1. Remainder of Section 30

Let F be a field. Recall a vector space over F is an abelian group $(V, +)$ together with a scalar multiplication operation defining $a\alpha \in V$ for any $a \in F$, $\alpha \in V$, and satisfying a few axioms.

Example. The group F^n is a vector space over F.

If E is an extension field of F, then E is a vector space over F.

Recall also a collection $\alpha_1, \cdots, \alpha_n \in V$ spans V if every $\beta \in V$ can be written

$$\beta = a_1\alpha_1 + \cdots a_n\alpha_n, \qquad a_i \in F.$$

The sequence $\alpha_1, \ldots, \alpha_n$ is linearly independent if

$$a_1\alpha_1 + \cdots + a_n\alpha_n = 0 \quad a_i \in F.$$

implies that $a_1 = \cdots = a_n = 0$.

Finally, a sequence $\alpha_1, \ldots, \alpha_n \in V$ is a basis for V if the α_i both span V and are linearly independent.

Example. In F^n, the vectors $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ form a basis.

Example. If $E = F(\alpha)$ is a field extension of F with α algebraic and $\deg(\alpha, F) = n$, then $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of E.

Finally, recall that V is finite-dimensional if there is a finite set $\alpha_1, \ldots, \alpha_n$ which spans V.

Theorem. *Let V be a finite-dimensional vector space. Then*

1. *V has a finite basis $\beta_1, \ldots, \beta_n \in V$.*
2. *If $\beta_1', \ldots, \beta_m' \in V$ is another basis, we have $m = n$.*
3. *If $\alpha_1, \ldots, \alpha_k \in V$ span V, we must have $k \geq n$.*
4. *If $\alpha_1, \ldots, \alpha_k \in V$ are linearly independent, we must have $k \leq n$.*

Definition. If V has a basis $\beta_1, \ldots, \beta_n \in V$, we call n the **dimension of V**.

Section 31 – Algebraic and finite field extensions

Definition. Let $F \leq E$ be a field extension. We say E is an **algebraic extension of** F if every element $\alpha \in E$ is algebraic over F

Example.

- The field $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$, since any $a + ib \in \mathbb{C}$ is a zero of the polynomial
$$(x - a - ib)(x - a + ib) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x].$$
- The field $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$, since $e \in \mathbb{R}$ is transcendental over $\mathbb{Q}$.

Definition. Let $F \leq E$ be a field extension. We say E is a **finite** extension of E if E is finite-dimensional as a vector space over F.

The dimension of E as a vector space over F is called the **degree** of the extension, and is denoted $[E : F]$

Example. If $E = F(\alpha)$ with $\alpha \in E$ algebraic over F, then E is a finite extension of F. With $n = \deg(\alpha, F)$, we have that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of E over F, so $[F(\alpha) : F] = n$.

Since $\mathbb{C} = \mathbb{R}(i)$ and $\deg(i, \mathbb{R}) = 2$, we have $[\mathbb{C} : \mathbb{R}] = 2$.

The elements $1, e, e^2, \ldots \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$, so $\mathbb{R}$ is not a finite field extension of $\mathbb{Q}$.

Theorem. *If E is a finite field extension of F, then E is an algebraic extension.*

Proof. Let n be the dimension of E as a vector space over F, and let $\alpha \in E$. Then the $n+1$ elements $1, \alpha, \ldots, \alpha^n \in E$ must be linearly dependent, so there exist $a_0, \ldots, a_n \in F$, not all 0, such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

This means $f(\alpha) = 0$, where

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x],$$

and $f(x) \neq 0$, so α is algebraic over F. □

Example. If $E = F(\alpha)$ with α algebraic, then $F(\alpha)$ is an algebraic extension of F.

Theorem. *Let $F \leq E$ and $E \leq K$ be finite field extensions. Then $F \leq K$ is finite, and*

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

Proof. Let $[E : F] = m$, $[K : E] = n$. Let

$$\alpha_1, \ldots, \alpha_m$$

be a basis for E over F, and let

$$\beta_1, \ldots, \beta_n$$

be a basis for K over E.

Claim: The mn elements $\alpha_i\beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$ form a basis for K over F.

Proof of claim. We only prove that the elements span K, omitting the proof of linear independence. Any $\gamma \in K$ can be written

$$\gamma = a_1\beta_1 + \cdots + a_n\beta_n, \qquad a_i \in E.$$

Each a_i can be written

$$a_i = \sum_{j=1}^{m} b_{ij}\alpha_j, \qquad b_{ij} \in F.$$

Hence

$$\gamma = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\alpha_i\beta_j, \qquad b_{ij} \in F,$$

so the $\alpha_i\beta_j$ span K as a vector space over F.

□

Since the $\alpha_i\beta_j$ form a basis of K over F, we have

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

□

Corollary. *Let $F_1 \leq F_2$, $F_2 \leq F_3$, …, $F_{n-1} \leq F_n$ be finite field extensions. Then $F_1 \leq F_n$ is a finite field extension, and*

$$[F_n : F_1] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_2 : F_1].$$

Definition. Let $F \leq E$ be a field extension, and let $\alpha_1, \ldots, \alpha_n \in E$. We define the field $F(\alpha_1, \ldots, \alpha_n)$ as the smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$.

Concretely, the elements of $F(\alpha_1, \ldots, \alpha_n)$ are all the elements of E which you can obtain starting from elements of F, the $\alpha_1, \ldots, \alpha_n$, and the operations of addition, subtraction, multiplication and division.

Example. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) < \mathbb{R}$ contains elements like

$$\frac{5}{4}, \sqrt{2}, \frac{\sqrt{3}\sqrt{2} + 4\sqrt{3}^7}{2 - 5\sqrt{2}}, \ldots$$

Given $F \leq E$, $\alpha_1, \ldots, \alpha_n \in E$, we have for all k

$$F(\alpha_1, \ldots, \alpha_k) = F(\alpha_1, \ldots, \alpha_{k-1})(\alpha_k),$$

so the field extension $F(\alpha_1, \ldots, \alpha_{k-1}) \leq F(\alpha_1, \ldots, \alpha_k)$ is simple.

Theorem. *Let $F \leq E$ be a field extension. Then E is finite if and only if we can find elements $\alpha_1, \ldots, \alpha_n \in E$ which are algebraic over F such that $E = F(\alpha_1, \ldots, \alpha_n)$.*

Example. Since $\sqrt{2}, \sqrt{3}$ are algebraic over $\mathbb{Q}$, the field extension $\mathbb{Q} < \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is finite.

Proof. Assume $E = F(\alpha_1, \ldots, \alpha_n)$ with each α_i algebraic over F. Then for each i, α_i is also algebraic over $F(\alpha_1, \ldots, \alpha_{i-1})$. Hence

$$F(\alpha_1, \ldots, \alpha_{i-1}) \leq F(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i) = F(\alpha_1, \ldots, \alpha_i)$$

is finite. Therefore $F \leq F(\alpha_1, \ldots, \alpha_n)$ is finite, with

$$[F(\alpha_1, \ldots, \alpha_n) : F] = [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \cdots [F(\alpha_1) : F]$$

Assume now that $F \leq E$ is finite of degree n. We can find a basis $\alpha_1, \ldots, \alpha_n$ of E as a vector space over F, then $E = F(\alpha_1, \ldots, \alpha_n)$. Since $F \leq E$ is a finite extension, it is algebraic. Hence the α_i are algebraic over F. □

Example. Let's compute $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. We have

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

Note $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, so $\deg(\sqrt{2}, \mathbb{Q}) = 2$, so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

To analyse $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$, first see

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}).$$

Let's accept without proof that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, i.e. there is no way to find $a, b \in \mathbb{Q}$ such that

$$\sqrt{3} = a + b\sqrt{2}.$$

Then $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. It follows that $\mathrm{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$, so $\deg(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = 2$ and so

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = (2)(2) = 4.$$

Since $1, \sqrt{2}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $1, \sqrt{3}$ is basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$, we find that

$$(1)(1), (1)(\sqrt{2}), (\sqrt{3})(1), (\sqrt{3})(\sqrt{2}) = 1, \sqrt{2}, \sqrt{3}, \sqrt{6}$$

is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.