Definition 1. An extension E/F is said to be *simple* if $E = F(\alpha)$ for some $\alpha \in E$. Such an element is called a *primitive element* of E over F.

Example 2. (0) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is clearly a simple extension.

(1) The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is also simple.
(Why?) In fact, we claim that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Clearly, $K := \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that $(\sqrt{2} + \sqrt{3})^2 \in K$ implies $\sqrt{6} \in K$. Thus $\sqrt{6}(\sqrt{2} + \sqrt{3}) \in K$ or $2\sqrt{3} + 3\sqrt{2} \in K$. Now using the fact that $\sqrt{2} + \sqrt{3} \in K$ we get that $\sqrt{2}, \sqrt{3} \in K$. Therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(2) Let $\mathbb{F}_q$ denote the field with q element. Recall from Module 1 that $\mathbb{F}_q^\times$ is cyclic, say generated by α. Thus $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ and so $\mathbb{F}_{p^n}/\mathbb{F}_p$ has a primitive element.

(3) (An example of finite extension which is not simple) Let k be a field with p elements. Let $E := k(X, Y)$ and $F := k(X^p, Y^p)$. Then the extension E/F has no primitive element. Indeed, if possible, assume that $E = F(\alpha)$ for some $\alpha \in E$. By using Freshman's dream it is easy to verify that $\alpha^p \in F$. Thus $[F(\alpha) : F] \leq p$, whereas $[E : F] = p^2$. So, E has no primitive element over F.

We proved the Primitive Element Theorem

Theorem 3 (Primitive Element Theorem)**.** *Let $E = F[\alpha_1, \alpha_2, \ldots, \alpha_r]$ be a finite extension of F. Assume that $\alpha_2, \ldots, \alpha_r$ are seperable over F (but α_1 need not be seperable). Then there is an element $\gamma \in E$ such that $E = F[\gamma]$.*

Remark 4. Suppose F is infinite and $F[\alpha_1, \alpha_2, \ldots, \alpha_r]/F$ is a finite Galois extension. Then the proof of the above theorem shows that an element γ of the form

$$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r$$

is a primitive element provided it is moved by every nontrivial element of the Galois group.

Example 5. In example 1, we know that the Galois group of E/F is the Klein-4 group $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ where

$$\sigma(\sqrt{2}) = \sqrt{2}, \quad \sigma(\sqrt{3}) = -\sqrt{3}$$
$$\tau(\sqrt{2}) = -\sqrt{2}, \quad \tau(\sqrt{3}) = \sqrt{3}.$$

Since E/F is Galois in this example and for every nonzero c in $\mathbb{Q}$ the element $\sqrt{2} + c\sqrt{3}$ is moved by every nontrivial element in the Galois group, $E = \mathbb{Q}(\sqrt{2} + c\sqrt{3})$ for every nonzero c in $\mathbb{Q}$. Similarly, every element of the form $b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ is also a primitive element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ for every nonzero $b, c \in \mathbb{Q}$.

Remark 6. The element $\sqrt{3}$ is a primitive element for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ but not for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.