

Galois Theory

Robert F. Coleman

Lecture 31

Inverse Problem

Theorem. (Hilbert) *The Galois group of the splitting field of a random polynomial of degree n over \mathbf{Q} is S_n .*

Corollary. *If G is a finite group there exists subfields F and K of \mathbf{C} such that $[K : \mathbf{Q}] < \infty$, F/K is normal and $\text{Gal}(F/K) = G$.*

Hilbert's Inverse Problem. *Can one prove the previous statement with $K = \mathbf{Q}$?*

The General Equation

Let x_1, \dots, x_n be variables. Let $N_n = \mathbf{Q}(x_1, \dots, x_n)$. Let

$$P_n(T) = \prod_{i=1}^n (T - x_i) = \sum_{j=1}^n e_j(x_1, \dots, x_n) T^j.$$

Let $E_n = \mathbf{Q}(\{e_j(x_1, \dots, x_n) : 1 \leq j \leq n\})$.

Proposition. N_n/E_n is normal and $\text{Gal}(N_n/E_n) \cong S_n$.

Proof. N_n is the splitting field over E_n of P_n .

There exists an injective homomorphism $S_n \rightarrow \text{Aut}_{\mathbf{Q}}(N_n)$.

$$N_n^{S_n} \supseteq E_n.$$

We know $[N_n : N_n^{S_n}] = |S_n|$.

Proposition. $N_n \cong K_n$.

More generally,

Proposition. If $\alpha_1, \dots, \alpha_n$ are algebraically independent over \mathbf{Q} , $K_n \cong \mathbf{Q}(\alpha_1, \dots, \alpha_n)$. ■

Transcendence

The elements $\alpha_1, \dots, \alpha_n$ in F are said to be **algebraically independent** over K if

The set $\alpha_1, \dots, \alpha_n$ is said to be a **transcendence basis** for F/K if F is algebraic over $K(\alpha_1, \dots, \alpha_n)$ and n called the **transcendence degree** of F/K .

Proposition. *Transcendence degree is well defined.*

Proof.

Read §12.5-§12.8

Final Problems

1. Let p be a prime and $r \geq 1$ an integer. Show $x^{p^r} - x$ is the product of all the monic irreducible polynomials over \mathbf{F}_p of degree dividing r .
2. Let $F_n(x) = \sum_{i=0}^n x^i/i!$. Show the Galois group of the splitting field of $F_n(x)$ over \mathbf{Q} is isomorphic to a subgroup of A_n if $4|n$.
3. True-False. If false, give a counterexample.
 - (i) Every field has a normal extension of degree 2.
 - (ii) The intersection of a quadratic and a cubic extension of a field K is K .
 - (iii) A normal extension with a solvable Galois group is a radical extension.
 - (iv) A non-normal extension of a non-normal extension is not normal.
 - (v) Two extensions of \mathbf{Q} in \mathbf{C} are isomorphic if and only if they are equal.
4. Suppose F and K are normal extensions of \mathbf{Q} in \mathbf{C} . Show $\text{Gal}(\mathbf{Q}(F \cup K)/\mathbf{Q})$ injects into $\text{Gal}(F/\mathbf{Q}) \times \text{Gal}(K/\mathbf{Q})$.
5. Find an extension of \mathbf{Q} with Galois group $C_3 \times C_3 \times C_3$. (This group might be changed if this question appears on the exam.)
6. Suppose $a, b \in \mathbf{Q}^*$. show $\mathbf{Q}(\sqrt{a}) \cong \mathbf{Q}(\sqrt{b})$ if and only if $ab \in \mathbf{Q}^2$.