Galois extensions

Definition

An algebraic extension K/k is called Galois if it is normal and separable.

Remark

K/k is allowed to be infinite.

If K/k is a Galois extension, we let

$$\mathrm{Gal}(K/k)$$

be the group of auotomorphisms of K over k.

Theorem

Let K/k be a finite Galois extension. Then,

$$F \mapsto \mathrm{Gal}(K/F)$$

induces a bijection between subextensions of K/k and subgroups of $\mathrm{Gal}(K/k)$.

Note that this bijection reverses the inclusion relations.

Proof of injectivity

First we show that

$$K^{\mathrm{Gal}(K/k)} = k.$$

Indeed, if $\alpha \in K^{\mathrm{Gal}(K/k)}$, any embedding of $k(\alpha)$ into K maps α to itself. This shows that $[k(\alpha) : k]_s = 1$. Since K/k is separable, so is $k(\alpha)/k$ and conclude that $k(\alpha) = k$. This means $\alpha \in k$.

More generally, if F and F' are two subextensions of K/k such that $H = \mathrm{Gal}(K/F) = \mathrm{Gal}(K/F')$, then the above argument shows that $K^H = F = F'$. This shows the injectivity.

We record the primitive element theorem, which will be used in the proof of the surjectivity.

Theorem

Let E/k be a finite extension. There exists an element $\alpha \in E$ with $E = k(\alpha)$ if and only if there exists only a finite number of subextensions of E/k.

We will only use $\Leftarrow$ part in the proof. For this part, we deal with finite and inifinite fields separately. Finite fields have cyclic multiplicative groups, so the assertion holds true. For infinite fields the argument is as follows. For any $\alpha, \beta \in E$, find distinct $c_1, c_2 \in k$ with $k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$. Then, $k(\alpha + c_1\beta) = k(\alpha + c_2\beta) = k(\alpha, \beta)$.

Proof of surjectivity

Let $H \subset \mathrm{Gal}(K/k)$ be a subgroup. Let $F = K^H$. Then, we have an injective map $H \to \mathrm{Gal}(K/F)$. To show this is an isomorphism, it suffices to show that $[K : F] \leq |H|$, because $|\mathrm{Gal}(K/F)| = [K : F]_s = [K : F]$.

We may use the primitive element theorem, since the injectivity part shows that the number of subextensions is at most the number of subgroups of $\mathrm{Gal}(K/k)$ which is finite. Now it suffices to show that every element $\alpha \in K$ has degree at most $|H|$ over F. This is true because

$$\prod_{\sigma \in H} (X - \sigma\alpha) \in F[X].$$

Question

Complete the other half, ($\Rightarrow$) of the primitive element theorem:-

Theorem

Let E/k be a finite extension. There exists an element $\alpha \in E$ with $E = k(\alpha)$ if and only if there exists only a finite number of subextensions of E/k.