Last time: finite fields

If F a fin field $\Rightarrow F$ has char $p > 0 \Rightarrow \mathbb{F}_p \subset F$

If $n = [F : \mathbb{F}_p] \Rightarrow \#F = p^n = q$

Thm Given prime p & $n \geq 1$, $\exists$ finite fields w/ p^n elts & ! up to $\cong$

Rmk If $q = p^n$, write $\mathbb{F}_q$ for field w/ q elts.

Warning $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$

Lemma $\#F = q \Rightarrow a^q = a \quad \forall a \in F$

$$\Rightarrow x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

Pf $F^\times$ is grp of ord $q-1$ so $\forall a \in F^\times \; a^{q-1} = 1$

$\Rightarrow a^q = a$

If $a = 0 \Rightarrow a^q = a$ too

$\Rightarrow$ each elt in F is a root of $x^q - x$

as $\#F = \deg(x^q - x)$, that gives this factorization.

Cor F is a splitting field of $x^q - x \in \mathbb{F}_p[x]$

Pf 1) We know $x^q - x$ factors in linear pieces / F

2) The roots of $x^q - x$ gen F as every $\alpha \in F$ is a root!

Cor 2 If F_1 and F_2 are finite fields of $q = p^n$ elts $\Rightarrow \cong$ isom!

Pf Splitting fields unique!

Existence! let $q = p^n$ given. let F be the splitting field of $x^q - x$.

Cl. $\#F = q$

Sub Cl. $\#F \leq q$

let $\phi : F \longrightarrow F$

$x \longmapsto x^q$

Obs, ϕ is a field isomorphism (q^n power in char p so binom)

As ϕ is a field isomorphism $\{x \in F \mid \phi(x) = x\}$ is a subfield of F.

$\Rightarrow$ This field must be all of F as it contains the roots of $x^q - x$, here gen F.

$\Rightarrow \forall x \in F$ have $\phi(x) = x$ i.e $x^q - x = 0$

Since this poly has at most q roots $\#F \leq q$

Sub Cl. $\#F \geq q$

Since $f(x) = x^q - x$ splits into lin factors IF

$\Rightarrow \#F \geq \#$ distinct roots of poly of f.

Obs! if a is a multiple root $\Rightarrow f'(a) = 0$

purely alg $\longleftarrow$ where $f'(x) =$ deriv of x

but! $f'(x) = qx^{q-1} - 1 = -1$ as $q = 0$ in $\mathbb{F}_p$

$\Rightarrow f(x)$ has q distinct roots $\Rightarrow \#F \geq q$ $\square$.

Rmk) if K is any field $f(x) \in K[x]$ $f'(x) = \sum_{i=0}^{?} i a_i x^{i-1}$

Q What is the best way to constr $\mathbb{F}_{p^2}$?

Idea if -1 not a sqr in $\mathbb{F}_p$ (p odd)
x^2+1 is an irred poly / $\mathbb{F}_p$

$\Rightarrow \frac{\mathbb{F}_p[x]}{(x^2+1)}$ " = " $\mathbb{F}_p[i]$ is a field of deg 2 over $\mathbb{F}_p$
$i^2=-1$

If $-1 = a^2$ in $\mathbb{F}_p$ $\Rightarrow x^2+1 = (x-a)(x+a)$
as $a=-a$

Rk $\frac{\mathbb{F}_p[x]}{(x^2+1)} \cong \frac{\mathbb{F}_p[x]}{(x-a)} \times \frac{\mathbb{F}_p[x]}{(x+a)}$ $\rightarrow$ not irred!

$\cong \mathbb{F}_p[x]^2$ not a field

Rmk -1 is sqr in $\mathbb{F}_p$ iff $p \equiv 1 \pmod 4$ or $p=2$
$(p \neq 2)$

Idea if $a \in \mathbb{F}_p$ not sqr $\rightarrow x^2-a$ irred!

$\Rightarrow \frac{\mathbb{F}_p[x]}{(x^2-a)}$ " = " $\mathbb{F}_p[\sqrt{a}]$ is a field w p^2 elts!

for $(p-2)$ $\frac{\mathbb{F}_2[x]}{(x^2+x+1)}$ is a field w 4 elts!

Prop $n, m \geq 1$ $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff $n \mid m$

Pf If $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ then

$[\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p]$
$\quad m \quad = \quad ? \quad \cdot \quad n$

$\Rightarrow n \mid m$

$\mathbb{F}_{p^m}$ | $\mathbb{F}_{p^n}$ | $\mathbb{F}_p$

$\Leftarrow$ say $n \mid m$

Cl 1 $x^{p^n} - x$ splits into linear pieces over $\mathbb{F}_{p^m}$

Recall $p^n - 1 \mid p^m - 1$ as $n \mid m$ $\quad \frac{p^{nm}-1}{p^n-1} = 1 + p^n + p^{2n} + \cdots + p^{(n-1)n}$

$= x^{p^{n-1}} - 1 \mid x^{p^n - 1} - 1$

$\Rightarrow x^{p^n-1} - 1$ splits in F_{p^n} $\quad (x^{p^n} - x = x(x^{p^n-1} - 1))$

$\Rightarrow x^{p^n-1} - 1$ splits $\Rightarrow x^{p^n} - x$ splits!

So F_{p^n} contains splitting field for $x^{p^n} - x$ over F_{p^n}

Def A field Ω is algebraically closed if $\forall$ nonconst poly w/ coeff in Ω has a root in Ω.

e.g. $\Omega = \mathbb{C}$ (FTA)

Prop Ω is alg closed $\iff$ every alg ext of Ω is trivial (degree 1)!

Pf ($\Rightarrow$) say K/Ω is an alg extension!

Let $a \in K$ be given, consider its min poly $f_a(x) \in \Omega[x]$

Since, $f(x)$ is irred / Ω & has a root in Ω

$\Rightarrow$ be deg 1 $\Rightarrow f_a(x) = x - a \Rightarrow a \in \Omega$

So $K \subseteq \Omega \rightarrow$ trivial extn!

($\Leftarrow$) Say every alg extn of Ω trivial!

Let $f(x) \in \Omega[x]$ be given WTS $f(x)$ has a root in Ω

Let K = Splitting field of f / Ω

This is alg ext of $\Omega \rightarrow K = \Omega$

$\Rightarrow f$ Splits over Ω!

Def F any field. An algebraic closure of F is an alg extn Ω/F with Ω alg closed!

ex $\mathbb{C}/\mathbb{R}$ is alg closure of $\mathbb{R}$

non ex $\mathbb{C}/\mathbb{Q}$ is not alg closure of $\mathbb{Q}$ (not alg extn)