

3/29/07

Recall Given $p(x) \in F[x]$, \exists a unique (up to \cong) splitting field in which $p(x)$ factors into linear terms. If $\deg p(x) = n$, this is at most $n!$ degree extension. Such extensions are called normal.

Algebraic Closures

Def \bar{F} is an algebraic closure of F if \bar{F} is an algebraic extension of F and every $f(x) \in F[x]$ splits in \bar{F} .

Def K is algebraically closed if every polynomial in $K[x]$ splits in K .

Remark

1. Not obvious such fields exist
2. Assuming they do then K alg closed $\iff K = \bar{K}$.

Prop. \bar{F} is algebraically closed.

Proof Let $f(x) \in \bar{F}[x]$ with $f(x) \neq 0$. Then $\bar{F}(x) : \bar{F}$ is algebraic so $\bar{F}(x) = F$ is algebraic so α satisfies a polynomial in $F[x]$ so $\alpha \in \bar{F}$.

The Algebraic Closures Exist

Proof Start with F . For every monic polynomial $f(x) \in F[x]$ w/ degree > 0 , choose a variable x_f .

Consider $F[x_1, \dots, x_n]$

Let $I = (\text{all } f(x_f))$

Lemma $1 \notin I$.

Proof Suppose $g_1 f_1(x_1) + \dots + g_n f_n(x_n) = 1$
where g_i 's are poly in x_{f_i} .

Let $x_i = x_{f_i}$ $i=1, 2, \dots, n$

Let x_{n+1}, \dots, x_m be rest of variables in the g_i 's.

$$g_1(x_1, \dots, x_m) f_1(x_1) + \dots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$$

Extend to a field F' containing a root α_i of $f_i(x)$.

Set $x_i = \alpha_i$, $x_{n+1}, \dots, x_m = 0$ to get $0 = 1 \notin I$

Thus I is in a maximal ideal M . Let

$K = F[x_1, \dots, x_n] / M$ is a field,
containing F , and see that each f has a root
namely \bar{x}_f .

Now repeat on K_1 to get K_2 .

$$F \subset K_0 \subset K_1 \subset K_2 \subset \dots$$

Let $K = \bigcup K_i$ a field, all poly have a root.

$$\text{Thus } K = \bar{K}.$$

So F lies inside an algebra closed field.

Lemma Let $F \subset K = \bar{K}$. Then $\{ \alpha \in K \mid \exists \text{ poly } f \in F[x] \text{ s.t. } f(\alpha) = 0 \}$ is an algebraic closure of F , unique up to \cong .

Proof

1. \bar{F} is algebraic over F . Every poly ^{in $F[x]$} factors completely over K but this factorization is in \bar{F} .

Example 1, (FTA) $\mathbb{C} = \bar{\mathbb{Q}}$

2. Thus $\bar{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \mid \exists \text{ poly } f \in \mathbb{Q}[x] \text{ s.t. } f(\alpha) = 0 \}$

SEPARABLE EXTENSIONS

Def A polynomial is separable if it has no multiple roots
otherwise inseparable.

Rem Do not need to specify a field extension.

Example

$F = \mathbb{F}_2(t)$ rational functions, roots in \mathbb{F}_2

$f(x) = x^2 - t$ is irreducible,

Consider an extension field $F(\sqrt{t})$.

Then $(x - \sqrt{t}) \mid (x - \sqrt{t}) = x - t$

so inseparable.

Prop $f(x)$ has a multiple root α iff α is a
root of $f'(x)$. Thus

$f(x)$ is separable iff $\gcd(f(x), f'(x)) = 1$.

Proof Product rule

Rem When not separable,

min poly of $\alpha \mid$ both f & f'

Examples 1. $x^2 - t = f(t)$
 $f'(x) = 2x = 2(x - \sqrt{t}) \equiv 0$

2. $x^{p^n} - x$ over \mathbb{F}_p $f'(x) = -1$.

3. x^{n-1} separable, in characteristic 0.

4. $\text{char } F = p \mid n$ then x^{n-1} not separable.

5. $\text{char } F = 0 \Rightarrow$ any irreducible is separable.
 Thus separable \Leftrightarrow product of distinct irreducibles.

Proof $\deg f(x) = n$ $\deg f'(x) = n-1$ \leftarrow requires $\text{char } F$
 Can't have a multiple irreducible

Frobenius Maps

Lemma $\text{char } F = p$ $(a+b)^p = a^p + b^p$
 $(a^p)^p = a^{p^2}$

Called Frobenius endomorphism

Cor In a finite field all elements are p^m powers.

Prop Any irreducible over finite field is separable

Proof Suppose not. Then $p'(x) = 0$

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

$$= a_0 + a_1 x^p + a_2 x^{2p} + \dots$$

$$= q(x^p) = (a_0 + a_1 x^p + a_2 x^{2p})^p$$

*

* Irreducible occurs only in infinite fields char p

Def. char $K = p$ is perfect if p^m power map onto

Also char 0 called perfect.