

4/10/07

Recall

COR  $K/F$  finite. Then  $|\text{Aut}(K/F)| \leq [K:F]$  w/equality iff

$$F = K^{\text{Aut}(K/F)}$$

Recall This equality called  
 $K/F$  is Galois

COR Suppose  $G_1 \neq G_2$  distinct finite subgroups of  $\text{Aut } K$ . Then

$$K^{G_1} \neq K^{G_2}$$

Proof Suppose not. Then  $K^{G_1}$  is fixed by  $G_2$  so  $G_2 \leq G_1$ .  
And reverse.

RMK Thus distinct finite subgroups of  $\text{Aut } K$  give distinct  
fixed fields, each of which  $K$  is a Galois extension.

Recall Prop  $E$  a spl field  $/F$  of  $\text{fix}$ . Then

$$|\text{Aut}(E/F)| \leq [E:F]$$

w/equality iff  $\text{fix}$  is separable.

\* spl fields are Galois iff poly is separable \*

Thm  $K/F$  is Galois iff  $K$  is the splitting field of some separable polynomial  $f \in F$ .

Further every irreducible w/coefs in  $F$  which has a root in  $K$  is separable w/all roots in  $K$ . In particular  $K/F$  is separable.

i.e. Galois  $\iff$  normal, separable, finite

Proof  $\leftarrow$  already done

$\rightarrow$   
Suppose  $K/F$  is Galois,  $p(x) \in F[x]$  <sup>irred</sup>. Let  $\alpha \in K$  be a root of  $p(x)$ .  
Let  $G = \text{Gal}(K/F)$

Consider  $\{ \alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha) \}$   $G = \{ \sigma_1, \dots, \sigma_n \}$

Remove repeats,  $\alpha_1, \alpha_2, \dots, \alpha_r =$  orbit of  $\alpha$  under  $G$ .

Let  $\tau \in G$ . Then  $\tau$  permutes these. Thus

$$f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r) \text{ coefs fixed by } G$$

Thus coefs in  $F$ .

Any poly w/ root  $\alpha$  has  $\alpha$  and  $\tau(\alpha)$  as roots. Thus  $f(x) | p(x) \implies f(x) = p(x)$

Thus  $p(x)$  is separable, all roots in  $K$ , proving last part of Thm.

Now let  $K/F$  be finite w/ basis  $\{w_1, \dots, w_n\}$   
Let  $P(x)$  be min poly  $w_1$ .

Thus  $K$  is S.F. of  $\mathbb{P}_{P(x)}$ 's by previous

Now remove repeats //

Def Let  $K/F$  be Galois. The elements in the orbit of  $\alpha$  under  $\text{Gal}(K/F)$  are the Galois conjugates of  $\alpha$ .

COR  $K/F$  Galois,  $\alpha \in K$ . Then  $m_{\alpha, F}(x) = \prod_{\alpha'} (x - \alpha')$   
conjugates  
of  $\alpha$

RMK If any poly in  $F[x]$  has a root in  $K$  but not all roots in  $K$ ,  $K/F$  not Galois.

Summary Galois extensions and  $K/F$

1. Splitting fields of separable polys in  $F[x]$
2. Fields where  $F = K^{\text{Aut}(K/F)}$
3. Fields where  $[K:F] = |\text{Aut}(K/F)|$
4. Finite normal, separable extension.

(4)

## Fundamental Theorem of Galois Theory

Let  $K/F$  be Galois,  $G = \text{Gal}(K/F)$ . Then  $\exists$  a bijection

$$\left\{ \begin{array}{l} \text{subfields} \\ E \\ \text{---} \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgroups} \\ H \\ \text{---} \\ G \end{array} \right\}$$

Given by

$$E \longmapsto \{ \sigma \in G \mid \sigma(e) = e \ \forall e \in E \} = H = \text{Aut}(K/E)$$

$$K^H \longleftarrow H$$

which are inverse to each other, and such that

1. Both correspondences are inclusion reversing
2.  $[K:E] = |H|$ ,  $[E:F] = [G:H]$
3.  $K/E$  is always Galois,  $\text{Gal}(K/E) = H$
4.  $E/F$  is Galois  $\iff H \trianglelefteq G$ . In this case  

$$\text{Gal}(E/F) \cong G/H$$
5. If  $E_1 \leftrightarrow H_1$ ,  $E_2 \leftrightarrow H_2$  then  

$$E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$$

$$E_1 E_2 \leftrightarrow H_1 \cap H_2$$

Thus lattices are the same  
(upside down!)

Example SF  $x^8 - 2 / \mathbb{Q}$ .

Let  $\zeta_8 = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ ; so  $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$   
Let  $\theta = \sqrt[8]{2}$

So SF is  $\mathbb{Q}(\theta, \zeta_8) = \mathbb{Q}(\theta, i)$

$\mathbb{Q}(\theta, i)$

$\downarrow 2$   
 $\mathbb{Q}(\theta)$   
 $\downarrow 8$   
 $\mathbb{Q}$

Thus degree 16 extension, Galois group has 16 elements

But  $i$  must map to  $\pm i$ ,  $\theta^k \mapsto \theta^k$   $0 \leq k \leq 7$

So these 16 maps all give field automs

Def  $\sigma: \begin{cases} \theta \rightarrow \theta^3 \\ i \rightarrow i \end{cases}$       $\tau: \begin{cases} \theta \rightarrow \theta \\ i \rightarrow -i \end{cases}$

Now  $\zeta = \frac{1}{2}(1+i)\theta^4$  since  $\zeta = \frac{1}{2}(1+i)\sqrt{2}$

$\sigma: \zeta \rightarrow -\zeta$       $\tau: \zeta \rightarrow \zeta^7$

Check

$\text{Gal}(\mathbb{Q}(\sqrt[8]{2}, i) / \mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^{-3} \rangle$

quasidihedral.