Math 8202 Fields and extensions (D&F Chap. 13, 14)

Studying how fields sit inside each other turns out to be useful in solving equations, among other things.

DEFINITION: A *field extension* $\mathbb{K}/\mathbb{F}$ or $\begin{array}{c}\mathbb{K}\\ | \\ \mathbb{F}\end{array}$

is an inclusion $\mathbb{F} \subseteq \mathbb{K}$ or

equivalently, a nonzero map $\mathbb{F} \xrightarrow{\varphi} \mathbb{K}$

(since this forces $\ker\varphi = 0$, $\mathbb{F} \xrightarrow{\sim} \operatorname{im}\varphi \subseteq \mathbb{K}$)

A *tower* of fields is just a sequence $\mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \dots$

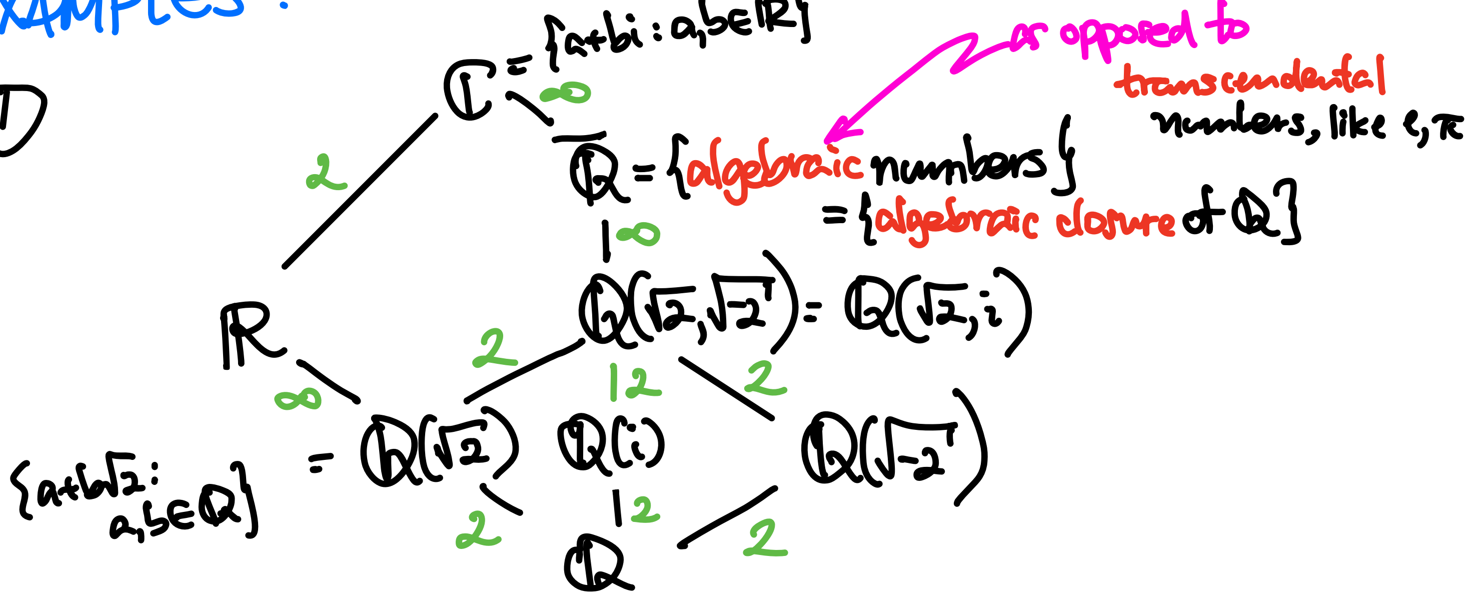
Note $\mathbb{F} \subset \mathbb{K}$ makes $\mathbb{K}$ an $\mathbb{F}$-vector space,

and one defines the *extension degree* $[\mathbb{K}:\mathbb{F}] := \dim_{\mathbb{F}} \mathbb{K}$,

allowing $[\mathbb{K}:\mathbb{F}] = \infty$.

EXAMPLES:

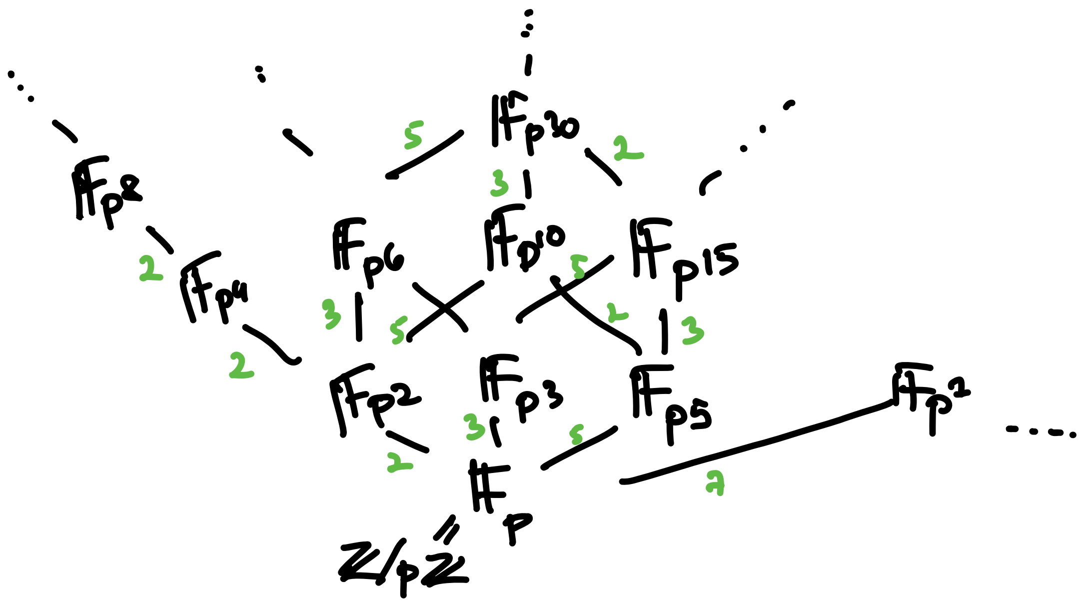
①



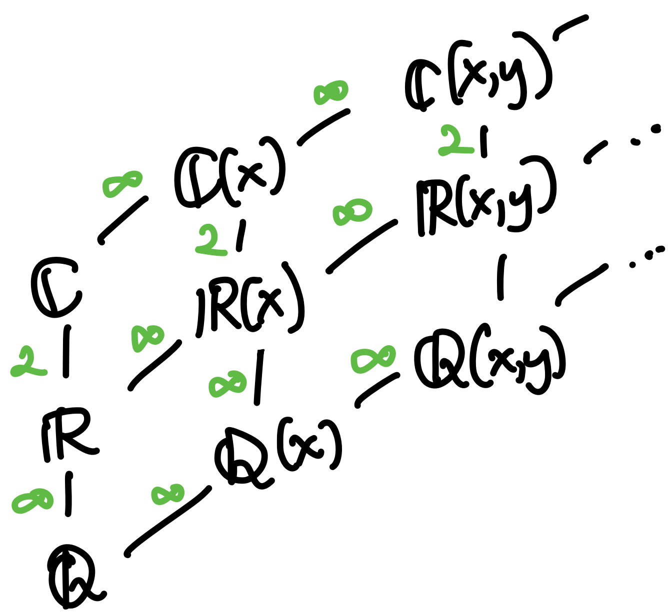
② We are going to build finite fields $\mathbb{F}_q$ with $|\mathbb{F}_q| = p^d$ for primes p and $d = 1, 2, \ldots$

$\overline{\mathbb{F}}_p$ ← algebraic closure of $\mathbb{F}_p$ (not finite)

$\cup$



③



The notation $[\mathbb{K}:\mathbb{F}]$ is suggestive of index $[G:H] = |G/H|$ in group theory, and of this fact:

PROPOSITION: In a tower of fields
$$\begin{array}{c} \mathbb{L} \\ |\, e \\ \mathbb{K} \\ |\, d \\ \mathbb{F} \end{array} \quad de$$

one has $\overset{de}{[\mathbb{L}:\mathbb{F}]} = \overset{e}{[\mathbb{L}:\mathbb{K}]}\,\overset{d}{[\mathbb{K}:\mathbb{F}]}$ (allowing ∞'s)

since an $\left\{\begin{array}{l} \mathbb{F}\text{-basis } \{\kappa_i\}_{i\in I} \text{ for } \mathbb{K} \\ \mathbb{K}\text{-basis } \{\lambda_j\}_{j\in J} \text{ for } \mathbb{L} \end{array}\right\}$ give an $\mathbb{F}$-basis for $\mathbb{L}$. $\{\kappa_i\lambda_j\}_{\substack{i\in I\\ j\in J}}$

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

proof: Straightforward:

SPANNING: $\lambda \in \mathbb{L}$ has $\lambda = \sum_{j\in J} k_j \lambda_j$ with $k_j \in \mathbb{K}$

and each $k_j = \sum_{i\in I} f_{ij}\kappa_i$ with $f_{ij}\in\mathbb{F}$, so $\lambda = \sum_{\substack{j\in J\\ i\in I}} f_{ij}\kappa_i\lambda_j$

INDEPENDENCE: $0 = \sum_{\substack{j\in J\\ i\in I}} f_{ij}\kappa_i\lambda_j$ in $\mathbb{L}$

$$= \sum_{j\in J} \underbrace{\Big(\sum_{i\in I} f_{ij}\kappa_i\Big)}_{\substack{\text{must be } 0\\ \text{since } \{\lambda_j\}\\ \text{indep over } \mathbb{K}}}\lambda_j \Rightarrow \text{each } f_{ij} = 0 \text{ since } \{\kappa_i\} \text{ indep. over } \mathbb{F}$$

$\blacksquare$

Every field extends a smallest field within it.

DEFINITION-PROPOSITION For a field $\mathbb{F}$, the unique ring map

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{F} \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 1+1 \\ 3 & \longmapsto & 1+1+1 \\ \vdots & & \end{array}$$

either has $\ker\varphi = p\mathbb{Z}$ and $\operatorname{im}\varphi \cong \mathbb{F}_p \subset \mathbb{F}$ for some prime p, called the characteristic $\operatorname{char}(\mathbb{F}) := p$,

or $\ker\varphi = \{0\}$ and $\operatorname{im}\varphi \cong \mathbb{Z} \subset \mathbb{F}$, generating a subfield isomorphic to $\mathbb{Q}$ inside $\mathbb{F}$, and one says $\operatorname{char}(\mathbb{F}) = 0$.

In either case $\mathbb{F}_p$ or $\mathbb{Q}$ is the smallest subfield of $\mathbb{F}$, contained in any other, generated by $\{1\}$, called its prime subfield.

proof: Since $\operatorname{im}(\varphi) \subset \mathbb{F}$, a domain, $\operatorname{im}(\varphi)$ is a domain.

Hence $\mathbb{Z}/\ker(\varphi) \cong \operatorname{im}(\varphi) \Rightarrow$

$\ker(\varphi) \subset \mathbb{Z}$ is a prime ideal, so either $\{0\}$ or $p\mathbb{Z}$ for some prime p. The rest follows. $\blacksquare$

COROLLARY: A finite field $\mathbb{F}$ always has $\operatorname{char}(\mathbb{F}) = p$ a prime, and cardinality $|\mathbb{F}| = p^d$ for $d = [\mathbb{F} : \mathbb{F}_p]$.

proof: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{F}$ cannot inject if $\mathbb{F}$ is finite.

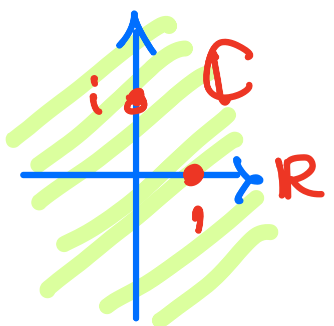
So $\operatorname{im}\varphi = \mathbb{F}_p \subset \mathbb{F}$, and $\mathbb{F} \cong (\mathbb{F}_p)^d$ for $d = \dim_{\mathbb{F}_p}(\mathbb{F})$
$= [\mathbb{F} : \mathbb{F}_p]$ $\blacksquare$

How to build them?

Same way that we built $\mathbb{C}$ from $\mathbb{R}$, by **adjoining a root** i for the irreducible $x^2+1 \in \mathbb{R}[x]$ that had no roots in $\mathbb{R}$:

$$\underbrace{\mathbb{R}[x]/(\overbrace{x^2+1}^{\text{a maximal ideal, since } x^2+1 \text{ irreducible/prime/maximal in the PID } \mathbb{R}[x]})}_{\text{a field}} \xrightarrow{\sim} \mathbb{C}$$

$$\bar{x} \longmapsto i$$



PROPOSITION: If $f(x) \in \mathbb{F}[x]$ is irreducible, then $\mathbb{K} = \mathbb{F}[x]/(f(x))$ is a field extension in which $\alpha := \bar{x}$ is a root of $f(y) \in \mathbb{K}[y]$.

$$\begin{array}{c} \mathbb{K} \\ | \\ \mathbb{F} \end{array}$$

Furthermore, $[\mathbb{K}:\mathbb{F}] = \deg(f) =: d$ since $\mathbb{K}$ has $\mathbb{F}$-basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$

proof: $(f(x)) \subset \mathbb{F}[x]$ is prime, so maximal, so $\mathbb{K} = \mathbb{F}[x]/(f(x))$ is a field, and $\alpha := \bar{x}$ has $f(\bar{x}) = \overline{f(x)} = \bar{0}$ in $\mathbb{K}$, and $\mathbb{K}$ has $\mathbb{F}$-basis $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1}\} = \{1, \alpha, \ldots, \alpha^{d-1}\}$ $\blacksquare$

EXAMPLE: We classified low-degree irreducibles in $\mathbb{F}_2[x]$

deg 1	deg 2	deg 3	deg 4
x	x^2+x+1	x^3+x+1	x^4+x+1
$x+1$		x^3+x^2+1	x^4+x^3+1
			$x^4+x^3+x^2+x+1$

$\Rightarrow$ we can build finite fields ...

$\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1)$ with $\alpha = \bar{x}$ satisfying $\boxed{\alpha^2+\alpha+1=0}$ i.e., $\alpha^2 = \alpha+1$

$\mathbb{F}_4 = \mathbb{F}_{2^2}$

$= \operatorname{span}_{\mathbb{F}_2}\{1, \alpha\}$

$= \{0, 1, \alpha, \alpha+1\}$

mult. inverses: $\alpha(\alpha+1) = \alpha^2+\alpha = 1$

$\mathbb{F}_8 := \mathbb{F}_2[x]/(x^3+x+1)$ or $\mathbb{F}_8' := \mathbb{F}_2[x]/(x^3+x^2+1)$

$\mathbb{F}_8 = \mathbb{F}_{2^3}$

(Later we'll see why $\mathbb{F}_8 \cong \mathbb{F}_8'$ as fields, because all $\mathbb{F}_q$ of same size $q=p^d$ are isomorphic)

This viewpoint also helps us understand extension degrees when we generate subfields inside bigger fields.

DEFINITION: Given $\mathbb{F} \subset \mathbb{K}$ and $\alpha \in \mathbb{K}$,

let $\mathbb{F}[\alpha]$ = smallest subring of $\mathbb{K}$ containing $\mathbb{F}, \alpha$

$\mathbb{F}(\alpha)$ = smallest subfield of $\mathbb{K}$ containing $\mathbb{F}, \alpha$

So $\mathbb{F} \subseteq \mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}$,

and similarly for $\mathbb{F}[\alpha_1, \ldots, \alpha_m]$ given $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$.

$\mathbb{F}(\alpha_1, \ldots, \alpha_m)$

Extensions $\mathbb{F} \subset \mathbb{F}(\alpha)$ are called simple extensions.

EXAMPLES:

① $\mathbb{Q} \subsetneq \mathbb{Q}[i] \subsetneq \mathbb{C}$

$$\mathbb{Q}[i] = \mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$$

② $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{-2}] = \mathbb{Q}[i, \sqrt{2}] \subsetneq \mathbb{C}$

$$\mathbb{Q}[\sqrt{2}, \sqrt{-2}] = \mathbb{Q}(\sqrt{2}, \sqrt{-2}) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$$

not obvious; we'll see why later

③ $\mathbb{Q} \subsetneq \mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi) \subsetneq \mathbb{R}$, $\pi := 3.14159\ldots$

$$\mathbb{Q}[\pi] \cong \mathbb{Q}[x], \quad \mathbb{Q}(\pi) \cong \mathbb{Q}(x)$$

polynomials rational functions

transcendental - a root of no $f(x) \in \mathbb{Q}[x]$

There is a dichotomy in simple extensions:

DEFINITION-PROPOSITION: Given an extension $\mathbb{F} \subset \mathbb{K}$ and $\alpha \in \mathbb{K} - \mathbb{F}$, the ring map $\mathbb{F}[x] \xrightarrow{\varphi} \mathbb{K}$

defined by $x \longmapsto \alpha$

(so $f(x) \longmapsto f(\alpha)$)

either has

- $\ker \varphi = \{0\}$, in which case α is called **transcendental over $\mathbb{F}$** (e.g. $\alpha = \pi \in \mathbb{R} - \mathbb{Q}$)

  and one has $\mathbb{F} \subsetneq \mathbb{F}[\alpha] \subsetneq \mathbb{F}(\alpha) \subsetneq \mathbb{K}$

$$\begin{array}{ccc} \mathbb{F}[\alpha] & \subsetneq & \mathbb{F}(\alpha) \\ \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} \\ \mathbb{F}[x] & \subsetneq & \mathbb{F}(x) \end{array}$$

polynomials $f(x)$ → $\mathbb{F}[x]$; rational functions $f(x)/g(x)$ → $\mathbb{F}(x)$

or

- $\ker \varphi = (m_{\alpha,\mathbb{F}}(x)) \subset \mathbb{F}[x]$ for some unique **monic, irreducible** polynomial $m_{\alpha,\mathbb{F}}(x) \subset \mathbb{F}[x]$, called the **minimal polynomial of α over $\mathbb{F}$**

  In this case, α is called **algebraic over $\mathbb{F}$**

  (e.g. $\alpha = \sqrt{2} \in \mathbb{R} - \mathbb{Q}$ has $m_{\alpha,\mathbb{Q}} = x^2 - 2 \in \mathbb{Q}[x]$)

  and one has $\mathbb{F} \subsetneq \mathbb{F}[\alpha] = \mathbb{F}(\alpha) \subsetneq \mathbb{K}$.

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

proof: • When $\ker\varphi = \{0\}$, φ is a ring isomorphism

$$\mathbb{k}[x] \xrightarrow{\sim} \operatorname{im}\varphi = \mathbb{F}[\alpha].$$

so $\mathbb{F}[\alpha] \cong \mathbb{k}[x]$. But then

$$\begin{array}{ccc} \operatorname{Frac}(\mathbb{F}[\alpha]) & = & \mathbb{F}(\alpha) \\ \cong & & \cong \\ \operatorname{Frac}(\mathbb{F}[x]) & = & \mathbb{F}(x) \end{array}$$

• When $\ker\varphi \neq \{0\}$, it's an ideal in $\mathbb{F}[x]$.
But $\operatorname{im}\varphi \subset \mathbb{K}$ implies $\operatorname{im}\varphi$ is a domain, and $\mathbb{F}[x]/\ker\varphi \cong \operatorname{im}\varphi$ implies $\ker\varphi$ is a prime ideal in $\mathbb{F}[x]$. But then it is also maximal in $\mathbb{F}[x]$,
so $\mathbb{F}[\alpha] \cong \mathbb{F}[x]/\ker\varphi$ is a field,
and a subfield of $\mathbb{K}$ containing $\mathbb{F}, \alpha$, so $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.
Naming the monic generator $m_{\alpha,\mathbb{F}}(x)$ for $\ker\varphi = (m_{\alpha,\mathbb{F}}(x))$, the rest follows from Noether's 1st ∎

REMARK: In a tower $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$, any $\alpha \in \mathbb{L}$ will have $m_{\alpha,\mathbb{K}}(x)$ dividing $m_{\alpha,\mathbb{F}}(x)$ in $\mathbb{K}[x]$.

EXAMPLE: $\mathbb{Q} \underset{2}{\subset} \mathbb{Q}(\sqrt{7}) \underset{2}{\subset} \mathbb{Q}(\sqrt[4]{7}) \ni \alpha := \sqrt[4]{7}$

has $m_{\sqrt[4]{7},\mathbb{Q}(\sqrt{7})}(x) = x^2 - \sqrt{7}$

dividing $m_{\sqrt[4]{7},\mathbb{Q}}(x) = x^4 - 7 \; \left(= (x^2 - \sqrt{7})(x^2 + \sqrt{7}) \text{ in } \mathbb{Q}(\sqrt{7})[x] \right)$

COROLLARY: A simple extension $\mathbb{K} = \mathbb{F}(\alpha)$ / $\mathbb{F}$

has $\underbrace{[\mathbb{K}:\mathbb{F}] \text{ finite}}_{\text{called a finite extension}} \iff \alpha$ is algebraic over $\mathbb{F}$.

proof: We've seen α algebraic over $\mathbb{F}$

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

Conversely, if $[\mathbb{F}(\alpha):\mathbb{F}] =: d < \infty$, then $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}, \alpha^d\}$ are $\mathbb{F}$-linearly dependent in $\mathbb{F}(\alpha)$,

so $\exists\, c_0, \dots, c_d \in \mathbb{F}$ with $c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_d\alpha^d = 0$

i.e. α is a root $f(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{F}[x]$. ■

COROLLARY: An extension $\mathbb{K}/\mathbb{F}$ has $[\mathbb{K}:\mathbb{F}]$ finite

$\iff \mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_r)$ for finitely many algebraic elements $\alpha_1, \dots, \alpha_r \in \mathbb{K}$.

In this case $[\mathbb{K}:\mathbb{F}] \le \prod_{i=1}^{r} \underbrace{[\mathbb{F}(\alpha_i):\mathbb{F}]}_{= \deg m_{\alpha_i,\mathbb{F}}(x)}$

proof: $(\Rightarrow)$: If $[\mathbb{K}:\mathbb{F}] < \infty$, show $\mathbb{K}(\alpha_1, \dots, \alpha_r)$

by induction on $[\mathbb{K}:\mathbb{F}]$. Either $\mathbb{K} = \mathbb{F}$, or

$\exists\, \alpha_1 \in \mathbb{K} \setminus \mathbb{F}$, so one has $\mathbb{F} \subsetneq \mathbb{F}(\alpha_1) \subseteq \mathbb{K}$,

and by induction on $[\mathbb{K} : \mathbb{F}(\alpha_1)]$, one has

$$\mathbb{K} = \mathbb{F}(\alpha_1)(\alpha_2, \ldots, \alpha_m) = \mathbb{F}(\underbrace{\alpha_1, \alpha_2, \ldots, \alpha_m}_{\text{all algebraic over } \mathbb{F}, \text{ since } [\mathbb{K}:\mathbb{F}] \text{ finite}})$$

($\Leftarrow$): Consider the tower

$$\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \mathbb{F}(\alpha_1, \alpha_2) \subset \ldots \subset \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbb{K}$$

and
$$[\mathbb{K} : \mathbb{F}] = \prod_{i=1}^{r} \underbrace{[\mathbb{F}(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})]}_{\substack{= \deg m_{\alpha_i, \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})}(x) \\ \leq \deg m_{\alpha_i, \mathbb{F}}(x) = [\mathbb{F}(\alpha_i) : \mathbb{F}]}}$$

$$\leq \prod_{i=1}^{r} [\mathbb{F}(\alpha_i) : \mathbb{F}] \qquad \blacksquare$$