Math 491, Monday, April 13 Finite Fields

Mon - 22

Tue - 22 Bring Your Pet To Class Day

Thu - 22

Fri - 23, RQ

Mon - Problems
Sage 22

Office Hours
- Regular Times (Pacific)

---

derivative

<u>Theorem</u> f is seperable polynomial $\iff$ f & f' are relatively prime

<u>"Proof"</u> $f = (x-2)^2 (x+1)$ (not seperable)

$f' = (x-2)^2 \frac{d}{dx}(x+1) + \frac{d}{dx}(x-2)^2 (x+1)$

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

common factor

Theorem $|F| = p^n$, finite field $\Rightarrow$ F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$

Proof $f = x^{p^n} - x$

$f' = p^n x^{p^n - 1} - 1$

$= 0 x^{p^n - 1} - 1$ $\quad$ char$(\mathbb{Z}_p) = p$

$= -1$

So f & f' are relatively prime $\Rightarrow$ f seperable

$R =$ set of all roots of $x^{p^n} - x$ in splitting field

$|R| = p^n$ (f seperable & degree p^n)

R is a field (all by itself)

Closure?

$r_1, r_2 \in R$ know $r_1^{p^n} - r_1 = 0 \longrightarrow r_1^{p^n} = r_1$

$r_2^{p^n} - r_2 = 0 \longrightarrow r_2^{p^n} = r_2$

Is $r_1 r_2 \in R$? $(r_1 r_2)^{p^n} = r_1^{p^n} r_2^{p^n} = r_1 r_2 \longrightarrow r_1 r_2$ root of $x^{p^n} - x$

Is $r_1 + r_2 \in R$? $\underbrace{(r_1+r_2)^{p^n} = r_1^{p^n} + r_2^{p^n}}_{\text{Freshman's Dream}} = r_1 + r_2 \longrightarrow r_1 + r_2$ root of $x^{p^n} - x$

So R is a field w/ <u>all</u> the roots of $x^{p^n} - x$ and so must be the <u>smallest</u> field with all the roots.

So R is a splitting field of $x^{p^n} - x$ of order p^n.

Grab any other field of order p^n, it too will be a splitting field of $x^{p^n} - x$, and splitting fields are unique

"<u>The</u> field of order p^n."

<u>Sub fields</u>

<u>Fact</u> F field of order p^n, K subfield

$\iff |K| = p^m$, with $m \mid n$.

<u>Ex</u> $|F| = p^6$ subfields have order p^1, p^2, p^3, p^6 (<u>not</u> p^4, p^5)

$\Rightarrow$ $|F| = p^n$, K subfield

$\mathrm{char}(F) = p \Rightarrow \mathrm{char}(K) = p$ (both contain $\mathbb{Z}_p$)

$\Rightarrow |K| = p^m$ for some m (OR, K subgroup F <u>additively</u> Lagrange's Theorem)

then $[F:\mathbb{Z}_p] = [F:K][K:\mathbb{Z}_p]$

$n = [F:K]\, m \Rightarrow m \mid n$

$$\begin{array}{c|c} & F \\ n & | \\ & K \\ & | \quad m \\ & \mathbb{Z}_p \end{array}$$

$\Leftarrow$ Assume $|F| = p^n$, $m \mid n$, create a subfield of order p^m

Algebra $\quad n = ms$

$$p^n - 1 = p^{ms} - 1 = (p^s)^m - 1$$

$$= \underline{\underline{(p^s - 1)}}\left(\underline{(p^s)^{m-1}} + \underline{(p^s)^{m-2}} + (p^s)^{m-3} \cdots + (p^s)^1 + 1\right)$$

$$= (p^s)^m + \cancel{(p^s)^{m-1}} + \cdots + \cancel{(p^s)^2} + \cancel{p^s}$$
$$- \cancel{(p^s)^{m-1}} - \cdots - \cancel{(p^s)^2} - \cancel{p^s} - 1 = (p^s)^m - 1$$

$$x^{p^n} - x = x\left(x^{p^n - 1} - 1\right)$$

$$= x\left(x^{(p^s - 1)(\ )} - 1\right)$$

$$= x\left(x^{(p^m - 1)\ell} - 1\right)$$

$$= x\left(\left(x^{p^m - 1}\right)^\ell - 1\right)$$

switch s & m

$$\ell = (p^m)^{s-1} + (p^m)^{s-2} + \cdots + p^m + 1$$

$= x\,(x^{p^m-1}-1)\left((x^{p^{m-1}})^{l-1} + (x^{p^{m-1}})^{l-2} + \cdots + (x^{p^{m-1}})^1 + 1\right)$

So $x(x^{p^m-1}-1) = x^{p^m} - x$ is a factor of $x^{p^n}-x$

So the roots of $x^{p^m}-x$ are roots of $x^{p^n}-x$

(when $m|n$) $\Rightarrow$ splitting field of $x^{p^m}-x$ is a subfield of F with order p^m

Calculus geometric series

$$\frac{x^k-1}{x-1} = x^{k-1} + x^{k-2} + \cdots + x^1 + 1$$

$$\frac{1}{1-r} \qquad \frac{a}{1-r}$$