Field Extensions

If \( p(x) \in F[x] \) is irreducible, then \( F[x]/(p(x)) \) is a field.

Examples

1. \( F = \mathbb{R} \), then the only irreducible polynomials are quadratic, e.g. \( x^2 + 1 \)

2. \( C = \mathbb{R}[x]/(x^2 + 1) \)

3. \( F = \mathbb{Q} \). There are many irreducible polynomials and hence many field extensions.
Prop 10.2.2 Let $F \leq E$ be fields with $x \in E$.

In $E$ let

$F[x] = \{ f(x) : f(x) \in F[x] \}$ = subring of $E$

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

= subfield of $E$. Then

1) $F[x]$ is a subring of $E$ containing $F$ and $x$

2) $F(x)$ is the smallest such subring

3) $F(x)$ is a subfield of $E$ containing $F$ and $x$

4) $F(x)$ is the smallest such subfield.

Proof 1) and 3) are obvious
2) We need to show that any subring of $E$ containing both $F$ and $J$ also contains $F[x]$. Since $x \in R$, so is $x^n \in R$, so any element of $F[x]$ is in $R$.

4) Similar argument. (Q.E.D.)

Qd: If $F \leq E$ are fields, we say $E$ is an extension (or field extension) of $F$. $F \leq F(x) \leq E$, $F(x)$ in the extension obtained by adjoining $x$. 
FLT: There is no solution to
\[ x^n + y^n = z^n \quad \text{for} \quad n > 2, \quad x, y, z \geq 0 \text{integers} \]

It suffices to prove it for each odd prime \( p \) and \( n = 4 \).

Suppose \( x^6 + y^6 = z^6 \) for \( x, y, z > 0 \)
\[ (x^2)^3 + (y^2)^3 = (z^2)^3 \]

1847 Kummer proved FLT for many primes, e.g., all \( p < 100 \) except \( p = 37, 59, 67 \).
Theorem 10.2.5 (Kronecker)

Let \( F \) be a field and \( p(x) \in F[x] \) be nonconstant. Then there is an extension \( E \) of \( F \) and \( \alpha \in E \) s.t. \( p(\alpha) = 0 \).

Proof: Suppose \( p(x) \) is irreducible. Let \( E = F[x] / (p(x)) \) with \( \alpha = x \). Then \( p(\alpha) = 0 \). If \( p(x) \) is not irreducible, then
\[ p(x) = p_1(x) p_2(x) \cdots p_n(x) \]
where each \( p_i(x) \) is irreducible.

Let \( E = F[x] / (p_i(x)) \) for some \( i \).

And let \( \alpha = x \) as before.
\[ p(x) := \phi_1(x) \phi_2(x) \cdots \phi_m(x) = \phi_i(x) \text{ \textit{- something}} = 0 \text{ since } \phi_i(x) = 0 \quad \text{QED} \]

\underline{Def 10.2.45}: Let \( F \subseteq E \) be fields. Then \( \alpha \in E \) is \underline{algebraic over} \( F \) if \( \exists f(x) \neq 0 \) in \( F[x] \) with \( f(\alpha) = 0 \); if not, \( \alpha \) is \underline{transcendental over} \( F \).

\underline{Example}: \( \pi \) is \underline{transcendental over} \( \mathbb{Q} \).

\( e \) is \underline{algebraic} \( / \mathbb{Q} \) since \( e^3 - 17 = 0 \).

\( \alpha = \sqrt[3]{17} \) is \underline{algebraic} \( / \mathbb{Q} \) since \( \alpha^3 - 17 = 0 \).
Thm 10.2.2. Let \( F \subseteq E \) be fields and let \( \alpha \in E \) be algebraic over \( F \). Then \( F(\alpha) \) is a field and there exists a unique \( F \)-monic polynomial \( \phi(x) \in F[x] \) (the minimal polynomial of \( \alpha \)) with

1) \( \phi(\alpha) = 0 \)
2) \( \phi(x) \) is irreducible
3) if \( \psi(x) \in F[x] \) with \( \psi(\alpha) = 0 \), then \( \phi(x) \mid \psi(x) \).
Example \( F = \mathbb{Q} \) \( \rightarrow \) \( E = \mathbb{R} \)

\[
\alpha = \sqrt{2} + \frac{1}{\sqrt{2}}
\]

\[
\alpha^2 = (\sqrt{2} + \frac{1}{\sqrt{2}})^2 = 2 + 2\sqrt{2}\cdot\frac{1}{\sqrt{2}} + \frac{1}{4}
\]

\[
= 2 + 2\sqrt{32} + \frac{3}{4}
\]

\[
\alpha^3 = (\sqrt{2} + \frac{1}{\sqrt{2}})^3 = \sqrt{8} + 3\sqrt{8}\cdot\frac{1}{\sqrt{2}} + 3\sqrt{8}\cdot\frac{1}{4} + 2
\]

\[
= 2\sqrt{2} + 6\sqrt{2} + 3\sqrt{8}\cdot16 + 2
\]

\[
= 2\sqrt{2} + 6\sqrt{2} + 6\sqrt{2} + 2
\]

Note each is a paly in \( \sqrt{2} = \beta \)

\[
\alpha = \beta^3 + \beta^2
\]

\[
\alpha^2 = \beta^6 + 2\beta^5 + \beta^4
\]

\[
\alpha^3 = 2 + 2\beta^5 + \beta^4
\]

The vector space \( E = \mathbb{R} \) \( \mathbb{Q} \) has
\[ \dim 6 \quad \text{and} \quad \beta^* = 2 \]

Proof. Consider the set \( J \) of all polynomials \( g(x) \in F[x] \) with \( g(h) = 0 \). Claim:

This is an ideal. \( J \neq (0) \) because \( h \) is algebraic. Since \( F[x] \) is a PID, it is generated by some monic \( p(x) \).

Suppose \( p(x) = p_1(x) p_2(x) \), with

\[ \deg p_1, \deg p_2 < \deg p. \]

Then \( p(h) = p_1(h) \phi_2(h) = 0 \in E \).
Since \( E \) is a domain, either \( \phi_1(x) = 0 \) or \( \phi_2(x) = 0 \). Hence \( \phi_1(x) \) or \( \phi_2(x) \) is in \( J \).

This is a **CONTRADICTION**. Hence \( \phi(x) \) is irreducible. Q.E.D.

**Def 10.2.10** For \( F \subset E \), let \( x \in E \) and \( \phi(x) \) as above. The degree of \( \phi(x) \) is the degree of \( x \) over \( \mathbb{F} \), \( \deg_\mathbb{F}(x) \).

**Thm 10.2.11** Let \( F \subset E \), \( x \in E \) with minimal poly \( \phi(x) \) of degree \( n \), then
1) \( F(\alpha) \cong \mathbb{F}[x]/(p(x)) \)

2) \( \{1, x, x^2, \ldots, x^{n-1}\} \) is a basis of \( F(\alpha) \) over \( F \).

3) \( \dim_F F(\alpha) = \deg p(x) = \deg p(x) = n. \)

**Proof (1)** Consider the evaluation map \( \mathbb{F}[x] \xrightarrow{\phi} \mathbb{E} \)

defined by \( \phi(f(x)) = f(\alpha) \). It is a ring homomorphism.

Its image is \( \mathbb{F}[\alpha][x] \) by definition. 

Let kernel \( \ker \phi = \{ f(x) \in \mathbb{F}[x] : f(\alpha) = 0 \} \)

\( = (p(x)). \)

Since \( p(x) \) is irreducible, \( \mathbb{F}[x]/(p(x)) \) is a field.

So \( \mathbb{F}[\alpha] = \mathbb{F}(\alpha). \)
2) Consider
\[ S = \text{Span}\{1, x, \ldots, x^{n-1}\} \]
\[ = \{ \sum_{i=0}^{n-1} c_i x^i : c_i \in F \} \]

Since \( F[x] \) consists of polynomials in \( x \), \( S \subseteq F[x] \).

Want to \( F[x] \subseteq S \).

Let \( \beta_i \) be \( x^i \) for \( \beta_i \in F \).

\[ p(x) = x^n - \sum_{i=0}^{n-1} \beta_i x^i \]

Hence \( x^n = \sum_{i=0}^{n-1} \beta_i x^i \) in \( F \).
\[ x^{n+1} = \sum_{i=0}^{n-1} \beta_i x^i \] 

\[ = \sum_{i=0}^{n-2} \beta_i x^i + \beta_{n-1} x^{n-1} + \beta_{n-1} (\sum_{i=0}^{n-2} \beta_i x^i) \] 

\[ \in S \]

Similarly, \( x^n \in S \) for all \( m \). Hence \( F[x^j] \leq S \).

3) follows from 2).

QED