We have proved the following:

Theorem. Suppose $\alpha \in \mathbb{C}$ is an algebraic number. Then

1. There exists a monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ s.t.
   \[
   \text{for } f(x) \in \mathbb{Q}[x], f(\alpha) = 0 \iff m_\alpha(x) \mid f(x).
   \]

2. $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$.

3. $\mathbb{Q}[\alpha] := \{ \text{the smallest subring of } \mathbb{C} \text{ that contains } \mathbb{Q} \text{ as a subring and } \alpha \text{ as an element} \}$

   $\mathbb{Q}[\alpha]/\langle m_\alpha(x) \rangle$ is a field.

In this short lecture we prove:

(a). $\mathbb{Q}[\alpha] = \{ a_0 + a_1 \alpha + \ldots + a_{d-1} \alpha^{d-1} \mid a_i \in \mathbb{Q} \}$ where $d = \deg m_\alpha(x)$.

(b). If $p(x) \in \mathbb{Q}[x]$ is irreducible and $p(\alpha) = 0$, then $p(x) = c \cdot m_\alpha(x)$ for some $c \in \mathbb{Q}$.

Proof (a). We have seen that $\mathbb{Q}[\alpha] = \{ h(\alpha) \mid h(x) \in \mathbb{Q}[x] \}$. For any $h(x) \in \mathbb{Q}[x]$ by long division there are $q(x), r(x) \in \mathbb{Q}[x]$ s.t.

   $h(x) = m_\alpha(x)q(x) + r(x)$ and $\deg r < \deg m_\alpha = d$. 
Hence \( h(x) = p(x) = \frac{\partial}{\partial x} \sum_{\underset{i}{i}} a_i x^i = r(x) = r(x) \). Since \( \deg r \leq d \)\
\( r(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} \) for some \( a_i \in \mathbb{Q} \). Therefore \( h(x) = r(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} \); and claim follows. 

(b) Since \( p(x) = 0 \), \( m_\alpha(x) \mid p(x) \); this means \( \exists q(x) \in \mathbb{Q}[x] \) s.t. \( p(x) = m_\alpha(x) q(x) \). As \( p(x) \) is irreducible in \( \mathbb{Q}[x] \), either \( m_\alpha(x) \in \mathbb{Q}^\times \) or \( q(x) \in \mathbb{Q}^\times \). Since \( m_\alpha(x) \) is irreducible in \( \mathbb{Q}[x] \), \( m_\alpha(x) \notin \mathbb{Q}^\times \). Thus \( q(x) = c \in \mathbb{Q}^\times \); and claim follows.

The (b) part is an effective way to find the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \).

The (a) part shows that the main reason to have \( \mathbb{Q}[i] = \{ a + bi \mid a, b \in \mathbb{Q} \} \) or \( \mathbb{Q}[\sqrt{2}] = \{ a + b \sqrt{2} \mid a, b \in \mathbb{Q} \} \) is that the degree of minimal polynomials \( m_i(x) = x^2 + 1 \) and \( m_{\sqrt{2}}(x) = x^2 - 2 \) is 2. For instance \( \mathbb{Q}[\sqrt{3}] = \left\{ \frac{3}{2} x + \sqrt{2} \right\} \) a, b, c ∈ \( \mathbb{Q} \)