Degrees of field extensions

Last lecture we introduced the notion of algebraic and transcendental elements over a field, and we also introduced the *degree* of a field extension. Recall that for a field extension E of F, we may view E as a vector space over F, and the degree of the extension E is given by

$$\dim_F E = [E : F]$$

Today we will study the relationship between algebraic extensions and degrees of extensions. We first begin with a few examples.

Examples

1. Consider the extension $\mathbb{Q}(\sqrt{2})$ of the field $\mathbb{Q}$. We know that $\mathbb{Q}(\sqrt{2})$ consists of numbers $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Let $v_1 = 1$ and $v_2 = \sqrt{2}$. Then $S = \{v_1, v_2\}$ is a linearly independent subset of $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$, and S spans $\mathbb{Q}(\sqrt{2})$. Thus S is a basis for $\mathbb{Q}(\sqrt{2})$ viewed as a vector space over $\mathbb{Q}$. From this we conclude

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$$

Thus the degree of the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is equal to 2.

2. Consider $\mathbb{C}$ as an extension of $\mathbb{R}$. We can write every complex number uniquely as $a + bi$ where $a, b \in \mathbb{R}$. Then $S = \{1, i\}$ is a basis for $\mathbb{C}$ viewed as a vector space over $\mathbb{R}$, and

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

Thus the degree of the extension $\mathbb{C}$ over $\mathbb{R}$ is equal to 2.

3. Consider $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ as an extension of $\mathbb{Q}(\sqrt{2})$. We saw last lecture that $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ so this is in fact an extension. In fact, we can argue that

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

Indeed, clearly $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and as we showed that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ the reverse inclusion also holds. Every element in this extension can be written uniquely as

$$x + \sqrt{3}y = (a + b\sqrt{2}) + \sqrt{3}(c + d\sqrt{2}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

where $a, b, c, d \in \mathbb{Q}$. Thus $S = \{1, \sqrt{3}\}$ is a basis of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ over the field $\mathbb{Q}(\sqrt{2})$, and

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = \dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2} + \sqrt{3}) = 2$$

At the same time we see that as a vector space over $\mathbb{Q}$, the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ and so is of degree 4 over $\mathbb{Q}$:

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

We say that an extension E of a field F is *finite* if the degree $[E : F]$ is a finite number, i.e. if E is a finite dimensional vector space over the field F.

▸ **If E is a finite extension of F, then E is an algebraic extension over F.**

Proof. Suppose $[E : F] = n$. Let $\alpha \in E$. Consider the elements $1, \alpha, \dots, \alpha^n$. As there are $n + 1$ elements here, and $\dim_F E = n$, they must be linear dependent, i.e. there is a relation

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 1 = 0$$

where not all of the $a_0, \dots, a_n \in F$ are zero. Then α is a root of the polynomial $f(x) \in F[x]$ given by $f(x) = \sum_{i=0}^{n} a_i x^i$, and so α is algebraic over F. As α was an arbitrary element of E, we conclude that E is an algebraic extension of F. □

▸ **Suppose $F \subset E$ and $E \subset K$ are finite extensions. Then**

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

In particular, K is a finite extension of F.

Proof. Suppose $[E : F] = n$ and $[K : E] = m$. Let $\{v_1, \dots, v_n\} \subset E$ be a basis for E as a vector space over F, and $\{w_1, \dots, w_m\} \subset K$ a basis for K as a vector space over E. Then we claim that $S = \{v_i w_j\} \subset K$ where $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$ is a basis for K as a vector space over F. To establish this we must show that S is linearly independent and also spans K.

We first show S is linearly independent. Suppose we have a relation

$$\sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} a_{ij} \cdot v_i w_j = 0$$

where $a_{ij} \in F$. Then we can write this expression as

$$\sum_{1 \leqslant j \leqslant m} c_j \cdot w_j = 0 \qquad \text{where} \qquad c_j = \sum_{1 \leqslant i \leqslant n} a_{ij} v_i \in E$$

Since the w_j are linearly independent in K over E, we must have $c_j = 0$ for $1 \leqslant j \leqslant m$. Then

$$c_j = \sum_{1 \leqslant i \leqslant n} a_{ij} v_i = 0$$

and as the v_i are linearly independent in E over F, we must have, for each j, that $a_{ij} = 0$ for $1 \leqslant i \leqslant n$. Thus all $a_{ij} = 0$. This shows that S is linearly independent over F.

We show S spans K over F. Let $k \in K$. As the w_j are a basis for K over E, we can write

$$k = \sum_{j=1}^{m} c_j w_j$$

for some $c_j \in E$. As the v_i are a basis of E over F, we can write $c_j = \sum_{i=1}^n a_{ij} v_i$ for some $a_{ij} \in F$. Then $k = \sum a_{ij} v_i w_j$. This show S spans K over F Hence S is a basis for K over E.

Finally, the basis S contains nm elements and we compute

$$\dim_F K = [K : F] = nm = [K : E][E : F]$$ □

You might have already noticed this property in the last example we studied above: we have

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

▸ **Let α be algebraic over F with minimal polynomial $p(x) \in F[x]$. Then**

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

Proof. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \in F$. Then since α is a root of $p(x)$ we have $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. We claim $S = \{1, \alpha, \ldots, \alpha^{n-1}\} \subset F(\alpha)$ is a basis of $F(\alpha)$ as a vector space over F. First, if a non-trivial linear combination of these elements with coefficients in F is zero, it would show α is the root of a polynomial of degree $< n$, contradicting the minimality of $p(x)$. Thus S is linearly independent. To see that S spans $F(\alpha)$, make use of the isomorphism $F(\alpha) \cong F[x]/(p(x))$. □

▸ **The following are equivalent statements for a field extension $F \subset E$.**

(i) E is a finite extension of F.

(ii) There are algebraic elements $\alpha_1, \ldots, \alpha_n$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.

Proof. In (ii), note that we have a sequence of algebraic extensions

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

As each of these algebraic extensions is of finite degree by the previous result, we have that (ii) implies (i).

To see that (i) implies (ii), choose $\alpha_1 \in E$ to be an element not in F. Then

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$$

Next, choose $\alpha_2 \in E$ not in $F(\alpha_1)$. Then we have

$$[E : F] = [E : F(\alpha_1, \alpha_2)][F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F]$$

Continue in this fashion, and choose $\alpha_3 \in E$ not in $F(\alpha_1, \alpha_2)$, and so on. Since $[E : F]$ is finite, this process must eventually terminate at a step in which $E = F(\alpha_1, \ldots, \alpha_n)$. □

▶ **Let $F \subset E$. The set of elements in E algebraic over F form a field.**

Proof. From the previous result, $F(\alpha, \beta)$ is a finite extension of F, and hence is an algebraic extension of F. As this extension contains the elements $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ $(\beta \neq 0)$, these are all algebraic elements over F. This shows that the subset of E of algebraic elements over F is a subfield of E, and is in particular a field. □

We now return to our example from last lecture of the number

$$\sqrt[5]{\frac{\sqrt{2}-1}{\sqrt[3]{4+\sqrt{5}}}}$$

It is at this point easy to deduce that this is an algebraic element over $\mathbb{Q}$. First, we note that an n^{th} root of a number algebraic over $\mathbb{Q}$ is also algebraic over $\mathbb{Q}$. To prove this, if α is algebraic, then it satisfies $p(\alpha) = 0$ for some $p(x) \in \mathbb{Q}[x]$; then $\sqrt[n]{\alpha}$ is a root of $p(x^n) \in \mathbb{Q}[x]$, so it is also algebraic over $\mathbb{Q}$.

Then all that is left to observe is that the number displayed above is obtained from rational numbers and the field operations (addition, subtraction, multiplication, division) and taking n^{th} roots; all of these operations preserve the class of algebraic elements.