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

$$\Rightarrow \quad F(a) \approx F[x]/\langle p(x) \rangle$$

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

Application 2 $\quad F(a) = \{ \varphi^{-1}(c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 + \langle p(x) \rangle) \}$

$$= \{ c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 \mid c_i \in F \}$$

is a vector space over F.

Corollary $\quad a \in E \supseteq F, \quad b \in E' \supseteq F,$

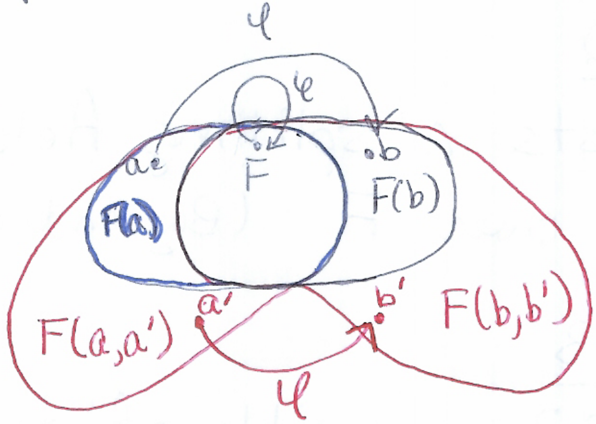
$p(a) = 0 = p(b)$

$$\Rightarrow \quad F(a) \approx F(b).$$

Corollary to Theorem 20.4 Splitting fields are unique up to isomorphism.

$f(x) = p(x)g(x) \in F[x]$, $p(x)$ irreducible

$p(a) = 0 = p(b)$; $a \in E \supseteq F$, $b \in E' \supseteq F$



$p(x) = p_1(x)p_2(x)$ over $F(a)$

$p_1(x)$ irreducible over $F(a)$

$p_1(a') = 0 = \varphi(p_1(x))(b')$

Extend $\varphi : F(a, a') \to F(b, b')$

by setting $\varphi(a') = b'$.

<u>Theorem 20.5</u> $\exists\, a \in E \supseteq F$ such that $(x-a)^2 \mid f(x)$ over E iff $\deg(\gcd_F(f(x), f'(x))) > 0$.

(gcd over F means "largest degree polynomial dividing both over F")

<u>Example</u> $f(x) = (x^2+1)^2 \qquad f'(x) = 2(x^2+1)2x$

$\gcd_F(f(x), f'(x)) = x^2+1$ (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.

<u>Theorem 20.6</u> $f(x)$ irreducible over $F[x]$.

$\text{char } F = 0 \Rightarrow$ no multiple zeros.

$\text{char } F = p \Rightarrow$ multiple zeros iff $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

$$\text{multiple zeros} \overset{20.5}{\Rightarrow} \deg(\gcd_F(f(x), f'(x))) > 0$$

$$\overset{f \text{ irred}}{\Rightarrow} f'(x) = 0$$

$$\Rightarrow \begin{cases} f(x) = a_0, & \text{char } F = 0 \quad ⨳ \\ f(x) = a_{pm}x^{pm} + a_{p(m-1)}x^{p(m-1)} + \cdots + a_p x^p + a_0, & \text{char } F = p. \end{cases}$$

$\frac{d}{dx}(a_{pj}x^{pj}) = pj\,a_{pj}x^{pj-1} = 0$ in characteristic p

Perfect fields

Fields F with

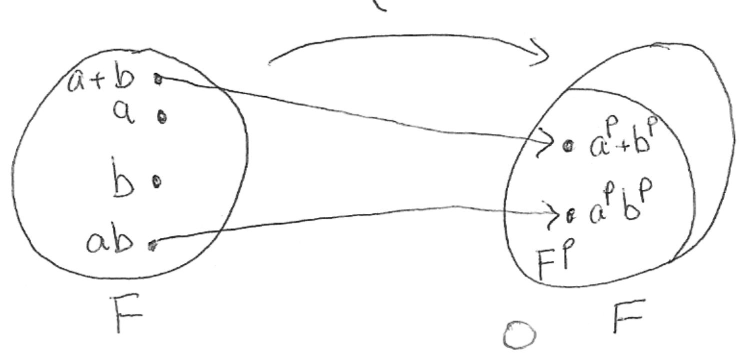
(i) $\operatorname{char} F = 0$

(ii) $\operatorname{char} F = p$ + $F = F^p = \{a^p \mid a \in F\}$

Theorem 20.7 Finite fields are perfect

$\varphi : F \to F^p$

$\varphi(a) = a^p$



$$\varphi(a+b) = (a+b)^p = a^p + \overset{0}{\cancel{\binom{p}{1}}} a^{p-1} b + \cdots + \overset{0}{\cancel{\binom{p}{p-1}}} a b^{p-1} + b^p$$
$$= a^p + b^p$$

$\operatorname{Ker} \varphi = \varphi^{-1}(0) = \{a \in F \mid a^p = 0\} = \{0\}$.

$\Rightarrow \varphi$ 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.

$\operatorname{char} F = 0$: by Theorem 20.6

$\operatorname{char} F = p$: multiple zeros $\Rightarrow f(x) = g(x^p)$

$$= a_n x^{pn} + \cdots + a_1 x^p + a_0 \overset{(\text{perfect})}{=} b_n^p x^{pn} + \cdots + b_1^p x^p + b_0^p \overset{(\text{char } p)}{=} (b_n x + \cdots + b_1 x + b_0)^p$$

#

Multiplicity of zeros of irreducible $f(x)$ over F

Char $F = 0$ — Each zero has multiplicity 1.

Char $F = p$

- $|F| < \infty$ — Each zero has multiplicity 1

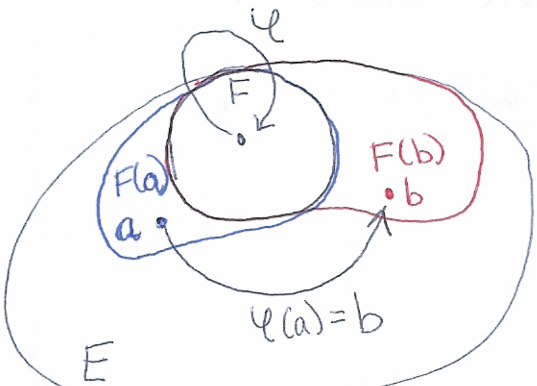
perfect fields

- $|F| = \infty$ and $F^p = F$ — Each zero has multiplicity 1

- $|F| = \infty$ 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 $f(a) = 0 = f(b)$



Picture by Thm. 20.4

$\varphi : E \to E$ automorphism

$\varphi : F \to F$ identity

$\varphi(a) = b$

so $f(x) = \varphi(f(x))$

$$\begin{array}{ccc} f(x) & = & \varphi(f(x)) \\ \| & & \| \\ (x-a)^r g(x) & & (x-b)^r \varphi(g(x)) \end{array}$$

Corollary $f(x)$ irreducible over F, E a splitting field of $f(x)$ over F. Then $\exists\, n \in \mathbb{Z}^+$ with

$$f(x) = \underbrace{a}_{\in F} \underbrace{(x-\underset{\sim}{a_1})^n (x-\underset{\sim}{a_2})^n \cdots (x-\underset{\sim}{a_t})^n}_{\in E,\ \text{distinct}}$$

If F is perfect, then $n = 1$.

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

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

$x^p - t$ is irreducible over F

$\frac{d}{dx}(x^p - t) = 0 \Rightarrow$ multiple root.