Project: Compute Galois corresp.
Will release on Mon.
due Fri 3/3

Today: finite fields

p: prime, $q = p^n$

Recall: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ w/ $+, -, \cdot, /$ defined mod p

Prop (§13.5, p. 549): For every prime power $q = p^n$, $\exists!$ field of order q. For any other integer, there is no fin. field of that order.

Pf: Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. $Df = -1$, so f is separable.
Let $\mathbb{F}_q$ be the set of roots of f (in some splitting field).

If $\alpha, \beta \in \mathbb{F}_q$

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \qquad (\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$$

$$(\alpha+\beta)^{p^n} \underset{\text{Frobenius}}{=} \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

So $\mathbb{F}_q$ is a field! $\mathbb{F}_p \subseteq \mathbb{F}_q$ since $1^{p^n} = 1$, so $\mathbb{F}$ is the splitting field for f. Since $|\mathbb{F}_p| = p$, $|\mathbb{F}_q| = p^n$, $[\mathbb{F}_q : \mathbb{F}_p] = n$.

Conversely, let $\mathbb{F}$ be a finite field w/ char $\mathbb{F} = p$. Then $\mathbb{F}_p$ is the prime subfield of $\mathbb{F}$, and $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]} =: p^n$ is a power of p. Since $|\mathbb{F}^\times| = p^n - 1$, by Lagrange's Thm, $\alpha^{p^n-1} = 1$ for all $\alpha \in \mathbb{F}^\times$, so $\alpha^{p^n} = \alpha$ $\forall \alpha \in \mathbb{F}$. But this means

that $\mathbb{F}$ is the splitting field for $x^{p^n} - x$ (using order arguments),
so $\mathbb{F} \cong \mathbb{F}_q$ by uniqueness of splitting fields.

Cor: If $f(x) \in \mathbb{F}_p[x]$ is irreducible of deg n, the splitting field for f over $\mathbb{F}_p$ is isom. to $\mathbb{F}_{p^n}$.

Cor: $\mathbb{F}_{p^n} / \mathbb{F}_p$ is Galois

Let $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ Frobenius automorphism

$\alpha \mapsto \alpha^p$ since finite

$\sigma_p^n = id$ since $\alpha^{p^n} = \alpha \ \forall \alpha \in \mathbb{F}_{p^n}$

but if $m<n$, $\sigma_p^m \neq id$ since otherwise $x^{p^m} - x$ would have too many roots

So

$$\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p) \cong \langle \sigma_p \rangle = \mathbb{Z}/n\mathbb{Z}$$

Sub gps: $\mathbb{Z}/d\mathbb{Z}$, $d \mid n \longleftrightarrow \mathbb{F}_{p^d}$ (intermediate field)

Example: $\mathbb{F}_{64}$ $p = 2$, $n = 6$

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\langle \sigma_2^2 \rangle \arrow[dr, dash, "2"'] & & \langle \sigma_2^3 \rangle \arrow[dl, dash, "3"] \\
 & \langle \sigma_2 \rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{F}_{64} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\mathbb{F}_4 \arrow[dr, dash, "2"'] & & \mathbb{F}_8 \arrow[dl, dash, "3"] \\
 & \mathbb{F}_2 &
\end{tikzcd}$$

Everything is Galois (since Gal. gp. is abelian)

Prop 17: $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple i.e. $\exists$ an irred. poly of deg. n over $\mathbb{F}_p$ $\forall n \geq 1$.

Pf: The mult. gp. of a field is cyclic, so if θ is a generator of $\mathbb{F}_{p^n}^\times$, then $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. $m_{\theta, F}$ is irred. of deg n.

Prop 18: $x^{p^n} - x = \prod$ all irred. polys of deg $d | n$

Pf: If f is an irred poly of deg $d | n$, and α is a root of f, then $\alpha \in \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, so $f \mid x^{p^n} - x$. Other degrees, this doesn't hold.

Since $x^{p^n} - x$ is sep., each factor only appears once

Cor: There are only finitely many irred. polys of each deg. over $\mathbb{F}_p$.

Ex: Over $\mathbb{F}_2$, $x^4 - x = \prod$ irred polys of deg 1, 2

Polys of deg 1 : x, $x+1$

$$\frac{x^4+x}{x(x+1)} = x^2+x+1$$ only irred. deg. 2 poly.

$x^8 - x = \prod$ irred polys of deg 1, 3

$$\frac{x^8-x}{x(x-1)} = x^6+x^5+x^4+x^3+x^2+x+1 = (x^3+x+1)(x^3+x^2+1)$$

irred / $\mathbb{Q}$

Irred polys / $\mathbb{F}_2$ of deg ≤ 3:

x

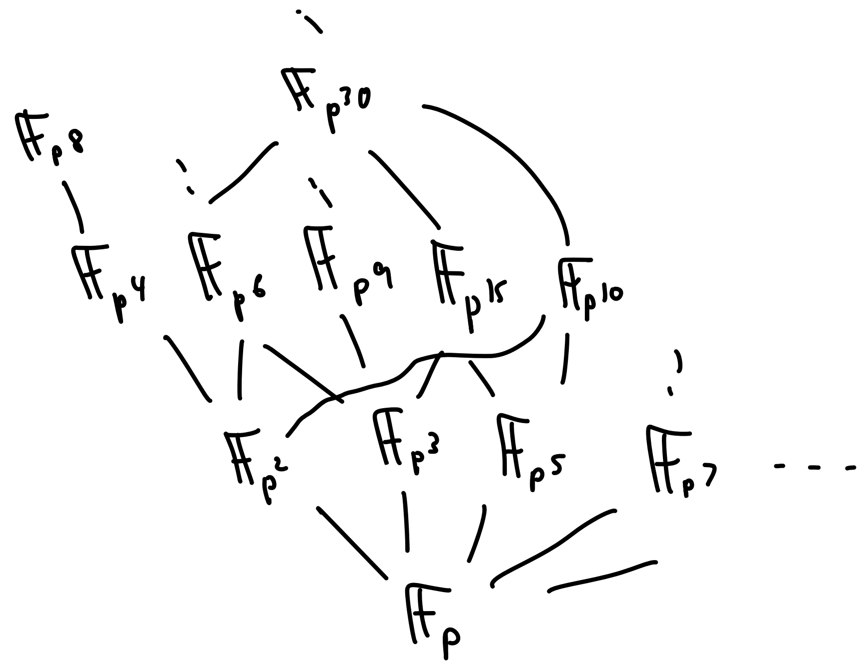
$x+1$

x^2+x+1

x^3+x+1

x^3+x^2+1

Let's extend the containment diagrams infinitely:



Notice that $\mathbb{F}_{p^{n_1}}, \dots, \mathbb{F}_{p^{n_k}} \subseteq \mathbb{F}_{p^{n_1 \cdots n_k}}$

So the alg. closure is

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

Next time: composite ext'ns