a) = \left\{ \frac{f(a)}{g(a)} \mid f, g \in F[x], g(a) \neq 0 \right\}$$

Though we can actually get a simpler structure for $F(a)$.

1.2.2 Definition

Let K/F be a field extension with $a \in K$, then define the **evaluation homomorphism** at a to be the homomorphism $\psi_a: F[x] \rightarrow K$ defined by $\psi_a(s) = s$ for $s \in F$ and $\psi_a(x) = a$. This uniquely defines

$$\psi_a\left(\sum \alpha_i x^i\right) = \sum \alpha_i a^i$$

1.2.3 Definition

Let K/F be a field extension, then $a \in K$ is **transcendental** if the kernel of the evaluation homomorphism is trivial: $\ker \psi_a = 1$. Otherwise a is **algebraic**.

If a is transcendental then $\ker \psi_a = 1$ and so by the isomorphism theorem

$$\text{Im} \psi_a = \{f(a) \mid f \in F[x]\} = F[a] \cong F[x] / \ker \psi_a \cong F[x]$$

In fact we can extend ψ_a to a homomorphism $F(x) \rightarrow F(a)$, and we similarly get an isomorphism $F(x) \cong F(a)$. Thus in the case that a is transcendental, we get

$$\begin{array}{ccccc} F & \subseteq & F[a] & \subseteq & F(a) \subseteq K \\ & & \cong & & \cong \\ & & F[x] & & F(x) \end{array}$$

Otherwise, suppose a is algebraic. Since $F[x]$ is a Euclidean domain, it is a PID, and therefore every ideal is a prime ideal. In particular $\ker \psi_a$ must be generated by some polynomial h_a . This means that $\ker \psi_a = (h_a) = h \cdot F[x]$, and so $h_a(a) = 0$ and if $f(a) = 0$ as well then h_a divides f . h_a is therefore called the *minimal polynomial* of a .

Now if $n = \deg h$ then $F[a] = \text{span}\{1, a, \dots, a^{n-1}\}$ since if $f \in F[x]$ then $f = h_a q + r$ for $\deg r < n$ by Euclidean division, and so $f(a) = r(a)$. And $r(x)$ is in $\text{span}\{1, \dots, a^{n-1}\}$ due to its dimension being at most $n - 1$. Thus $\{1, \dots, a^{n-1}\}$ spans $F[a]$, and it is a basis since any linear combination cannot be zero as $h_a(x)$ is minimal and has degree n . Therefore $F[a]$ is a F -linear space of dimension n .

Notice that

$$F[x] / (h_a) = F[x] / \ker \psi_a \cong \text{Im} \psi_a = \{f(a) \mid f \in F[x]\} = F[a] = \text{span}\{1, \dots, a^{n-1}\} \subseteq K$$

Since K is an integral domain, so is $F[a]$. Therefore (h_a) is a prime ideal, since a quotient ring is an integral domain iff the ideal is prime. Since $F[x]$ is a PID, prime and maximal ideals are the same, so (h_a) is maximal and therefore $F[a]$ is a field.

So we have proven

1.2.4 Proposition

Let K/F be a field extension and $a \in K$ algebraic in F . Let h_a be a 's minimal polynomial over F , then

- (1) h_a is irreducible,
- (2) $F[a]$ is a field,
- (3) $[F[a] : F] = n = \deg h_a$ and has a basis $\{1, a, \dots, a^{n-1}\}$.

In particular we have shown that when a is algebraic, $F(a) = F[a]$.

1.2.5 Proposition

Suppose $F \subseteq K$ where F is a field and K is an integral domain. Further suppose $[K : F]$ is finite. Then every element of K is algebraic and K is a field.

Proof: let $a \in K$, then

$$[K : F] = [K : F[a]] \cdot [F[a] : F]$$

meaning $[F[a] : F]$ must be finite and so a must be algebraic (as otherwise $F[a] \cong F[x]$ which has infinite degree). Since $F[a]$ is a field, it must have a multiplicative inverse for a , meaning K is a field. ■

Notice that $[F[a, b] : F[a]] \leq [F[b] : F]$, since the minimal polynomial of b relative to F , h_b , is also a zeroing a polynomial of b over $F[a]$. And so $[F[a, b] : F[a]] \leq \deg h_b = [F[b] : F]$. Thus we have that by multiplicity

$$[F[a, b] : F] = [F[a, b] : F[a]] \cdot [F[a] : F] \leq [F[b] : F] \cdot [F[a] : F]$$

And inductively we can show

1.2.6 Proposition

Suppose K/F is a field extension and a_1, \dots, a_n then

$$[F[a_1, \dots, a_n] : F] \leq \prod_{i=1}^n [F[a_i] : F]$$

1.2.7 Definition

Call a field extension K/F **algebraic** if every $a \in K$ is algebraic over F .

1.2.8 Lemma

Suppose $F_3/F_2/F_1$ are field extensions such that F_2/F_1 is algebraic and $a \in F_3$ is algebraic over F_2 . Then it is also algebraic over F_1 .

Proof: there exists an $f \in F_2[x]$ such that $f(a) = 0$. Suppose $f = \sum b_i x^i$, then a is algebraic over $F_1[b_0, \dots, b_n]$. Then

$$[F_1[b_0, \dots, b_n, a] : F_1] = [F_1[b_0, \dots, b_n, a] : F_1[b_0, \dots, b_n]] \cdot [F_1[b_0, \dots, b_n] : F_1]$$

and since a is algebraic over $F_1[b_0, \dots, b_n]$ and $b_i \in F_2$ are algebraic over F_1 , the right-hand side is finite. Thus a is algebraic over F_1 by the left-hand side, as required. ■

1.2.9 Theorem

Let K/F be a field extension, then

$$\text{Alg}_F(K) := \{a \in K \mid a \text{ is algebraic over } F\}$$

is a field. Furthermore, every element in $K \setminus \text{Alg}_F(K)$ is transcendental over $\text{Alg}_F(K)$.

Proof: notice that $F[a \cdot b], F[a + b] \subseteq F[a, b]$ and $[F[a, b] : F] \leq [F[a] : F] \cdot [F[b] : F] < \infty$ for $a, b \in \text{Alg}_F(K)$. So $\text{Alg}_F(K)$ is closed under addition and multiplication. It is also obviously closed under additive inverses since $F[-a] = F[a]$. And since $F[a]$ is a field, $a^{-1} \in F[a]$ so $F[a^{-1}] \subseteq F[a]$ and thus $[F[a^{-1}] : F] \leq [F[a] : F] < \infty$, so a^{-1} is algebraic over F . So $\text{Alg}_F(K)$ is indeed a field.

Now suppose $a \in K \setminus \text{Alg}_F(K)$ is algebraic over $\text{Alg}_F(K)$. Then by the above lemma, it is algebraic over F since $\text{Alg}_F(K)/F$ is trivially algebraic. But then $a \in \text{Alg}_F(K)$ by definition, in contradiction. ■

1.3 Splitting Fields

1.3.1 Proposition

Let F be a field and $f \in F[x]$ be an irreducible polynomial. Then there exists a field extension K/F such that f has a root in K and $[K : F] = \deg f$.

Proof: since f is irreducible, (f) is maximal (since $F[x]$ is a PID so prime ideals are maximal). Thus $K = F[x]/(f)$ is a field. The dimension of K is $\deg f$ since it has a basis $\{1, x, \dots, x^{\deg f-1}\}$.

By the second isomorphism theorem,

$$F/F \cap (f) \cong F + (f)/(f) \subseteq F[x]/(f) = K$$

But $F \cap (f) = 0$, and so $F/F \cap (f) = F/0 \cong F$. Thus we can embed F into K , so we can view K/F as a field extension.

Now, define $\alpha = x + (f)$, and suppose $f(x) = \sum_{i=0}^n a_i x^i$ for $a_i \in F$. Then

$$f(\alpha) = \sum_{i=0}^n a_i (x + (f))^i = \sum_{i=0}^n a_i (x^i + (f)) = \sum_{i=0}^n a_i x^i + \sum_{i=0}^n a_i (f) = f + (f) = 0$$

Thus α is a root of f in K . ■

1.3.2 Corollary

Let F be a field and $f \in F[x]$ a polynomial. Then there exists a field extension K/F such that f has a root in K and $[K : F] \leq \deg f$.

Proof: take an irreducible factorization of f and apply the above result to one of its factors. ■

1.3.3 Definition

Suppose F is a field and $f \in F[x]$. Then f **splits** in F if there exist $\alpha_1, \dots, \alpha_n \in F$ such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$.

1.3.4 Proposition

Let $f \in F[x]$ then there exists a field extension K/F such that f splits in K and $[K : F] \leq (\deg f)!$.

Proof: by induction on $n = \deg f$. For $n = 1$, f is linear and thus has a root so we can take $K = F$. Now suppose $\deg f = n + 1$, then by corollary 1.3.2 there exists a field extension K_0/F such that f has a root in K_0 and $[K_0 : F] \leq n + 1$. Now suppose $\alpha \in K_0$ is a root of f , then there exists a $g(x) \in K_0[x]$ such that $(x - \alpha)g(x) = f(x)$ and so $\deg g \leq n$. Therefore inductively there is a field extension K/K_0 which splits $g(x)$ and thus $f(x)$ and

$$[K : F] = [K : K_0] \cdot [K_0 : F] \leq n! \cdot (n + 1) = (n + 1)!$$

as required. ■

1.3.5 Definition

Suppose K/F is a field extension and $\varphi: F \hookrightarrow E$ is an embedding into some other field E . Then an **extension** of φ to K is an embedding $\bar{\varphi}: K \hookrightarrow E$ such that $\bar{\varphi}|_F = \varphi$ ($\bar{\varphi}$ is equal to φ on F). Let us then define

$$\eta_{K/F}^\varphi := \#\{\bar{\varphi} \mid \bar{\varphi} \text{ is an extension of } \varphi\}$$

In other words, an extension is an embedding $\bar{\varphi}$ such that the following diagram commutes:

$$\begin{array}{ccc} & E & \\ \varphi \nearrow & & \nwarrow \bar{\varphi} \\ F & \xrightarrow{\iota} & K \end{array}$$

Where $\iota: F \rightarrow K$ is the inclusion embedding.

Suppose f, g are two field homomorphisms $F(a_1, \dots, a_n) \rightarrow K$ such that $f(x) = g(x)$ for all $x \in F$ and $f(a_i) = g(a_i)$ for $1 \leq i \leq n$. Then $f(x) = g(x)$ on all of $F(a_1, \dots, a_n)$. This is since $\{r \in F(a_1, \dots, a_n) \mid f(r) = g(r)\}$ is a field containing F and a_1, \dots, a_n and thus $F(a_1, \dots, a_n)$.

In particular if $\varphi: F \hookrightarrow E$ is an embedding, then an extension $\bar{\varphi}: F(a_1, \dots, a_n) \rightarrow E$ is defined entirely by its image on a_1, \dots, a_n .

1.3.6 Proposition

Suppose $K = F[\alpha]$, then $\eta_{K/F}^\varphi$ is equal to the number of distinct roots the minimal polynomial of α has in E . Formally, if $h(x) = \sum_{i=0}^n a_i x^i$ then define $\hat{h}(x) = \sum_{i=0}^n \varphi(a_i) x^i$, and $\eta_{K/F}^\varphi$ is equal to the number of roots $\hat{h}(x)$ has in E .

In particular $\eta_{K/F}^\varphi$ is independent of the choice of φ .

Proof: let $h(x) \in F[x]$ be the minimal polynomial of α , and $\bar{\varphi}$ be an extension of φ to K , then

$$\hat{h}(\bar{\varphi}(\alpha)) = \sum_{i=0}^n \varphi(a_i) \bar{\varphi}(\alpha)^i = \sum_{i=0}^n \bar{\varphi}(a_i) \bar{\varphi}(\alpha^i) = \bar{\varphi}\left(\sum_{i=0}^n a_i \alpha^i\right) = \bar{\varphi}(h(\alpha)) = \bar{\varphi}(0) = 0$$

Thus $\bar{\varphi}(\alpha)$ must be a root of $\hat{h}(x)$, and as explained above extensions of embeddings to $K = F[\alpha]$ are dependent only on their image of α . So there are at most as many extensions as there are distinct roots of \hat{h} .

Now suppose $\beta \in E$ is a root of \hat{h} , then we claim that there exists an extension with $\bar{\varphi}(\alpha) = \beta$. Indeed, $\alpha \notin F$ and β is not in the image of φ (as then $0 = \hat{h}(\varphi(a)) = \varphi(\hat{h}(a))$ so a is a root of $\hat{h}(x)$ but \hat{h} is irreducible), so this is well-defined. ■

1.3.7 Definition

A polynomial f which splits over E is called **separable** over E if its linear factors are all distinct (ie. it has $n = \deg f$ distinct roots in E).

When we have an embedding $\varphi: F \hookrightarrow E$ and a polynomial $f \in F[x]$ and we say that f has some property in E (eg. splits over E , separable over E), then we mean that its image under φ has that property. Meaning if $f(x) = \sum_{i=0}^n a_i x^i$ then $\sum_{i=0}^n \varphi(a_i) x^i$ has said property.

1.3.8 Theorem

Let K/F be a finite extension, and let $\varphi: F \hookrightarrow E$ be an embedding. Then

- (1) $\eta_{K/F}^E \leq [K : F]$;
- (2) if $K = F[\alpha_1, \dots, \alpha_n]$ where α_i are roots of some $f \in F[x]$ which splits over E , then $1 \leq \eta_{K/F}^\varphi$.

Meaning there exists at least one extension of φ to K ;

- (3) if f is also separable over E , then $\eta_{K/F}^\varphi = [K : F]$.

Proof: since K/F is finite, we have that $K = F[\alpha_1, \dots, \alpha_n]$ (we can take $\{\alpha_1, \dots, \alpha_n\}$ to be a basis for K as a F -linear space).

- (1) We proceed inductively on n . For $n = 1$, by the previous proposition $\eta_{K/F}^\varphi$ is equal to the number of roots h_{α_1} (the minimal polynomial of α_1) has in E .

For the inductive step, define $F_1 = F[\alpha_1]$, and so

$$\begin{aligned} \eta_{K/F}^\varphi &= \#\{\varphi'' : K \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \#\bigcup\{\varphi'' : K \longrightarrow E \text{ is an extension of } \varphi' \mid \varphi' : F_1 \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \sum_{\varphi'} \eta_{K/F_1}^{\varphi'} \end{aligned}$$

By our inductive hypothesis, $\eta_{K/F_1}^{\varphi'} \leq [K : F_1]$ and $\eta_{F_1/F}^\varphi \leq [F_1 : F]$ so

$$\leq \sum_{\varphi'} [K : F_1] = [F_1 : F] \cdot [K : F] = [K : F]$$

as required.

- (2) Again, we proceed inductively on n . For $n = 1$, $K = F[\alpha]$ and $\eta_{K/F}^\varphi$ is equal to the number of roots h_α has in E . But since $f(\alpha) = 0$ and h_α is minimal, h_α must divide f and therefore split in E , meaning it has at least one root in E . So $1 \leq \eta_{K/F}^\varphi$ as required.

Inductively, set $F_1 = F[\alpha_1]$ and so there exists an extension of φ to $\varphi' : F_1 \hookrightarrow E$ by our base case. And there then exists an extension of φ' to $\varphi'' : K \hookrightarrow E$, so there exists at least one extension as required.

- (3) If we review the proof of (2), for the base case we must have that f is separable and splits in E , which means that h_α does as well. Then h_α has precisely $\deg h_\alpha$ distinct roots in E , so $\eta_{K/F}^\varphi = \deg h_\alpha = [K : F]$ as required. The rest of the proof proceeds similarly. ■

1.3.9 Definition

Let $f \in F[x]$ be any polynomial over F . Then a field $F \subseteq K$ is called a **splitting field** if f splits over K and it contains no other field over which f splits (meaning it is the smallest field which splits f).

Notice that if K is a splitting field of $f \in F[x]$, then K is of the form $K = F[\alpha_1, \dots, \alpha_n]$ where α_i are roots of f in K . Then

$$[K : F] \leq \prod_{i=1}^n [F[\alpha_i] : F] < \infty$$

so K/F is a finite extension.

1.3.10 Theorem

Any two splitting fields of a polynomial $f \in F[x]$ are isomorphic.

Proof: let K be a splitting field of f , and suppose f splits in E , where $F \subseteq E$. By the above theorem, there must exist an extension of the inclusion embedding $F \hookrightarrow E$ to an embedding $K \hookrightarrow E$. This embedding gives rise to an embedding of F -linear spaces, meaning $[K : F] \leq [E : F]$. In particular, if E is another splitting field of f then $[E : F] \leq [K : F]$ as well, so that K and E are isomorphic F -linear spaces, and thus are isomorphic as fields. ■