

## Section 12.2 part 3

$F \subseteq K$  - field extension       $\text{Gal}_F K = \{ \sigma : K \rightarrow K \mid \sigma(c) = c \text{ for every } c \in F \}$

field isomorphism  
automorphism

$\sigma|_F = \text{identity map}$

Intermediate fields

$$F \subseteq E \subseteq K$$

### Galois Correspondence

Subgroups

$$\text{Gal}_E K \subseteq \text{Gal}_F K$$

$$E_H = \{ \sigma \in K \mid \sigma(\ell) = \ell \text{ for every } \ell \in H \}$$

fixed field of  $H$

$$H \subseteq \text{Gal}_F K$$

### Extreme cases

$$E = K$$



$$\langle \iota \rangle = \text{Gal}_K K \subseteq \text{Gal}_F K$$

$$E = F$$

$$\text{Gal}_F K \subseteq \text{Gal}_F K$$

$$F = \mathbb{Q} \quad K = \mathbb{Q}(\sqrt[3]{2})$$

$$\text{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \langle \iota \rangle = \text{Gal } \mathbb{Q}(\sqrt[3]{2}) / \mathbb{Q}(\sqrt[3]{2})$$

it may happen that  $\text{Gal}_F K$  fixes a subfield  $E > F$ .

In general, what may go wrong?

$$E \rightsquigarrow H = \text{Gal}_E K \rightsquigarrow E_H$$

Clearly,  $E_H \supseteq E$

Is every intermediate subfield the fixed field of some subgroup

However, elements of  $\text{Gal}_E K$  may fix a bigger subfield besides  $E$

$$E_H \neq E$$

of  $\text{Gal}_F K$ ? - NO

Under which extra conditions the answer is YES? (Th 12.9)

$$\text{Gal}_F K \supseteq H \Leftrightarrow E_H \text{ is } \text{Gal}_{E_H}^K$$

Is every subgroup  $H \subseteq \text{Gal}_F K$  the Galois group of an intermediate field? (Th 12.8) - Yes

$$\text{Clearly, } H \subseteq \text{Gal}_{E_H}^K$$

However, there may be elements of  $\text{Gal}_{E_H}^K$  are not in  $H$  but still fix  $E_H$

Lemma 12.7

Let  $K$  be a finite-dimensional extension of  $F$        $K \supseteq F$        $\left\{ \begin{array}{l} \text{finite-dimensional} \\ \text{implies algebraic} \end{array} \right.$   
Let  $H \subseteq \text{Gal}_F K$ .

Let  $E_H$  be the fixed field of  $H$ .

The the extension  $K \supseteq E_H$  is simple, normal, separable

Reve  $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$  is not normal: the polynomial  $x^3 - 2 \in \mathbb{Q}[x]$   
has a root,  $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$  but does not split completely.

Pf

Pick any  $u \in K$ . There may be only finitely many  
element  $\sigma(u)$  for all  $\sigma \in H$  (nothing but the roots  
of the minimal polynomial of  $u$ ).

Let those which occur be  $u_1, \dots, u_t \in K$  (all distinct).

Consider  $f = (x - u_1) \dots (x - u_t) \in K[x]$

Claim:  $f \in E_H(x)$ . That happens because every  $\sigma \in H$   
performs a permutation of  $u_1, \dots, u_t$ .

Thus every  $\sigma \in H$  only permutes the factors

in  $f$ , but does not alter  $f$  itself.  
 Therefore, every  $\sigma \in H$  fixes all coefficients  
 of  $f$ . Thus  $f \in E_H[x]$ .

We conclude that every element  $u \in K$  is a root of  
 a separable polynomial  $f \in E_H[x]$  ( $f$  is constructed  
 starting from  $u$  - the construction depends on  $u$ ).

That means  $E_H \subseteq K$  is separable (by the def of separability).

Furthermore,  $E_H \subseteq K$  is finite-dimensional (because  $F \subseteq K$   
 is finite-dimensional) therefore finitely generated.

By Th II.18      finitely generated } imply simple     $K = E_H(u)$   
 separable     $u \in K$

Take all  $\sigma(u)$  for  $\sigma \in H$  call them

$u_1, \dots, u_t \in K$ , and consider  $f = (x-u_1) \dots (x-u_t) \in E_H[x]$

$f$  splits completely in  $K$ .

Thus  $K$  is the splitting field of  $f \in E_H[x]$ ,  
 therefore normal by Th II.15.

} Construction  
 of  $f$   
 repeated  
 with specific  
 $u$

Th 12.2 Let  $K$  be finite-dimensional over  $F$   $K \supseteq F$

Let  $H \subseteq \text{Gal}_F K$  - subgroup.

Let  $E_H = E$  be the fixed field of  $H$ .

Then  $H = \text{Gal}_E K$  and  $|H| = [K:E]$ .

Pf

From Lemma 12.7,  $K \supseteq E$  is simple  $K = E(u)$ ,  $u \in K$ .

Thus by Th 11.7,  $[K:E] = \deg p = n$ , where  $p$  is the minimal polynomial of  $u$ .

For distinct  $\sigma \in \text{Gal}_E K$ , the elements  $\sigma(u)$  are distinct roots of  $p$ .  
(Th 12.2, 12.4)

Thus  $|\text{Gal}_E K| \leq n$

Clearly,  $H \subseteq \text{Gal}_E K$  (by the definition of  $E_H$ )

Thus  $|H| \leq |\text{Gal}_E K| \leq n = [K:E]$

Wanted: an opposite inequality.

Consider all distinct  $\sigma(u)$  for  $\sigma \in H$ . Call them  $u_1, \dots, u_t$ , and let

$$f = (x - u_1) \dots (x - u_t)$$

$$|H| \geq t$$

Since  $f(u) = 0$ , we have  $p | f$  because the minimal polynomial

of  $u$  divides any polynomial which has  $u$  as a root.

Thus  $\deg p \leq \deg f$

We have so far

$$\underline{\underline{|H|}} \geq t = \deg f \geq \deg p = h = [K:E] - \text{the opposite inequality}$$

Thus  $|H| = n = \text{Gal}_E K = [K:E]$ .

From  $H \subseteq \text{Gal}_E$  and  $|H| = \text{Gal}_E K$   
we conclude that  $H = \text{Gal}_E$ .