§15.3 Extension degree

We'll get a lot of mileage out of considering a field extension $\mathbb{K} \supset \mathbb{F}$ as an $\mathbb{F}$-vector space with the usual $+$ on $\mathbb{K}$ as vector addition and $\mathbb{F}$-scaling $\mathbb{F} \times \mathbb{K} \longrightarrow \mathbb{K}$, $(c, \alpha) \longmapsto c\alpha$ just restricting the multiplication in $\mathbb{K}$, $\mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$, $(\beta, \alpha) \longmapsto \beta\alpha$

DEFN. (15.3.1) The extension degree $[\mathbb{K}:\mathbb{F}] := \dim_{\mathbb{F}}(\mathbb{K})$ = dimension of $\mathbb{K}$ as an $\mathbb{F}$-vector space (maybe ∞ ?)

REMARK: Not a coincidence that it looks like $[G:H] = \text{index of } H \text{ in } G = |G/H|$

EXAMPLES: ① Recall we've seen finite fields $\mathbb{F}$ always have characteristic p a prime, and a copy of $\mathbb{F}_p = \{0, 1, \frac{1+1}{2}, \dots, \frac{1+1+\cdots+1}{p-1}\}$ inside them. So we get an extension $\mathbb{F}_p \subset \mathbb{F}$, and if $d := [\mathbb{F}:\mathbb{F}_p] = \dim_{\mathbb{F}_p}(\mathbb{F})$, then $|\mathbb{F}| = p^d = |(\mathbb{F}_p)^d|$ because $\mathbb{F} \cong (\mathbb{F}_p)^d$ as $\mathbb{F}_p$-vector space

② **PROPOSITION (15.3.4):** If $\alpha \ni \mathbb{K} \supset \mathbb{F}$, then

α is algebraic over $\mathbb{F} \iff [\mathbb{F}(\alpha):\mathbb{F}]$ is finite

in which case, $[\mathbb{F}(\alpha):\mathbb{F}] = \deg\left(m_{\mathbb{F},\alpha}(x)\right)$ (called the degree of α over $\mathbb{F}$)

(In particular $\alpha \in \mathbb{F} \iff [\mathbb{F}(\alpha):\mathbb{F}] = 1$)

Proof: When α is algebraic over $\mathbb{F}$, we know $\mathbb{F}(\alpha) = \mathbb{F}[\alpha] \cong \mathbb{F}[x]/\left(m_{\mathbb{F},\alpha}(x)\right) \cong \mathbb{F}^{\deg(m_{\mathbb{F},\alpha}(x))}$ as $\mathbb{F}$-vector spaces

i.e. $[\mathbb{F}(\alpha):\mathbb{F}] = \deg\left(m_{\mathbb{F},\alpha}(x)\right)$

When α is transcendental over $\mathbb{F}$, $\mathbb{F}(\alpha) \supset \mathbb{F}[\alpha] \cong \mathbb{F}[x]$ which is not finite-dimensional over $\mathbb{F}$ e.g. $\{1, x, x^2, \dots\}$ are $\mathbb{F}$-linearly independent ∎

e.g. $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ since $m_{\mathbb{Q},\sqrt{2}}=x^2-2$

$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$ $\quad m_{\mathbb{Q},\sqrt[4]{2}}=\underbrace{x^4-2}$ ↑ irred. by Eisenstein at $p=2$

$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]=2$ since $m_{\mathbb{Q}(\sqrt{2}),\sqrt[4]{2}}(x)$ divides into $x^2-\sqrt{2}$ and it can't have degree 1 since $\sqrt[4]{2}\notin\mathbb{Q}(\sqrt{2})$ ← EXERCISE!

$\mathbb{Q}(\sqrt[4]{2})$ — 4 — $\mathbb{Q}(\sqrt{2})$ — 2 — $\mathbb{Q}$

$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})$

degree 2 · degree 2 = degree 4

The most crucial property of extension degree:

THEOREM (5.3.5): For a tower of field extensions $\mathbb{F}\subset\mathbb{K}\subset\mathbb{L}$

one has $[\mathbb{L}:\mathbb{F}]=[\mathbb{K}:\mathbb{F}]\cdot[\mathbb{L}:\mathbb{K}]$. (call this m; call this n)

$\mathbb{L}$ — n — $\mathbb{K}$ — m — $\mathbb{F}$) mn

In particular, $[\mathbb{K}:\mathbb{F}]$, $[\mathbb{L}:\mathbb{K}]$ both divide $[\mathbb{L}:\mathbb{F}]$

Proof: Pick an $\mathbb{F}$-basis $\{\alpha_1,\dots,\alpha_m\}$ for $\mathbb{K}$ and an $\mathbb{K}$-basis $\{\beta_1,\dots,\beta_n\}$ for $\mathbb{L}$ } assuming m,n finite for the moment

and we'll show the mn products $\{\alpha_i\beta_j\}_{\substack{i=1,\dots,m\\ j=1,\dots,n}}$ give an $\mathbb{F}$-basis for $\mathbb{L}$

They span $\mathbb{L}$ over $\mathbb{F}$ since any $\ell\in\mathbb{L}$ can be written $\ell=\sum_{j=1}^{n}k_j\beta_j$ with $k_j\in\mathbb{K}$

and then each k_j can be written $k_j=\sum_{i=1}^{m}c_{ij}\alpha_i$ with $c_{ij}\in\mathbb{F}$

$$\text{so } \ell=\sum_{j=1}^{n}k_j\beta_j=\sum_{j=1}^{n}\sum_{i=1}^{m}c_{ij}\alpha_i\beta_j$$

(This also shows m,n finite $\Rightarrow$ $[\mathbb{L}:\mathbb{F}]$ finite)

They're linearly independent since if $\sum_{i,j}c_{ij}\alpha_i\beta_j=0$

then $\{\beta_1,\dots,\beta_n\}$ indep. over $\mathbb{K}$ $\Rightarrow$ $\sum_i c_{ij}\alpha_i=0$ for each $j=1,\dots,n$

and $\{\alpha_1,\dots,\alpha_m\}$ indep. over $\mathbb{F}$ $\Rightarrow$ $c_{1j}=\dots=c_{mj}=0$ for each $j=1,\dots,n$

i.e. all $c_{ij}=0$

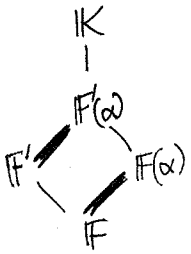
If $[\mathbb{K}:\mathbb{F}]=\infty$ then $\exists$ $\mathbb{F}$-lin. indep. $\{\beta_1,\beta_2,\dots\} \subset \mathbb{K} \subset \mathbb{L}$, so $[\mathbb{L}:\mathbb{F}]=\infty$.

If $[\mathbb{L}:\mathbb{F}]$ is finite then any finite $\mathbb{F}$-spanning set $\{\gamma_1,\dots,\gamma_N\}$ for $\mathbb{L}$ also gives a $\mathbb{K}$-spanning set for $\mathbb{L}$, so $[\mathbb{L}:\mathbb{K}]$ is finite ∎

This has lots of corollaries.

COROLLARY: (15.3.6) (a) In a finite extension $[\mathbb{K}:\mathbb{F}]=n<\infty$, every $\alpha\in\mathbb{K}$ is algebraic over $\mathbb{F}$, with degree d dividing n

(since $n=[\mathbb{K}:\mathbb{F}]=[\mathbb{K}:\mathbb{F}(\alpha)]\,[\mathbb{F}(\alpha):\mathbb{F}]$, where $[\mathbb{F}(\alpha):\mathbb{F}]$ = degree of α over $\mathbb{F}$ = d)



(b) In a tower $\mathbb{F}\subset\mathbb{F}'\subset\mathbb{K}$ if $\alpha\in\mathbb{K}$ is algebraic over $\mathbb{F}$, then it is algebraic over $\mathbb{F}'$, with $[\mathbb{F}'(\alpha):\mathbb{F}'] \le [\mathbb{F}(\alpha):\mathbb{F}]$ (degree of α over $\mathbb{F}'$ ≤ degree of α over $\mathbb{F}$)

(c) $[\mathbb{K}:\mathbb{F}]$ is finite $\iff$ $\mathbb{K}=\mathbb{F}(\alpha_1,\alpha_2,\dots,\alpha_n)$ for a finite subset of algebraic (over $\mathbb{F}$) elements $\{\alpha_1,\dots,\alpha_n\}\subset\mathbb{K}$

(d) In any field extension $\mathbb{F}\subset\mathbb{K}$, $\mathbb{K}_{\text{algebraic over }\mathbb{F}} := \{\alpha\in\mathbb{K}: \alpha \text{ algebraic over } \mathbb{F}\}$ is a subfield of $\mathbb{K}$

proof: (a): we saw already.

(b): Note that $m_{\mathbb{F},\alpha}(x)\in\mathbb{F}[x]\subset\mathbb{F}'[x]$ gives a polynomial satisfied by α, but there may be one of lower degree in $\mathbb{F}'[x]$.

(c): If $[\mathbb{K}:\mathbb{F}]=n$ is finite, any $\mathbb{F}$-basis $\{\alpha_1,\dots,\alpha_n\}$ for $\mathbb{K}$ will have $\mathbb{K}=\mathbb{F}(\alpha_1,\alpha_2,\dots,\alpha_n)$
Conversely, if $\mathbb{K}=\mathbb{F}(\alpha_1,\dots,\alpha_n)$ with each α_i algebraic over $\mathbb{F}$, then consider the tower

$$\mathbb{F}\subset\mathbb{F}(\alpha_1)\subset\mathbb{F}(\alpha_1,\alpha_2)\subset\cdots\subset\mathbb{F}(\alpha_1,\dots,\alpha_n)=\mathbb{K}$$

which has each step $[\mathbb{F}(\alpha_1,\dots,\alpha_{i-1},\alpha_i):\mathbb{F}(\alpha_1,\dots,\alpha_{i-1})]$ finite, since α_i is algebraic over $\mathbb{F}$ so algebraic over $\mathbb{F}(\alpha_1,\dots,\alpha_{i-1})$
Thus $[\mathbb{K}:\mathbb{F}]=\prod_i [\mathbb{F}(\alpha_1,\dots,\alpha_{i-1},\alpha_i):\mathbb{F}(\alpha_1,\dots,\alpha_{i-1})]$ is also finite.

(d): If $\alpha,\beta\in\mathbb{K}$ are algebraic over $\mathbb{F}$, then so are $\alpha+\beta$, $\alpha\beta$ (using (a) since they lie in $\mathbb{F}(\alpha,\beta)$ which has $[\mathbb{F}(\alpha,\beta):\mathbb{F}]$ finite by (c). ∎