date: wednesday, march 27, 2024

Field Extensions and Linear Algebra

Observation: If E is an extension of the field F, then E is also an F-vector space.
Ie. the elements of E are the "vectors", the elements of F are the "scalars", with scalar multiplication

$$F \times E \to E$$
$$(f, e) \mapsto fe.$$

eg. $\mathbb{C}$ is an extension of $\mathbb{R}$. So $\mathbb{C}$ is an $\mathbb{R}$-vector space

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C}$$
$$(r, a+bi) \mapsto r(a+bi) = ra + rbi$$

To do: check that all axioms of a vector space field hold.

Theorem: Let $E = F(\alpha)$ be simple extension of F, where $\alpha \in E$ is algebraic over F. Suppose degree of $\alpha = n$ (= degree of minimum polynomial of α).
Then every element of $F(\alpha)$ can be written uniquely as

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

with $b_i \in F$.

eg. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Proof: see text

eg. $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$.

Recall: If E is an F-vector space, the dimension of E over F is

$$\dim_F E = \text{number of basis elements.}$$

Corollary: If $E = F(\alpha)$ is a simple extension with $\alpha \in E$ algebraic over F, then
$$\dim_F E = n = \text{degree of } \alpha.$$

Proof
$F(\alpha)$ is a F-vector space. By previous result,
$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$
is a basis for $F(\alpha)$ over F.

$\square$

eg. $\dim_{\mathbb{R}} \mathbb{C} = 2$ and $\dim_{\mathbb{C}} \mathbb{C} = 1$

eg. $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$

Def^n: If E is an extension of F, we let $[E:F] = \dim_F E$. We say E has finite extension of degree $n = [E:F]$ over F.

eg. $[\mathbb{C} : \mathbb{R}] = 2$.

Theorem: If $[E:F] < \infty$, then E is an algebraic extension of F.

Proof
Let $n = [E:F]$. Let $\alpha \in E$. Consider $1, \alpha, \alpha^2, \dots, \alpha^n$. We have $n+1$ "things" = "vectors" in E since $[E:F] = n$, these vectors are linearly dependent. So exists $b_0, \dots, b_n \in F$ such that
$$b_0 \cdot 1 + b_1 \cdot \alpha + \dots + b_n \alpha^n = 0.$$
Create the polynomial $p(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n$. So α is a root of the polynomial. So E is algebraic over F.

$\square$

Note: There are fields E that are algebraic but $[E:F] = \infty$.

eg. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \dots)$

eg. Since π is not algebraic over $\mathbb{Q}$, $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Theorem: If E has extension of F and K is an extension of E, then K is an extension of F. ($F \subseteq E \subseteq K$).
If these are finite extensions, then

$$[K:F]=[K:E]=[E:F].$$

$$\left.\begin{array}{l}\left.\begin{array}{l}K\\E\end{array}\right\}n_2\\ \left.\begin{array}{l}E\\F\end{array}\right\}n_1\end{array}\right\}n_1n_2$$

<u>Proof Idea</u>

Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis for E over F and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is a basis for K over E.
Claim: $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for K over F.
Need to show this set is linearly independent and span K over F.
By claim: $[K:F]=mn=[E:F][K:F]$.

$\square$

Corollary: If F_1 is a finite extension of F_0.
F_2 is a finite extension of F_1.
$\vdots$
F_t is a finite extension of F_{t-1}.
Then,

$$[F_t:F_0]=[F_t:F_{t-1}][F_{t-1}:F_{t-2}]\cdots[F_1:F_0].$$

Corollary: If $\alpha \in E$ is algebraic over F with minimal polynomial $p(x)$ and $\beta \in F(\alpha)$ with the minimal polynomial $q(x)$, then $\deg q(x) \mid \deg p(x)$.

<u>Proof</u>

We have $\beta \in F(\alpha)$, so $F(\beta) \leq F(\alpha)$. So

$$[F(\alpha):F]=[F(\alpha):F(\beta)][F(\beta):F]$$

so

$$\deg p(x) = [F(\alpha):F(\beta)] \deg q(x).$$

$\square$

Theorem: Let E be a field extension of F. The following are equivalent:

1. E is a finite extension of F
2. There exists a finite number of algebraic elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.
3. There exists a sequence of fields
$$F(\alpha_1, \ldots, \alpha_n) \supseteq F(\alpha_1, \ldots, \alpha_{n-1}) \supseteq F(\alpha_1, \ldots, \alpha_{n-2}) \supseteq \cdots \supseteq F$$
such that each $[F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{i-1})]$ is finite and a_i is algebraic over $F(\alpha, \ldots, \alpha_{i-1})$.

eg. $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$
$$\mathbb{Q}(\sqrt{5}i, \sqrt[3]{5}) \underbrace{\supseteq}_{x^2+5} \mathbb{Q}(\sqrt[3]{5}) \underbrace{\supseteq}_{x^3-5} \mathbb{Q}$$

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

eg. Is $\mathbb{Q}(\sqrt{3}) \simeq \mathbb{Q}(\sqrt{2})$?
As vector spaces over $\mathbb{Q}$, they are isomorphic because
$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

As vector spaces $\mathbb{Q}(\sqrt{3}) \simeq \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}^2$.

Note: isomorphic as fields.

Consider $1 \in \mathbb{Q}(\sqrt{2})$ and suppose you have a ring isomorphism
$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$$

where $\varphi(1) = 1$.
So
$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2.$$
Then,
$$\varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = 2.$$
So $\varphi(\sqrt{2})^2 = 2$. So $\varphi(\sqrt{2})$ is a root of 2 in $\mathbb{Q}(\sqrt{3})$. But in $\mathbb{Q}(\sqrt{3})$, if $(a + b\sqrt{3})^2 = 2 \Rightarrow a^2 + 2ab\sqrt{3} + 3b^2 = 2$. Since $\sqrt{3}$ is irrational,

$a=0$ or $b=0$.

But if $a=0$, $3b^2=2$ and $b\in\mathbb{Q}$ $\Rightarrow\Leftarrow$.

$b=0$, $a^2=2$ and $a\in\mathbb{Q}$ $\Rightarrow\Leftarrow$.