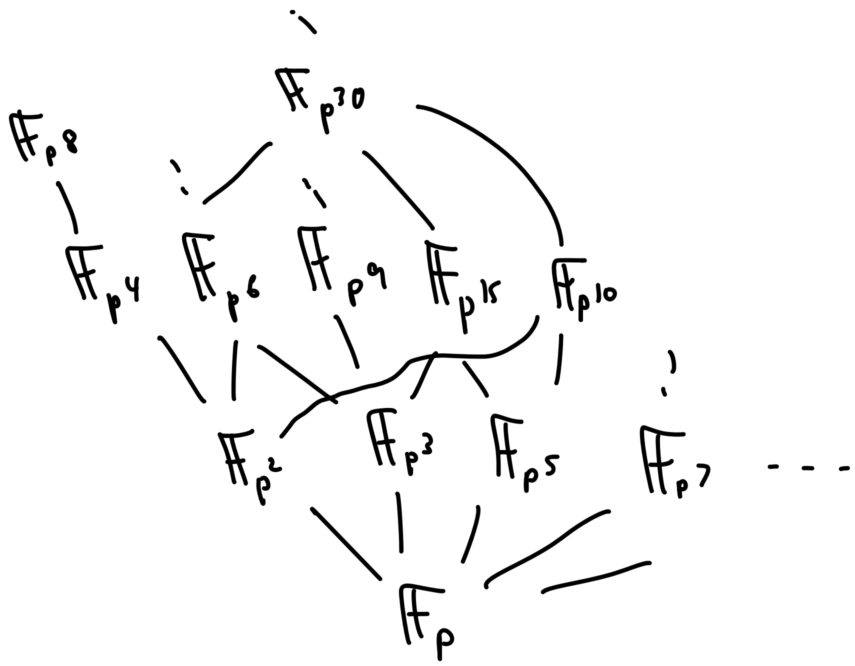
Project posted (due 3/3 noon)

H/W 6 first half posted (due 3/7 noon)

Last bit of finite fields:

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

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

§14.4: Composite ext'ns & simple ext'ns

Prop 19: K/F Galois, F'/F any ext'n.

Then, KF'/F Galois and

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K\cap F')$$

$$\begin{tikzcd}
 & KF' & \\
K \arrow[ur, dash] & & F' \arrow[ul, dash] \\
 & K\cap F \arrow[ul, dash] \arrow[ur, dash] & \\
 & F \arrow[u, dash] &
\end{tikzcd}$$

Pf: Let $f \in F[x]$ be sep & irred. w/ splitting field K over F. Then the splitting field of f over F' is KF', so KF'/F' is Galois.

The map
$$\mathrm{Gal}(KF'/F') \longrightarrow \mathrm{Gal}(K/F)$$
$$\sigma \longmapsto \sigma|_K$$
is an inj. hom. w/ image $\mathrm{Gal}(K/K\cap F)$

(details in D&F) $\square$

Cor 20: With the same setup,

$$[KF':F] = \frac{[K:F][F':F]}{[K\cap F':F]}$$

Pf: Use Tower Law, noting that

$$[KF':F'] = |\mathrm{Gal}(KF'/F')| = |\mathrm{Gal}(K/K\cap F')| = [K:K\cap F']$$ $\square$

Prop 21: K_1/F, K_2/F Galois.

Then,

a) $(K_1\cap K_2)/F$ Galois

b) K_1K_2/F Galois, and

$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma,\tau) \mid \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\}$$
$$\subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2,F)$$

Colloquially, pick an autom. of each field ext'n, but make sure they don't conflict.

Cor 22: K_1/F, K_2/F Galois, $K_1 \cap K_2 = F$

Then,
$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

Def: Let E/F be sep. $K \supseteq E$ is called the <u>Galois closure</u> of E over F if K/F Galois, and if $L \supseteq E$, L/F Galois, then $K \subseteq L$.

Cor 23: This always exists (and is unique).

Pf: Recall: E/F sep. $\Leftrightarrow$ every elt. of E is a root of a sep. poly. over F.

Let $\omega_1, \ldots, \omega_n$ be a basis for E/F, and let f be the squarefree prod. of their min'l polys. The splitting field of f contains E and is Galois $/F$, so take K to be the intersection of all such fields. $\square$

Prop 24: K/F finite. Then,
$$K/F \text{ simple} \Leftrightarrow \exists \text{ finitely many int. fields } F \subseteq E \subseteq K.$$

called "primitive elt."

Pf: $\Rightarrow$: Let $K = F(\theta)$, and suppose $F \subseteq E \subseteq K$.

Let $f(x) = m_{\theta,F}(x)$, $g(x) = m_{\theta,E}(x)$; then $g \mid f$ over E.

Let $E' = F(\text{coeffs. of } g(x))$. Then $E' \subseteq E$, and since $m_{\theta,E}(x) = g(x) = m_{\theta,E'}(x)$, $E = E'$.

Since E was arbitrary, any int. field is gen'd by the coeffs. of (monic) factors of f $\Rightarrow$ finitely many.

$\Leftarrow$: If F finite, done (Prop 17), so assume F infinite.

If $K = F(\alpha, \beta)$, then finitely many int. fields $\Rightarrow$ $\exists c \neq c' \in F$ s.t. $F(\alpha + c\beta) = F(\alpha + c'\beta)$. But then

$\beta \in \frac{1}{c-c'}(\alpha + c\beta - \alpha - c'\beta) \in F(\alpha + c\beta)$, and so

$F(\alpha, \beta) = F(\alpha + c\beta)$ simple.

General K follows by induction. $\square$

E.g.: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Thm 25 (Primitive Element Theorem):

K/F finite, sep. $\Rightarrow$ K/F simple

In particular K/F finite, char 0 $\Rightarrow$ simple since irred. polys in char 0 are sep.

Pf: Let L be the Galois closure of K over F.

$\mathrm{Gal}(L/F)$ finite $\Rightarrow$ finitely many subgps. of $\mathrm{Gal}(L/F)$

$\Rightarrow$ finitely many int. fields $F \subseteq E \subseteq L$

$\Rightarrow$ finitely many int. fields $F \subseteq E \subseteq K$

$\Rightarrow$ K/F simple

Prop 24

Next time: when is $\mathrm{Gal}(K/F)$ abelian?