

# Primitive Element Theorem

Ali Berhan Palabıyık

8 January 2026

## 1 Theorem and Proof

Today in “Einführung in die Algebra” class we proved one my favourite theorems regarding field extensions: The Primitive Element Theorem. In this short article I’ll prove the theorem and give an explicit calculation of a primitive element for three examples. I assume the reader knows what finite and separable field extensions are. First we start with a definition:

**Definition 1.1.** Let  $L/K$  be a finite field extension. An element  $a \in L$  is called a primitive element for  $L/K$  if

$$L = K(a).$$

Now the theorem is as follows:

**Theorem 1.2.** *Let  $L/K$  be a finite separable field extension. Then there exists a primitive element for  $L/K$ .*

*Proof.* First there are two cases to consider: when  $K$  is finite and when  $K$  is infinite. The case where  $K$  is finite is actually much easier to prove using some elementary group theory. However, since most of the interesting applications are when  $K$  is infinite we will only prove the second case here.

Let also  $K$  be infinite. Since  $L/K$  is finite we know that there exist  $a_1, \dots, a_n \in L$  such that

$$L = K(a_1, \dots, a_n).$$

Using induction we reduce the problem to the case where  $L = K(b, c)$ . If the theorem holds for this case, we can successively find a primitive element by adjoining the remaining  $n - 2$  elements one by one.

In this case we only need that  $c$  is separable over  $K$  (in the general case this corresponds to  $a_2, \dots, a_n$  being separable over  $K$ ).

Let  $b_1, \dots, b_r$  be the pairwise distinct zeroes of  $f = \mu_{b,K}$  in  $\overline{K} = \overline{L}$ .

Now let  $c_1, \dots, c_s$  be the pairwise distinct zeroes of  $g = \mu_{c,K}$  in  $\overline{K}$ .

We can assume without loss of any generality that  $b = b_1$  and  $c = c_1$ .

Now we are looking for an element  $a \in K(b, c)$  such that

$$K(a) = K(b, c).$$

Here we use a little trick: one possible candidate for a primitive element is an algebraic relation of the elements we already have. Among all such relations, the simplest one is a linear relation. Thus we hope that  $a$  is of the form  $\lambda b + \gamma c$  with  $\lambda, \gamma \in K$ . Dividing by  $\lambda$  we may assume

$$a = b + uc$$

for some  $u \in K$ .

We now observe that it suffices to show that  $c \in K(a)$ , since then  $b = a - uc \in K(a)$  follows immediately.

Let  $G = f(a - uX) \in K(a)[X]$ . Then

$$G(c) = f(a - uc) = f(b) = 0,$$

The idea behind  $G$  is to obtain a polynomial that shares one (and only one!) common root with  $g$

We claim that we can choose  $u \in K$  such that  $c$  is the only common zero of  $G$  and  $g$  in  $\overline{K}$ .

For  $2 \leq j \leq s$  we have

$$\begin{aligned} G(c_j) = 0 &\iff \text{there exists } 1 \leq i \leq r \text{ such that } a - uc_j = b_i \\ &\iff \text{there exists } 1 \leq i \leq r \text{ such that } b + uc - uc_j = b_i \\ &\iff \text{there exists } 1 \leq i \leq r \text{ such that } u = \frac{b_i - b}{c - c_j}. \end{aligned}$$

Since there are only finitely many such values and  $K$  is infinite, we can choose  $u \in K$  such that

$$u \neq \frac{b_i - b}{c - c_j} \quad \text{for all } 1 \leq i \leq r \text{ and } 2 \leq j \leq s.$$

Let  $h := \gcd(G, g) \in K(a)[X]$ . Then  $h$  is also the greatest common divisor of  $G$  and  $g$  in  $\overline{K}[X]$ .

Since  $g$  is separable over  $K$  and  $c$  is the only common zero of  $G$  and  $g$ , we obtain

$$h = X - c.$$

Thus  $c \in K(a)$ , since  $h \in K(a)[X]$ .

□

## 2 Examples

### 2.1 A primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

Here we use the same notation as in the proof. Let

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad b = \sqrt{2}, \quad c = \sqrt{3}.$$

Then  $L = K(b, c)$ .

The minimal polynomials are

$$f = \mu_{b,K} = X^2 - 2, \quad g = \mu_{c,K} = X^2 - 3.$$

Hence the pairwise distinct zeroes in  $\bar{K}$  are

$$b_1 = \sqrt{2}, \quad b_2 = -\sqrt{2}, \quad c_1 = \sqrt{3}, \quad c_2 = -\sqrt{3}.$$

We may assume that  $b = b_1$  and  $c = c_1$ .

As in the proof, we look for  $a = b + uc$  with  $u \in K$ . We must find  $u$  such that

$$u \neq \frac{b_i - b}{c - c_j} \quad \text{for } 1 \leq i \leq 2, \quad 2 \leq j \leq 2.$$

The only nontrivial value is (for  $b_i = 1$  we have  $u = 0$ )

$$u \neq \frac{-\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = -\sqrt{\frac{2}{3}}.$$

Thus we may choose  $u = 1$  and set

$$a = b + c = \sqrt{2} + \sqrt{3}.$$

Then

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

## 2.2 A primitive element for $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$

We again use the same notation. Let

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}, i), \quad b = \sqrt{2}, \quad c = i.$$

Then  $L = K(b, c)$ .

The minimal polynomials are

$$f = \mu_{b,K} = X^2 - 2, \quad g = \mu_{c,K} = X^2 + 1.$$

Hence the pairwise distinct zeroes in  $\bar{K}$  are

$$b_1 = \sqrt{2}, \quad b_2 = -\sqrt{2}, \quad c_1 = i, \quad c_2 = -i.$$

We may assume that  $b = b_1$  and  $c = c_1$ .

As in the proof, we look for  $a = b + uc$  with  $u \in K$ . We must avoid

$$u = \frac{b_i - b}{c - c_j} \quad \text{for } 1 \leq i \leq 2, \quad 2 \leq j \leq 2.$$

The only nontrivial value is

$$u = \frac{-\sqrt{2} - \sqrt{2}}{i - (-i)} = -\frac{\sqrt{2}}{i} = i\sqrt{2} \notin \mathbb{Q}.$$

Thus we may choose  $u = 1$  and set

$$a = b + c = \sqrt{2} + i.$$

Then

$$\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i).$$

### 2.3 A primitive element for $\mathbb{Q}(\sqrt[4]{2}, \sqrt{7})/\mathbb{Q}$

Once again we are in the following situation:

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt[4]{2}, \sqrt{7}), \quad b = \sqrt[4]{2}, \quad c = \sqrt{7}.$$

For the minimal polynomials (using Eisenstein with  $p = 2$  and  $p = 7$ ) of  $b, c$  we have:

$$f = \mu_{b,K} = X^4 - 2, \quad g = \mu_{c,K} = X^2 - 7.$$

The pairwise distinct zeroes of  $f$  and  $g$  in  $\overline{K}$  are

$$\begin{aligned} b_1 &= \sqrt[4]{2}, & c_1 &= \sqrt{7}, \\ b_2 &= -\sqrt[4]{2}, & c_2 &= -\sqrt{7}, \\ b_3 &= i\sqrt[4]{2}, \\ b_4 &= -i\sqrt[4]{2}. \end{aligned}$$

We're looking for  $a = b + uc$  with  $u \in K$ .

Once again we're looking for a  $u$  such that

$$u \neq \frac{b_i - b}{c - c_j} \quad \text{for } 1 \leq i \leq 4 \text{ and } j = 2.$$

So we have

$$u \neq \frac{b_i - \sqrt[4]{2}}{\sqrt{7} - (-\sqrt{7})} = \frac{b_i - \sqrt[4]{2}}{2\sqrt{7}}.$$

Since we know that  $u$  is a rational number we only need to test  $b_1$  and  $b_2$ . Therefore we immediately obtain

$$u \neq 0 \quad \text{and} \quad u \neq -\sqrt[4]{\frac{2}{7}}.$$

Therefore we can pick  $u$  to be 1 and obtain  $a = \sqrt[4]{2} + \sqrt{7}$  and hence

$$\boxed{\mathbb{Q}(\sqrt[4]{2} + \sqrt{7}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{7})}.$$