Lecture 7.1

Last time:

- A complex number $\alpha \in \mathbb{C}$ is algebraic if $p(\alpha) = 0$ for some $p(x) \in \mathbb{Q}[x]$. Otherwise, α is transcendental.

- The minimal polynomial of an algebraic number α is the unique monic irreducible $p_\alpha(x) \in \mathbb{Q}[x]$ such that $\ker(\varphi_\alpha) = (p_\alpha)$, where
$$\varphi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$$
$$f(x) \mapsto f(\alpha).$$

Theorem (1) For any algebraic $\alpha \in \mathbb{C}$, the minimal polynomial p_α is irreducible over $\mathbb{Q}$.

(2) For every monic irreducible polynomial $p \in \mathbb{Q}[x]$, there is some algebraic $\alpha \in \mathbb{C}$ with $p_\alpha = p$.

Pf: (1) Suppose $p_\alpha = fg$ for some $f, g \in \mathbb{Q}[x]$. Then

$$0 = p_\alpha(\alpha) = f(\alpha)g(\alpha) \text{ in } \mathbb{C}$$

so $f(\alpha) = 0$ or $g(\alpha) = 0$, say $f(\alpha) = 0$.

Dividing by the leading coefficient, we

may assume f is monic.

But p_α is the unique monic polynomial of smallest degree with α as a root, so $f = p_\alpha$ and $g = 1$.

Therefore p_α is irreducible.

(2) Let $p \in \mathbb{Q}[x]$ be monic and irreducible. By the Fundamental Theorem of Algebra, p has a root $\alpha \in \mathbb{C}$ with minimal polynomial p_α.

Then $p \in (p_\alpha)$, i.e. $p = p_\alpha f$ for some $f \in \mathbb{Q}[x]$ but p is irreducible and monic, so $p = p_\alpha$. $\square$

Def A **simple (algebraic) extension** of $\mathbb{Q}$ is an extension of the form

$$\mathbb{Q}(\alpha) = \bigcap_{\substack{\text{subfields} \\ \alpha \in K \subseteq \mathbb{C}}} K$$

for some (algebraic) $\alpha \in \mathbb{C}$.

Theorem Every simple algebraic extension $K/\mathbb{Q}$ is isomorphic to $\mathbb{Q}[x]/(p)$ for some p, which may be chosen to be the minimal polynomial of some $\alpha \in K$.

Pf: Let $K = \mathbb{Q}(\alpha)$ be a simple extension and p_α the minimal polynomial of α.

Then $\varphi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ has Kernel (p_α) and since this is a maximal ideal, $\mathbb{Q}[x]/(p_\alpha)$ is a field.

If we can show $\mathrm{im}(\varphi_\alpha) = K$, the First Isomorphism Theorem will give us

$$\mathbb{Q}[x]/(p_\alpha) \cong K.$$

On one hand, $\alpha = \varphi_\alpha(x) \in \mathrm{im}(\varphi_\alpha)$, so $K = \mathbb{Q}(\alpha) \subseteq \operatorname{im}(\varphi_\alpha)$.

On the other hand,

$$\operatorname{im}(\varphi_\alpha) = \{ f(\alpha) \mid f \in \mathbb{Q}[x] \}$$

$$= \{ a_0 + a_1\alpha + \dots + a_n\alpha^n \mid a_j \in \mathbb{Q} \}$$

$\subseteq \mathbb{Q}(\alpha)$ by ring operations.

So $\operatorname{im}(\varphi_\alpha) = K$. $\square$

$\boxed{\text{Corollary}}$ If $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are simple algebraic extensions with $p_\alpha = p_\beta$, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$.

Remark: All of the above definitions and results hold if we replace $\mathbb{Q}$ by any subfield $K \subseteq \mathbb{C}$, with essentially the same proofs.

We have shown that the following sets are in bijection:

$$\begin{tikzcd}
& \{\text{algebraic } \alpha \in \mathbb{C}\} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] & \\
\left\{\begin{array}{c}\text{monic, irred.} \\ p(x) \in \mathbb{Q}[x]\end{array}\right\} & & \left\{\begin{array}{c}\text{simple algebraic} \\ \text{ext'ns } K/\mathbb{Q}\text{, up} \\ \text{to isomorphism}\end{array}\right\}
\end{tikzcd}$$

$$\alpha \longleftrightarrow p_\alpha(x) \qquad \alpha \longleftrightarrow \mathbb{Q}(\alpha)$$

$$p \longleftrightarrow \mathbb{Q}[x]/(p)$$

Corollary Let $\mathbb{Q}(\alpha)/\mathbb{Q}$ be a simple algebraic extension and $p_\alpha \in \mathbb{Q}[x]$ the minimal polynomial. Then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space, where $n = \deg(p_\alpha)$.

Pf: By the Theorem, $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p_\alpha)$ via the evaluation map

$$\begin{aligned} \mathbb{Q}[x]/(p_\alpha) &\longrightarrow \mathbb{Q}(\alpha) \\ f(x) + (p_\alpha) &\longmapsto f(\alpha). \end{aligned}$$

If $\deg(f) < n$, $f(\alpha)$ is already a linear

If $\deg(f) < n$, $f(\alpha)$ is already a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.

If $\deg(f) \geq n$, use the Polynomial Division Algorithm to replace $f(x)$ with some $r(x)$ in the same coset with $\deg(r) < n$.

Such an $r(x)$ is unique, so the linear combination expressing $f(\alpha) = r(\alpha)$ in terms of $1, \ldots, \alpha^{n-1}$ is unique. $\square$

Corollary For any simple algebraic extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(p_\alpha)$.

Remark: For a set $S \subseteq \mathbb{C}$, define set $S \subseteq \mathbb{C}$, define

$$\mathbb{Q}(S) = \bigcap_{\substack{\text{subfields} \\ S \subseteq K \subseteq \mathbb{C}}} K.$$

When $S = \{\alpha\}$, $\mathbb{Q}(S) = \mathbb{Q}(\alpha)$ is a simple extension but the converse need not be true.

$\boxed{\text{Ex}}$ 1 $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 as a field extension of $\mathbb{Q}$. There are a few ways to prove this.

<u>Claim 1</u>: $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $K/\mathbb{Q}$.

Pf: Certainly any linear combination of $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ lies in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ by field axioms.

On the other hand, one can solve a linear system to show that every

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

with $a, b, c, d \in \mathbb{Q}$ not all 0, has an inverse in $\mathrm{Span}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, showing $K \subseteq \mathrm{Span}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

If $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ then

$$a + b\sqrt{2} = -\sqrt{3}(c + d\sqrt{2})$$

which is only possible if $a = b = c = d = 0$.

Therefore $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for K. $\square$

Claim 2: $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Pf: On one hand, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq K$ since $\sqrt{2}+\sqrt{3} \in K$.

On the other hand,

$$(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6} \qquad (i)$$

$$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3} \qquad (ii)$$

$$(\sqrt{2}+\sqrt{3})^4 = 49 + 20\sqrt{6} \qquad (iii)$$

Set $\alpha = \sqrt{2} + \sqrt{3}$. Then

$$\sqrt{6} = \frac{\alpha - 5}{2} \quad \text{by (i)}$$

$$\sqrt{2} = \frac{\alpha^3 - 9\alpha}{2} \quad \text{by (ii)}$$

$$\sqrt{3} = \alpha - \frac{\alpha^3 - 9\alpha}{2} = \frac{11\alpha - \alpha^3}{2} \quad \text{also by (ii).}$$

So $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, showing they are equal. $\square$

Claim 3: The minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is

$$p_\alpha(x) = x^4 - 10x + 1.$$

Pf: (i) and (iii) imply α is a root of $p_\alpha(x)$.

On the other hand, $p_\alpha(x)$ is irreducible since, for example, it is irreducible over $\mathbb{F}_5$. (Check it!)

Since it is also monic, it must be the minimal polynomial of α. $\square$

Either Claim 1 or Claim 3 implies

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

More generally:

Theorem (Tower Law) If $L/K/F$ is

a "tower" of field extensions, meaning L/K and K/F are each field extensions,

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

Pf: Assume for simplicity that both extensions are finite — the infinite degree case is basically the same.

Let $\{x_1, \dots, x_n\} \subseteq K$ be an F-basis of K and let $\{y_1, \dots, y_m\}$ be a K-basis of L.

We want to show that $\{x_1 y_1, \dots, x_n y_m\}$ is an F-basis of L, so that

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

First, since the y_j span L/K, any element of L is of the form

$$\alpha = a_1 y_1 + \ldots + a_m y_m$$

for some $a_j \in K$.

But K/F is spanned by the x_i, so each

$$a_j = b_{1j} x_1 + \ldots + b_{nj} x_n$$

for some $b_{ij} \in F$.

Putting them together,

$$\alpha = (b_{11} x_1 + \ldots + b_{n1} x_n) y_1 \ldots ($$

$$\ldots + b_{n1} x_n) y_1 + \ldots + (b_{1m} x_1 + \ldots + b_{nm} x_n) y_m$$

so L/F is spanned by the $a_i b_j$.

On the other hand, suppose

$$b_{11} x_1 y_1 + \ldots + b_{nm} x_n y_m = 0.$$

Grouping terms, we get

$$(b_{11} x_1 + \ldots + b_{n1} x_n) y_1 + \ldots + (b_{1m} x_1 + \ldots + b_{nm} x_n) y_m = 0$$

but since the y_j are a basis for L/K, each coefficient is 0:

$$b_{1j} x_1 + \ldots + b_{nj} x_n = 0.$$

Now $x_1, \ldots, x_n$ are a basis for K/F, so $b_{1j} = \cdots = b_{nj} = 0$ and this holds for all j. $\square$

Ex 1, cont'd. This gives us a fast way to check that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$ by showing that

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

In the tower $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, we know $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2.

But part of our previous work showed that

$\sqrt{3} \notin \mathrm{Span}_{\mathbb{Q}}\{1, \sqrt{2}\} = \mathbb{Q}(\sqrt{2})$, so

$x^2 - 3$ remains irreducible over $\mathbb{Q}(\sqrt{2})$

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

Next time: ruler-compass constructions.