Lecture 9: Algebraic Extensions

Last time:

Thm: $K = F(\alpha)$. If $[K:F] < \infty$, then $\exists$ an irred poly $p(x) \in F[x]$ with $p(\alpha) = 0$ and $K \cong F[x]/(p(x))$.

If $[K:F] = \infty$, then $K \cong F(x)$, the field of rat'l fns in x.

Consider K/F and $\alpha \in K$

Algebraic: $\exists\, p(x) \in F[x]$ with $p(\alpha) = 0$.

Trancendental: not algebraic.

Ex: $\mathbb{R}/\mathbb{Q}$: Alg: $\sqrt{2}$, $\sqrt{2}+\sqrt{5}$, $\sqrt[3]{\sqrt{2}+19}$, ...

Tran: π, e, $e+\pi$, e^{π} [most all elts of $\mathbb{R}$ by cardinality.]

Prop: α alg. over F. There is a unique monic irred $p(x) \in F[x]$ with $p(\alpha) = 0$. A poly $f(x) \in F[x]$ has α as a root iff p divides f in $F[x]$.

Ex: $\sqrt{2}$ over $\mathbb{Q}$: $p(x) = x^2 - 2$ $\quad f(x) = x^3 + x^2 - 2x - 2$

$= (x+1)(x^2-2)$

Proof: Let $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$. As it is an ideal and $F[x]$ a PID, have $I = (p(x))$ where we can take p to be monic. Moreover p must be irred, as otherwise some proper factor is in I. ▨

The poly $p(x)$ is called the minimal poly. of α over F, and denoted $m_{\alpha,F}(x)$. Thus

$$F(\alpha) \cong F[x] \big/ (m_{\alpha,F}(x))$$

Def: K/F is algebraic if every $\alpha \in K$ is alg. over F.

Prop: If $[K:F] < \infty$, then K/F is algebraic.

Pf: Given $\alpha \in K$, if $[K:F] = n$ then

$1, \alpha, \alpha^2, \ldots, \alpha^n$ are K-linearly dependent ▨

$\Rightarrow$ gives $f(x) \in F[x]$ with $f(\alpha) = 0$.

Ex: $K \subseteq \mathbb{R}$ given by $K = \mathbb{Q}(\{\sqrt[n]{2} \mid n \in \mathbb{N}\})$

Each $\sqrt[n]{2}$ is alg, as its a root of $x^n - 2$ which is irred. Reason: By Gauss' Lemma, if its red it is so over $\mathbb{Z}[x]$. Say $p(x) = a(x)\,b(x)$. Now mod 2 get $x^n = a(x)\,b(x) \Rightarrow$ const terms of a, b are even, a contradiction since there prod is -2.

(This is Eisenstein's Criterion)

So $[K:\mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n \Rightarrow [K:\mathbb{Q}] = \infty$

Is $K/\mathbb{Q}$ alg? E.g. is $\dfrac{\sqrt[3]{2}+\sqrt[5]{2}}{13+\sqrt[4]{2}+17\sqrt{2}}$ alg?

In this case yes since its in $\mathbb{Q}(\sqrt[60]{2})$. Same idea works in general, so $K/\mathbb{Q}$ is alg.

Ex: $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ ← The algebraic numbers.

Q: Is $\overline{\mathbb{Q}}$ a field? A. Yes, as follows from:

Thm: Consider K/F. If α, β are algebraic over F, then $F(\alpha,\beta)$ consists entirely of elts alg over F.

Ex: As $\sqrt{2}$ and $\sqrt{5}$ are alg, so must be $\sqrt{2}+\sqrt{5}$.

Pf: Consider

$$\begin{array}{c} F(\alpha,\beta) \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

Now β is alg over $F(\alpha)$ as it sat a poly in $F(\alpha)[x]$. So $[F(\alpha,\beta):F(\alpha)] = \deg(m_{\beta,F(\alpha)}(x)) < \infty$.

Let $\gamma_1, \dots, \gamma_n$ be a $F(\alpha)$ basis for $F(\alpha,\beta)$ and $\alpha_1, \dots, \alpha_m$ a F-basis of $F(\alpha)$.

Then any $\gamma \in F(\alpha,\beta)$ is an F-linear combination

of the $\{\alpha_i \gamma_j\}$. Thus $[F(\alpha,\beta):F] \leq nm < \infty$.
So $F(\alpha,\beta)$ is algebraic. $\blacksquare$

Thm: Suppose $F \subseteq K \subseteq L$. Then $[L:F] = [L:K][K:F]$

[Makes sense even when some degrees are infinite]

Pf: If $[L:F] < \infty$ then so is $[K:F]$ (since K is a subspace of L)
and $[L:K]$ (since an F-basis for L K-spans L.)

So assume $[K:F]$ and $[L:K]$ are both finite.

Let $\alpha_1, \ldots, \alpha_n$ be an F-basis for K and
$\beta_1, \ldots, \beta_m$ be a K-basis for L.

Then $\gamma_{ij} = \alpha_i \beta_j \in L$ are $n \cdot m$ elts which K-span L.

Suppose they are K-linearly dependent:

$$\sum_{i,j} k_{ij} \alpha_i \beta_j = 0 \quad \text{with not all } k_{ij} = 0.$$

Then

$$\sum_j \overbrace{\Big(\sum_i k_{ij} \alpha_i\Big)}^{\text{in } K, \text{ not all } 0 \text{ since } \{\alpha_i\} \text{ are a basis.}} \beta_j = 0$$

Contradicting linear indep of $\{\beta_j\}$. So $\{\gamma_{ij}\}$ are a F-basis for L. So $[L:F] = n \cdot m$. $\blacksquare$

<u>Thm</u>: $F \subseteq K \subseteq L$. If L/K and K/F are alg., so is L/F.

<u>*Proof*</u>: Let $\beta \in L$, and $m_{\beta,K}(x) = \alpha_n x^n + \cdots + \alpha_0$.

Consider

$$\begin{array}{c} F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta) \\ | \\ F(\alpha_0, \alpha_1, \ldots, \alpha_n) \\ | \\ F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \\ \vdots \\ F(\alpha_0, \alpha_1) \\ | \\ F(\alpha_0) \\ | \\ F \end{array}$$

Each extension is primitive and algebraic $\Rightarrow$ degree is finite.

$\Rightarrow [F(\alpha_0, \ldots, \alpha_n, \beta) : F]$ is finite. Hence β is alg. over F.

$\blacksquare$