

Galois Theory

Robert F. Coleman

Lecture 24

Viete Explained

Let M be a field of characteristic different from 3, \overline{M} an algebraic closure of M and $f(X) = X^3 + 3BX - 2Z \in M[X]$. Let $\beta_1, \beta_2, \beta_3$ be the roots of $f(X)$ in \overline{M} i.e., $f(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$. Thus

$$\beta_1 + \beta_2 + \beta_3 = 0, \quad \beta_1\beta_2\beta_3 = 2Z$$

and
$$\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = 3B.$$

Now let ζ be a primitive cube root of 1 in \overline{M} and

$$S = \{(\rho_1\beta_1 + \rho_2\beta_2 + \rho_3\beta_3)/3 : \{\rho_1, \rho_2, \rho_3\} = \{1, \zeta, \zeta^2\}\}$$

Claim:

$$g(X) =: \prod_{s \in S} (X - s) = X^6 + 2ZX^3 - B^3.$$

$$(\rho_1\beta_1 + \rho_2\beta_2 + \rho_3\beta_3)(\rho_1^{-1}\beta_1 + \rho_2^{-1}\beta_2 + \rho_3^{-1}\beta_3) =$$

$$\rho_1\beta_1 + \rho_2\beta_2 + \rho_3\beta_3 + \rho_1^{-1}\beta_1 + \rho_2^{-1}\beta_2 + \rho_3^{-1}\beta_3 =$$

$$g(X) = (X^2 - \beta_1X - B)(X^2 - \beta_2X - B)(X^2 - \beta_3X - B)$$

Solvable Groups

A group G is said to be **solvable** if and only if there a sequence of subgroups

$$H_0 = (e) \subset H_1 \subset \cdots \subset H_r = G$$

such that H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

Examples.

Theorem. S_n is not solvable for $n \geq 5$.

Lemma. If G is solvable and H is either a sub or quotient group of G , then H is solvable.

Proof.

Let G be a group. The intersection of all subgroups of G with Abelian quotient $D(G)$ is called the **commutator subgroup** of G . If $\sigma, \tau \in G$, the **commutator** of σ and τ is

$$[\sigma, \tau] =: \sigma\tau\sigma^{-1}\tau^{-1}.$$

Lemma. if G is solvable $D(G) \neq G$.

Proof.

Read §11.5-§11.7.

Homework for Monday

Let K be the splitting of f over M . Give examples of all possibilities for $\text{Gal}(K/M)$.