

Math 491, Monday, April 13 Finite Fields

Mon - 22

Office Hours

Tue - 22 Bring Your Pet
To Class Day

- Regular Times (Pacific)

Thu - 22

Fri - 23, RQ

Mon - Problems
Sage 22

Theorem

f is separable_n $\iff f \neq f'$ are relatively prime
polynomial

"Proof"

$$f = (x-2)^2(x+1) \quad (\text{not separable})$$

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

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

derivative

common factor

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

Proof

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

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

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

$$= -1$$

So $f \nmid f'$ are relatively prime $\Rightarrow f$ separable

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

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

R is a field (all by itself)

Closure?

$r_1, r_2 \in R$ Know $r_1^{p^n} - r_1 = 0 \rightarrow r_1^{p^n} = r_1$
 $r_2^{p^n} - r_2 = 0 \rightarrow r_2^{p^n} = r_2$

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

Is $r_1 + r_2 \in R$? $(r_1 + r_2)^{p^n} \stackrel{\text{Freshman's Dream}}{=} r_1^{p^n} + r_2^{p^n} = r_1 + r_2 \rightarrow r_1 + r_2$ root of $X^{p^n} - X$

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

"The field of order p^n ."

Sub fields

Fact F field of order p^n , K subfield
 $\Leftrightarrow |K| = p^m$, with $m | n$.

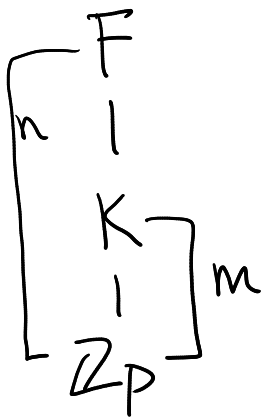
Ex $|F| = p^6$ subfields have order p^1, p^2, p^3, p^6 (not p^4, p^5)

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

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

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

then $[F : \mathbb{Z}_p] = [F : K] [K : \mathbb{Z}_p]$
 $n = [F : K] m \Rightarrow m | n$



← Assume $|F| = p^n$, $m|n$, create a subfield of order p^m

Algebra

$$n = ms$$

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

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

$$= \underbrace{(p^s)^m}_{\equiv} + \cancel{(p^s)^{m-1}} + \dots + \cancel{(p^s)^2} + \cancel{p^s} - \cancel{(p^s)^{m-1}} - \dots - \cancel{(p^s)^2} - \cancel{p^s} - 1 = (p^s)^m - 1$$

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

$$= x(x^{(p^s-1)l} - 1)$$

$$= x(x^{(p^m-1)l} - 1)$$

$$= x((x^{p^m-1})^l - 1)$$

switch $s \nleftrightarrow m$

$$l = (p^m)^{s-1} + (p^m)^{s-2} + \dots + p^m + 1$$

$$= X (X^{p^m} - 1) \left((X^{p^{m-1}})^{p-1} + (X^{p^{m-1}})^{p-2} + \dots + (X^{p^{m-1}})^1 + 1 \right)$$

So $X(X^{p^m} - 1) = X^{p^m} - X$ 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

$$\frac{X^k - 1}{X - 1} = X^{k-1} + X^{k-2} + \dots + X^1 + 1$$

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