The degree formula and algebraic extensions

DEGREE FORMULA: Let $F \subseteq L \subseteq K$ be field extensions. Then $[K : F] = [K : L] \cdot [L : F]$. In particular, K/F is finite if and only if K/L and L/F are both finite.

DEFINITION: A field extension L/F is **algebraic** if every $\alpha \in L$ is algebraic over F.

PROPOSITION: Any finite field extension is algebraic.

THEOREM: Let $F \subseteq L \subseteq K$ be field extensions. Then K/F is algebraic if and only if K/L and L/F are both algebraic.

(1) Using the Degree Formula: Consider the field $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) Let $E = \mathbb{Q}(\sqrt{2})$. Use the polynomials $x^2 - 2 \in \mathbb{Q}[x]$ and $x^2 - 3 \in E[x]$ to quickly show that $[E : \mathbb{Q}] \leq 2$ and $[F : E] \leq 2$.

(b) Explain why $\mathbb{Q} \subsetneq E \subsetneq F$, and deduce that $[E : \mathbb{Q}] = 2$ and $[F : E] = 2$.

(c) Show that $[F : \mathbb{Q}] = 4$.

(d) We showed earlier that $F = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and that $\sqrt{2}+\sqrt{3}$ is a root of the polynomial $p(x) = x^4 - 10x^2 + 1$. Deduce from these facts and from (c) that $p(x)$ is irreducible over $\mathbb{Q}[x]$.

(a) Since $\sqrt{2}$ is a root of $x^2 - 2$, the degree of its minimal polynomial is at most 2. Thus $[E : \mathbb{Q}] \leq 2$. Likewise for $\sqrt{3}$.

(b) Once we show that these inclusions are proper, the degree must be greater than 1. We know that $E \neq \mathbb{Q}$ since $\sqrt{2}$ is irrational. To see that $F \neq E$, we just need to show $\sqrt{3} \notin E$. If $(a + b\sqrt{2})^2 = 3$ with $a, b \in \mathbb{Q}$, then $a^2 + 2b^2 = 3$ and $2ab\sqrt{2} = 0$. This implies $a = 0$ or $b = 0$, and either way would contradict that $\sqrt{3} \notin \mathbb{Q}$.

(c) This follows from the Degree Formula.

(d) We know that $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}$ has degree 4 since $\sqrt{2} + \sqrt{3}$ generates an extension of degree 4. We also know that p is a multiple of this minimal polynomial. Since the degrees agree and p is monic, p must equal the minimal polynomial, and thus, be irreducible.

(2) Use[1] the Degree Formula to prove the Proposition.

Consider $F \subseteq F(\alpha) \subseteq L$. By the Degree Formula, $F \subseteq F(\alpha)$ is finite. Thus α is algebraic over F.

(3) Proof of Theorem (using the Degree Formula):

(a) Prove the $(\Longrightarrow)$ direction using the definitions.

(b) For the $(\Longleftarrow)$ direction, take $\alpha \in K$. Explain why there exist $a_0, a_1, \ldots, a_n \in L$ such that α is algebraic over $F(a_0, \ldots, a_n)$.

[1] Hint: If L/F is finite and $\alpha \in L$, consider $F \subseteq F(\alpha) \subseteq L$.

(c) Consider the tower of field extensions

$$F \subseteq F(a_0) \subseteq F(a_0, a_1) \subseteq \cdots \subseteq F(a_0, \ldots, a_n) \subseteq F(a_0, \ldots, a_n, \alpha).$$

Explain why each inclusion is finite. Then explain why $F(a_0, \ldots, a_n, \alpha)/F$ is finite.

(d) Deduce the Theorem.

> **(a)** To show that K/L is algebraic, let $\alpha \in K$. Then α is a root of a polynomial with coefficients in F by assumption; such a polynomial can also be considered as a polynomial with coefficients in L. Thus α is algebraic over L. To show that L/F is algebraic, let $\alpha \in L$. In particular, $\alpha \in K$. Then α is algebraic over F by assumption.
>
> **(b)** We know that α is a root of some polynomial $a_n x^n + \cdots + a_0 \in L[x]$. This polynomial is also a polynomial with coefficients in $F(a_0, \ldots, a_n)$.
>
> **(c)** Note that a_i is algebraic over F, and hence algebraic over $F(a_0, \ldots, a_{i-1})$. Thus, by the structure of simple extensions, these are finite. Likewise for $F(a_0, \ldots, a_n) \subseteq F(a_0, \ldots, a_n, \alpha)$. The Degree Formula applied repeatedly shows that $F(a_0, \ldots, a_n, \alpha)/F$ is finite.
>
> **(d)** The Proposition implies that $F(a_0, \ldots, a_n, \alpha)/F$ is algebraic. In particular, α is algebraic over F. This is what we needed to show!

(4) Prove the Degree Formula.

THEOREM (SIMPLE EXTENSIONS): Let L/F be a field extension and $\alpha \in L$.

(1) $I := \{f(x) \in F[x] \mid f(\alpha) = 0\}$ is an ideal in $F[x]$.

(2) $I \neq 0 \iff \alpha$ is algebraic over F.

(3) If α is algebraic over F, then the unique monic generator of I, denoted $m_{\alpha,F}(x)$, is irreducible.

(4) If α is algebraic over F, then $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$.

(5) α is algebraic over $F \iff [F(\alpha) : F] < \infty$.
In this case, $[F(\alpha) : F] = \deg(m_{\alpha,F})$.

(6) α is transcendental over $F \iff [F(\alpha) : F] = \infty$.
In this case, $F(\alpha) \cong F(x)$, the field of rational functions in one variable over F.