Thm | If $E$ is a finite extension of $F$, $K$ is a finite extension of $E$, then $K$ is a finite extension of $F$ ($F \subseteq E \subseteq K$) and

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

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for $E$ as an $F$-vector space and $\{\beta_1, \ldots, \beta_m\}$ be a basis for $K$ as a $E$-vector space

Show $\{\alpha_i \beta_j\}$ forms a basis for $K$ over $F$.

Show spans $K$. Let $u \in K$ arbitrary, then

$$u = \sum_{i=1}^{m} b_i \beta_i$$

and $b_i \in E$.

Since $b_i \in E \Rightarrow b_i = \sum_{j=1}^{n} a_{ij} \alpha_j$, $a_{ij} \in F$.

$\therefore u = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_j \beta_i$

$\therefore \{\alpha_i \beta_j\} \mid i = 1, \ldots, m, j = 1, \ldots, n \}$ spans $K$ over $F$.

Show $\{\alpha_i \beta_j\}$ is lin. independent.
\[
\begin{align*}
    u &= \sum_{i=1}^n \sum_{j=1}^m c_{ij} a_i b_j = 0 \quad E \forall k, \quad c_{ij} \in E \\
    &= \sum_{j=1}^m \left( \sum_{i=1}^n c_{ij} a_i \right) b_j = 0 \\
    &\quad \quad \quad \quad \text{since } b_j \text{ are lin. ind. over } E \\
    \Rightarrow \sum_{i=1}^n c_{ij} a_i &= 0 \\
    \Rightarrow c_{ij} &= 0 \quad \text{since } a_i \text{'s are lin. ind. over } F \\
    \therefore \{a_i b_j\} \text{ is a basis }
\end{align*}
\]

**Cor.** If \( F_i \) is a field, \( i=1, \ldots, k \), \( F_i \subset \cdots \subset F_k \) and if \( F_{i+1} \) is a finite extension of \( F_i \) then \( F_k \) is a finite extension of \( F_1 \) and
\[
[F_k : F_i] = [F_k : F_{k-1}] [F_{k-1} : F_{k-2}] \cdots [F_2 : F_1].
\]

**Cor.** Let \( E \) be an extension field of \( F \). If \( \alpha \in E \) is alg. over \( F \) with minimal poly. \( p(\alpha) \) and \( \beta \in F(\alpha) \) with min poly \( q(\alpha) \) (associated to \( F(\alpha) \) over \( F(\beta) \)) then \( \deg(q(\alpha)) | \deg(p(\alpha)) \).
Proof: $\deg(p(x)) = [F(x) : F]$

$\deg(q(x)) = [F(x) : F(B)]$

$F \subset F(B) \subset F(x) \subset F$

$= \deg(p(x)) = \deg(q(x))$

$[F(x) : F] = [F(x) : F(B)] \cdot [F(B) : F]$

$\therefore$ Since $[F(B) : F] \in \mathbb{Z}_+$

$\Rightarrow \deg(q(x)) | \deg(p(x))$

Exercise Determine $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

The min. poly of $\sqrt{3} + \sqrt{5}$ is

$x^4 - 16x^2 + 4$

$[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 4$

* $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$ with min poly $x^2 - 3$

* $\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$, with min poly $x^2 - 5$.

$\{1, \sqrt{3}, \sqrt{5}, \sqrt{3} \cdot \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.
and \( \dim \mathbb{Q}(\mathbb{Q}(\sqrt{3}, \sqrt{5})) = 4 \), i.e. \([\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4\)

\(\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})\)

\(\therefore \mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})\)

and this is actually a simple extension of degree 4.

Can have \( F(\alpha_1, \ldots, \alpha_n) = F(\alpha) = F[x]/\langle p(\alpha) \rangle \)

Note \([\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2\)

and min. poly of \( \sqrt{5} \) over \( \mathbb{Q}(\sqrt{3}) \) is still \( x^2 - 5 \).

**Thm** Let \( E \) be a field extension of \( F \). The following are equivalent:

1) \( E \) is a finite extension of \( F \)

2) \( E \) is a finite number of algebraic elements \( \alpha_1, \ldots, \alpha_n \in E \), s.t. \( E = F(\alpha_1, \ldots, \alpha_n) \)

3) There exists a sequence of fields

\[ E = F(\alpha_1, \ldots, \alpha_n) \supseteq F(\alpha_1, \ldots, \alpha_{n-1}) \supseteq \cdots \supseteq F(\alpha_1) \supseteq F \]

**Thm** Let \( E \) be a field extension of \( F \). The set \( \mathcal{A}_F \) of elements in \( E \) that are algebraic over \( F \) forms a field.
Proof: Let $\alpha, \beta \in K \Rightarrow \alpha, \beta$ are alg. over $F$.

$\Rightarrow F(\alpha, \beta)$ is a finite extension

and all elements of $F(\alpha, \beta)$ are alg. over $F$.

$\Rightarrow \alpha \pm \beta, \alpha \beta, \frac{\alpha}{\beta}, \frac{1}{\beta}, \frac{1}{\alpha} (\beta \neq 0, \alpha \neq 0$ respectively)

are algebraic over $F$.

$\Rightarrow K \subseteq \mathbb{A}_F$

$\therefore \mathbb{A}_F$ is a field.

Q.E.D. The set of all algebraic numbers = algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$ is a field.

Def: Let $E$ be a field extension of $F$.

$\overline{F} =$ algebraic closure of $F$ in $E$ is the field consisting of all $x \in E$ s.t. $x$ is alg. over $F$.

$\cdot \overline{F}$ is algebraically closed ($\overline{F} = \overline{E}$) if every non-constant polynomial in $F[x]$ has a root in $\overline{F}$.

Ex: $\overline{\mathbb{Q}} =$ set (field) of algebraic numbers

$\mathbb{C}$ is algebraically closed.
**Theorem**

A field $F$ is algebraically closed if and only if every non-constant polynomial factors into linear factors in $F[x]$.

**Proof (sketch)**

Assume $F$ is closed:

- For any polynomial $p(x) \in F[x]$, if $\deg(p) = n$, then there exists at least one zero $a \in F$ such that $p(a) = 0$.

Suppose $x \in F$ is this zero, then $p(x) = (x-a)q(x)$, where $\deg(q, a) = \deg(p) - 1$.

This gives a linear factorization.

Conversely, if $F$ has a linear factorization for every polynomial, then the roots must be in $F$.

**Corollary**

An algebraically closed field $F$ has no proper algebraic extension $E$.

**Theorem**

Every field $F$ has a unique algebraic closure (up to isomorphism).

**Theorem** *(Fundamental Theorem of Algebra)*

$F$ is algebraically closed.
Splitting Fields

Q: over what (smallest) extension field may we factor \( p(x) \in \mathbb{F}[x] \) into linear factors?

**Def:** Let \( \mathbb{F} \) be a field, \( p(x) \in \mathbb{F}[x] \), \( \text{deg}(p) = n \geq 1 \)

An extension field \( E \) of \( \mathbb{F} \) is a **splitting field of** \( p(x) \)

if \( \exists \alpha_1, \ldots, \alpha_n \in E \) s.t. \( E = \mathbb{F}(\alpha_1, \ldots, \alpha_n) \) and \( p(x) = (x-\alpha_1) \cdots (x-\alpha_n) \)

- \( p(x) \in \mathbb{F}[x] \) splits in \( E \) if it is the product of linear factors in \( E[x] \).

\[
\begin{align*}
\mathbb{F}[x] & \quad p(x) = x^4 + 2x^2 - 8 \in \mathbb{Q}[x] \\
& = (x^2 - 2)(x^2 + 4)
\end{align*}
\]

**Splitting field of** \( p(x) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}, \sqrt{-2}, -2i, 2i) \)

\[
p(x) = (x - \sqrt{2})(x + \sqrt{2})(x - 2i)(x + 2i)
\]

Q: Are splitting fields unique?

A: Yes, up to isomorphisms of \( \mathbb{F} \)

**Lemma:** Let \( \phi: E \rightarrow F \), \( \phi \) is a isomorphism, \( E \leq K \), \( K \) an extension field of \( E \), \( \alpha \in K \) alg. over \( E \) with min. poly \( p(x) \)

\( F \in \mathbb{L} \) \( \beta \) is a root of \( \phi(p(x)) \). Then \( \phi \) extends to a unique isomorphism \( \phi: E(\alpha) \rightarrow F(\beta) \) s.t. \( \phi(\alpha) = \beta \)
and \( \overline{\phi}(E) = \phi(C) \)

\[ \text{same as } \overline{\phi} \text{ on } E. \]

**Proof Sketch**

**Isomorphism**

\[ \Phi : E \rightarrow F \]

**Idea:**

\[ \Phi : E[x] \rightarrow F[x] \]

\[ a_0 + a_1 x + \cdots + a_n x^n \rightarrow \Phi(a_0) + \Phi(a_1) x + \cdots + \Phi(a_n) x^n \]

induces an isomorphism \( E(\alpha) \rightarrow F(\beta) \)

where \( \min. \text{poly. of } \alpha \text{ over } E = \varphi(x) = \Phi(p(x)) \)

[Diagram]

\[ E[x]/(p(x)) \leftarrow \psi \rightarrow F[x]/(\varphi(x)) \]

\[ \phi(\langle p(x) \rangle) = \langle \varphi(x) \rangle \]

**Theorem**

\( \Phi : E \rightarrow F \) is an isomorphism of fields

\[ p(x) \in E[x] \text{ non-constant, } \varphi(x) = \Phi(p(x)). \text{ If } K \text{ is a splitting field of } p(x) \text{ and } L \text{ is a splitting field of } \varphi(x) \]
then $\phi$ extends to an isomorphism $\Psi : K \to L$.

**Cor** 
Let $p(x) \in \mathbb{F}[x]$. Then there exists a unique (up to isomorphism) splitting field of $p(x)$.

**Ex** 
$x^2 - 4 = (x+2)(x-2)$ \Rightarrow Splitting field is $\mathbb{Q}$

$x^2 + 4 \Rightarrow Splitting field \mathbb{Q}(i) = \mathbb{Q}(2i, -2i)$

\[(x + 2i)(x - 2i)\]

$x^2 + 2 \Rightarrow Splitting field is \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(-i\sqrt{2}, i\sqrt{2})$

\[(x - i\sqrt{2})(x + i\sqrt{2})\]

---

**Structure of a finite field**

**Prop** 
If $F$ is a finite field $\Rightarrow \text{char}(F) = p$, $p$ prime

**Proofs** 
If $\text{Char}(F) = n$, $n$ composite

then $n = ij$ \(j\) times are in $F$

\[a = 1 + \cdots + 1, \text{ and } \overbrace{a}^{i \text{ times}} \text{ and } \overbrace{b}^{j \text{ times}} \]

Check $a \cdot b = 0$  

---

**Running assumption** $p = \text{Prime.}$
\( \mathbb{Z}/p\mathbb{Z} \) is a finite field of characteristic \( p \).

What about \( |F| = n \) where \( p \nmid n \), i.e., \( |F| = p^m \)?

**Prop:** If \( F \) is a finite field (\( \text{char}(F) = p \)), then \( |F| = p^n \) for some \( n \in \mathbb{N} \).

**Proof:** Define a ring hom by
\[
\phi: \mathbb{Z} \rightarrow F, \quad n \rightarrow n \cdot 1 = 1 + 1 + \cdots + 1
\]

\( \text{Char}(F) = p \) \implies \( \ker(\phi) = p\mathbb{Z} \).

\( \implies \) by 1st iso. theorem
\[
\phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}
\]

\( \uparrow \)

This is a subfield of \( F \).

Let \( K = \phi(\mathbb{Z}) \), since \( F \) is a finite field
\( \implies \) finite extension of \( K \).

\( \implies F \) is a finite dimensional vector space over \( K \), say \( \dim_K(F) = n \), i.e., \( [F:K] = n \).

\( \implies \exists \) a basis of \( F \), say \( \{x_1, \ldots, x_n\} \in F \).
For any \( \alpha \in \mathbb{F} \)

\[
\alpha = a_1 \alpha_1 + \cdots + a_n \alpha_n, \quad a_i \in \mathbb{K}
\]

But \( |\mathbb{K}| = p \) \( \implies \) an exactly \( p \) choices for each \( a_i \)

\( \exists \) \( p^n \) linear combinations of \( \alpha_i \)'s

\( \therefore |\mathbb{F}| = p^n \)

**Lemma**

Let \( \mathbb{P} \) be prime, \( \mathbb{D} \) an integral domain, \( \text{char}(\mathbb{D}) = p \). Then

\[
(a + b)^p = a^p + b^p \quad \text{then } a, b \in \mathbb{D}
\]

**Proof:** induction, Binomial formula.

**Def:** Let \( \mathbb{F} \) be a field, \( f(x) \in \mathbb{F}[x] \), \( \text{deg}(f) = n \)

is **separable** if it has \( n \) distinct roots in the splitting field of \( f(x) \)

- An extension \( \mathbb{E} \) of \( \mathbb{F} \) is a separable extension of \( \mathbb{F} \) if every element in \( \mathbb{E} \) is a root of a separable polynomial in \( \mathbb{F}[x] \).

**Ex:** \( x^2 - 2 \) is separable over \( \mathbb{Q} \)

\[
x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})
\]

\( \mathbb{Q}(\sqrt{2}) \) is in fact a separable extension.
All \( x \in \mathbb{Q}(\sqrt{2}) \) are of the form \( x = a + b\sqrt{2} \), \( a, b \in \mathbb{Q} \).

- \( b = 0 \Rightarrow x \) is a root of \( x - a \), which is separable.
- \( b \neq 0 \Rightarrow x \) is a root of

\[
x^2 - 2ax + a^2 - 2b^2 = (x - (a + b\sqrt{2}))(x - (a - b\sqrt{2}))
\]

Let \( f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x] \)

**Def:** The derivative of \( f(x) \) is \( f'(x) = a_1 + 2a_2x + \cdots + nanx^{n-1} \)

**Lemma:** \( f(x) \) is separable iff \( \gcd(f(x), f'(x)) = 1 \)

**Proof:** Write \( f(x) \) in factored form in splitting field, take the derivative, check \( \gcd \).

**Thm:** For every prime \( p \), every \( n \in \mathbb{N} \) \( \exists \) a finite field \( \mathbb{F} \) with \( p^n \) elements; \( \mathbb{F} \) is isomorphic to the splitting field of \( f_{\mathbb{F}} = x^{p^n} - x \) over \( \mathbb{Z}_p \).

**Proof:** Let \( \mathbb{F} = \text{splitting field of } f_{\mathbb{F}} = x^{p^n} - x \)

\[
f'(x) = p^n x^{p^n-1} - 1 = -1
\]

\[\gcd(f(x), f'(x)) = 1 \Rightarrow f \text{ is a separable polynomial} \]
\[ f \text{ has } p^n \text{ distinct roots,} \]

show that \( F = \text{roots of } f(x) \)

First show roots of \( f(x) = x^{p^n} - x \) form a subfield of \( F \).

Check that 0, 1, \( a + b, -a, a \beta, d^l \) are roots of \( f(x) \) for any roots \( a, \beta \) of \( f(x) \).

\[
(a + b)^{p^n} - (a + b) = a^{p^n} + b^{p^n} - a - b = 0 \implies a + b \text{ is a root.}
\]

\[ \therefore \text{ the set of roots of } f(x) \text{ form a subfield of } F \]

and \( f(x) \) splits in this subfield \( \therefore \text{ the set of roots is the splitting field of } x^{p^n} - x \).

\[ \therefore \text{ Always exists a finite field with } p^n \text{ elements} \]

uniques (upto 130)

Suppose \( E \) is a field, \( |E| = p^n \), \( \implies |E^*| = p^n - 1 \)

\[ \therefore \forall a \in E \quad a^{p^n - 1} = 1 \]

\[ \therefore \forall a \in E \quad a^{p^n} - a = 0 \]

\[ \therefore E \text{ has all roots of } f(x) \]

\[ \therefore \text{ Since splitting fields are unique} \]

\[ \implies E \cong \text{ splitting field of } f(x) \]

\[ \text{Def} \]
Galois field of order \( p^n = \text{unique finite field with } p^n \)

\[ GF(p^n) \]

splitting field of \( x^{p^n} - x \) over \( \mathbb{Z}_p \)
**Thm/** Every subfield of $GF(p^n)$ has $p^m$ elements where $m|n$. Conversely if $m|n$ then a unique subfield of $GF(p^n)$ isomorphic to $GF(p^m)$.

**Proof:**

Let $E$ be a subfield of $E = GF(p^n)$.

Then $F$ is an extension of $k = \mathbb{Z}/p$.

If $F$ contains $p^m$ elements for some $m | n$, then $[E:F] = m$.

Hence, $[E:K] = [E:F] [F:K] = \frac{n}{m}$.

Point: $[E:K] = n$ since we know that $E$ is a dimension $n$ K-vector space from our earlier proof that constructed $E$ as an extension field of $\mathbb{Z}/p\mathbb{Z}$.

**Ex.**

$GF(p^{24})$
For each field $F$ we have a multiplicative group of non-zero elements $F^*$.

**Thm.** If $G$ is a finite subgroup of $F^*$ (for any $F$), then $G$ is cyclic.

**Cor.** $F^*$ is cyclic whenever $F$ is a finite field.

**Cor.** Every finite extension $E$ of a finite field $F$ is a simple extension.

**Proof.** Let $\alpha$ generate $E^* \implies E = F(\alpha)$.

End of material for final

<table>
<thead>
<tr>
<th>Field</th>
<th>Automorphisms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* want to establish a link between field theory and group theory</td>
</tr>
<tr>
<td></td>
<td>* use automorphisms of fields = isomorphisms $F \to F$.</td>
</tr>
</tbody>
</table>

**Proposition.** The set of all automorphisms of a field $F$ is a group under composition of functions.

**Proof.** $\sigma, \tau$ auto. of $F \implies \sigma \circ \tau, \tau^{-1}$ are automorphisms as well, and id - map is an automorphism.
Prop. Let $E$ be a field extension of $F$. Then the set of all automorphisms of $E$ that fix all elements of $F$, i.e. the set $\sigma : E \to E$ s.t.

$$\sigma(\alpha) = \alpha \quad \forall \alpha \in F$$

are a subgroup, denoted $G(E/F)$, of $\text{Aut}(E)$, group of Automorphisms of $E$.

Proof: need only show $G(E/F)$ is a subgroup of $\text{Aut}(E)$.

If $\sigma, \tau \in G(E/F)$

$$\Rightarrow \quad \tau \circ \sigma(\alpha) = \tau(\sigma(\alpha)) = \tau(\alpha) = \alpha \quad \forall \alpha \in F$$

and $\tau^{-1}(\alpha) = \alpha$, $\tau \in G(E/F)$.

Def: The Galois group of $E$ over $F$ is

$$G(E/F) = \{ \sigma \in \text{Aut}(E) \mid \sigma(\alpha) = \alpha \quad \forall \alpha \in F \}$$