

Galois Theory

Robert F. Coleman

Lecture 16

Main Theorem (continued)

Theorem. If N/K is normal and separable of finite degree, H is a normal subgroup of $G =: \text{Gal}(N/K)$ if and only if N^H is a normal extension of K . Moreover, $\text{Gal}(N^H/K) = G/H$.

Proof. Suppose $E = N^H$ is normal. Then we have the short exact sequence,

$$0 \rightarrow H \rightarrow G \rightarrow \text{Gal}(E/K) \rightarrow 0$$

Suppose $g \in G$. Suppose H is a normal subgroup and $\alpha \in N^H$. If $\beta = g\alpha$, then

$$h\beta = g(g^{-1}hg)\alpha = \beta.$$

Example. Recall if $f(x) = x^3 + 3Bx - 2Z$, $B, Z \in \mathbf{Z}$, Viète tells us to look at $g(E) = E^6 + 2ZE^3 - B^3$. Suppose $B > 0$. If α is a root of g , $\alpha \neq 0$ and $B/\alpha - \alpha$ is a root of f . The 6 roots of g are $j^i\alpha$ and $-j^iB/\alpha$, $0 \leq i \leq 2$. Note, $(\alpha^3 + Z)^2 = B^3 + Z^2$ and $(j - j^{-1})^2 = -3$. Let K be the splitting field of g . Let's compute $\text{Gal}(K/\mathbf{Q})$ when f is irreducible.

Claim: Let θ be a root of f . Then the splitting field L of f is

$$\mathbf{Q}(\theta, \sqrt{-3(B^3 + Z^2)})$$

and $\text{Gal}(L/\mathbf{Q}) \cong S_3$ iff $-3(B^3 + Z^2)$ is not a square. (By 7.1.1, this is true even when $B \leq 0$.)

Galois groups and Permutation groups

Theorem. *If $f(x)$ is an irreducible polynomial of degree n over K , $f'(x) \neq 0$ and N is a splitting field for f , $\text{Gal}(N/K)$ is isomorphic to a transitive subgroup of S_n .*

If $f(x) = x^3 - 3ax^2 + b$, f has local extrema at 0 and $2a$. $f(2a) = -4a^3 + b < -0$ if $4a^3 > b$. So if $a = b = 2$, f is irreducible and has 3 real roots.

Homework for Monday

Suppose m and n are non-zero integers. Show $\mathbf{Q}(\sqrt{m}) \cong \mathbf{Q}(\sqrt{n})$ if and only if mn is a square. Compute $\text{Gal}(\mathbf{Q}(\sqrt{m}, \sqrt{n})/\mathbf{Q})$.