MTHSC 852: Fields & Galois Theory

1. Field extensions

Throughout, F, K, and L will denote fields.

Def: If $F \subseteq K$ are fields, then F is a <u>subfield</u> of K, or K is an <u>extension field</u> of F. We also write this as K/F, and say "K over F."

In this case, K is an F-vector space (assuming axiom of choice), with dimension the <u>degree</u> of K over F, denoted $[K:F]$.

If $[K:F] < \infty$, then K/F is a <u>finite</u> extension.

Ex: $\mathbb{R}$ is an infinite extension of $\mathbb{Q}$. (it is a $\mathbb{Q}$-vector space!)

If K/F, and S is a subset of K, define the extension of F generated by S to be

$$F(S) = \bigcap_{S \subseteq L \subseteq K} L \qquad (L \text{ is an extension field of } k).$$

If $a \in K$, then $F(a) := F(\{a\})$ is a <u>simple extension</u>, generated by a, which is a primitive element for $F(a)/F$.

<u>Recall</u>: $F(a)$ is the field of fractions:

$$\begin{tikzcd} F[a] \arrow[r, hook] \arrow[dr] & F(a) \arrow[d, dashed] \\ & L \end{tikzcd}$$

i.e, $F(a) = \left\{ f(a)/g(a) : f(x), g(x) \in F[x],\ g(a) \neq 0 \right\}$.

<u>Prop 1.1</u>: Let $F \subseteq L \subseteq K$ be a chain of fields. If A is a basis for L/F and B is a basis for K/L, then $AB = \{ab : a \in A,\ b \in B\}$ is a basis for K/F.

<u>Pf</u>: Let $c \in K$, with $c = u_1 b_1 + \cdots + u_k b_k$, $u_j \in L$, $b_j \in B$.

and $u_j = v_{j1} a_1 + \cdots + v_{jm_j} a_{m_j}$, $v_{ji} \in F$, $a_i \in A$.

Now, $c = \sum_{j=1}^{k} u_j b_j = \sum_{j=1}^{k} \sum_{i=1}^{m_j} v_{ji} a_i b_j \Rightarrow AB$ spans K ✓

Next, suppose $0 = \sum_{i,j} (v_{ji} a_i) b_j = \sum_{j=1}^{k} u_j b_j \Rightarrow u_j = 0$.

so $u_j = \sum_{i=1}^{m_{ij}} v_{ij} a_i = 0 \Rightarrow v_{ij} = 0 \Rightarrow AB$ is lin. independ. ✓ $\square$

<u>Def</u>: If F is a field, then the <u>prime field</u> of F is

$$F_0 := \bigcap_{\emptyset \neq L \subseteq F} L.$$

$\exists$ ring homom. $f : \mathbb{Z} \longrightarrow F_0$, $f(1) = 1_F$ (so $f(n) = n \cdot 1$).

If f is 1-1, then $\mathbb{Z} \hookrightarrow F_0$, so $F_0 \cong \mathbb{Q}$ (Field of fractions of $\mathbb{Z}$).

If f isn't 1-1, then $\ker f \subseteq \mathbb{Z}$ is an ideal, say $\ker f = (n)$.

If $a, b \in \mathbb{Z}$, and $n \mid ab$, then $0 = (ab)1 = (a1)(b1) =$

$\Rightarrow a1 = 0$ or $(b1) = 0 \Rightarrow n \mid a$ or $n \mid b \Rightarrow n$ is prime

Thus, $\operatorname{Im}(f) \cong \mathbb{Z}_p$, so $F_0 \cong \mathbb{Z}_p$.

If $F_0 \cong \mathbb{Z}_p$, we say F has <u>characteristic</u> p.

Otherwise, it has characteristic 0.
We denote this as char(F).

If $a \in K$ and K/F, then a is <u>algebraic</u> over F if $f(a)=0$ for some $0 \neq f(x) \in F[x]$.

A <u>minimal polynomial</u> of a is any monic polynomial $m(x) \in F[x]$ s.t. $m(a)=0$, of minimal positive degree.

<u>Prop 1.2:</u> If $a \in K$ is algebraic over F, it has a unique min'l polynomial $m_a(x)$ and it is irreducible. Moreover, if $f(a)=0$ for some non-zero $f(x) \in F[x]$, then $m_a(x) \mid f(x)$.

<u>Pf:</u> If $m_a(x)$ is not irreducible, write $m_a(x) = g(x)h(x)$.

Then $m_a(a) = g(a)h(a) = 0 \Rightarrow g(a)=0$ or $h(a)=0$. ✓

Next, write $f(x) = m_a(x)q(x) + r(x)$ $\deg r(x) < \deg m_a(x)$.

$$\Rightarrow 0 = f(a) = m_a(a)q(a) + r(a)$$

$$\Rightarrow r(a) = 0 \Rightarrow m_a(x) \mid f(x). \checkmark$$

Uniqueness is easy: If $k(x)$ were also a min'l poly, then $k(x) \mid m_a(x)$ & $m_a(x) \mid k(x) \Rightarrow m_a(x) \sim k(x)$.

Since they're both monic, $m_a(x) = k(x)$. ✓ □

<u>Cor:</u> $F[x]/(m_a(x)) \cong F[a]$.

<u>Pf:</u> Exercise, (Define $\varphi : F[x] \to F[a]$, $\varphi : f(x) \longmapsto f(a)$, apply FIHT for Rings).

<u>Prop 1.3</u>: Suppose K/F and $a \in K$ is algebraic over F, with min'l poly $m(x) = m_a(x)$. If $\deg m(x) = n$, then $[F(a):F] = n$ and $\{1, a, a^2, \ldots, a^{n-1}\}$ is an F-basis for $F(a)$.

<u>Pf</u>: Write $0 = c_0 1 + c_1 a + c_2 a^2 + \ldots + c_{n-1} a^{n-1}$, $c_i \in F$.

Then if $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in F[x]$, $f(a) = 0$. Since $\deg f(x) < \deg m(x)$, $f(x) = 0$, and so each $c_i = 0 \Rightarrow \{1, a, a^2, \ldots, a^{n-1}\}$ is lin. indep. ✓

Next, we must show that $\{1, a, a^2, \ldots, a^{n-1}\}$ spans $F(a)$.

Recall: $F(a) = \{ f(a)/g(a) : f(x), g(x) \in F[x],\ g(a) \neq 0 \}$.

If $f(a)/g(a) \in F(a)$, then $(m(x), g(x)) = 1$ (since $m(x)$ is irreducible, and $g(a) \neq 0$).

Write $1 = b(x)\, m(x) + c(x)\, g(x)$

$$\Rightarrow 1 = b(a)\, m(a) + c(a)\, g(a) = c(a)\, g(a).$$

$$\Rightarrow f(a) = f(a)\, c(a)\, g(a) \Rightarrow f(a)/g(a) = f(a)\, c(a).$$

Thus, $F(a) = \{ h(a) : h(x) \in F[x] \}$.

Write $h(x) = m(x)\, q(x) + r(x)$, $\deg r(x) < \deg m(x)$.

$$h(a) = \cancel{m(a)}^{\,0} q(a) + r(a) = r(a) \in \mathrm{Span}\{1, a, \ldots, a^{n-1}\} \checkmark$$

Therefore, $\{1, a, \ldots, a^{n-1}\}$ is an F-basis for $F(a)$. $\square$

Cor: If $a \in K$ is algebraic over F, then $F(a) = F[a]$.

Def: An extension K/F is <u>algebraic</u> if every $a \in K$ is algebraic over F.

Prop 1.4: If $[K:F] < \infty$, then K/F is algebraic.

Pf. Let $[K:F] = m$. If $a \in K$, then $\{1, a, a^2, \ldots, a^m\}$ is linearly dependent, so $\exists$ $c_0, c_1, \ldots, c_m \in F$ (not all zero) s.t. $c_0 1 + c_1 a + \cdots + c_m a^m = 0$

Set $f(x) = c_0 + c_1 x + \cdots + c_m x^m \in F[x]$.

Then $f(a) = 0 \Rightarrow a$ is algebraic over F.

Prop 1.5: If K/L is algebraic and L/F is algebraic, then K/F is algebraic

Pf: Pick $a \in K$. Then $\exists$ $0 \neq f(x) = c_0 + c_1 x + \cdots + c_m x^m \in L[x]$ s.t. $f(a) = 0$.

By Props 1.1 & 1.3, each of $F(c_0)$, $F(c_0, c_1)$, ..., $F(c_0, c_1, \ldots, c_m) = L'$ is a finite extension of F.

Clearly, $f(x) \in L'[x]$, and since $f(a) = 0$,

Prop 1.4 $\Rightarrow$ $L'(a)/F$ is algebraic

$\Rightarrow$ a is algebraic over F. $\square$

Prop 1.6: If K/F is a field extension, then the set $E := \{a \in K : a \text{ is algebraic over } F\}$ is a field.

Pf: If $a, b \in E$, then $a \pm b$, ab, & a/b $(b \neq 0)$ are all in $F(a,b)$, and $[F(a,b):F] < \infty$.

By Prop 1.4, $F(a,b)/F$ is algebraic, so $a \pm b$, ab, $a/b \in E$. $\square$

Example: Define $\mathbb{A} = \{a \in \mathbb{C} : a \text{ is algebraic over } \mathbb{Q}\}$
$= \{\text{roots of polynomials in } \mathbb{Q}[x]\}$.

These are the "algebraic numbers"

If $f(x) \in F[x]$ and K/F, $a \in K$ and $f(a) = 0$, then a is a *root* of $f(x)$ in K.

Recall: (Rings, Cor to Prop 2.5): If $a \in K$ is a root of $f(x) \in K$, then $x - a \mid f(x)$ in $K[x]$.

Def: If $(x-a)^k \mid f(x)$ but $(x-a)^{k+1} \nmid f(x)$ then we say that a is a root of $f(x)$ with *multiplicity* k.

Prop 1.7: If K/F and $f(x) \in F[x]$ with $\deg f(x) = n$, then $f(x)$ has at most n roots in K.

Pf: $K[x]$ is a UFD, so $f(x)$ factors into irreducibles, unique up to associates, and the sum of the degrees is n. The number of roots of $f(x)$ in K is the number of degree-1 factors, which $\leq n$. $\square$

Prop 1.8: If $f(x) \in F[x]$ has degree $n \geq 1$, then $\exists\ K/F$

s.t. (i) $f(x)$ has a root $a \in K$,

(ii) $[K:F] \leq n$.

Pf: Let $g(x)$ be a non-const. irreducible factor of $f(x)$.

$(g(x))$ is prime $\Rightarrow (g(x))$ is max'l ($F[x]$ is a PID).

Thus, $K = F[x]/(g(x))$ is a field.

Note:
$$\begin{aligned} F &\hookrightarrow K \\ b &\longmapsto b + (g(x)). \end{aligned}$$

Set $a = x + (g(x)) \in K$.

for some $h(x) \in F[x]$

Then, $f(a) = f(x) + (g(x)) = g(x)\,h(x) + (g(x)) = 0 \in K$

Note: $K = F(a)$, a is the root of the irreducible polynomial $g(x) \in F[x] \Rightarrow [K:F] = \deg g(x) \leq n$. $\square$

Cor: If $f(x) \in F[x]$ has degree n, then $\exists\ K/F$ with $[K:F] \leq n!$ such that $f(x)$ splits over K.

Def: Let $\mathcal{F} \subseteq F[x]$. An extension K of F is a splitting field for $\mathcal{F}$ over F if

(i) Every $f(x) \in \mathcal{F}$ splits over K

(ii) K is minimal s.t. (i) holds

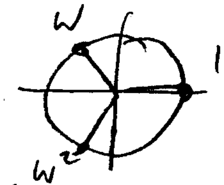
Equivalently, K/F is the splitting field for $\mathcal{F}$ if:

(i) Every $f(x) \in F[x]$ splits in K

(ii) $F(\{\text{roots of polynomials in } \mathcal{F}\}) = K$.

Example: Let $f(x) = x^3 - 1 \in \mathbb{Q}[x]$.

Then $f(x) = (x-1)(x-\omega)(x-\omega^2) \in \mathbb{C}[x]$



So $\mathbb{Q}(\{1, \omega, \omega^2\}) = \mathbb{Q}(\omega)$ is the splitting field over $\mathbb{Q}$.

Def: • F is algebraically closed if every non-constant $f(x) \in F[x]$ has a root in F (and thus splits over F).

• An algebraic closure of F is any algebraic extension of F that is algebraically closed. (We'll later show that these exist & are unique.

Examples • $\mathbb{C}$ is algebraically closed. $\mathbb{Q}$ & $\mathbb{R}$ are not.

• $\mathbb{A}$ is an algebraic closure of $\mathbb{Q}$ (contains all roots in $\mathbb{Q}[x]$, & $\mathbb{A}/\mathbb{Q}$ is algebraic).

• $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$, since $\mathbb{C}/\mathbb{Q}$ is not algebraic. (e.g., $\pi \in \mathbb{C}$).

• $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. (Fund. Thm. Algebra)

* Loosely speaking, an algebraic closure of F is:

• The "largest" algebraic extension of F.

• The "smallest" algebraically closed field containing F.

• The splitting field for $\mathcal{F} = F[x]$ over F.

<u>Note</u>: By substition, any field isomorphism $\phi: F_1 \longrightarrow F_2$ extends to an isomorphism

$$\phi: F_1[x] \longrightarrow F_2[x]$$
$$x \longmapsto x$$

$$\begin{tikzcd}
F_1 \arrow[rr, hook] \arrow[dr, "\phi"'] & & F_1[x] \arrow[dd, dashed, "E_x"] \\
& F_2 \arrow[dr, hook] & \\
& & F_2[x]
\end{tikzcd}$$

<u>Prop 1.9</u>: Let $\phi: F_1 \longrightarrow F_2$ be a field isomorphism.

Let K_1/F_1 be an extension with $a_1 \in K_1$ algebraic over F_1, with min'l poly. $m_1(x) \in F_1[x]$.

Let $m_2(x) = \phi(m_1(x))$ and a_2 be <u>any</u> root of $m_2(x)$.

Then, the isomorphism ϕ extends to an isomorphism:

$$F_1(a_1) \longrightarrow F_2(a_2)$$
$$a_1 \longmapsto a_2.$$

<u>Pf</u>: $m_2(x)$ is the min. poly. of a_2 over F_2.

Let $\eta_i: F_i[x] \longrightarrow F_i[x]/(m_i(x))$ be the canonical quotient maps.

$$\begin{tikzcd}
F_1[x] \arrow[r, "\phi"] \arrow[d, "\eta_1"'] & F_2[x] \arrow[d, "\eta_2"] \\
F_1(a_1) \cong F_1[x]/(m_1(x)) \arrow[r, dashed, "\theta"] & F_2[x]/(m_2(x)) \cong F_2(a_2)
\end{tikzcd}$$

Then, $\ker(\eta_2\phi) = \ker(\eta_1) = (m_1(x))$, so by FHT for rings, $\exists!$ homom. θ s.t. $\theta\eta_1 = \eta_2\phi$, thus $F(a_1) \cong F(a_2)$, (and $a_1 \longmapsto x + (m_1(x)) \longmapsto x + (m_2(x)) \longmapsto a_2$). $\square$

<u>Note</u>: Alternatively, we could just construct an explicit map $\phi: F_1(a_1) \longrightarrow F_2(a_2)$, $\phi(a_1) = a_2$ and check that this works.

<u>Cor</u>: If K/F and $a_1, a_2 \in K$ have the same min'l polynomial over F, then $\exists$ isom $\phi: F(a_1) \longrightarrow F(a_2)$ s.t. $\phi(a_1) = a_2$ and $\phi|_F = id_F$.

In fact, these results hold more generally:

<u>Thm 1.10</u>: Suppose $\phi: F_1 \longrightarrow F_2$ is a field isomorphism, Say $f_1(x) \in F_1[x]$, $f_2(x) = \phi(f_1(x)) \in F_2[x]$, and K_i is a splitting field for $f_i(x)$. Then ϕ extends to an isomorphism $\theta: K_1 \longrightarrow K_2$.

<u>Pf</u>: Use induction on $n = \deg f_1(x)$. Clear if $n=1$.

Let $n>1$, and suppose it's true for lower degree polynomials.

Let $a_1 \in K_1$ be a root of a monic irred. divisor $h(x)$ of $f_1(x)$.
Let $a_2 \in K_2$ be a root of $\phi(h(x))$ in K_2.

Prop 1.9 $\Rightarrow$ ϕ extends to an isom. $F_1(a_1) \longrightarrow F_2(a_2)$.

Write $\begin{cases} f_1(x) = (x-a_1)\, g_1(x) \\ f_2(x) = (x-a_2)\, g_2(x) \end{cases}$ $\quad g_i(x) \in F_i(a_i)[x]$.

$$\begin{tikzcd} F_1 \arrow[r, "\phi"] \arrow[d] & F_2 \arrow[d] \\ F_1(a_1) \arrow[r, "\text{By Prop 1.9}"] \arrow[d] & F_2(a_2) \arrow[d] \\ K_1 \arrow[r, dashed, "\text{By IHOP}"] & K_2 \end{tikzcd}$$

Now,
- $g_2(x) = \phi(g_1(x))$
- K_i is a splitting field for $g_i(x)$
- $\deg g_i(x) < n$.

Apply IHOP: ϕ can be extended from
$F_1(a_1) \longrightarrow F_2(a_2)$ to $K_1 \longrightarrow K_2$. $\square$

<u>Def</u>: If K_1 & K_2 are extensions of F, then an <u>F-isomorphism</u> from K_1 to K_2 is any isom. $\theta: K_1 \longrightarrow K_2$ s.t. $\theta|_F = id$ (i.e., $\theta(b) = b$ $\forall b \in F$).

<u>Cor</u>: (Uniqueness of splitting field of $f(x)$): If K_1 & K_2 are splitting fields over F for $f(x) \in F[x]$, then there is an F-isomorphism $\theta: K_1 \to K_2$.

Actually, uniqueness of splitting fields holds not just for a single polynomial, but for sets of polynomials:

<u>Thm 1.11</u>: Let $\phi: F_1 \to F_2$ be a field isomorphism. Say $\mathcal{F}_1 \subseteq F_1[x]$, $\mathcal{F}_2 = \phi(\mathcal{F}_2) \subseteq F_2[x]$, and K_i is a splitting field for $\mathcal{F}_i$. Then ϕ extends to an isomorphism $\theta: K_1 \to K_2$.

<u>Pf</u>: Let $S = \{(F_\alpha, \phi_\alpha) : F_1 \subseteq F_\alpha \subseteq K_1,\ \phi_\alpha : F_\alpha \hookrightarrow K_2,\ \phi_\alpha|_{F_1} = \phi\}$.

Partially order S: $(F_\alpha, \phi_\alpha) \leq (F_\beta, \phi_\beta)$ iff $F_\alpha \subseteq F_\beta$ and $\phi_\beta|_{F_\alpha} = \phi_\alpha$.

<u>Note</u>: $S \neq \emptyset$ because $(F_1, \phi) \in S$.

Apply Zorn's lemma: $\exists$ max'l elt $(F_0, \theta) \in S$.

If $F_0 \neq K_1$, then $\exists f_1(x) \in \mathcal{F}_1$ that does <u>not</u> split over F_0 (and so $\theta(f_1(x))$ doesn't split over $\theta(F_0)$).

In this case, $f_1(x) \in F_0[x]$, $\theta(f_1(x)) \in \theta(F_0)[x]$, and there are splitting fields L_1, L_2 of $f_1(x)$ & $\theta(f_1(x))$, over F_0 & $\theta(F_0)$, respectively, i.e.,

$$F_0 \subsetneq L_1 \subseteq K_1 \text{ and } \theta(F_0) \subsetneq L_2 \subseteq K_2.$$

By Thm 1.10, we can extend $\theta: F_0 \to \theta(F_0)$ to $\theta': L_1 \to L_2$.

But then $(F_0, \theta) \lneq (L_1, \theta')$. $\lightning$ (maximality of (F_0, θ)).

Thus, $F_0 = K_1 \Rightarrow \theta(K_1) \subseteq K_2$ is a splitting field for $\theta(\mathcal{F}_1) = \mathcal{F}_2$

$\Rightarrow \theta(K_1) = K_2$ (by minimality of splitting fields). $\square$

<u>Cor</u>: (<u>Uniqueness</u> of algebraic closures): If K_1, K_2 are algebraic closures of F, then there is an F-isomorphism $\theta : K_1 \to K_2$.

<u>Pf</u>: An algebraic closure is a splitting field of $\mathcal{F} = F[x]$. $\square$

<u>Thm 1.12</u>: (<u>Existence</u> of algebraic closures): If F is a field, then F has an algebraic closure.

<u>Pf</u>: <u>Caution</u>! The class S of algebraic extensions of F need not be a set! (Exercise).

Let S be a <u>set</u> s.t (i) $F \subset S$
(ii) $|S| > \max\{\aleph_0, |F|\} =: \alpha$.

Let $\mathcal{R} = \{L \subset S : L \text{ is an algebraic ext. of } F\}$.

Partially order $\mathcal{R}$ by $L_1 \leq L_2$ iff $L_1 \subseteq L_2$ is an algebraic ext.

By Zorn's lemma, $\exists$ max'l elt $L_0 \in \mathcal{R}$

<u>Claim</u>: L_0 is an algebraic closure of F.

Assume not. Then there exists non-const. $f(x) \in L_0[x]$ that has no roots in L_0.

Let K be a splitting field for $f(x)$ over L_0, and so
$|L_0| \leq |K| \leq \alpha \implies |S \setminus L_0| = |S| > |K \setminus L_0|$.

Thus, $\exists \phi : K \hookrightarrow S$ s.t $\phi|_{L_0} = id$.

The element $\phi(K)$ (with algebraic field structure inherited) in S is maximal <u>and</u> $L_0 \lneq \phi(K)$. $\lightning$

$\square$