Last time:

Given irred $f(x) \in F[x]$ a stem field was $(E/F, a)$ where $a \in E$ a root of $f(x)$ & $E = F(a)$

We proved, Stem fields unique up to isom

thinking of $f \in E[x]$ it might have more roots or only a

E.g.1: $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$

$f(x) = x^3 - 2$, $a = \sqrt[3]{2}$

$(E/F, a)$ is a stem field for $f(x)$

a is the only root of f in E (others are cmplx)

Def) given any poly $f(x) \in F[x]$ a splitting field for f is a field extn E/F s.t. $f(x)$ factors into linear facts / E & E gen'd by roots of f.

Prop: Splitting fields exist + unique up to F isom!

Pf) Existence
- pick irred factor $g(x)$ of $f(x)$
- $(E_0/F, a)$ be stem field for $g(x)$
- Write $f(x) = (x-a) f_0(x)$, $f_0 \in E_0[x]$
- Let E be an extn of E_0 that's a splitting field for f_0 (exists by ind on degree)
- E is spl field for f.

Unique: Say E, E' are two splitting fields for f.

let $g(x)$ be an irred factor of $f(x)$

Since $g | f$ & f factors into deg 1 pieces so does g

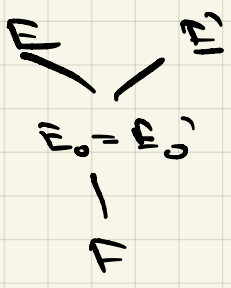
$\Rightarrow \exists$ root $a \in E$ and $a' \in E'$ of g

let $E_0 = F(a) \subset E$, $E_0' = F(a') \subset E'$

Note E_0 and E_0' are stem fields for g

$\Rightarrow \exists!$ F-isom $E_0 \to E_0'$

$a \longmapsto a'$



let $f(x) = (x-a) f_0(x) \in E_0[x]$
$= (x-a') f_0(x) \in E_0'[x]$ ||

Then E and E' are splitting fields for f_0 (rel to E_0)
By ind on degree $\exists$ E_0-isom $E \to E'$ (this is automatically F isom)

Warning! If E, E' are splitting fields for E, there will (typically) be many F-isomorphisms $E \to E'$.
(When $E = E'$ typically lots trivial F-auto. $E \to E$)

e.g. $\mathbb{C}/\mathbb{R}$ splitting of x^2+1
$\mathbb{C}$ has 2 $\mathbb{R}$ aut id, complex conj.

Def f has no multiple roots.
A "marked splitting field" is $(E/F, \alpha_1, \dots, \alpha_n)$
so $f(x) = \prod_{i=1}^{n} (x-\alpha_i)$ & $E = F(\alpha_1, \dots, \alpha_n)$
If $(E'/F, \alpha_1', \dots, \alpha_n')$ is another one,
$\exists$ at most one F isom $\sigma: E \to E'$ so $\sigma(\alpha_i) = \alpha_i'$

But, doesn't have to exist in gen!

e.g. $F = \mathbb{Q}$, $f(x) = x^4 - 1$ $E = \mathbb{Q}(i)$ is a spl field.
$(E/\mathbb{Q}, 1, i, -1, -i)$
$(E/\mathbb{Q}, i, -i, 1, -1)$
} not isom as marked sp fields (can't take 1 anyway)

2) $F = \mathbb{Q}$, $f(x) = \frac{x^5-1}{x-1} = 1 + x + \dots + x^4$ (roots are prim 5^{th} roots of 1)
$\zeta = e^{2\pi i/5}$ $E = \mathbb{Q}(\zeta)$
$(E/\mathbb{Q}, \zeta, \zeta^2, \zeta^3, \zeta^4)$
$(E/\mathbb{Q}, \zeta, \zeta^3, \zeta^2, \zeta^4)$
} No marked isom
as $\zeta \longmapsto \zeta$
$\Rightarrow \zeta^2 \longmapsto \zeta^2$

Def A finite field is a field w/ fin many elts.

Say F is a finite field.

Certainly $\mathbb{Q} \not\subset F$ $\Rightarrow$ $\mathrm{char}\ F = p$ for p prime (→ more)

& $\mathbb{F}_p \subseteq F$

F is finite, it is fin dim'l as a $\mathbb{F}_p$ v.s.

$\Rightarrow F \cong \mathbb{F}_p^n$ (as a v.s.) $\Rightarrow \#F = p^n$

Prop F a finite field $\Rightarrow$ $F^\times$ cyclic

generally if E is any field any finite subgp of $E^\times$ is cyclic.

Pf Say $G \subset E^\times$ is finite. (→ abelian gp)

Write $G[n] = \{x \in G \mid x^n = 1\}$ $\Leftrightarrow$ $x^n = 1$, $x^n - 1 = 0$

Since the poly $x^n - 1$ has at most n roots in E

$\Rightarrow \#G[n] \leq n$

Lemma if G is a finite ab grp s.t. $\#G[n] \leq n$ $\forall n$ $\Rightarrow$ G cyclic.

Pf By struct thm $G \cong \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \cdots$

$m_2 \mid m_1$, $m_2 \mid m_2$, ...

$\Rightarrow G[m_2] \supseteq (\mathbb{Z}/m_2)[m_2] \times \mathbb{Z}/m_2$

$\Rightarrow \#G[m_2] \geq m_2^2 \Rightarrow m_2 = 1$

Def An integer a is a primitive root mod p if a gen's $\mathbb{F}_p^\times$

e.g. • 2 is a prim root mod 5

• 3 mod 7 (but 2 isn't as $2^3 = 1$)

Conj | if a is an integer that is not a square, not -1, a is a prim root mod infinitely many primes. (Artin).

Status | At most 2^{prime} counter examples

↳ e.g. true for at least one of 2, 3, 5.

Discrete log prob | given a prim root a mod p and some $b \in \mathbb{F}_p^\times$. find i s.t. $b = a^i$ [$i = \log_a b$]