Math 5402

4/13/20

Week 12

Study guide for test 2
is on the website.
Covers ≤ 13.2
See website for HW covered

13.4 continued...

<u>Def:</u> If K is an algebraic extension of F and is the splitting field over F for a collection of polynomials in $F[x]$, then K is called a <u>normal extension</u> of F.

Ex: $F = \mathbb{Q}$

$K = \mathbb{Q}(\sqrt{2})$

K is the splitting field of x^2-2 over F, so K is a normal extension of F.

Ex: Consider x^4+4 over $\mathbb{Q}$.

Note that

$$x^4+4 = \underbrace{(x^2+2x+2)}\underbrace{(x^2-2x+2)}$$

Eisenstein with $p=2$ shows these are irreducible over $\mathbb{Q}$

roots of these polys are $\pm 1 \pm i$, ie $1+i, 1-i, -1+i, -1-i$.

Let $K = \mathbb{Q}(i)$

$K = \mathbb{Q}(i)$ is the splitting field of $x^4 + 4$ over $\mathbb{Q}$.

$$
\begin{tikzcd}
K = \mathbb{Q}(i) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}
\qquad
\boxed{\min_{i,\mathbb{Q}}(x) = x^2 + 1}
$$

$$\mathbb{Q}(i) = \{ a + bi \mid a, b \in \mathbb{Q} \}$$

Theorem (Thm 27 in the book)

Let $\varphi : F \to F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$.

$$\boxed{f(x) = \sum_{k=0}^{n} a_k x^k \longmapsto f'(x) = \sum_{k=0}^{n} \varphi(a_k) x^k}$$

Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'.

Then the isomorphism φ extends to an isomorphism $\sigma : E \to E'$ where $\sigma|_F = \varphi$ [ie $\sigma(x) = \varphi(x)\ \forall x \in F$]

$$\begin{array}{ccc}
\sigma : E & \longrightarrow & E' \\
| & & | \\
\varphi : F & \longrightarrow & F'
\end{array}$$

pg 5

Let $F = F'$, $f(x) = f'(x)$, φ = identity function in the previous thm, we get:

<u>Corollary</u>: Any two splitting fields for a polynomial $f(x) \in F[x]$ over F are isomorphic.

$\boxed{\text{commentary:}}$

$$K = F[x]/(f(x)) \cong F(\theta)$$

θ is a root of f

$$\begin{array}{c} K \\ | \\ F \end{array}$$

irr. poly $= f(x)$

Def: Let F be a field and let $f(x) \in F[x]$. Let E be a splitting field for $f(x)$. In E we can factor f into

$$f(x) = c(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct elements from E, and $c \in F$, and $n_i \geq 1$ for all i.

We say that α_i is a <u>multiple root</u> of f if $n_i \geq 2$, otherwise α_i is called a <u>simple root</u> if $n_i = 1$.

n_i is called the <u>multiplicity</u> of α_i

<u>Def:</u> Let $f(x) \in F[x]$.

We say that f is <u>separable</u> if it has no multiple roots in a splitting field, ie all its roots are simple. Otherwise we call f <u>inseparable</u>.

<u>Ex:</u> $x^2 - 2$ is separable over $\mathbb{Q}$ since

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

<u>Ex:</u> $x^4 - 4x^2 + 4$ is inseparable over $\mathbb{Q}$ since

$$x^4 - 4x^2 + 4 = (x^2 - 2)(x^2 - 2)$$
$$= (x - \sqrt{2})^2 (x + \sqrt{2})^2$$

<u>Def:</u> Given

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $f(x) \in F[x]$, define the derivative of f to be

$$D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$$

<u>Note:</u> $D_x f(x) \in F[x]$

Also, here the coefficients from the powers are positive integers so can be embedded into the field. Ex: $5 = 1+1+1+1+1$

where 1 is the identity of F

D_x will satisfy the usual properties like

$$D_x[f(x)+g(x)] = D_x f(x) + D_x g(x)$$

$$D_x[f(x)g(x)] = D_x f(x)\cdot g(x) + D_x g(x)\cdot f(x)$$

<u>Proposition:</u> Let F be a field and $f(x) \in F[x]$. Let E be a splitting field for $f(x)$ over F. Then $f(x)$ has a multiple root α iff α is also a root of $D_x f(x)$.

So, $f(x)$ is seperable iff $f(x)$ and $D_x f(x)$ share no common roots.

proof:

($\Rightarrow$) Suppose α is a multiple root of $f(x)$.

Then, $f(x) = (x-\alpha)^n g(x)$ where $g(x) \in E[x]$ and $n \geq 2$.

$n-1 \geq 1$

Then

$$D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$$

$$D_x f(\alpha) = n(\alpha-\alpha)^{n-1} g(\alpha) + (\alpha-\alpha)^n D_x g(\alpha) = 0$$

So, α is a root of $D_x f(x)$.

($\Leftarrow$) Suppose α is a root of $f(x)$ and $D_x f(x)$.

pg 11

Then, $f(x) = (x-\alpha)h(x)$
where $h(x) \in E[x]$.

Thus,

$$D_x f(x) = h(x) + (x-\alpha) D_x h(x).$$

We know $D_x f(\alpha) = 0$.

So,

$$0 = h(\alpha) + \underbrace{(\alpha-\alpha) D_x h(\alpha)}_{0}$$

Thus, $h(\alpha) = 0$.

So, $h(x) = (x-\alpha)h_1(x)$
where $h_1(x) \in E[x]$.

Thus, $f(x) = (x-\alpha)h(x)$
$= (x-\alpha)^2 h_1(x)$.

So, α is a multiple root of f. $\blacksquare$

Ex: Let p be a prime, pg 12

Consider $x^{p^n} - x$ over $\mathbb{Z}_p$.

$\boxed{\text{Ex: } x^{2^3} - x = x^8 - x \text{ over } \mathbb{Z}_2}$

Then,

$$D_x[x^{p^n} - x] = \bar{p}^n x^{p^n - 1} - \bar{1}$$
$$= \bar{0}^n x^{p^n - 1} - \bar{1}$$
$$= \overline{-1} \neq \bar{0} \text{ in } \mathbb{Z}_p.$$

Since $D_x[x^{p^n} - x]$ has no roots, it has no common roots with $x^{p^n} - x$ in a splitting field.

So, $x^{p^n} - x$ is separable over $\mathbb{Z}_p$

Idea later:

E ← splitting field for $x^{p^n}-x$

$\mathbb{Z}_p$

Then E will be a finite field of size p^n

$$x^{p^n}-x = x\left[x^{p^n-1}-1\right]$$