The Fundamental Theorem of Galois Theory

Kevin James

Definition

A (linear) character of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$.

Definition

The characters $\chi_1, \chi_2, \ldots, \chi_n$ of G are said to be linearly independent over L if they are linearly independent as functions on G.

Theorem (Linear Independence of Characters)

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.

Corollary

If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular, distinct automorphisms of a field K are linearly independent as functions on K.

Theorem

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then,

$$[K : F] = n = |G|.$$

Corollary

Let K/F be any finite extension. Then

$$|\mathrm{Aut}(K/F)| \leq [K : F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. (-i.e. K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$).

Corollary

Let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, (-i.e. $\mathrm{Aut}(K/F) = G$), so that K/F is Galois with Galois group G.

Corollary

If $G_1 \neq G_2$, are distinct finite subgroups of automorphisms of a field K then their fixed fields are also distinct.

Theorem

The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (so in particular K/F is a separable extension).

Definition

Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the conjugates (or Galois conjugates) of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the conjugate field of E over F.

Note

We now have four characterizations of Galois extensions K/F.

1. Splitting fields of separable polynomials over F.
2. Fields where F is precisely the set of elements fixed by $\mathrm{Aut}(K/F)$
3. Fields with $[K : F] = |\mathrm{Aut}(K/F)|$
4. Finite, normal and separable extensions.

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and set $G = \mathrm{Gal}(K/F)$. Then there is a bijection

$$\{F \subseteq E \subseteq K \quad | \quad E \text{ is a field}\} \longleftrightarrow \{H \leq G\}$$

given by the correspondences

$$E \mapsto \{\sigma \in G \quad | \quad \sigma \text{ fixes } E \text{ pointwise}\},$$

and

$$H \mapsto \{\alpha \in K \quad | \quad \sigma(\alpha) = \alpha, \forall \alpha \in H\}$$

which are inverse to each other. Under this correspondence

1. *If $E_1, E_2 \subseteq K$ correspond to $H_1, H_2 \leq G$ then $E_1 \subseteq E_2$ if and only if $H_1 \geq H_2$.*
2. $[K : E] = |H|$ *and* $[E : F] = [G : H]$.
3. *K/E is always Galois, with Galois group $\mathrm{Gal}(K/E) = H$.*
4. ....

Theorem (Fundamental Theorem of Galois Theory (continued))

1. *If* $E_1, E_2 \subseteq K$ *correspond to* $H_1, H_2 \leq G$ *then* $E_1 \subseteq E_2$ *if and only if* $H_1 \geq H_2$.
2. $[K : E] = |H|$ *and* $[E : F] = [G : H]$.
3. K/E *is always Galois, with Galois group* $\mathrm{Gal}(K/E) = H$.
4. E *is Galois over* F *if and only if* $H \trianglelefteq G$ *and if this is the case then* $\mathrm{Gal}(E/F) \cong G/H$.
5. *If* $E_1, E_2 \subseteq K$ *correspond to* $H_1, H_2 \leq G$, *then* $E_1 \cap E_2$ *corresponds to* $< H_1, H_2 >$ *and* $E_1 E_2$ *corresponds to* $H_1 \cap H_2$.