Lecture 8: Field extensions II

Last time:

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

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

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

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

$$\Longrightarrow [K:F] = \deg p.$$

Think of K as adding a root of $p(x)$ to F. Explicitly, set $\theta = x + (p(x))$. Then $p(\theta) = p(x) + (p(x)) = 0$.

A F basis of K is $1, \theta, \theta^2, \dots, \theta^n$ where $n = \deg p - 1$.

<u>Ex</u>: $F = \mathbb{R}$, $p = x^2+1$ $\quad F = \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$$1 \longleftrightarrow 1$$
$$\theta \longleftrightarrow i \ (\text{or } -i)$$

<u>Notation</u>: $\alpha_1, \dots, \alpha_n \in K$ with $F \subseteq K$. Then

$K(\alpha_1, \alpha_2, \dots, \alpha_n)$ = field gen by F and the α_i

[i.e. the smallest subfield of K which contains them.]

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

<u>Simple extension</u>: $K = F(\alpha)$ for some α in K
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\uparrow$ primitive element

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

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

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

<u>Thm</u>: $p(x) \in F[x]$ irred. Suppose K is a simple extension of F with primitive elt α. If $p(\alpha) = 0$, then
$$L = F[x]/_{(p(x))} \cong K$$

<u>Pf</u>: Consider $\phi : L \to K$ given by $g(x) + (p(x)) \longmapsto g(\alpha)$; makes sense because $f(a) = 0$ if $f \in (p(x))$. Note ϕ is a ring homom. by the basic ring axioms.

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

<u>Reason</u>: $\ker \psi = \{\psi(\alpha) = 0 \mid \alpha \in L\}$ is an ideal, hence either 0 or L as every non-zero elt of L is a unit.

Our ϕ is not trivial, since $\phi|_{\text{const polys}}$ is an isom to F. So ϕ is 1-1, and moreover ϕ is onto since its image contains F and α. So ϕ is an isom. $\square$

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

<u>Ex</u>: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$

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

<u>Pf</u>: As $\dim_F K = n$, the elts $1, \alpha, \alpha^2, \dots, \alpha^n$ must be linearly dependent, i.e. $\exists\, a_i \in F$ with

$$a_0 \cdot 1 + a_1 \alpha + \cdots + a_n \alpha^n = 0$$

Set $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. If $p(x)$ is reducible, replace it by an irreducible factor for which α is also a root. $\blacksquare$

<u>Note</u>: A posteriori, p must be irred. as

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

<u>Ex</u>: $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ has $\mathbb{Q}$-basis $1, \sqrt{2}, \sqrt{5}, \sqrt{10}$.

We compute

$$\begin{aligned} \alpha &= \sqrt{2} + \sqrt{5} \\ \alpha^2 &= 7 + 2\sqrt{10} \\ \alpha^3 &= 17\sqrt{2} + 11\sqrt{5} \\ \alpha^4 &= 89 + 28\sqrt{10} \end{aligned}$$

$$\Rightarrow \alpha^4 - 14\alpha^2 + 9 = 0$$

What about simple extensions where $[F(\alpha) : F] = \infty$?

Then $p(\alpha) \neq 0$ for all non-zero $p \in F[x]$. ← Otherwise, $F(\alpha) = F[x]/q(x)$ for some irred. factor of $p(x)$.

<u>Ex</u>: $\mathbb{Q}(\pi)$, $\mathbb{Q}(e)$.

<u>Ex</u>: Field of rational fns with base field F.

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

$[F(x) : F] = \infty$ since $1, x, x^2, \ldots$ are linearly indep $/F$.

Any simple ext $F(\alpha)/F$ of ∞ degree is isomorphic to $F(x)$, because

$$\phi: F(x) \longrightarrow F(\alpha)$$
$$\frac{p(x)}{q(x)} \longmapsto \frac{p(\alpha)}{q(\alpha)}$$

makes sense as $q(\alpha) \neq 0$ if $q \neq 0$ in $F[x]$. As before, ϕ must be an isomorphism. So $F(\alpha) \cong F(x)$.

<u>Cor.</u> $\mathbb{Q}(\pi)$, $\mathbb{Q}(e)$, $\mathbb{Q}(\ln 2)$ are all isom. fields (to $\mathbb{Q}(x)$).