403/503 L35

Example

Find a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)/\mathbb{Q}$.

Since $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ we know $\sqrt{5}i \notin \mathbb{Q}(\sqrt[3]{5})$. On the other hand $\sqrt{5}i$ is a root of $x^2+5 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[3]{5})[x]$ so x^2+5 is the minimum polynomial for $\sqrt{5}i$ over $\mathbb{Q}(\sqrt[3]{5})$. So

$$[\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i) : \mathbb{Q}(\sqrt[3]{5})] = 2$$

and $\{1, \sqrt{5}i\}$ is a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$ over $\mathbb{Q}(\sqrt[3]{5})$.

Also, $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ is a basis for $\mathbb{Q}(\sqrt[3]{5})$ over $\mathbb{Q}$ (since $\sqrt[3]{5}$ is a root of the irr pol $x^3-5 \in \mathbb{Q}[x]$), Therefore the following is a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$ over $\mathbb{Q}$:

$$\{1, \sqrt{5}i, \sqrt[3]{5}, \sqrt[3]{5}\cdot\sqrt{5}i, (\sqrt[3]{5})^2, (\sqrt[3]{5})^2\sqrt{5}i\}$$

$$= \{1, 5^{3/6}i, \underbrace{5^{2/6}}_{=-(5^{1/6}i)^2}, 5^{5/6}i, 5^{4/6}, \underbrace{5^{7/6}}_{\text{replace by } 5^{1/6}i}i\}$$

(still get a basis over $\mathbb{Q}$)

We see that in fact with $\alpha = \sqrt[6]{5}\cdot i$
$\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^5\}$ is a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$ over $\mathbb{Q}$.

So $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i) = \mathbb{Q}(\sqrt[6]{5}i)$.

(Both have degree 6 over $\mathbb{Q}$ ~~and~~

Since $\alpha = \sqrt[6]{5}i$ satisfies $x^6 + 5 \in \mathbb{Q}[x]$

irr by Eisenstein $p = 5$.

And $\sqrt[6]{5}i \in \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$ by

$(\sqrt[3]{5})^2 \sqrt{5}i = 5^{7/6} i = 5 \cdot \sqrt[6]{5}i$

So $\mathbb{Q}(\sqrt[6]{5}i) \subseteq \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$

Since both have dimension 6 over $\mathbb{Q}$,

Th. 21.22 Let E/F be a field extension.

TFAE

i) E/F is finite (i.e. $[E:F] < \infty$)

ii) $\exists$ finitely many algebraic elements

$\alpha_1, \ldots, \alpha_n \in E$ such that

$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

iii) $\exists$ a seq of fields

$E = F(\alpha_1, \ldots, \alpha_n) \supseteq F(\alpha_1, \ldots, \alpha_{n-1}) \supseteq \cdots \supseteq F(\alpha_1) \supseteq F$

Where each $F(\alpha_1, \ldots, \alpha_k)$ is algebraic over $F(\alpha_1, \ldots, \alpha_{k-1})$.

Proof

i) ⟹ ii) : Let E/F be a finite extension. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for E over F.

Each α_i is algebraic over F (since E/F finite ⟹ E/F algebraic)

and

$$E = \mathrm{span}_F\{\alpha_i\} \subseteq F(\alpha_1, \dots, \alpha_n) \subseteq E$$

implies $E = F(\alpha_1, \dots, \alpha_n)$.

ii) ⟹ iii) : Suppose $E = F(\alpha_1, \dots, \alpha_n)$ where each α_i is algebraic over F. Then

$$[F(\alpha_1, \dots, \alpha_i) : F] = \underbrace{[F(\alpha_1, \dots, \alpha_{i-1})(\alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]}_{\leq [F(\alpha_i):F] < \infty} \underbrace{[F(\alpha_1, \dots, \alpha_{i-1}) : F]}_{< \infty \text{ by Induction Hyp.}}$$

We claim

$[F(\alpha_1, \dots, \alpha_i) : F] < \infty$ for $i = 1, 2, \dots, n$.

We prove it by induction:

$[F(\alpha_1) : F] < \infty$ since α_1 is algebraic/F.

Thus $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$ so E/F is algebraic.

iii) $\Rightarrow$ i): Suppose

$$E = F(\alpha_1, \ldots, \alpha_n) \supseteq \cdots \supseteq F(\alpha_1) \supseteq F$$

where each $F(\alpha_1, \ldots, \alpha_i)/F(\alpha_1, \ldots, \alpha_{i-1})$ is algebraic. Then

$$[F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]$$

$= [K_{i-1}(\alpha_i) : K_{i-1}]$, $K_{i-1} = F(\alpha_1, \ldots, \alpha_{i-1})$

$< \infty$ since α_i is algebraic over K_{i-1}

By the Degree Formula:

$$[E:F] = [\underbrace{K_n : K_{n-1}}_{<\infty}][\underbrace{K_{n-1} : K_{n-2}}_{<\infty}] \cdots [\underbrace{K_1 : F}_{<\infty}] < \infty$$

proving i). ∎

Example. $\mathbb{Q}(\sqrt[5]{7}, \sqrt[3]{2}\, i)$ is a finite extension of $\mathbb{Q}$ since $\sqrt[5]{7}$ and $\sqrt[3]{2}\, i$ are both algebraic over $\mathbb{Q}$. So $\mathbb{Q}(\sqrt[5]{7}, \sqrt[3]{2}\, i)/\mathbb{Q}$ is algebraic. For example:

$$\sqrt[5]{7} \pm \sqrt[3]{2}\, i, \quad \sqrt[5]{7} \cdot \sqrt[3]{2}\, i, \quad \sqrt[5]{7} / \sqrt[3]{2}\, i$$

must be algebraic over $\mathbb{Q}$.

Algebraic Closure.

Thm Let E/F be an extension of fields. The set of $\alpha \in E$ that are algebraic over F is a subfield of E containing F.

Proof If $\alpha, \beta \in E$ are algebraic over F then, by Th 21.22, $F(\alpha,\beta)/F$ is finite hence algebraic. So $\alpha \pm \beta$, α/β (if $\beta \neq 0$), $\alpha \cdot \beta$ which all belong to $F(\alpha,\beta)$ must be algebraic over F. ∎

Def Given a field extension E/F, the algebraic closure of F in E is the set of all $\alpha \in E$ that are algebraic over F.

Example Let M be the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$. Then $\sqrt[3]{2} \in M$, but $\sqrt{5}\, i \notin M$.

$$\begin{array}{c} \mathbb{R} \\ | \\ M \\ | \\ \mathbb{Q} \end{array}$$

Thm TFAE for a field K:

1) Every nonconstant $p(x) \in K[x]$ factors into linear factors over K, i.e.:
$p(x) = (x-\lambda_1) \cdots (x-\lambda_n)$
for some $\lambda_i \in K$.

2) Every nonconstant $p(x) \in K[x]$ has a root in K.

3) K has no algebraic extension field (other than K itself).

Proof 1) $\Rightarrow$ 2): Trivial.

2) $\Rightarrow$ 3): If E/K is algebraic and $E \neq K$, pick $\alpha \in E$, $\alpha \notin K$. Let $m(x)$ be the minimum polynomial for α over K. By 2), $m(x)$ has a root in K. This contradicts that $m(x)$ is irreducible.

3) $\Rightarrow$ 1): It suffices to show every irreducible polynomial$/K$ has degree 1. Suppose $p(x) \in K[x]$ is irreducible. Then $E := K[x]/(p(x))$ is an algebraic extension of K. By 3), $E = K$ which means $\deg p(x) = 1$

Def A field satisfying the above equivalent conditions is called algebraically closed.

Theorem Let F be any field. Then there exists a field extension $\overline{F}/F$ such that

i) $\overline{F}$ is algebraically closed

ii) The algebraic closure of F in $\overline{F}$ equals $\overline{F}$

Furthermore, if E/F is any such field extension, then $E \cong \overline{F}$.

Def $\overline{F}$ is called the algebraic closure of F.

(We skip the proof.)

Example $\overline{\mathbb{R}} = \mathbb{C}$

$\overline{\mathbb{Q}} = \mathbb{A} = \{$ field of algebraic numbers $\} =$

$= \{ z \in \mathbb{C} \mid p(z) = 0$ for some $p(x) \in \mathbb{Q}[x] \}$

$=$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.