existence of the minimal polynomial

Canonical name	ExistenceOfTheMinimalPolynomial
Date of creation	2013-03-22 13:57:24
Last modified on	2013-03-22 13:57:24
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	7
Author	alozano (2414)
Entry type	Theorem
Classification	msc 12F05
Related topic	FiniteExtension
Related topic	Algebraic

Proposition 1. *Let K/L be a finite extension of fields and let $k \in K$. There exists a unique polynomial $m_k(x) \in L[x]$ such that:*

1. *$m_k(x)$ is a monic polynomial;*
2. *$m_k(k) = 0$;*
3. *If $p(x) \in L[x]$ is another polynomial such that $p(k) = 0$, then $m_k(x)$ divides $p(x)$.*

Proof. We start by defining the following map:

$$\psi\colon L[x] \to K$$

$$\psi(p(x)) = p(k)$$

Note that this map is clearly a ring homomorphism. For all $p(x), q(x) \in L[x]$:

- $\psi(p(x) + q(x)) = p(k) + q(k) = \psi(p(x)) + \psi(q(x))$
- $\psi(p(x) \cdot q(x)) = p(k) \cdot q(k) = \psi(p(x)) \cdot \psi(q(x))$

Thus, the kernel of ψ is an ideal of $L[x]$:

$$\mathrm{Ker}(\psi) = \{p(x) \in L[x] \mid p(k) = 0\}$$

Note that the kernel is a **non-zero** ideal. This fact relies on the fact that K/L is a finite extension of fields, and therefore it is an algebraic extension, so every element of K is a root of a non-zero polynomial $p(x)$ with coefficients in L, this is, $p(x) \in \mathrm{Ker}(\psi)$.

Moreover, the ring of polynomials $L[x]$ is a principal ideal domain (see example of PID). Therefore, the kernel of ψ is a principal ideal, generated by some polynomial $m(x)$:

$$\mathrm{Ker}(\psi) = (m(x))$$

Note that the only units in $L[x]$ are the constant polynomials, hence if $m'(x)$ is another generator of $\mathrm{Ker}(\psi)$ then

$$m'(x) = l \cdot m(x), \quad l \neq 0, \quad l \in L$$

Let α be the leading coefficient of $m(x)$. We define $m_k(x) = \alpha^{-1}m(x)$, so that the leading coefficient of m_k is 1. Also note that by the previous remark, m_k is the unique generator of $\mathrm{Ker}(\psi)$ which is monic.

By construction, $m_k(k) = 0$, since m_k belongs to the kernel of ψ, so it satisfies (2).

Finally, if $p(x)$ is any polynomial such that $p(k) = 0$, then $p(x) \in \mathrm{Ker}(\psi)$. Since m_k generates this ideal, we know that m_k must divide $p(x)$ (this is property (3)).

For the uniqueness, note that any polynomial satisfying (2) and (3) must be a generator of $\mathrm{Ker}(\psi)$, and, as we pointed out, there is a unique monic generator, namely $m_k(x)$.

$\square$