1. Field extensions

Throughout, \( F, K, \) and \( L \) will denote fields.

**Def:** If \( F \subseteq K \) are fields, then \( F \) is a **subfield** of \( K \), or \( K \) is an **extension field** 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 **degree** of \( K \) over \( F \), denoted \( [K:F] \).

If \( [K:F] < \infty \), then \( K/F \) is a **finite** 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

\[
F(S) = \bigcap_{L \subseteq K} L \quad (L \text{ is an extension field of } K).
\]

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

Recall: \( F(a) \) is the **field of fractions**: \( F[a] \rightarrow F(a) \)

i.e., \( F(a) = \{ f(a)/g(a) : f(a), g(a) \in F[x], g(a) \neq 0 \} \).
Prop 1.1: 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 $K/F$.

Proof: Let $c \in K$, with $c = u_1 b_1 + \ldots + u_k b_k$, $u_j \in L$, $b_j \in B$.

and $u_j = v_{j1} a_1 + \ldots + v_{jm} a_m$, $v_{ji} \in F$, $a_i \in A$.

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

Next, suppose $0 = \sum_{j=1}^{k} u_j b_j \Rightarrow u_j = 0$.

so $u_j = \sum_{i=1}^{m} v_{ji} a_i = 0 \Rightarrow v_{ij} = 0 \Rightarrow AB$ is lin. independ. \qed

Definition: If $F$ is a field, then the prime field of $F$ is

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

There is a homomorphism $f : \mathbb{Z} \rightarrow F_0$, $f(n) = n\cdot 1_F$ (so $f(n) = n\cdot 1$).

If $f$ is 1-1, then $\mathbb{Z} \rightarrow F_0$, 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 $n | ab$, then $0 = (ab)1 = (a1)(b1) = a1 = 0$ or $b1 = 0 \Rightarrow n | a$ or $n | b \Rightarrow n$ is prime.

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

If $F_0 \cong \mathbb{Z}_p$, we say $F$ has characteristic $p$. 
Otherwise, it has characteristic 0. We denote this as \( \text{char}(F) \).

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

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

**Prop 12:** If \( a \in K \) is algebraic over \( F \), it has a unique minimal polynomial \( m_a(x) \) and it is irreducible. Moreover, if \( f(a) = 0 \) for some non-zero \( f(x) \in F[x] \), then \( m_a(x) \mid f(x) \).

**PF:** If \( m_a(x) \) is not irreducible, write \( m_a(x) = g(x) \cdot h(x) \).

Then \( m_a(a) = g(a) \cdot h(a) = 0 \Rightarrow g(a) = 0 \) or \( h(a) = 0 \), ✓

Next, write \( f(x) = m_a(x) \cdot g(x) + r(x) \) \( \deg r(x) < \deg m_a(x) \).

\( \Rightarrow 0 = f(a) = m_a(a) \cdot g(a) + r(a) \)

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

Uniqueness is easy: If \( k(x) \) were also a minimal poly, then \( k(x) \mid m_a(x) \iff m_a(x) \mid k(x) \Rightarrow m_a(x) = k(x) \).

Since they're both monic, \( m_a(x) = k(x) \), ✓

**Cor:** \( F[x]/(m_a(x)) \cong F[a] \).

**PF:** Exercise, (Define \( \phi : F[x] \rightarrow F[a] \), \( \phi : f(x) \mapsto f(a) \), apply FIT for Rings).
**Prop 13:** Suppose $K/F$ and $a \in K$ is algebraic over $F$, with min 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 $F(a)$.

**Pf:** 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 $f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} \in F[x]$, $f(a) = 0$. 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: $F(a) = \{ f(x)/g(x) : f(x), g(x) \in F[x], g(x) \neq 0 \}$.

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

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

Write $h(x) = m(x) g(x) + r(x)$, $\deg r(x) < \deg m(x)$, $h(a) = m(a) g(a) + r(a) = r(a) \in \text{Span}\{1, a, \ldots, a^{n-1}\}$ ✓

Therefore, $\{1, a, \ldots, a^{n-1}\}$ is an $F$-basis for $F(a)$. □
**Cor.** If $a \in K$ is algebraic over $F$, then $F(a) = F[a]$.

**Def.** An extension $K/F$ is algebraic 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. $c_0 + c_1a + \ldots + c_ma^m = 0$.

Set $f(x) = c_0 + c_1x + \ldots + c_mx^m \in F[x]$.

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 $\exists \ c \neq 0 \ : f(x) = c_0 + c_1x + \ldots + c_mx^m \in L[x]$, 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 $f(a) = 0$,

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

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

Proof: If $a, b \in E$, then $a + b, ab, \frac{a}{b}$ (if $b \neq 0$) are all in $F(a, b)$, and $[F(a, b) : F] < \infty$.

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

Example: Define $A = \{ a \in C : a \text{ is algebraic over } \mathbb{Q} \}$

$= \{ \text{roots of polynomials in } \mathbb{Q}[x] \}$.

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 $f(x) \in K[x]$, 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 $K$.

Because $K[x]$ 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) $[K:F] \leq n$.

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

$(g(x))$ is prime $\Rightarrow (g(x))$ is maximal ($F[x]$ is a PID).

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

Note: $F \xrightarrow{b} K$

$b \mapsto b + (g(x))$

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

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 \( F \) if:

1. Every \( f(x) \in F[x] \) splits in \( K \)
2. \( F(\{ \text{roots of polynomials in } x] \}) = K \).

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

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

So \( \mathbb{Q}(\{1, w, w^2\}) = \mathbb{Q}(w) \) 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 there exist \( F \) 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 \( \mathbb{Q}[x] \), i.e., \( \mathbb{A}/\mathbb{Q} \) is algebraic).

- \( \mathbb{C} \) is not an algebraic closure of \( \mathbb{Q} \), since \( \mathbb{C}/\mathbb{A} \) 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 \( F = F[x] \) over \( F \).
Note: By substitution, any field isomorphism $\phi: F_1 \to F_2$ extends to an isomorphism $\phi: F_1[x] \to F_2[x]$

\[ x \mapsto x \]

Prop 1.9: Let $\phi: F_1 \to F_2$ be a field isomorphism.

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

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

Then, the isomorphism $\phi$ extends to an isomorphism:

\[ F_1(a_1) \cong F_2(a_2) \]

Proof: $m_2(x)$ is the min. poly. of $a_2$ over $F_2$.

Let $\eta_1: F_1[x] \to F_1[x]/(m_1(x))$ be the canonical quotient maps.

Then, $\ker(\eta_2 \circ \phi) = \ker(\eta_1) = (m_1(x))$, so by FHT for rings,

\[ \exists \text{ homom. } \theta \text{ s.t. } \theta \eta_1 = \eta_2 \phi, \text{ thus } F(a_1) \cong F(a_2) \]

and $a_1 \mapsto x + (m_1(x)) \mapsto x + \theta(m_1(x)) \mapsto a_2$.

Note: Alternatively, we could just construct an explicit map $\phi: F_1(a_1) \to F_2(a_2), \phi(a_1) = a_2$ and check that this works.
Cor: If $K/F$ and $a_1, a_2 \in K$ have the same minimal polynomial over $F$, then there is an isomorphism $\phi: F(a_1) \to F(a_2)$ s.t. $\phi(a_1) = a_2$ and $\phi|_{F} = \text{id}_F$.

In fact, these results hold more generally:

**Thm 1.10:** Suppose $\phi: F_1 \to F_2$ 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 $\phi$ extends to an isomorphism $\Theta: K_1 \to K_2$.

**Pf:** Use induction on $n = \text{deg} f_1(x)$. 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 irreducible 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:** $\phi$ extends to an isom. $F_1(a_1) \to F_2(a_2)$.

Write $\begin{cases} F_1(x) = (x-a_1) g_1(x) \\ F_2(x) = (x-a_2) g_2(x) \end{cases} g_1(x) \in F_1(a_1)[x].$

Now, $g_2(x) = \phi(g_1(x))$.

- $K_i$ is a splitting field for $g_i(x)$
- $\text{deg} g_i(x) < n$.

Applying Thm: $\phi$ can be extended from $F_1(a_1) \to F_2(a_2)$ to $K_1 \to K_2$.

**Def:** If $K_1$ and $K_2$ are extensions of $F$, then an $F$-isomorphism from $K_1$ to $K_2$ is any isom. $\Theta: K_1 \to K_2$ s.t. $\Theta|_{F} = \text{id}$ (i.e., $\Theta(b) = b \forall b \in F$).
Cor.: (Uniqueness of splitting field of \( f(x) \)): If \( K_1 \) and \( K_2 \) are splitting fields over \( F \) for \( f(x) \in F[x] \), then there is an \( F \)-isomorphism \( \theta : K_1 \rightarrow K_2 \).

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

**Thm 1.11:** Let \( \phi : F_1 \rightarrow F_2 \) be a field isomorphism.

Say \( F_1 = F_1[x] \), \( F_2 = \phi(F_1) = F_2[x] \), and \( K_1 \) is a splitting field for \( F_1 \). Then \( \phi \) extends to an isomorphism \( \theta : K_1 \rightarrow K_2 \).

**Proof:** Let \( S = \{ (F_2, \phi_2) : F_2 \subseteq F_2 \subseteq K_1 \}, \phi_2 : F_2 \rightarrow K_2 \), \( \phi_2|_{F_1} = \phi \} \).

Partially order \( S : (F_2, \phi_2) \leq (F_2, \phi_2') \) iff \( F_2 \subseteq F_2 \) and \( \phi_2'|_{F_2} = \phi_2 \).

Note: \( S \neq \emptyset \) because \( (F_2, \phi) \in S \).

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

If \( F_0 \neq K_1 \), then \( \exists f(x) \in F_1 \) that does not split over \( F_0 \)
(\( \text{and so } \theta(f_1(x)) \text{ doesn't split over } \theta(F_0) \)).

In this case, \( f_1(x) \in F_0[x] \), \( \theta(f_1(x)) \in \theta(F_0) \), \( \theta(f(x)) \), and there are splitting fields \( L_1, L_2 \) of \( f_1(x) \) over \( F_0 \) i.e., \( F_0 \subseteq L_1 \subseteq K_1 \) and \( \theta(F_0) \subseteq L_2 \subseteq K_2 \).

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

But then \( (F_0, \theta) \leq (L_1, \theta') \), \( \theta' \) (maximality of \( (F_0, \theta) \).

Thus, \( F_0 = K_1 \rightarrow \theta(K_1) \subseteq K_2 \) is a splitting field for \( \theta(F_1) = F_2 \).

\( \Rightarrow \theta(K_1) = K_2 \) (by minimality of splitting fields).
Cor. (Uniqueness of algebraic closures): If $K_1, K_2$ are algebraic closures of $F$, then there is an $F$-isomorphism $\Theta: K_1 \to K_2$.

**Pf:** An algebraic closure is a splitting field of $\mathcal{F}=\mathcal{F}[x]$.

**Thm 1.12:** (Existence of algebraic closures): If $F$ is a field, then $F$ has an algebraic closure.

**Pf:** Caution! The class $\mathcal{S}$ of algebraic extensions of $F$ need not be a set! (Exercise).

Let $\mathcal{S}$ be a set s.t.

1. $F \in \mathcal{S}$
2. $|\mathcal{S}| > \max\{\gamma_0, |F|\} = \aleph$

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

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

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

Claim: $L_0$ is an algebraic closure of $F$.

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

Let $K$ be a splitting field for $f(x)$ over $L_0$, and so $|L_0| \leq |K| < \aleph \Rightarrow |\mathcal{S} \setminus L_0| = |\mathcal{S}| > |K \setminus L_0|$. 

Thus, $\exists \Phi: K \to \mathcal{S}$ s.t. $\Phi|_{L_0} = \text{id}$.

The element $\Phi(K)$ (with algebraic field structure inherited) in $\mathcal{S}$ is maximal and $L_0 \subseteq \Phi(K)$. $\square$