

Announcements

Midterm course feedback form (see email)

HW6 posted (due Wed. 3/12)

Separable Extensions (cont.)

Recall: f is separable if all its roots/ K are simple. Otherwise it's inseparable.

Separability Criterion: Let $f(x) \in F[x]$.

a) α is a multiple root of $f \iff \alpha$ is a root of f and Df

b) $f(x)$ is separable $\iff \gcd(f, Df) = 1$

Thm: If

a) $\text{char } F = 0$ or

b) F is finite,

then every irred. $f(x) \in F[x]$ is separable.

Last time: proved a) by noting that
 $\deg(Df) = \deg(f) - 1$, so if f irred,
 $\gcd(f, Df) = 1$

Q: Why do we need $\text{char}(F) \neq 0$?

A: To show $\deg Df = n-1$. In fact, the above proof holds for any f s.t. Df isn't the 0-poly.

e.g. $f(x) = x^2 + t \in \mathbb{F}_2(t)[x]$

$$Df = 2x = 0 \in \mathbb{F}_2(t)[x]$$

$$\gcd(f, Df) = x^2 + t$$

Note: this doesn't guarantee that f is not sep.

Let $\text{char } F = p$.

Def: The Frobenius map $\psi: F \rightarrow F$ is

$$\text{Frob}(a) = \psi(a) \mapsto a^p$$

Prop: a) ψ is an inj. homom.

b) If F is finite, ψ is an isom.

$$\text{Pf: } \varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

$$\varphi(a+b) = (a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \dots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p = \varphi(a) + \varphi(b)$$

Injectivity: $\ker \varphi$ is an ideal; hence $\{0\}$ or F , but $\varphi(1) = 1$

b) F finite, φ injective $\Rightarrow \varphi$ bijective

□

Note: φ is not surj. if $F = \mathbb{F}_p(t)$, since $t \notin \text{im } \varphi$.

Pf of b): actually, we will prove:

If φ is onto, every irred. $f \in F[x]$ is sep.

Let $f(x) \in F[x]$ be irred., inseparable.

Then by the Sep. Crit., $\gcd(f, Df) \neq 1$, so $Df = 0$.

Therefore, $f(x)$ has the form

$$\begin{aligned} f(x) &= a_n x^{pn} + a_{n-1} x^{p(n-1)} + \dots + a_1 x^p + a_0 \\ &= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \dots + b_1^p x^p + b_0^p \quad (b_i := \varphi^{-1}(a_i)) \\ &= (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0)^p \quad (\varphi \text{ is homom.}) \end{aligned}$$

so f is reducible, a contradiction.

□

Def: F is perfect if:

a) $\text{char } F = 0$ or

b) $\text{char } F = p$ and φ is onto \leftarrow i.e. an isom.

Cor: If F perfect, every irred. $f \in F[x]$ is sep.

Perfect fields include:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc. (anything of char 0)

finite fields

alg. closed fields (e.g. $\overline{\mathbb{F}_p}$) since

$\varphi^{-1}(a)$ is a root of $x^p - a$

Finite fields

Prop: Let $n > 0$, p : prime. There exists a finite field w/ p^n elts., unique up to isom.

PF: Existence

$$\text{Let } f(x) := x^{p^n} - x \in \mathbb{F}_p, \quad F := S_{\mathbb{F}_p}(f) =: \mathbb{F}_{p^n}$$

Since \mathbb{F}_p is sep., f has p^n distinct roots in F
and such a root α satisfies $\alpha^{p^n} = \alpha$

These roots form a subfield of F :

$$(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta, \quad (\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1},$$

$$(\alpha + \beta)^{p^n} = \underbrace{\text{Frob}(\dots(\text{Frob}(\alpha + \beta)\dots))}_n$$

$$= \text{Frob}(\dots(\text{Frob}(\alpha)\dots) + \text{Frob}(\dots(\text{Frob}(\beta)\dots))$$

$$= \alpha^{p^n} + \beta^{p^n}$$

So by minimality, $F = \{\text{roots of } x^{p^n} - x\}$

$$|F| = p^n, \quad [F : \mathbb{F}_p] = n$$

Let K be any field of order p^n . Then $\text{char } K = p$,
 $[K : \mathbb{F}_p] = n$.

We have $|K^\times| = |K| - 1 = p^n - 1$, so if $\alpha \in K$,

$$\alpha^{p^n - 1} = 1, \quad \text{so} \quad \alpha^{p^n} = \alpha, \quad \alpha \text{ is a root of } x^{p^n} - x.$$

Since K has $|K| = p^n$ roots of this poly, it is the splitting field of $x^{p^n} - x$ over \mathbb{F}_p , which is unique up to isom.

□