

## Lecture 27:

73

$K/F$  Galois, so is the splitting field of some  $f(x) \in F[x]$ . Assume  $K$  is simple (e.g. char = 0), and so can assume that  $f$  is irred.

Let  $\alpha_1, \dots, \alpha_n$  be the roots of  $f$ , so  $K = F(\alpha_1, \dots, \alpha_n)$ .

Have  $\text{Gal}(K/F) \leq S_n$ .

Discriminant:  $D = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in F$

Since  $D$  is a symmetric function in the  $\alpha_i$ , we can express it in terms of the elem sym fns, i.e. the coeff of  $f(x)$ .

Ex:  $n=2$ .  $D = (\alpha_1 - \alpha_2)^2 = S_1^2 - 4S_2$

where  $S_1 = \alpha_1 + \alpha_2$

So if  $f = x^2 + bx + c$ ,

$S_2 = \alpha_1 \alpha_2$

$$D = (-b)^2 - 4c = b^2 - 4c.$$

(as seen in the quad. formula.)

Ex:  $f(x) = x^3 + ax^2 + bx + c$

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Now  $D$  is a square in  $K$ , with

$$\sqrt{D} = \prod_{i < j} (\alpha_i - \alpha_j)$$

Suppose  $G = \text{Gal}(K/F) = S_n$ .

Then  $\exists \sigma \in G$  with  $\sigma(\sqrt{D}) = -\sqrt{D}$ , e.g.  $\sigma = (12)$

So, if char  $\neq 2$ , have  $\sqrt{D} \notin F$ .  
standing assumption.

$n=2$ : Since  $f$  is irred,  $[K:F] = 2$  and

$$G = \text{Gal}(K/F) \cong \mathbb{Z}_2 \cong S_2. \text{ So } K = F(\sqrt{D})$$

(Which we knew since roots of  $x^2 + bx + c$  are  $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$ )

$n=3$ :  $G \leq S_3$

Q: Could  $G = \langle (12) \rangle$ ? A: No, as  $f$  is irred, have to be able to take any root to any other.

So  $G = \mathbb{Z}_3 = \langle (123) \rangle \iff [K:F] = 3$   
or  $G = S_3 \iff [K:F] = 2$

So

$D$  not a square in  $F \implies G = S_3$ .

$D$  a square in  $F \implies G = \mathbb{Z}_3$ .

General info from  $\sqrt{D}$ :

Any  $\sigma \in S_n$  is a prod. of transpositions  $(ij)$   
called even or odd dep. on how many there are.

Gives  $S_n \rightarrow \mathbb{Z}_2$  with  
kernel the set of even perms  $A_n$ .

$n=4$ :

Prop: if  $D$  is not a square, then  $G = S_4$ .

Proof: Call  $H \leq S_4$  transitive if can take any  
 $i$  to  $j$ . As  $f$  is irred, know  $G$  is transitive.

The trans. subgps are (up to conjugation)

$$S_4, A_4, C = \langle (1234) \rangle, K = \langle (12)(34), (13)(24) \rangle$$

$$D_8 = \langle (1234), (12)(34) \rangle$$