

Galois Correspondence.

Given $F \subset K$ satisfying ...

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

Inter. Subfields



Subgroups of G

K

$|$

L

$|$

F

} degree



$$\text{Aut}(K/L) \subset G$$

index.

Taking $L=K$ gives

$\deg(K/F) = |G|.$

||
 $\deg(L/F)$

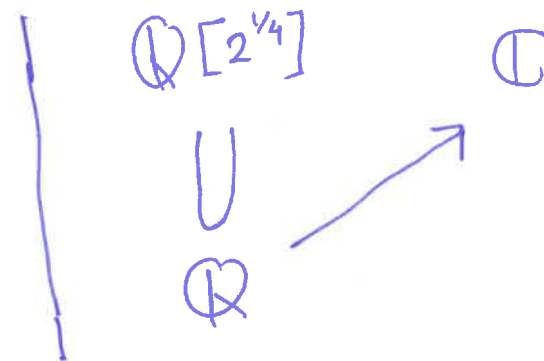
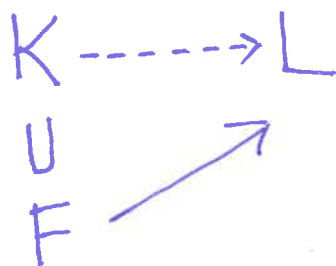
Today + tomorrow
Counting symmetries.

Counting

Setup:

$F \subset K$ any finite extension

L any field, $F \rightarrow L$ ring hom.



Q: How many $\xrightarrow{\quad}$ can there be?

Rules: Ring hom — ①
diagram commutes — ②

Example:

$$K = \mathbb{Q}[2^{1/4}] \dashrightarrow \mathbb{C}$$

\cup

$$F = \mathbb{Q}[\sqrt{2}]$$

$$\nearrow \sqrt{2} \mapsto \sqrt{2}$$

Write a presentation
of K over F

$$K \cong F[x] / (x^2 - \sqrt{2}) \dashrightarrow \mathbb{C}$$

$x \mapsto 2^{1/4}, -2^{1/4}$

$2^{1/4} \leftrightarrow x$

\cup
 F

\Rightarrow 2 dotted
arrows!
 \checkmark

Replace \mathbb{C} by $\mathbb{Q}[\sqrt{2}] \Rightarrow 0$ dotted maps.

\dashrightarrow = Roots of $(x^2 - \sqrt{2})$ in the target
field L .

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] \dashrightarrow \mathbb{C}$$



\mathbb{Q}

2 dotted arrows.

sols of (x^2-2) in \mathbb{C} .

For every intermediate \dashrightarrow , get two top \dashrightarrow .

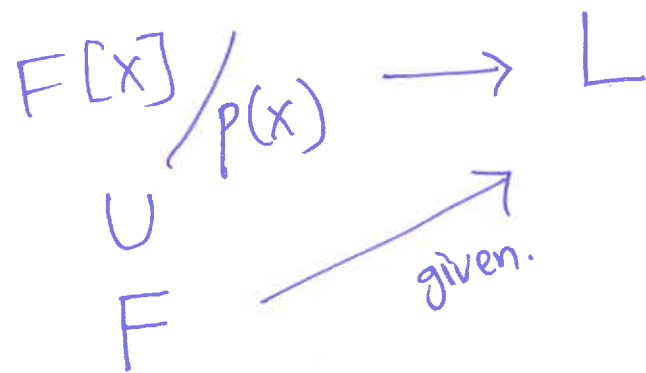
So total 4 \dashrightarrow = deg ext $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Prop: $\begin{array}{ccc} K & \xrightarrow{\quad} & L \\ U & & \\ F & \nearrow & \end{array}$ $\left\{ \begin{array}{l} \text{Given. } F \subset K \text{ ext}^n \text{ of deg } n. \\ \Rightarrow F \rightarrow L. \end{array} \right.$

Then $\#$ Ring homs $K \rightarrow L$ making the diagram commute is at most n .

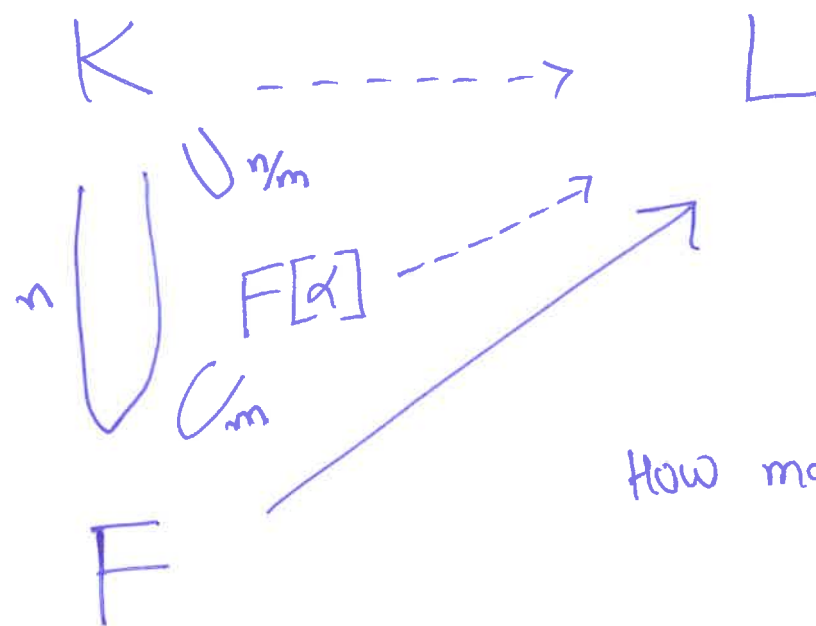
pf: Case 1: Suppose $K \cong F[x]/p(x)$
Then $\deg p(x) = n$.

Want.



$x \mapsto \alpha$
 $\Rightarrow \alpha$ is a root
of $p(x)$ in L .
 \Rightarrow at most n
choices.

In general, induct on $n. = \deg(K/F)$



choose $\alpha \in K$
 $\alpha \notin F$.

$$m = \deg(\alpha/F).$$

How many intermediate \dashrightarrow ?
At most m .

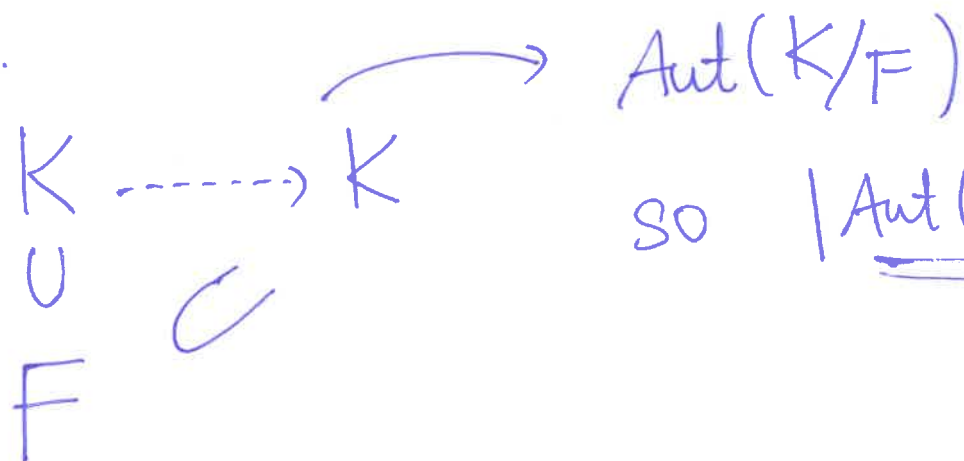
For every intermediate \dashrightarrow ,
how many top \dashrightarrow ?

At most n/m
 \hookrightarrow (ind. hyp.)

\Rightarrow At most $m \cdot \left(\frac{n}{m}\right)$ top \dashrightarrow .

□

Example:



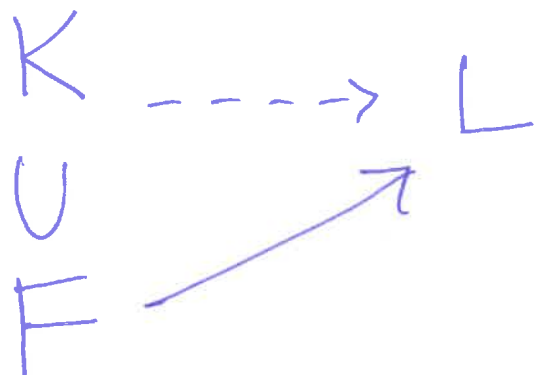
$$\text{so } |\underline{\text{Aut}(K/F)}| \leq \deg(K/F).$$

\downarrow
4

Can be strict

$$F = \mathbb{Q}$$

$$K = \mathbb{Q}[2^{1/4}] \cong \mathbb{Q}[x]/(x^4 - 2)$$



$$\begin{aligned}
 \text{No. of } & \dashrightarrow \\
 & \leq \deg(K/F).
 \end{aligned}$$

Q: When can equality hold?

↳ L needs to be big enough to have sol^n to poly. we are solving.

L -Poly we are solving must not have repeated roots.

