proof of primitive element theorem

Canonical name	ProofOfPrimitiveElementTheorem
Date of creation	2013-03-22 14:16:27
Last modified on	2013-03-22 14:16:27
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	8
Author	alozano (2414)
Entry type	Proof
Classification	msc 12F05

Theorem. *Let F and K be arbitrary fields, and let K be an extension of F of finite degree. Then there exists an element $\alpha \in K$ such that $K = F(\alpha)$ if and only if there are finitely many fields L with $F \subseteq L \subseteq K$.*

Proof. Let F and K be fields, and let $[K : F] = n$ be finite.

Suppose first that $K = F(\alpha)$. Since K/F is finite, α is algebraic over F. Let $m(x)$ be the minimal polynomial of α over F. Now, let L be an intermediary field with $F \subseteq L \subseteq K$ and let $m'(x)$ be the minimal polynomial of α over L. Also, let L' be the field generated by the coefficients of the polynomial $m'(x)$. Thus, the minimal polynomial of α over L' is still $m'(x)$ and $L' \subseteq L$. By the properties of the minimal polynomial, and since $m(\alpha) = 0$, we have a divisibility $m'(x)|m(x)$, and so:

$$[K : L] = \deg(m'(x)) = [K : L'].$$

Since we know that $L' \subseteq L$, this implies that $L' = L$. Thus, this shows that each intermediary subfield $F \subseteq L \subseteq K$ corresponds with the field of definition of a (monic) factor of $m(x)$. Since the polynomial $m(x)$ has only finitely many monic factors, we conclude that there can be only finitely many subfields of K containing F.

Now suppose conversely that there are only finitely many such intermediary fields L. If F is a finite field, then so is K, and we have an explicit description of all such possibilities; all such extensions are generated by a single element. So assume F (and therefore K) are infinite. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for K over F. Then $K = F(\alpha_1, \ldots, \alpha_n)$. So if we can show that any field extension generated by two elements is also generated by one element, we will be done: simply apply the result to the last two elements α_{j-1} and α_j repeatedly until only one is left.

So assume $K = F(\beta, \gamma)$. Consider the set of elements $\{\beta + a\gamma\}$ for $a \in F^\times$. By assumption, this set is infinite, but there are only finitely many fields intermediate between K and F; so two values must generate the same extension L of F, say $\beta + a\gamma$ and $\beta + b\gamma$. This field L contains

$$\frac{(\beta + a\gamma) - (\beta + b\gamma)}{a - b} = \gamma$$

and

$$\frac{(\beta + a\gamma)/a - (\beta + b\gamma)/b}{1/a - 1/b} = \beta$$

and so letting $\alpha = \beta + a\gamma$, we see that

$$F(\alpha) = L = F(\beta, \gamma) = K.$$

$\square$