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 rational fns in x.

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

Algebraic: $\exists$ nonzero $p(x) \in F[x]$ 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: $\pi, e, e+\pi, e^{\pi}, \ldots$ [most elts of $\mathbb{R}$ by cardinality]

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

Ex: $\sqrt{2}$ over $\mathbb{Q}$: $p(x) = x^2 - 2$ Now $\sqrt{2}$ is also a root of

$$f(x) = x^3 + x^2 - 2x - 2 = (x+1)(x^2-2)$$

Proof: Let $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$. As I is an ideal in the PID $F[x]$, 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. $\square$

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

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

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

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

Pf: Given $\alpha \in K$ we know $1, \alpha, \alpha^2, \ldots, \alpha^n$ are F-linearly dependent, and so get $f \in F[x]$ with $f(\alpha) = 0$ $\square$

Ex: $K = \mathbb{Q}(\{\sqrt[n]{2} \mid n \in \mathbb{Z}_{>0}\}) \subseteq \mathbb{R}$

Now each $\sqrt[n]{2}$ is alg over $\mathbb{Q}$ as it's a root of $x^n - 2$.

Moreover $K/\mathbb{Q}$ is algebraic: for example $\dfrac{\sqrt[3]{2} + \sqrt[5]{2}}{13 + \sqrt[4]{2} + 17\sqrt{2}}$ is algebraic$/\mathbb{Q}$ as it lives in $\mathbb{Q}(\sqrt[60]{2})$ and $[\mathbb{Q}(\sqrt[60]{2}) : \mathbb{Q}] \le 60$. [Same reasoning works in gen.]

Now $m_{\sqrt[n]{2},\mathbb{Q}}(x)$ is actually $x^n - 2$ since it is irred in $\mathbb{Z}[x]$ by Eisenstein's Criterion. So

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

Ex: $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ [The set of algebraic #s]

In fact $\overline{\mathbb{Q}}$ is a field, because of

Thm: If $\alpha, \beta \in K$ are both alg. over F, then $F(\alpha,\beta)/F$ is algebraic.

Ex: As $\sqrt{2}$ and $\sqrt{5}$ are alg, so is $\sqrt{2}+\sqrt{5}$, $\sqrt{10}, \dots$

Pf: Consider $F(\alpha,\beta)$. Now β is alg over $F(\alpha)$. So

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

$[F(\alpha,\beta):F(\alpha)] = \deg(m_{\beta,F(\alpha)}(x)) < \infty.$

Let $\gamma_1, \dots, \gamma_n$ be an $F(\alpha)$-basis for $F(\alpha,\beta)$, and $\alpha_1, \dots, \alpha_m$ an F-basis for $F(\alpha)$. Then any elt of $F(\alpha,\beta)$ is an F-linear combination of the $\{\alpha_i \gamma_j\}$. Thus $[F(\alpha,\beta):F] \leq n \cdot m < \infty$. So $F(\alpha,\beta)/F$ is algebraic. $\square$

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

(a) $[K:F]$ (since K is a subspace of L)

(b) $[L:K]$ (since an F-basis for L also 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.

Let $\beta_1, \ldots, \beta_m$ be a K-basis for L.

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

Suppose they are F-linearly dependent:

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

Then

$$\sum_j \underbrace{\left(\sum_i f_{ij} \alpha_i \right)}_{} \beta_j = 0$$

in K, not all 0 since $\{\alpha_i\}$ are an F-basis of K.

contradicting K-linear indep of the $\{\beta_j\}$. So $\{\gamma_{ij}\}$ is an F-basis for L and so $[L:F] = n \cdot m$. $\square$