

## Galois Theory

Robert F. Coleman

### Lecture 23

#### Abelian Extensions

Last time we proved.

**Theorem.** Suppose  $|\mu_n(K)| = n$ . Then  $L/K$  is cyclic of degree dividing  $n$  if and only if  $L = K(b^{1/n})$  for some  $b \in K$ .

using,

**Lemma.** Suppose  $M$  is a linear operator on a vector space  $V$  over  $K$ ,  $v \neq 0$  and  $P(T) \neq 0 \in K[T]$ . If  $P(T)$  factors completely, is square free and  $P(M)v = 0$ , then  $v$  is a sum of eigenvectors.

*non-Example.*  $x^2 - x - 1$  over  $\mathbf{F}_2$ .

**Theorem.** Suppose  $|\mu_n(K)| = n$  and  $N/K$  is a normal extension of  $K$  of degree dividing  $n$ . Then  $\text{Gal}(N/K)$  is Abelian if and only if  $N = K(\alpha_1, \dots, \alpha_r)$  where  $\alpha_i^n \in K$ .

*Proof.*

*Example.* Let  $K$  be the splitting field of  $f(X) =: X^3 + 3BX - 2Z = 0$  over  $\mathbf{Q}$ . Let  $G = \text{Gal}(K/\mathbf{Q})$ . Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $f(X)$ . Suppose  $G \cong S_3$ . Let  $C = A_3 \subset G$  and  $F = K^C$ .

If  $d =: (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ ,  $F = \mathbf{Q}(d)$ .

$$d^2 = -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3)$$

$$= 27 \cdot (\alpha_1^2 + B)(\alpha_2^2 + B)(\alpha_3^2 + B)$$

$$f(\sqrt{-B})f(-\sqrt{-B}) = 4(B\sqrt{-B} - Z)(-B\sqrt{-B} - Z) = 4(B^3 + Z^2)$$

Let  $\zeta$  be a primitive cube root of unity,  $F' = F(\zeta)$  and  $K' = K(\zeta)$ . Then  $\text{Gal}(K'/F') \cong \text{Gal}(K/F)$ .

Let  $\sigma \sim (123)$ . Let

$$\begin{aligned} c &= \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 \\ -12Z + \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3(\zeta(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + \zeta^2(\alpha_1^2\alpha_3 + \alpha_3^2\alpha_2 + \alpha_2^2\alpha_1)) \\ &\quad \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 = \\ &\quad (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) + \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2 + \alpha_1^2\alpha_3 \end{aligned}$$

## 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  $n \geq 5$ .

**Read** §11.1-§11.4.

### Homework for Monday

Prove the above lemma for arbitrary  $P$ . Finish the above computation. Do 11.2.