Lecture 21.

Algebraic Extensions

defn: Let K, F be fields, where $F \subset K$.

① $\alpha \in K$ is *algebraic over* F if α is the root of some (nonzero) polynomial $f(x) \in F[x]$.

↳ If α is *not* algebraic, then we call it *transcendental*

eg. $\sqrt{2}$ is algebraic over $\mathbb{Q}$; π is not.

② The extension K/F is *algebraic* if every element $\alpha \in K$ is algebraic.

There is a "best choice" for $f(x) \in F[x]$ (as above) for $\alpha \in K$ algebraic over F:

prop. Let α be algebraic over F.

(a) Then there is a *unique* monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root.

(b) $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

Pf. (a) Let $g(x) \in F[x]$ be a polynomial of *minimal* degree having α as a root.

- multiply by a constant in F; WLOG, may assume $g(x)$ is monic.

Claim: $g(x)$ is irreducible

Suppose $g(x) = a(x)b(x)$, where $\deg a(x), \deg b(x) < \deg g(x)$.

Then $g(\alpha) = a(\alpha)\,b(\alpha)$; since F is an ID, it must be that $a(\alpha) = 0$ or $\beta(\alpha) = 0$, contradicting minimality of the deg of $g(x)$. //

(b) Now suppose $f(x) \in F[x]$ has α as a root.

Use the Euclidean Algorithm to write

$$f(x) = q(x)\cdot g(x) + r(x) \qquad \deg r(x) < \deg g(x).$$

($g(x)$: minimal degree as in (a))

$$f(\alpha) = q(\alpha)\cdot \cancel{g(\alpha)}^{\,0} + r(\alpha) = 0 \implies r(\alpha) = 0.$$

Contradicts minimality of $\deg g(x) = 0 \Rightarrow r(x) = 0$.

$$\Rightarrow f(x) = q(x)\cdot g(x).$$ ∎

Cor. If we have

$$\begin{array}{c} K \ni \alpha \\ | \\ L \\ | \\ F \end{array}$$

and α is algebraic over both L and F,

then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

dfn. • $m_{\alpha,F}(x)$ is the minimal polynomial of α over F

↪ sometimes write $m_\alpha(x)$ if F elided

• $\deg m_{\alpha,F}(x)$ = the degree of α.

* Gröbner bases.

Eg. $f(x) = x^n - 2$ is irred by Eisenstein. Let α be a root.

$$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$$

Observations

① also the degree of the extension $F(\alpha)$ over F:

$F(\alpha) \cong F[x]/(m_\alpha(x))$.

② α is algebraic over F iff $[F(\alpha):F]$ is finite.

$\Rightarrow$ $F(\alpha) \cong F[x]/(m_\alpha(x))$ has basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

$\Leftarrow$ If $[F(\alpha):F] < \infty$, then

$\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ is linearly dependent,

so there exists a nonzero polynomial $(b_i \in F)$

$$p(x) = \sum_{i=0}^{n} b_i x^i$$

where $p(\alpha) = 0 \Rightarrow \alpha$ is alg over F.

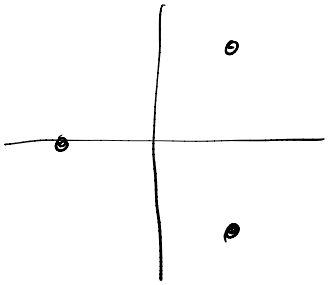
③ So if K/F is finite, it must be algebraic.

↳ can prove that K must be $F(\underbrace{\alpha_1, \alpha_2, \ldots, \alpha_k}_{\text{finite \# of generators}})$

where $\deg \alpha_i < \infty \ \forall\ i$.

Eg. $p(x) = x^3 - 3x - 1$ Recall Rational root theorem?

Roots:



Other facts (Try to prove them yourself / understand why they're true)

thm. Let $F \subseteq K \subseteq L$ be fields. Then $[L:F] = [L:K][K:F]$

Pf. idea

Key reminder: index = dim of VS

eg. if $\deg_{\mathbb{Q}} \alpha = 3$ then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$.

We need to use a VS basis.

Suppose $L = \mathrm{Span}_K\{\alpha_1, \dots, \alpha_m\}$ $\quad K = \mathrm{Span}_F\{\beta_1, \dots, \beta_n\}$.

Then show $L = \mathrm{Span}_F\{\alpha_i \beta_j\}_{i \in [m],\, j \in [n]}$.

(Need to show linear independence of this basis.)

On the other hand:

defn. An extension K/F is finitely generated if there are elements $\alpha_1, \alpha_2, \dots, \alpha_k$ such that $K = F(\alpha_1, \dots, \alpha_k)$.

note degree could be infinite, eg. $[\mathbb{Q}(\pi):\mathbb{Q}] = \infty$ and yet the extension is simple.

lemma $F(\alpha, \beta) = (F(\alpha))(\beta)$ (now induct; any fg. ext. can be built recursively)

Pf. Mat 108-style proof; double-inclusion; use minimality of generated fields.

Cor.

$$\begin{array}{l} F_k = K \\ \quad | \ [F_k : F_{k-1}] \\ F_{k-1} \\ \quad | \\ \quad \vdots \\ \quad | \ [F_1 : F_0] \\ F_0 \end{array} \quad \rightsquigarrow \quad [K:F] = \prod_{i=0}^{k-1} [F_{i+1} : F_i].$$

thm K/F is finite iff K is generated by a finite # of algebraic elements over F.

note If $[F(\alpha_i):F] = d_i$, then $[F(\{\alpha_i\}_{1\le i\le k}:F] \le \prod_{i=1}^{k} d_i$

Pf. think through this using the facts we've proven

$\Rightarrow$ Use the VS basis; these all have finite deg.

$\Leftarrow$ Use the note (build a set of VS generators). //

Cor. If α, β are algebraic over F, then $\alpha \pm \beta$, $\alpha\beta$, α/β (when $\beta \neq 0$) are all algebraic.

Cor Let L/F be an arbitrary extension. Then

$$L^{alg} = \{\ell \in L \mid \ell \text{ is algebraic over } F\}$$

forms a subfield of L.

Next time: Composite fields; splitting fields; alg. closures.