

# Math 5055

Recall:  $K$  is algebraically closed if  $\forall f \in K[x]$  has a root in  $K$ .

If  $F \subset K$  algebraic extension, and if  $\forall f \in F[x]$  has a root in  $K$ , then  $K$  is algebraically closed.

In this case,  $K$  is called an algebraic closure of  $F$ .

Thm (Assuming axiom of choice) Every field has an alg closure.

And it's unique up to iso — a version of uniqueness of splitting fields.

Pf (Artin): Consider the (massively) infinite polynomial ring

$$F[\dots, x_f, \dots]$$

where there is a generator  $x_f$  for every  $f \in F[x]$ .

Let's look at the ideal  $I \subset \mathbb{F}[\dots x_p \dots] = \mathbb{R}$

generated by all of the  $f(x_p)$

for each  $f \in \mathbb{F}[x]$ .  $I = (\dots f(x_p) \dots)_{f \in \mathbb{F}[x]}$ .

$I \neq (0)$

Is  $I = (1)$ ? Or is  $I \subsetneq \mathbb{R}$ ?

rule out

rule out.

Suppose  $I = (1)$ .

i.e.  $\exists$  finite set

$g_1(x_{f_1}^{\text{other}}) \dots g_r(x_{f_r}^{\text{other}})$

$f_1(x_{f_1}), \dots, f_r(x_{f_r})$

s.t.  $1 = \sum_{i=1}^r g_i(x_{f_1}, \dots, x_{f_r}) \cdot f_i(x_{f_i})$

i.e.: If  $I = (1)$ , then it would be true for  
some finitely many polys.

$$I \subset \mathbb{F}[x_1, \dots, x_p] = \mathbb{R} \cup \mathbb{F}[x_1, \dots, x_r] = \mathbb{R}'$$

(just finitely many).

Choose an extension  $\mathbb{F} \subset \mathbb{E}$  in which these finitely  
many polys have roots.

Choose those roots. Then  $\mathbb{R}' \rightarrow \mathbb{E}$   
 $x_i \mapsto$  choice of root.

$$I' \subseteq \ker(\mathbb{R}' \rightarrow \mathbb{E}).$$

This map is nonzero, so  
 $1 \notin I'$ . So  $1 \notin I$ .

So  $I \neq (1) \subset \mathbb{R}$ .

$\exists$  maximal ideal  $\mathfrak{m} \subset \mathbb{R}$ .

So, using choice:  $I \subset \mathfrak{m} \subset \mathbb{R}$

So look at  $\frac{\mathbb{R}}{\mathfrak{m}}$  same field.

In this field,  $[x_f] \in \frac{\mathbb{R}}{\mathfrak{m}}$  will solve  $f(x_f) = 0$ .

because  $I \subseteq \mathfrak{m}$ .

$\mathbb{F} \subset \frac{\mathbb{R}}{\mathfrak{m}}$

$\mathbb{K} :=$  all elts of  $\frac{\mathbb{R}}{\mathfrak{m}}$  algebraic over  $\mathbb{F}$ .

$\square$ .

Idea of the pf:

$R/I$  is the UFD freely built  
by adding a new root for every poly

e.s.:

$$\mathbb{F} = \mathbb{R}, \quad R/I \cong \mathbb{R}[x]/x^2=1.$$

→ either  $R/I = 0$ . [Some inconsistency between  
freey adding roots] ~~+~~

or  $R/I$  has a field among its quotients. ✓

$f \in \mathbb{F}[x]$  is separable if it has no repeated roots in its splitting field.

E.g.  $x^2 + 1$  is sep'd over  $\mathbb{F} = \mathbb{R}$ .

$x^2$  is not.

Given  $f(x)$ , let's look in a splitting field  $\mathbb{F} \subset \mathbb{E}$

factor  $f|_{\mathbb{F}} = \prod (x - a_i)^{d_i}$  in  $\mathbb{E}[x]$

all the  $a_i$ 's are distinct,  $d_i$  handles repeated roots.

$$df = \frac{df(x)}{dx}$$

$$d(x^n) = nx^{n-1} \text{ extend linearly.}$$

Algebraic fact:  $d(f \cdot g)$

$$= df \cdot g + f \cdot dg.$$

working in  $\mathbb{E}$ , if  $f = \prod_{i=1}^k (x-a_i)^{d_i}$

$$df = \sum_{i=1}^k \left( \prod_{j \neq i} (x-a_j)^{d_j} \right) \cdot d_i \cdot (x-a_i)^{d_i-1}$$

$\Rightarrow$  iff  $f$  has a repeated root, e.s.  $d_i \geq 2$  for some  $i$ ,

then  $f$  and  $df$  have a common factor  $(x-a_i)$

In other words:  
 $f$  is separable iff  $\gcd(f, df) = 1$ .

Euclid algorithm:  $\gcd(f, df)$  is calculable without leaving  $\mathbb{F}$ .

E.S.: Suppose  $f(x) \in \mathbb{F}[x]$  is primitive  
over  $\mathbb{F}$ .

Look at:

$$\gcd(f, df')$$

$$\deg(df') < \deg(f)$$

Find: If  $f$  is primitive, then

either

-  $f$  is separable

or

$$df' = 0.$$

$\hookrightarrow$  possible in positive char.

$$f(x) = x^n + \text{lower order.}$$

looks like

$$df' = nx^{n-1} + \dots$$

$$\neq 0.$$



Let  $\mathbb{F} \subset \mathbb{E}$  be a field extension.

The Galois group of this extension is

$$\text{Gal}(\mathbb{E}/\mathbb{F}) := \left\{ \begin{array}{l} \text{field autom. } \varphi: \mathbb{E} \rightarrow \mathbb{E} \\ \text{s.t. } \varphi|_{\mathbb{F}} = \text{id.} \end{array} \right\}.$$

Last time:  $\text{Gal}(\mathbb{R}/\mathbb{Q}) = \text{triv.}$       $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$   
 $\neq (\mathbb{Z}/2)^2.$

Splitting fields have larger Galois groups than non-splitting fields.  
of sep<sup>d</sup> polys

Given  $\mathbb{F} \subset \mathbb{E}$  and given  $G < \text{Gal}(\mathbb{E}/\mathbb{F})$

can look at the fixed subfield  $\mathbb{E}^G := \{ e \in \mathbb{E} \text{ s.t. } \underset{\cup, \mathbb{F}}{g}e = e \forall g \in G \}$ .

subgps of  
 $\text{Gal}(\mathbb{E}/\mathbb{F})$



sub extensions

$\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$

$G$



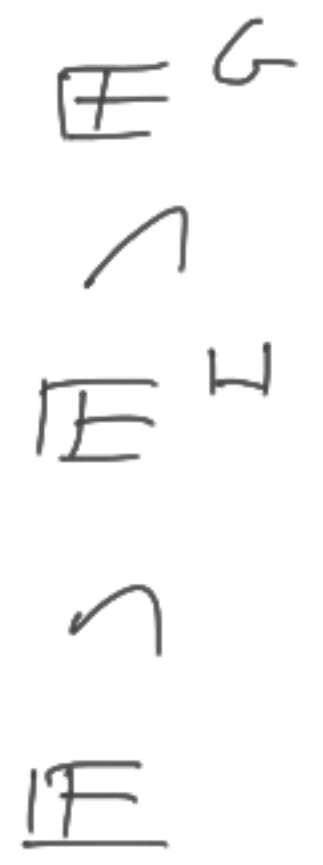
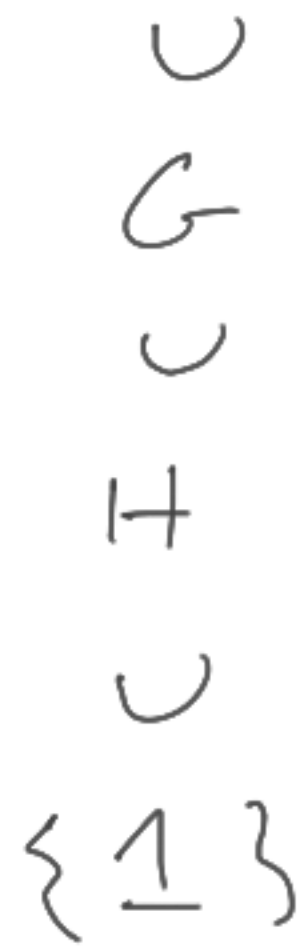
$\mathbb{E}^G$

$\text{Gal}(\mathbb{E}/\mathbb{K})$



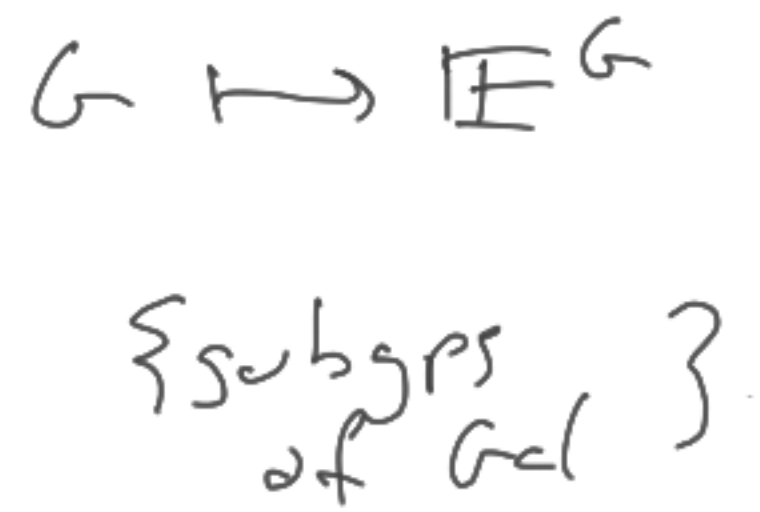
$\mathbb{K}$

$\text{Gal}(\mathbb{E}/\mathbb{F})$

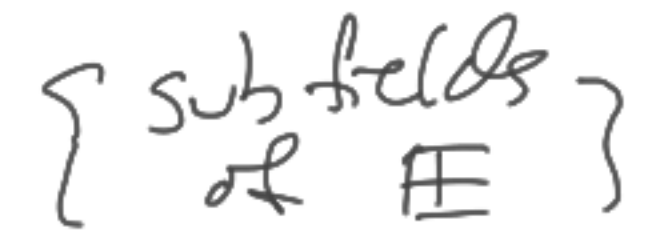


fixed for all of  $G$   
 fixed just by  $H$ .

In other words,  
 of posets



is an antimap <sup>contravariant map.</sup>



$\text{Gal}(\mathbb{E}/\mathbb{F})$

$\cup$

$\text{Gal}(\mathbb{E}/\mathbb{K})$

= autos of  $\mathbb{E}$   
that fix  $\mathbb{K}$ .

$\cup$

autos of  $\mathbb{E}$   
that fix  $\mathbb{L}$

$\{1\}$

So we have contravariant



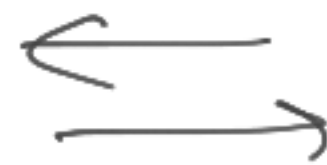
$\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$   
 $\mathbb{E} \supset \mathbb{L}$

...

if  $\text{Gal}(\mathbb{E}/\mathbb{F})$   
is "large"  
(e.g.  $\mathbb{E}$  is a splitting  
field of a set  
of sep'l polys)

then this will  
be an epimorphism  
contravariant.

$\{ \text{subgps of } \text{Gal}(\mathbb{E}/\mathbb{F}) \}$



$\{ \text{sub extensions of } \mathbb{F} \subset \mathbb{E} \}$