# Math 5055

Reminders:
- HW1 on course website, due monday
- OH tomorrow rather than today
- In person instruction begins 31 January (Monday week)

---

We are well on our way to proving Fund. Thm of Gal Thy.

Left to prove: If given $F \subset K \subset E$ with $F \subset E$ Galois, then $F \subset K$ is Galois iff $Gal(E/K) \subset Gal(E/F)$ is normal, in which case $Gal(K/F) \cong$ quotient gp.

We'll get this from a characterization of Galois extensions.

Recall: An algebraic extension $F \subset E$ is splitting

if any irred poly over $F$ which admits a root in $E$ in fact splits completely over $E$.

$F \subset E$ is separable if whenever an irred poly over $F$ admits a root in $E$, then that poly is separable — its roots in $E$ are distinct.

Thm: $F \subset E$ algebraic is Galois iff it is splitting and separable.

Pf alg + Galois $\Rightarrow$ splitting + sep.

Suppose $\mathbb{F} \subset \mathbb{E}$ Galois and pick $u \in \mathbb{E}$, and $p(x) \in \mathbb{F}[x]$ is its minimal poly.

Let $u_1, \ldots, u_r$ be the roots of $p$ which live in $\mathbb{E}$. (distinct!)

Want to show: $p(x) = (x-u_1)(x-u_2)\cdots(x-u_r)$ in $\mathbb{E}[x]$

$q(x)$.

Certainly $q(x)$ divides $p(x)$ over $\mathbb{E}$.

$Gal(\mathbb{E}/\mathbb{F})$ acts as permutations of $\{u_1, \ldots, u_r\}$

i.e. if $\tau \in Gal(\mathbb{E}/\mathbb{F})$ then $\tau \cdot u_i$ will be a root of $\tau \cdot p(x) = p(x)$ p was over $\mathbb{F}$.

$\Rightarrow$ $Gal(\mathbb{E}/\mathbb{F})$ fixes $q(x) = \prod_{i=1}^{r} (x - u_i)$.

So it fixes all the coefs, and since assumed $\mathbb{F} \subset \mathbb{E}$ was Galois, we find $q(x) \in \mathbb{F}[x]$.

Euclid: If $g(x)$ divides $p(x)$ in $\mathbb{E}[x]$, then it does so also in $\mathbb{F}[x]$.

But we assumed $p$ irred and

so $g = p$. $\square$.

---

Pf of Fundamental Thm of Galois Thy.

Let $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ with $\mathbb{F} \subset \mathbb{E}$ alg + Galois.

(in a moment it will be finite).

Recall: $\mathbb{K}$ is stable if

$Gal(\mathbb{E}/\mathbb{F})$ fixes $\mathbb{K}$ as a set.

Then we get a restriction map

$$Gal(\mathbb{E}/\mathbb{F}) \xrightarrow{res|_{\mathbb{K}}} Gal(\mathbb{K}/\mathbb{F})$$

From defn unpacking, $\ker(res|_{\mathbb{K}}) = Gal(\mathbb{E}/\mathbb{K})$.

To win: need: (a) $\mathbb{K}$ stable iff $\mathbb{F} \subset \mathbb{K}$ Galois,
(b) $res|_{\mathbb{K}}$ is surjective.

Pf (a) $\Leftarrow$: If $\mathbb{F} \subset \mathbb{K}$ is Galois, then it's splitting (and sep) so pick up any $u \in \mathbb{K}$, any $\tau \in Gal(\mathbb{E}/\mathbb{F})$.

then $\tau \cdot u$ solves same min poly as $u$.
So since $K$ splitting, $\tau \cdot u \in K$.

(a) $\Rightarrow$. Trivial since we assumed $F \subset E$ Galois.

---

All we need to do is prove surjectivity of $\text{res}|_K$.

$$\text{Gal}(E/F) \longrightarrow \text{Gal}(K/F).$$

In the case where $F \subset E$ is finite,

$F \subset K \subset E$ all Galois.

$$\#\,Gal\left(\frac{E}{K}\right) = [E:K]$$

$$\#\,Gal\left(\frac{E}{F}\right) = [E:F]$$

$$\#\,Gal\left(\frac{K}{F}\right) = [K:F]$$

So

$$\#\,Gal\left(\frac{K}{F}\right) = \frac{\#\,Gal(E/F)}{\#\,Gal(E/K)}.$$

$[E:F] = [E:K][K:F]$

but $\dfrac{Gal(E/F)}{Gal(E/K)} \hookrightarrow Gal(K/F)$

In general: Given $F \subset K \subset E$ all galois.

WTS: any $\tau : K \xrightarrow{\sim} K$ extends to $E$.

But $E$ is splitting over $K$ (because it's galois).

We already saw that isomorphisms extend to splitting fields. (more precisely we did this when $K \subset E$ is the splitting field of a single poly, which is to say it's splitting and finite. If it's infinite,

$\mathbb{K} \subset \mathbb{E}_1 \subset \mathbb{E}_2 \subset \mathbb{E}_3 \subset \ldots \subset \mathbb{E} = \bigcup_{k=1}^{\infty} \mathbb{E}_k$

each subextension finite and splitting,

$\tau \rightsquigarrow \tau_1 \rightsquigarrow \tau_2 \rightsquigarrow \tau_3 \rightsquigarrow \ldots$

define

$\tau_\infty : \mathbb{E} \to \mathbb{E}$

by:

if $u \in \mathbb{E}$, then $u \in$ some $\mathbb{E}_k$,

and so define $\tau_\infty \cdot u = \tau_k \cdot u$.

So far: Given any $F \subset E$, Galois connection

subextensions of $F \subset E$ $\rightleftarrows$ closed subgps of $Gal(E/F)$.

If $F \subset E$ is Galois and algebraic, then

 $= id$.

If $F \subset E$ is moreover finite, then

 $= : d$

otherwise, restrict attention to closed subgps.

set the feeling that

$F \subset K$ "looks like" $\frac{Gal(E/F)}{Gal(E/K)}$.

So far: If $F \subset E$ Galois and algebraic, then splitting and sep.

Last to show: If $F \subset E$ alg, splitting, + sep, then Galois.

In other words, WTS: if $u \in E \setminus F$, then $\exists\ \tau \in Gal(E/F)$ s.t. $\tau \cdot u \neq u$.

By assumption, $u$ alg, let $p(x) \in F[x]$ its min poly. Observe: since $u \notin F$, $\deg(p) > 1$.

Since $E$ is splitting, $p$ must split over $E$.

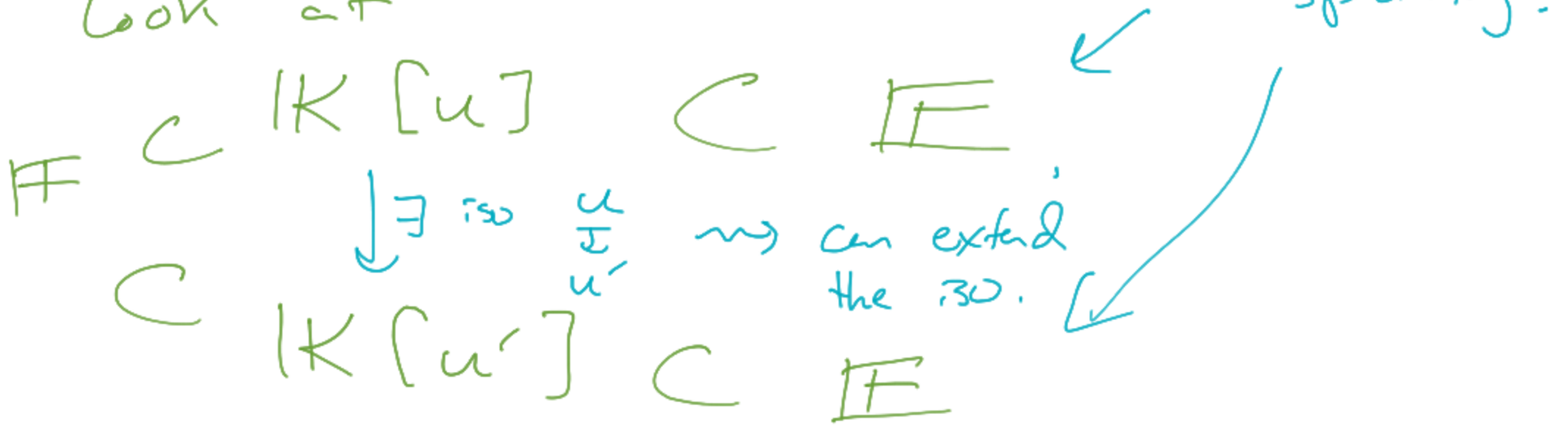
Since $\mathbb{E}$ separable, the roots of $p$ are all different.

In particular, $\exists\ u' \in \mathbb{E}$ also solving $p$.

$\neq$

$u$

So look at




So we just built an iso $\tau : \mathbb{E} \to \mathbb{E}$ s.t. $\tau|_{\mathbb{F}} = id$ but $\tau \cdot u = u'$. $\square$.