

9/3/07

p.551 #6, 7

p.566 #1, 4

Recall A polynomial $p(x) \in F[x]$ is separable if no multiple roots, in a split field.

Ex In char 0 all irreducibles are separable.

Thm Every irreducible over a finite field is separable.

Proof Suppose $p(x)$ is irreducible & inseparable. Then $p'(x) = 0$

Thus

$$p(x) = a_0 + a_1 x^p + a_2 x^{2p} + \dots \text{ so } p(x) = q(x^p) \text{ where}$$

$$q(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

Now each coef is a p^m power. Thus $a_i = b_i^p$

$$\text{Thus } q(x) = b_0^p + b_1^p x + b_2^p x^2 + \dots + b_m^p x^m$$

$$p(x) = b_0^p + b_1^p x^p + b_2^p x^{2p} + \dots + b_m^p x^{mp} = (b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m)^p \quad \neq !!$$

Thus inseparable polynomials occur only over infinite fields of characteristic p in which not every element is a p^m power.

Def A field is perfect if every elt is a p^m power.

Also char 0 fields are perfect.

Cor Any irreducible over a perfect field is separable.

Finite Fields

Consider $f(x) = x^{p^n} - x$ over \mathbb{F}_p . $f'(x) = -1$ so it is separable. Take $\alpha \in \mathbb{F}$.

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be roots

$$(\alpha_1 + \alpha_2)^{p^n} = \alpha_1^{p^n} + \alpha_2^{p^n} = \alpha_1 + \alpha_2$$

$$\alpha_1 \alpha_2^{p^n} = \alpha_1 \alpha_2$$

$$\alpha_1 \alpha_2 \alpha_3^{p^n} = \alpha_1 \alpha_2 \alpha_3$$

Cor. The splitting field of $x^{p^n} - x$ over \mathbb{F}_p is the unique finite field of order p^n up to \cong .

Recall $p(x)$ irred, insep $\Rightarrow p(x) = p_1(x^{p^k})$

Suppose $p(x)$ inseparable. Then $p(x) = p_2(x^{p^2})$ so $p(x) = p_2(x^{p^2})$

Eventually $p(x) = p_r(x^{p^r})$ where $p_r(x)$ is irreducible, separable

Def. The degree of $p_{sep}(x) = p_r(x)$ is the separable degree $\deg_s(p(x))$,

p^k is the inseparable degree $\deg_i(p(x))$

Remark 1. $p(x)$ separable \iff inseparable degree = 1

$$2. \deg p(x) = \deg_s p(x) \deg_i p(x)$$

Def An extension K/F is separable if every element of K is the root of a separable polynomial.
 (\iff all min polys are separable)
 Else say K/F is inseparable.

Ex Every finite extension of a perfect field is separable.
 \iff min polys are separable

GALOIS THEORY

Def

- Field autos
- $\text{Aut}(K/F)$

Result A Let $\alpha \in K/F$ algebraic, $\sigma \in \text{Aut}(K/F)$
 Then $\sigma(\alpha)$ has same minimal poly.

Prop Let $H \leq \text{Aut } K$. Then $K^H = \{ \alpha \in K \mid \sigma(\alpha) = \alpha \forall \sigma \in H \}$
 is a subfield, the fixed field of H

Prop The correspondence

| | | |
|----------|---------------|-------------|
| group | \rightarrow | fixed field |
| subfield | \rightarrow | group |

Reverses inclusions.

EX1 $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

EX2 $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$

Theorem Let $f(x) \in F[x]$ w/ spl. field E . Any $\cong \varphi: F \rightarrow F'$ extends to an $\cong \tilde{\varphi}: E \rightarrow E'$, where E' is a spl. field of poly $\varphi(f(x))$.

Moreover the # of such extensions $\tilde{\varphi}$ is $\leq [E:F]$ w/ equality iff $f(x)$ is separable.

Proof Induction, add 1 root.

Example $f(x) = x^2 - 2$ $F = \mathbb{Q}$ $\varphi = \text{id}$
 $\text{id}: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$
 $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$

Example $f(x) = x^3 - 2$ $[E:\mathbb{Q}] = 6$
Thus all 6 perms of roots occur.

Prop Let E/F be spl. field of $f(x)$. Then

$$|\text{Aut}(E/F)| \leq [E:F]$$

w/ equality iff $f(x)$ separable

Def. Let K/F be finite.
 K is Galois \iff K/F is a Galois extension.
 if $|Aut(K/F)| = [K:F]$.
 If so, $Gal(K/F) := Aut(K/F)$ is Galois group.

Exs \rightarrow 1. Any splitting field of a separable poly.
 2. Not $\mathbb{Q}(\sqrt[3]{2})$
 Only exs!!

Def. Let $f(x)$ be separable \iff the Galois group of $f(x)/F$ is the Galois group of the split field of $f(x)$.

Ex $f(x) = x^2 - 2 / \mathbb{Q}$ $Gal \cong \mathbb{Z}_2$

Ex $f(x) = (x^2 - 2)(x^2 - 3)$ $Gal \cong V$

Ex $x^3 - 2$ $Gal \cong S_3$

$\mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$

$\sqrt{2} \rightarrow \begin{matrix} \sqrt{2} \\ \sqrt{2}\rho \\ \sqrt{2}\rho^2 \end{matrix}$

$\rho \rightarrow \rho \cup \rho^2$

since $x^2 + x + 1 = (x - \rho)(x - \rho^2)$

Compositum