2.2 Algebraic Extensions

Throughout this section, assume F is a field and let K be an extension of F.

Definition 2.23. The element $\alpha \in K$ is said to be **algebraic** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, then α is called **transcendental** over F. The extension K/F is called **algebraic** if every element of K is algebraic over F.

Example 2.24. Here are a few short examples.

(1) Every field F is algebraic over itself. For $\alpha \in F$, α is a root of the polynomial $x - \alpha \in F[x]$.

(2) The real number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$.

(3) The complex number i is algebraic over $\mathbb{Q}$ since it is a root of the polynomial $x^2+1 \in \mathbb{Q}[x]$.

(4) It turns out that the real number π is transcendental over $\mathbb{Q}$ since there is no polynomial in $\mathbb{Q}[x]$ having π as a root. However, π is algebraic over $\mathbb{R}$ since it is a root of $x - \pi \in \mathbb{R}[x]$.

Theorem 2.25. Let α be algebraic over F. Then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ that has α as a root. Moreover, a polynomial $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Definition 2.26. The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial** for α over F. The degree of $m_{\alpha,F}(x)$ is called the **degree** of α.

The next theorem follows immediately from 2.18.

Theorem 2.27. Let α be algebraic over F. Then

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$$

and $[F(\alpha):F] = \deg(m_{\alpha,F}(x)) = \deg(\alpha)$.

Theorem 2.28. This got combined with Theorem 2.25.

Corollary 2.29. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Corollary 2.30. A monic polynomial $f(x) \in F[x]$ with α as a root is equal to $m_{\alpha,F}(x)$ iff $f(x)$ is irreducible over F.

Example 2.31. Here are a couple of examples.

(1) Consider the polynomial $x^n - 2 \in \mathbb{Q}[x]$ with $n > 1$. This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's Criteria (with prime 2). Then the positive nth root of 2, denoted by $\sqrt[n]{2}$ in $\mathbb{R}$, is a root. By Corollary 2.30, $x^n - 2$ is the minimal polynomial of $\sqrt[n]{2}$ and by Theorem 2.27, $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n$. In particular, the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ and $\sqrt{2}$ is of degree 2.

(2) Consider the polynomial $x^3 - 3x - 1 \in \mathbb{Q}[x]$. By the Rational Root Test, the only possible roots of this polynomial are ± 1. However, neither of these numbers are roots. Since the polynomial is of degree 3, it must be irreducible over $\mathbb{Q}$. This implies that if α is a root of $x^3 - 3x - 1$, then $x^3 - 3x - 1$ is the minimal polynomial of α and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Theorem 2.32. The element α is algebraic over F iff the simple field extension $F(\alpha)/F$ is finite. More specifically, if α is an element of an extension of degree n over F, then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F, then the degree of $F(\alpha)$ over F is at most n.

Corollary 2.33. If the extension K/F is finite, then it is algebraic.

Theorem 2.34. Let K/F and L/K be field extensions. Then $[L : K][K : F] = [L : F]$.

Corollary 2.35. Suppose L/F is a finite field extension and let K be any subfield of L containing F ($F \subseteq K \subseteq L$). Then $[K : F]$ divides $[L : F]$.

Example 2.36. Here are two examples.

(1) By the Intermediate Value Theorem, the polynomial $p(x) = x^3 - 3x - 1$ has a real root between 0 and 2. Actually, it has one such root. Let's call it α.

In Example 2.31(b), we argued that $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$ and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Is it possible that $\sqrt{2}$ is an element of $\mathbb{Q}(\alpha)$? The answer is no.

Arguing that $\sqrt{2}$ is not equal to a linear combination of $1, \alpha, \alpha^2$ would be annoying. Thankfully, there is an easier way.

We already know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (since $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$). If $\sqrt{2}$ is an element of $\mathbb{Q}(\alpha)$, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$. However, 2 does not divide 3, which implies that $\mathbb{Q}(\sqrt{2}) \nsubseteq \mathbb{Q}(\alpha)$.

(2) Let $\sqrt[6]{2}$ be the positive real 6th root of 2. It is quickly seen that $x^6 - 2$ is the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}$. This implies that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$.

Notice that $(\sqrt[6]{2})^3 = \sqrt{2}$. Then $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$. By the multiplicity of the degrees of the extensions, it must be the case that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$. This implies that the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ is of degree 3. We see that the polynomial $x^3 - \sqrt{2}$ is a monic polynomial of degree 3 over $\mathbb{Q}(\sqrt{2})$ that has $\sqrt[6]{2}$ as a root. It follows that $x^3 - \sqrt{2}$ is the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ (and hence irreducible).

Observe that showing $x^3 - \sqrt{2}$ is irreducible directly would not be an easy task.

Definition 2.37. A field extension K/F is **finitely generated** if there are elements $\alpha_1, \ldots, \alpha_k \in K$ such that $K = F(\alpha_1, \ldots, \alpha_k)$.

Theorem 2.38. Let F be a field. Then $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Example 2.39. Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\sqrt{3}$ is of degree 2 over $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ is at most 2. In fact, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ iff $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. But x^2-3 is irreducible iff it does not have a root in $\mathbb{Q}(\sqrt{2})$. That is, x^2-3 is reducible iff $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Suppose $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Squaring both sides, we obtain $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. We consider 3 cases. First, suppose $ab \neq 0$. In this case, we can write $\sqrt{2}$ as a rational number, which is impossible. Now, assume $b = 0$. Then we have $\sqrt{3} = a \in \mathbb{Q}$, which is absurd. Lastly, assume $a = 0$. Then $\sqrt{3} = b\sqrt{2}$. This implies that $\sqrt{6} = 2b \in \mathbb{Q}$, which is a contradiction since $\sqrt{6}$ is not rational.

We have shown that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. It follows that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. We have also shown that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Theorem 2.40. The field extension K/F is finite iff K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degrees $n_1, \ldots, n_k$ is algebraic of degree less than or equal to $n_1 \cdots n_k$.

Corollary 2.41. Suppose α and β are algebraic over F. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (for $\beta \neq 0$), and α^{-1} (for $\alpha \neq 0$) are all algebraic.

Corollary 2.42. Let L/F be an arbitrary field extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.