Galois theory

Jin-Woo Park

February 20, 2010

Review

- An extension field E of a field F is an *algebraic extension* of F if every element in E is algebraic over F.
- A field F is *algebraically closed* if every nonconstant polynomial in $F[x]$ has a zero in F.
- Let E be an extension field of F. Then

$$\bar{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

  is a subfield of E, the *algebraic closure* of F in E.
- A field $E \leq \bar{F}$ is *splitting field* over F if it is the splitting field of some set of polynomials in $F[x]$.

Review

Theorem

A field is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors in $F[x]$ into linear factors.

Corollary

An algebraically closed field F has no proper algebraic extensions. i.e) no algebraic extension E with $F \lneq E$.

Theorem

Every field F has an algebraic closure, that is, an algebraic extension $\bar{F}$ that is algebraically closed.

Review

- Let E be a finite extension of a field F. The number of isomorphisms of E onto a subfield of $\bar{F}$ leaving F fixed is the *index* $\{E : F\}$ of E over F.

Theorem

If $F \leq E \leq K$, where K is a finite extension field of the field F, then $\{K : F\} = \{K : E\}\{E : F\}$.

- If $F \leq E$ and $\alpha \in E$ is an algebraic over F, then $\{F(\alpha) : F\}$ is the number of distinct zeros of irreducible polynomial with a zero α.

Theorem

If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$.

Main Theory

- A finite extension E of F is a *separable extension* of F if $\{E : F\} = [E : F]$. An element α of $\bar{F}$ is *separable* over F if $F(\alpha)$ is a separable extension of F. An irreducible polynomial $f(x) \in F[x]$ is *separable* over F if every zero of $f(x)$ in $\bar{F}$ is separable over F.

Example

The field $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is separable over $\mathbb{Q}$ since $\{E : \mathbb{Q}\} = 4 = [E : \mathbb{Q}]$.

Main Theory

Theorem

If K is a finite extension of E and E is a finite extension of F, then K is separable over F if and only if K is separable over E and E is separable over F.

Corollary

If E is a finite extension of F, then E is separable over F if and only if each α in E is separable over F.

- A finite extension K of F is *finite normal extension* of F if K is a separable splitting field over F.
- If F, K be fields with $F \leq K$, then $G(K/F)$ is the group of all automorphisms of K leaving F fixed.

Theorem

Let K be a finite normal extension of F, and let E be an extension of F where $F \leq E \leq K \leq \bar{F}$. Then K is a finite normal extension of E, and $G(K/E)$ is the subgroup of $G(K/F)$

Main Theory

Theorem (Main theorem of Galois Theory)

Let K be a finite normal extension of F. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a $1-1$ map of the set of all such intermediate field E onto the set of all subgroups of $G(K/F)$. The following properties holds for λ;

1. $\lambda(E) = G(K/E)$ *and* $E = K_{G(K/E)} = K_{\lambda(E)}$.
2. *For* $H \leq G(K/F)$, $\lambda(K_H) = H$.
3. $[K : E] = |\lambda(E)|$ *and* $[E : F]$ *is the number of left cosets of* $\lambda(E)$ *in* $G(K/F)$.
4. E *is a normal extension of* F *if and only if* $\lambda(E)$ *is a normal subgroup of* $G(K/F)$. *When* $\lambda(E)$ *is a normal subgroup of* $G(K/F)$, *then* $G(E/F) \simeq G(K/F)/G(K/E)$.
5. *The diagram of subgroups of* $G(K/F)$ *is the inverted diagram of intermediate fields of* K *over* F.