MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Handout IV: Separability; the Theorem of the Primitive Element

4 Separability

Definition 4.1 Let $f(X)$ be an irreducible polynomial over a field F. We say that $f(X)$ is *separable* over F if it has no multiple roots in a splitting field.

Definition 4.2 Let $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial over some field F. The *formal derivative* of $f(X)$ is the polynomial

$$Df(X) = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Lemma 4.4 (Basic properties of formal differentiation) *Let $f(X)$ and $g(X)$ be polynomials in $F[X]$ and α and β be scalars in F. Then*

$$D\big(\alpha\, f(X) + \beta\, g(X)\big) = \alpha\, Df(X) + \beta\, Dg(X)$$
$$D\big(f(X)\, g(X)\big) = f(X) \cdot Dg(X) + Df(X) \cdot g(X)$$

Lemma 4.5 *Let $f(X)$ be a polynomial over a field F. Then $f(X)$ has a repeated root in a splitting field if and only if $f(X)$ and the formal derivative $Df(X)$ have a common factor of degree at least one.*

Proposition 4.6 *Let $f(X)$ be an irreducible polynomial over a field F of characteristic zero. Then $f(X)$ is separable.*

Example 4.7 Let t be an indeterminate and consider the field $F = \mathbb{F}_p(t)$ of rational functions over the finite field $\mathbb{F}_p$ in the indeterminate t. Define

$$f(X) = X^p - t,$$

a polynomial in the indeterminate X with coefficients in the field F. One can establish the following facts:

(i) $f(X) = 0$ has no roots in F;

(ii) if α is any root of $f(X)$ in a splitting field, then $f(X) = (X - \alpha)^p$;

(iii) $f(X)$ is irreducible over F.

Hence $f(X)$ is an inseparable polynomial over the field F. [See Problem Sheet IV, Question 5, for details.]

Separable extensions and the Theorem of the Primitive Element

Definition 4.8 Let K be an algebraic extension of a field F. We say that K is a *separable extension* of F if the minimum polynomial of every element of K over F is separable over F.

Corollary 4.9 *Every algebraic extension of a field of characteristic zero is a separable extension.*

Lemma 4.10 *Let L be a separable extension of an infinite field F and let $\beta, \gamma \in L$. Then there exists some $\alpha \in F(\beta, \gamma)$ such that*

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

Theorem 4.11 (Theorem of the Primitive Element) *Let K be a finite separable extension of an infinite field F. Then $K = F(\alpha)$ for some $\alpha \in K$.*

Corollary 4.12 *Every finite extension of a field of characteristic zero can be expressed as a simple extension.*