Lecture 8: Field Extensions II

Last time:

K/F a field extension means $F \subseteq K$.

$[K:F]$ = dim of K as an F-vector space.

$p(x)$ irred poly in $F[x]$. form a field

$$K = F[x]/(p(x)) \longleftrightarrow \begin{array}{l}\text{polys in } F[x] \\ \text{of deg} < \deg p\end{array}$$

$$\text{---------- } \circ \text{ ----------} \Rightarrow [K:F] = \deg p.$$

Think of K as adding a root of p to F.

Explicitly, set $\theta = x + (p(x))$. Then

$$p(\theta) = p(x) + (p(x)) = 0 \text{ in } K.$$

An F-basis of K is $1, \theta, \theta^2, \ldots, \theta^n$ where $n = (\deg p) - 1$.

Ex: $F = \mathbb{R}$, $p = x^2 + 1$

$$K = \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$$

$$1 \longleftrightarrow 1$$

$$\theta \longleftrightarrow i \text{ (or } -i)$$

Notation: $\alpha_1, \ldots, \alpha_n \in K$ with $F \subseteq K$ then

$F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ = field gen by elts of F and the α_i.

[i.e. the smallest subfield containing all of them.]

Ex: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. Here the large field is $\mathbb{C}$.

Simple Extension: $K = F(\alpha)$ for some $\alpha \in F$.
↑ primitive elt.

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$ is simple as $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha = \sqrt{2}+\sqrt{5})$

since $\sqrt{2} = \frac{1}{6}(\alpha^3 - 11\alpha)$

Will show: Any K/F with $[K:F] < \infty$ and $ch(F) = 0$ is primitive.

Thm: $p(x) \in F[x]$ irred. Suppose K is a simple ext. of F w/ primitive elt α. If $p(\alpha) = 0$, then

$$L = F[x]/(p(x)) \cong K$$

Proof: Consider $\phi: L \longrightarrow K$ given by

$$g(x) + (p(x)) \longmapsto g(\alpha)$$

Makes sense because $f(\alpha) = 0$ if $f \in (p(x))$ and

is a ring hom by the basic ring axioms.

Lemma: $\psi: L \to K$ a ring hom of fields.
Then either $\psi(L) = 0$ or ψ is 1-1.

Reason: $\ker(\psi) = \{\psi(\alpha) = 0 \mid \alpha \in L\}$ is an ideal
hence either 0 or L as every elt of $L \setminus \{0\}$ is a unit.

Our ϕ is not trivial as $\phi/_{\text{const polys}}$ is an isom to F,
so its 1-1. Moreover, ϕ is onto as its image
contains F and α. So ϕ is an isom. ▨

Thm: Suppose $K = F(\alpha)$ with $[K : F] = n < \infty$.
Then $\exists$ an irred poly $p(x) \in F[x]$ with
$p(\alpha) = 0$. Thus $K \cong F[x]/(p(x))$.

Ex: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$

$\mathbb{Q}(\alpha = \sqrt{2}+\sqrt{5}) = \mathbb{Q}[x]/x^4-14x^2+9$

Pf: As $\dim K$ as a F-vector space is n,

$$1, \alpha, \alpha^2, \dots \alpha^n$$

must be linearly dep, i.e. $\exists a_i \in F$ with

$$a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \dots + a_n \alpha^n = 0$$

So take $p(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$.

If $p(x)$ is red, replace it with an irred factor which also has α as a root. ▨

Note: A posteriori, p must be irred, as

$$\left[F[x]/(p(x)) : F \right] = \deg p$$

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ has $\mathbb{Q}$-basis $1, \sqrt{2}, \sqrt{5}, \sqrt{10}$

Above things follow easily by computing in this basis.

$$\alpha = \sqrt{2} + \sqrt{5}$$

$$\alpha^2 = 7 + 2\sqrt{10}$$

$$\alpha^3 = 17\sqrt{2} + 11\sqrt{5}$$

$$\alpha^4 = 89 + 28\sqrt{10}$$

What if $[F(\alpha):F] = \infty$? Then $p(\alpha) \neq 0$ for every $p \in F[x]$. Ex: $\alpha = \pi$, $F = \mathbb{Q}$

(Otherwise $F(\alpha) \cong F[x]/(q(x))$ for some irred factor q of p)

Consider the field of rat'l fns in x over F:

$$F(x) = \text{frac field of } F[x] = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p, q \in F[x],\ q \neq 0 \right\} / \sim$$

Then

$$\phi : F(x) \longrightarrow F(\alpha)$$

$$\frac{p(x)}{q(x)} \longrightarrow \frac{p(\alpha)}{q(\alpha)}$$

makes sense because $f(\alpha) = 0 \Rightarrow f = 0$ in $F[x]$

As before its an isom. So $F(\alpha) \cong F(x)$.

Cor: $\mathbb{Q}(\pi)$, $\mathbb{Q}(e)$, $\mathbb{Q}(\ln 2)$

are all isomorphic fields ($\cong$ to $\mathbb{Q}(x)$).