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 $\iff$ α is a root of f and Df

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

Thm: If

a) 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 $\mathrm{char}(F) = 0$?

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

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

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

Let $\mathrm{char}\, F = p$.

Def: The Frobenius map $\varphi: F \to F$ is

$$\mathrm{Frob}(a) = \varphi(a) \mapsto a^p$$

Prop: a) φ is an inj. homom.

b) If F: finite, φ is an isom.

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

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

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

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

$\square$

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

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., insep.

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

Therefore, $f(x)$ has the form

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

$$= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p \qquad (b_i := \varphi^{-1}(a_i))$$

$$\overset{*}{=} (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)^p \qquad (\varphi \text{ is homom.})$$

so f is reducible, a contradiction.

$\square$

* Justification below

Def: F is <u>perfect</u> if:

a) char $F = 0$ or

b) char $F = p$ and φ is onto ← 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 $x^p - a$

<u>Finite fields</u>

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

Pf: Existance

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

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

*Justification: $Df = p^n x^{p^n - 1} - 1 = -1$, which has no roots

These roots form a subfield of F:

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

$$(\alpha+\beta)^{p^n} = \underbrace{\mathrm{Frob}(\cdots(\mathrm{Frob}}_{n}(\alpha+\beta)\cdots)$$

$$= \mathrm{Frob}(\cdots(\mathrm{Frob}(\alpha)\cdots) + \mathrm{Frob}(\cdots(\mathrm{Frob}(\beta)\cdots)$$

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

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

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

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

We have $|K^\times| = |K| - 1 = p^n - 1$, so if $\alpha \in K$, $\alpha^{p^n - 1} = 1$, so $\alpha^{p^n} = \alpha$, α 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. $\square$

* Proof 1: $g(x) := b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$ is an elt. of the field $F(x)$, which has characteristic p.

The Frobenius map φ on this field is a homomorphism, and we have

$$\begin{aligned}\varphi(g) &= \varphi(b_n x^n) + \varphi(b_{n-1} x^{n-1}) + \cdots + \varphi(b_1 x) + \varphi(b_0) \\ &= b_n^p x^{np} + b_{n-1}^p x^{(n-1)p} + \cdots + b_1^p x^p + b_0^p \\ &= f\end{aligned}$$

$\square$

Proof 2: Consider the expression

$$(c_1 + c_2 + \cdots + c_n)^p,$$

of which $(g(x))^p$ is a special case.

The coefficient of the monomial $c_1^{e_1} \cdots c_n^{e_n}$ is the multinomial coefficient

$$\binom{p}{e_1, e_2, \ldots, e_n} = \frac{p!}{e_1! \cdots e_n!},$$

and unless all but one e_i is 0, this is divisible by p.

Therefore, $(c_1 + c_2 + \cdots + c_n)^p \equiv c_1^p + \cdots + c_n^p \pmod p$