Galois Theory and Finite Fields

Kevin James

Proposition

Suppose that K/F is Galois and the F'/F is any extention. Then KF'/F is Galois with Galois group

$$\mathrm{Gal}(KF'/F) \cong Gal(K/(K \cap F').$$

Proposition

Suppose that K/F is Galois and the F'/F is any extention. Then KF'/F is Galois with Galois group

$$\mathrm{Gal}(KF'/F) \cong Gal(K/(K \cap F')).$$

Corollary

Suppose K/F is Galois and F'/F is any finite extension. Then,

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proposition

Let K_1 and K_2 be Galois extensions of F. Then

1. *$K_1 \cap K_2$ is Galois over F.*
2. *$K_1 K_2$ is Galois over F. The Galois group is isomorphic to the subgroup*

$$H = \{(\sigma, \tau) \quad | \quad \sigma|_{K_1 \cap K_2} = \tau_{K_1 \cap K_2}\}$$

of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Proposition

Let K_1 and K_2 be Galois extensions of F. Then

1. *$K_1 \cap K_2$ is Galois over F.*
2. *K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup*

$$H = \{(\sigma, \tau) \quad | \quad \sigma|_{K_1 \cap K_2} = \tau_{K_1 \cap K_2}\}$$

of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Corollary

Let K_1 and K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$. Then,

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Conversely, if K is Galois over F and $G = \mathrm{Gal}(K/F) = G_1 \times G_2$, then K is the composite of two Galois extensions of K_1 and K_2 of F with $K_1 \cap K_2 = F$.

Corollary

Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.

Corollary

Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.

Definition

The Galois extension K/F containing E in the previous corollary is called the <u>Galois closure</u> of E over F.

Definition

An extension K/F is called simple if $K = F(\theta)$ for some $\theta \in K$. In this case, θ is called a primitive element for K.

Definition

An extension K/F is called simple if $K = F(\theta)$ for some $\theta \in K$. In this case, θ is called a primitive element for K.

Proposition

Let K/F be a finite extension. Then $K = F(\theta)$ for some $\theta \in K$ **iff** *there exist only finitely many subfields of K containing F.*

Definition

An extension K/F is called simple if $K = F(\theta)$ for some $\theta \in K$. In this case, θ is called a primitive element for K.

Proposition

Let K/F be a finite extension. Then $K = F(\theta)$ for some $\theta \in K$ **iff** *there exist only finitely many subfields of K containing F.*

Theorem (Primitive Element Theorem)

If K/F is finite and separable, then K/F is simple. In particular, any finite extension of a field of characteristic 0 is simple.