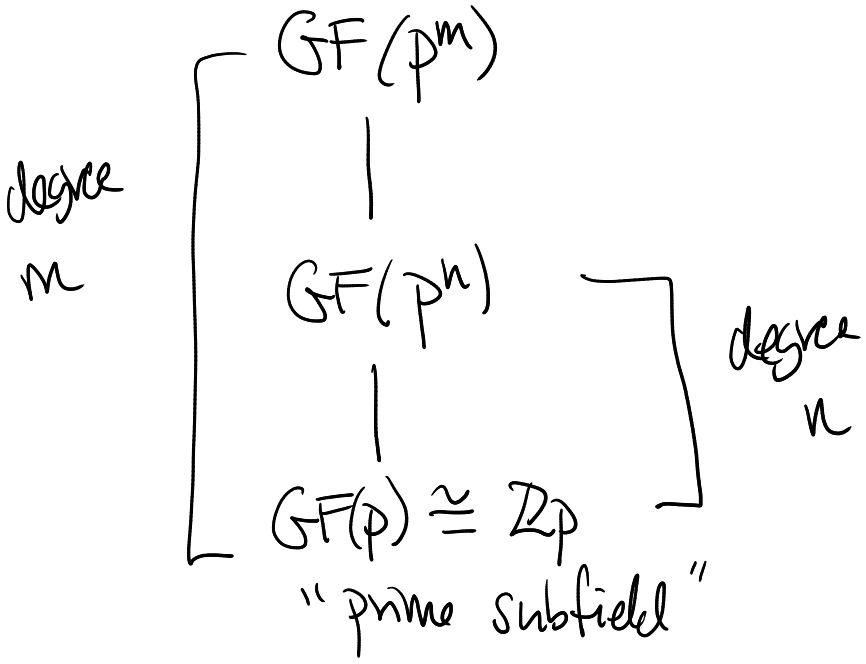
Math 491, Tuesday, April 21 Problem Session

22.2 $[GF(p^m) : GF(p^n)]$ $n \mid m$



any tower of extension fields

$[GF(p^m) : GF(p)] = [GF(p^m) : GF(p^n)][GF(p^n) : GF(p)]$

$m = [GF(p^m) : GF(p^n)]\ n$

$m/n = [GF(p^m) : GF(p^n)]$

(Generalizes all parts of #1)

22.15 $a \in F$, F finite field $\Rightarrow$ there exists b, c so that $a = b^2 + c^2$

$T = \{ x^2 \mid x \in F \}$ at most, at worst $x \to x^2$ is a 2-1 mapping

$2, -2 \to 4$

$3, -3 \to 9$

In F, $e \in F$ $e^2 = e^2$ (char 2 $-e = e$

$(-e)^2 = e^2$

$= (-1 \cdot e)^2 = (-1)^2 e^2 = 1e^2$

$-e = (-1)e$

Equation $x^2 = t$ has at most two solutions.

$0^2 = 0$

$|T| \geq \frac{1}{2}|F|$

Construct $S = \{ a - x^2 \mid x \in F \}$ Similarly $|S| \geq \frac{1}{2}|F|$

If $S \cap T = \emptyset$ then

$|F| \geq |S \cup T| = |S| + |T| - 0 \geq \frac{1}{2}|F| + \frac{1}{2}|F| = |F|$ $\Rightarrow\Leftarrow$

so $S \cap T \neq \emptyset$

Grab $l \in S \cap T \Rightarrow$ $l = b^2, l \in T$

$l = a - c^2, l \in S$

$\Rightarrow$ $b^2 = l = a - c^2$

$c^2 + b^2 = a$

12 $GF(2)$ $1+X+X^3$ has roots outside $GF(2)$

$GF(p)$ $1+x^{p+1} \overset{?}{\Rightarrow}$ $p+1$ distinct roots

$GF(p^n) = F$ $1 + (x-f_1)(x-f_2)\cdots(x-f_n)$

$F = \{f_1, f_2, \ldots, f_n\}$

no element of F is a root

$= 1 + x^{p^n} - x = x^{p^n} - x + 1$

$x^{p^n} - x$

has no roots in $GF(p^n)$

$GF(p^n)$ = splitting field of $x^{p^n}-x \in \mathbb{Z}_p[x]$

Sage: check

Factor $x^{p^n}-x+1$ in $GF(p^n)$

(no linear factors)