Announcements:

Midterm 1 graded

Median 46/70

Mean: 45.5/70

Std. dev: 11.2

Q1: 76%

Q2: 84%

Q3: 69%

Q4: 36%

Q5: 64%

Gradelines:

A-/A: 50 to 70 (out of 70)

B+/B/B-: 32 to 50 $-\varepsilon$

C+/C/C-: 14 to 32 $-\varepsilon$

D+/D/D-: 4 to 13 $-\varepsilon$

Sol'ns posted to website

$\underbrace{\text{"Where do I stand"}}_{\text{disclaimers!}}$ spreadsheet posted to website

Separable extensions

Let $f(x) \in F[x]$, monic; over $K = Sp_F f$, we have

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

distinct

n_i: multiplicity of α_i

α_i is simple if $n_i = 1$

α_i is multiple if $n_i > 1$

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

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

$$x^n - p = (x - \sqrt[n]{p})(x - \zeta_n \sqrt[n]{p}) \cdots (x - \zeta_n^{n-1} \sqrt[n]{p})$$

prime

$$x^2 + 1 = (x+i)(x-i)$$

$$x^2 - 1 = (x+1)(x-1)$$

all separable

Non-ex:

a) $x^2+2x+1 = (x+1)^2 \in \mathbb{Q}[x]$

-1 is a multiple root

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

irred. by Eisenstein, using the prime $t \in \underbrace{\mathbb{F}_2[t]}_{\text{UFD}}$

or rat'l root thm. for similar reasons

Let $K = \mathrm{Sp}\, f$, and let $\alpha \in K$ be a root of x^2+t i.e. $\alpha^2 = t$

$(x-\alpha)^2 = x^2 - 2\alpha x + t = x^2+t$

So f is <u>not</u> separable

Thm: If

a) char $F = 0$ or

b) F is finite,

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

Def: The derivative of $f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x]$ is

$$Df(x) = n a_n x^{n-1} + \dots + 2a_2 x + a_1 \in F[x]$$

No calculus needed! Product/chain rules hold as usual

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 $\iff$ $\gcd(f, Df) = 1$

Pf: a) $\Rightarrow$) $f(x) = (x-\alpha)^n g(x)$ $\quad n \geq 2$

$$Df = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n Dg$$
$$= (x-\alpha)\left[n(x-\alpha)^{n-2} g(x) + (x-\alpha)^{n-1} Dg\right] \Rightarrow Df(\alpha) = 0$$

$\Leftarrow$) $f(x) = (x-\alpha)h(x)$

$$Df = h(x) + (x-\alpha)Dh(x)$$

$$0 = Df(\alpha) = h(\alpha) + (\alpha-\alpha)Dh(\alpha) \Rightarrow h(\alpha) = 0 \Rightarrow (x-\alpha)^2 \mid f.$$

b) Will show for $p, q \in F[x]$ that

$\gcd(p,q) = 1 \iff p, q$ have no common roots in an ext'n field K where they split completely

Case p, q have common root α: then p, q are both divisible by $m_{\alpha,F}(x)$

Case no common root: If $\gcd(p,q) = r(x) \in F[x]$ nonconst. then any root of $r(x)$ in K is a common root of p & q. $\square$

Pf of Thm, part a):

Let char $F = 0$, and $f \in F[x]$.

Let $n := \deg f$

$n = 1$: clear, so assume $n \geq 2$

Then $\deg(Df) = n-1$ (since $0 = \operatorname{char} F \nmid n$)

So $g := \gcd(f, Df)$ has degree $< n \Rightarrow$ proper divisor of f

Since f is irred$/F$, g is a unit, so by the Sep. Crit., f is separable. $\square$

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

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

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 Thm, part 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

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

so f is reducible, a contradiction.

$\square$