Mathematics 6310

The Primitive Element Theorem

Ken Brown, Cornell University, October 2010

Given a field extension K/F, 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 1. *Suppose $K = F(\alpha_1, \dots, \alpha_n)$, with each α_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 γ as in the theorem is said to be a *primitive* element for the extension. You can find a proof of the theorem (or a slightly weaker version of it) in Section 14.4 of your text (Theorem 25 on p. 595), but this proof 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 γ to be any generator of the cyclic group $K^\times$. So we may assume 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 α and β algebraic over F and β separable. We will show that a random linear combination of α and β is primitive. More precisely, fix $\lambda \in F$, and let $\gamma := \alpha + \lambda\beta$. We will show that γ is primitive for all but finitely many choices of λ.

To show that γ is primitive, it suffices to show that the simple extension $F(\gamma)$ contains β and hence also $\alpha = \gamma - \lambda\beta$. To this end, we will show that (except for finitely many exceptional λ) the minimal polynomial of β over $F(\gamma)$ cannot have degree ≥ 2. Let f be the minimal polynomial of α over F, and let g be the minimal polynomial of β over F. Let L/K be an extension in which f and g both split completely. Note first that β satisfies $f(\gamma - \lambda\beta) = 0$, i.e., β is a root of the polynomial $h \in F(\gamma)[x]$ defined by

$$h(x) := f(\gamma - \lambda x).$$

The minimal polynomial of β 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 $F(\gamma)[x]$ cannot have degree ≥ 2. Suppose the greatest common divisor does have degree ≥ 2. Then g and h have a common root $\beta' \neq \beta$ in L. [This is where we use the separability of β.] Then $f(\gamma - \lambda\beta') = 0$, i.e.,

$$\gamma - \lambda\beta' = \alpha' \tag{1}$$

for some root α' of f in L. Remembering that $\gamma = \alpha + \lambda\beta$, we can rewrite (1) as

$$\alpha + \lambda\beta - \lambda\beta' = \alpha',$$

or $\lambda = (\alpha' - \alpha)/(\beta - \beta')$. Thus the bad values of $\lambda \in F$ are those that can be written as

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

in L, for some root α' of f and some root $\beta' \neq \beta$ of g. There are only finitely many such λ. $\square$

Exercise. Use the method of proof of the theorem to find a primitive element for $\mathbb{Q}(i, \sqrt[3]{2})$ over $\mathbb{Q}$. [With a little calculation, one can show that $\lambda = 1$ is a good choice in the proof of the theorem, so $i + \sqrt[3]{2}$ is in fact primitive, as claimed in class.]