Lecture 18: Positive characteristic

Aim Lecture: Study Galois theory of finite fields & separability.

Finite fields Recall following:

Facts: Let K = finite field. Then

(a) char $K = p > 0$ so K contains a unique copy of $\mathbb{F}_p$

(b) $|K| = p^{dp}$ where $d = [K : \mathbb{F}_p]$

Conversely

Prop 1: Let $d \in \mathbb{Z}$ be positive.

(a) The splitting field K of $x^{p^d} - x / \mathbb{F}_p$ has $|K| = p^d$.

(b) Any field L with $|L| = p^d$ is isomorphic to K.

(c) $K/\mathbb{F}_p$ is Galois with Galois group $G = \langle \varphi \rangle$ where $\varphi : K \to K$ is the Frobenius map. Δ $G \simeq \mathbb{Z}/d\mathbb{Z}$.

Proof: (a) Note $f(x) = x^{p^d} - x$ has p^d distinct roots $\alpha_1, \ldots, \alpha_{p^d}$ $\because f'(x) = -1$ is rel. prime to $f(x)$. Hence $|K| \geq p^d$. Now α is a root of $f(x)$ iff

$$\alpha = \alpha^{p^d} = \varphi^d(\alpha) \iff \alpha \in K^{\varphi^d}$$

so these p^d roots already form a field K^{φ^d} which must be K. We see $\varphi^d = 1_G$.

(b) By uniqueness of splitting fields, it suffices to note $L \supseteq \mathbb{F}_p$ & show L consists of the p^d roots of $f(x) = x^{p^q} - x = x(x^{p^q-1} - 1)$.

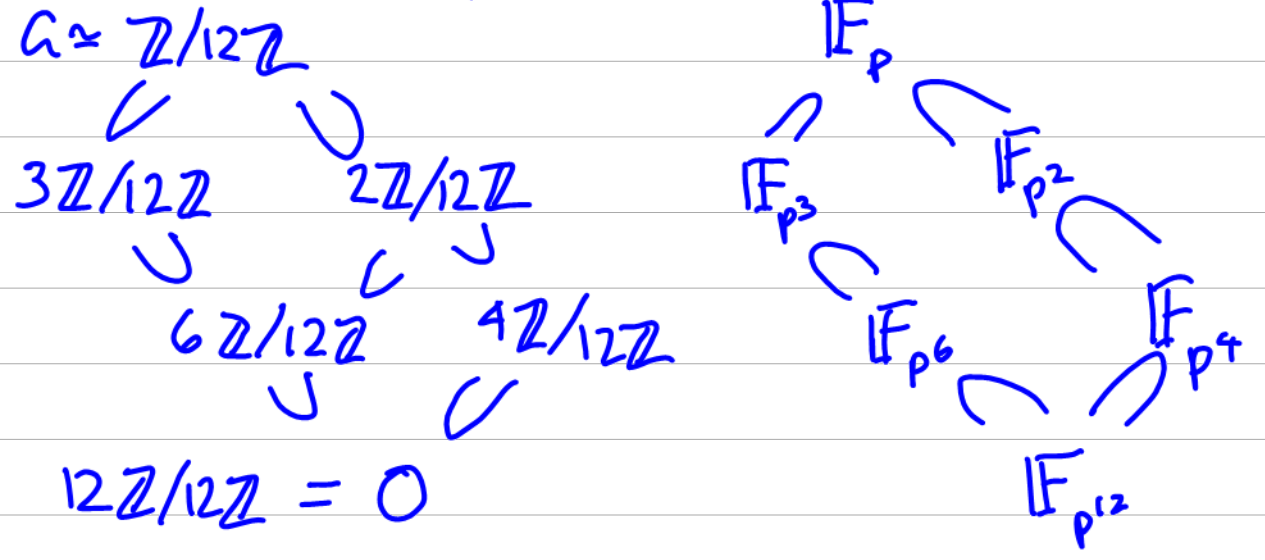
Now $|L^*| = p^q - 1$ so Lagrange's thm $\Rightarrow$ elts of L^* are the roots of $x^{p^q-1} - 1$. The last root of $f(x)$ is $x = 0$.

(c) $K^{\langle\varphi\rangle} = \{\alpha \in K \mid \alpha^p - \alpha = 0\}$ which has at most p elts. $\therefore K^{\langle\varphi\rangle} = \mathbb{F}_p$ & $K/\mathbb{F}_p$ is Galois with Galois group $G = \langle\varphi\rangle$. Since $|G| = [K:\mathbb{F}_p] = d$, $G \simeq \mathbb{Z}/d\mathbb{Z}$. □

Eg. 1. Let $K = \mathbb{F}_{p^d}$ be the field with p^d elts & $\varphi: K \to K$ be the Frob, so $G := \mathrm{Gal}(K/\mathbb{F}_p) = \langle\varphi\rangle$.

Let $e \mid d$ so $H = \langle\varphi^e\rangle \trianglelefteq G$ with $G/H \simeq \mathbb{Z}/e\mathbb{Z}$. Hence $K^H \subset K$ & $[K^H : \mathbb{F}_p] = e$.

Galois corresp. when $d = 12$



Maximal Separable Subextensions

Prop^{n} 2: Let K/F = separable field ext^{n}. Then every $\alpha \in K$ is separable $/F$.

Proof: We can assume K/F finite & even Galois by Galois closure. Then Lect. 2 Thm $\Rightarrow$ every $\alpha \in K$ has sep. min. poly. $/F$. $\square$

Cor-Def^{n}: Let K/F = field ext^{n}. The set L of elts $\alpha \in K$ separable $/F$ is an intermediate field called the *maximal separable subextension* of K/F.

We say K/F is *purely inseparable* if $L = F$.

Eg. 2. If $F = \mathbb{F}_p(t)$ then (ex.) $\alpha = \sqrt[p]{t} \notin F$.
Let $K = F(\alpha) = \mathbb{F}_p(\sqrt[p]{t})$.

Claim: The max. sep. subext^{n} L of K/F is F so K/F is purely insep.

Why? α is a root of $f(x) = x^p - t = (x - \alpha)^p$ (by Frob. hom).
$\alpha \notin F \Rightarrow f(x)$ irred. $/F$.
$\therefore [K:F] = \deg f(x) = p$.
Also $f'(x) = 0 \Rightarrow \alpha$ not separable $/F$
i.e. $\alpha \notin L$.

$\therefore L \subsetneq K$. But $[K:F]$ is prime so multiplicativity of degrees $\Rightarrow [L:F]=1$ i.e. $L=F$ & $\therefore$ K/F is purely insep.

Algebraic & Separable Closure

Def^{n}: A field F is algebraically closed if the irred. poly. in $F[x]$ are all linear (i.e. every non-constant poly. has a root in F).

An algebraic closure of a field F is an algebraic ext^{n} $\bar{F}/F$ with $\bar{F}$ algebraically closed.

The separable closure of F is the max. sep. subext^{n} F^{sep} of $\bar{F}/F$.

E.g. $\mathbb{C}$ is both the algebraic & separable closure of $\mathbb{R}$.

Thm: Any field F has an algebraic closure which is unique up to isom. /F,

Proof Sketch: Basic idea is to let $\bar{F}$ = "union" of all splitting fields of poly /F. Then $\bar{F}$ alg. closed $\because$ alg. ext^{n}s of algext^{n}s are alg.

To make union work need to embed splitting fields in suff. big fixed set Ω & use Zorn's lemma on subsets of Ω with field structure.