Theorem 20.1

\[ x + \langle p(x) \rangle \] is a zero of \( p(x) \)
in \( F[x] / \langle p(x) \rangle \) when \( p(x) \) is
irreducible.

Theorem 20.2

There exists a splitting field \( E \)
for \( f(x) \) over \( F \) (By induction on 20.1)

Theorem 20.3

\[ p(x) \in F[x] \] irreducible of degree \( n \), and
\[ p(a) = 0 \] for \( a \in \) extension \( E \) of \( F \)
\[ \Rightarrow \quad F(a) \cong F(x) / \langle p(x) \rangle \]

Application 1 \( \mathbb{Q}(i) \cong \mathbb{Q}[x] / \langle x^2 + 1 \rangle \)

Application 2 \( F(a) = \{ \mathbb{Q}^{-1} (c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 + \langle p(x) \rangle) \} \)
\[ = \{ c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 \mid c_i \in F \} \]
is a vector space over \( F \).

Corollary \( a \in E \supseteq F \), \( b \in E' \supseteq F \),
\[ p(a) = 0 = p(b) \]
\[ \Rightarrow \quad F(a) \cong F(b) \].
Corollary to Theorem 20.4: Splitting fields are unique up to isomorphism.

\[ f(x) = p(x)q(x) \in F[x], \quad p(x) \text{ irreducible} \]

\[ p(a) = 0 = p(b) ; \quad a \in E \cong F, \quad b \in E' \cong F \]

\[ p(x) = p_1(x)p_2(x) \text{ over } F(a) \]

\[ p_1(x) \text{ irreducible over } F(a) \]

\[ p_1(a') = 0 = \epsilon(p_1(x))(b') \]

Extend \( \epsilon : F(a,a') \to F(b,b') \)

by setting \( \epsilon(a') = b' \).
Theorem 20.5 \( \exists a \in E \ni F \) such that
\[(x-a)^2 \mid f(x) \text{ over } E \text{ iff } \deg\left(\gcd_F(f(x), f'(x))\right) > 0.\]
(\( \text{gcd over } F \text{ means "largest degree polynomial dividing both over } F." \))

Example
\[f(x) = (x^3+1)^2 \quad f'(x) = 2(x^3+1)2x\]
\[\gcd_F(f(x), f'(x)) = x^2 + 1 \quad (\text{up to a unit})\]
Thus \( f(x) \) has a multiple zero in some Extension field \( E \) of \( F \). (Illustrates converse.)
Note that \( f \) reduces over \( F \).

Theorem 20.6 \( \overline{\text{f(x) irreducible over } F[x]} \).
\[\text{char } F = 0 \Rightarrow \text{ no multiple zeros.}\]
\[\text{char } F = p \Rightarrow \text{ multiple zeros if } f(x) = g(x^p) \quad \text{for some } g(x) \in F[x].\]

\[\frac{\text{multiple zeros}}{\text{irred}} \Rightarrow \deg(\gcd_F(f(x), f'(x))) > 0\]
\[\Rightarrow f'(x) = 0\]
\[\Rightarrow\begin{cases}
  f(x) = a_0, \quad \text{char } F = 0 \quad \forall x \\
  f(x) = a_{pm}x^{p^m} + a_{p(m-1)}x^{p^{(m-1)}} + \cdots + a_p x^p + a_0, \\
  \text{char } F = p.
\end{cases}\]
\[\frac{\left(\frac{d}{dx}\left(a_{pj}x^{p^j}\right)\right)}{p!} = p!a_{pj}x^{p^j-1} = 0 \quad \text{in characteristic } p\]
Perfect fields

Fields \( F \) with

(i) \( \text{char } F = 0 \)

(ii) \( \text{char } F = p \) \( \iff \ F = F_p = \{ a^p | a \in F \} \)

Theorem 20.7 Finite fields are perfect

\( \varphi : F \rightarrow F_p \)

\[ \varphi(a) = a^p \]

\[ \varphi(a + b) = (a + b)^p = a^p + \left( \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} \right) + b^p = a^p + b^p \]

\( \ker \varphi = \{ a \in F | a^p = 0 \} = \{ 0 \} \)

\( \Rightarrow \) \( \varphi \) is 1-1.

\( \Rightarrow \) \( \varphi \) is onto since \( |F| < \infty \).

Why perfect fields?

Theorem 20.8 Over perfect fields, irreducible polynomials have no multiple zeros.

\( \text{Char } F = 0 \) \( \iff \) by Theorem 20.6

\( \text{Char } F = p \) \( \iff \) multiple zeros \( \Rightarrow \) \( f(x) = g(x^p) \)

\[ = a_n x^{p^n} + \cdots + a_1 x^p + a_0 \quad (\text{perfect}) \]

\[ = b_n x^{p^n} + \cdots + b_1 x^p + b_0 \quad (\text{char } p) \]

\[ \Rightarrow \]
Multiplicity of zeros of irreducible \( f(x) \) over \( F \)

- **Char \( F = 0 \)**: Each zero has multiplicity 1.
- **Char \( F = \mathbb{F} \)**
  - If \( |F| < \infty \)
    - Each zero has multiplicity 1.
  - If \( |F| = \infty \) and \( F^p = F \)
    - Each zero has multiplicity 1.
  - If \( |F| = \infty \) and \( F^p \subset F \)
    - \( \exists r \in \mathbb{Z}^+ \) such that each zero has multiplicity \( r \).

**Theorem 20.9**

\( f(x) \) irreducible over \( F \),
\( E \) a splitting field of \( f(x) \) over \( F \).

Then all zeros of \( f(x) \) in \( E \) has the same multiplicity.

**Proof sketch**

Let \( a, b \in E \) with \( f(a) = 0 = f(b) \).

- \( \varphi: E \rightarrow E \) automorphism
- \( \varphi: F \rightarrow F \) identity
- \( \varphi(a) = b \)

So

\[ f(x) = \varphi(f(x)) \]

\[ (x-a)^r g(x) \]

\[ (x-b)^r \varphi(g(x)) \]

Picture by Thm. 20.4
Corollary. \( f(x) \) irreducible over \( F \), \( E \) a splitting field of \( f(x) \) over \( F \). Then

\[
f(x) = a \prod_{\substack{w \in E \\ w \in \mathbb{F}}} (x-a_w)^n
\]

\( E \subset \mathbb{Z}^+ \) with

If \( F \) is perfect, then \( n = 1 \).

Remark. Non-perfect fields have unusual structure and we do not encounter them frequently.

\[
F = \mathbb{Z}_p(t) = \left\{ \frac{h(t)}{k(t)} \mid h(t), k(t) \in \mathbb{Z}_p[t], k(t) \neq 0 \right\}
\]

\( x^{p-1} \) is irreducible over \( F \)

\[
\frac{d}{dx}(x^{p-1}) = 0 \Rightarrow \text{multiple root}.
\]