proof of characterization of perfect fields

Canonical name	ProofOfCharacterizationOfPerfectFields
Date of creation	2013-03-22 14:47:44
Last modified on	2013-03-22 14:47:44
Owner	mclase (549)
Last modified by	mclase (549)
Numerical id	6
Author	mclase (549)
Entry type	Proof
Classification	msc 12F10

Proposition 1 *The following are equivalent:*

(a) Every algebraic extension of K is separable.

(b) Either $\operatorname{char} K = 0$ *or* $\operatorname{char} K = p$ *and the Frobenius map is surjective.*

Proof. Suppose (a) and not (b). Then we must have $\operatorname{char} K = p > 0$, and there must be $a \in K$ with no p-th root in K. Let L be a splitting field over K for the polynomial $X^p - a$, and let $\alpha \in L$ be a root of this polynomial. Then $(X - \alpha)^p = X^p - \alpha^p = X^p - a$, which has coefficients in K. This means that the minimum polynomial for α over K must be a divisor of $(X - \alpha)^p$ and so must have repeated roots. This is not possible since L is separable over K.

Conversely, suppose (b) and not (a). Let α be an element which is algebraic over K but not separable. Then its minimum polynomial f must have a repeated root, and by replacing α by this root if necessary, we may assume that α is a repeated root of f. Now, f' has coefficients in K and also has α as a root. Since it is of lower degree than f, this is not possible unless $f' = 0$, whence $\operatorname{char} K = p > 0$ and f has the form:

$$f = x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0.$$

with $a_o \neq 0$. By (b), we may choose elements $b_i \in K$, for $0 \leq i \leq n-1$ such that ${b_i}^p = a_i$. Then we may write f as:

$$f = (x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)^p.$$

Since $f(\alpha) = 0$ and since the Frobenius map $x \mapsto x^p$ is injective, we see that

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$$

But then α is a root of the polynomial

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

which has coefficients in K, is non-zero (since $b_o \neq 0$), and has lower degree than f. This contradicts the choice of f as the minimum polynomial of α.