

The Primitive Element Theorem

Given a field extension  $F \subseteq K$ , an element  $\alpha \in K$  is said to be *separable* over  $F$  if it is algebraic over  $F$  and its minimal polynomial over  $F$  is separable. Recall that this is automatically true in characteristic 0.

**Theorem.** *Suppose  $K = F(\alpha_1, \dots, \alpha_n)$ , with each  $\alpha_i$  algebraic over  $F$  and  $\alpha_2, \dots, \alpha_n$  separable. Then  $K$  is a simple extension of  $F$ , i.e.,  $K = F(\gamma)$  for some  $\gamma \in K$ . In particular, every finite extension is simple in characteristic 0.*

Any  $\gamma$  as in the theorem is said to be a *primitive* element for the extension. You can find a proof of the Theorem on p. 509 of your text, but this uses the full machinery of Galois theory. What follows is a more elementary proof, taken from van der Waerden.

*Proof.* If  $F$  is finite, then so is  $K$ , and we can take  $\gamma$  to be any generator of the cyclic group  $K^\times$ . So we may assume from now on that  $F$  is infinite. We may also assume that  $n = 2$ , since an easy induction reduces the general case to this case. So let  $K = F(\alpha, \beta)$ , with  $\beta$  separable over  $F$ . Fix  $\lambda \in F$  and let  $\gamma = \alpha + \lambda\beta$ . We will show that  $\gamma$  is primitive if  $\lambda \notin S$ , where  $S$  is a finite subset of  $F$  defined as follows: Let  $f$  be the minimal polynomial of  $\alpha$  over  $F$  and let  $g$  be the minimal polynomial of  $\beta$  over  $F$ . Extend  $K$  to a field  $L$  in which  $f$  and  $g$  both split completely. Then the exceptional set  $S$  consists of all  $\lambda \in F$  such that in  $L$ ,

$$\lambda = \frac{\alpha' - \alpha}{\beta' - \beta}$$

for some root  $\alpha'$  of  $f$  and some root  $\beta' \neq \beta$  of  $g$ .

To show that  $\gamma$  is primitive for  $\lambda \notin S$ , it suffices to show that the simple extension  $F(\gamma)$  contains  $\beta$  and hence also  $\alpha = \gamma - \lambda\beta$ . To this end, we will show that the minimal polynomial of  $\beta$  over  $F(\gamma)$  cannot have degree  $\geq 2$ . Note first that  $\beta$  satisfies  $f(\gamma - \lambda\beta) = 0$ , i.e.,  $\beta$  is a root of the polynomial  $h \in F(\gamma)[x]$  defined by  $h(x) = f(\gamma - \lambda x)$ . The minimal polynomial of  $\beta$  over  $F(\gamma)$  therefore divides both  $g$  and  $h$ , so we'll be done if we show that the greatest common divisor of  $g$  and  $h$  in  $F(\gamma)[x]$  has degree 1. Suppose not. Then  $g$  and  $h$  have a common root  $\beta' \neq \beta$  in  $L$ . [This is where we use the separability of  $g$ .] Hence  $f(\gamma - \lambda\beta') = 0$ , i.e., there is a root  $\alpha'$  of  $f$  such that

$$\gamma - \lambda\beta' = \alpha + \lambda(\beta - \beta') = \alpha'.$$

But this is exactly what we ruled out by choosing  $\lambda \notin S$ . □

**Exercise.** Find a primitive element for  $\mathbf{Q}(i, \sqrt[3]{2})$  over  $\mathbf{Q}$ .