Jan 5

**Fields** commutative unital ring $K$ st $K - \{0\}$ group

$\mathrm{Hom}(K, L) = \{$ ring maps $K \to L\}$
$\mathrm{Aut}(K)$ = group of automorphisms, typically non-commut

**Basic Facts**

- If $f : K \to L$ homo of fields, then $f$ injective
  We call $f$ an extension
- If $K$ is a field and $V$ a $K$-module, $V \cong K^n$ for some $n$. ($n$ possibly $\infty$, uniquely determined by $V$)
  $\dim_K(V) = n$.

**Corollary**
If $K \hookrightarrow L$ extension, then $L$ is a $K$-module and has dimension. $\dim_K(L) = [L : K]$ index of extension

Suppose $K \hookrightarrow L$ an extension, an element $u \in L$ is algebraic over $K$ if $\exists f(x) \in K(x)$ such that $f(u) = 0$ ($\neq 0$)
transcendental if not algebraic

Choice of $u \in L$ uniquely determines a ring map $K(x) \to L$ such that $x \mapsto u$ and extends $f : K \to L$

$\ker(K(x) \to L) = I$
ideal in $K(x)$
$u$ is algebraic iff this ideal $\neq 0$

We know $K(x)$ is a PID
If $u$ is algebraic, then $I = p(x)$ for some unique $p(x) \in K(x)$ monic.
This $p(x)$ is called the minimal polynomial of $u$.
$\deg(p(x)) = \deg(u) \in \mathbb{N}$

Example $\mathbb{Q} \subset \mathbb{R}$

2 is alg over $\mathbb{Q}$, minimal polynomial $x - 2$

$\sqrt{2}$ is alg over $\mathbb{Q}$, minimal polynomial $x^2 - 2$

## Jan 7

Given $F \subset E$, $\alpha \in E$ is algebraic if ring homo $F(x) \longrightarrow E$ has non-trivial kernel. $x \longmapsto \alpha$

$F(x) \longrightarrow F(\alpha) \subset E$
$x \longmapsto \alpha$

} Image is minimal subfield of $E$ containing $F$ and $\alpha$.

$[F(x) : F] = \dim_F F(\alpha)$
$\infty < "\deg(p(x))$ where $p = \ker(x \longmapsto \alpha)$
$= \deg(\alpha)$

If $[E : F] < \infty$ then every element of $E$ is algebraic.

If $\alpha \in E$ not algebraic, then transcendental.

$F(x) \hookrightarrow F(\alpha) \subsetneq E$
↑ not a field

Example $\mathbb{Q}(\pi) \subset \mathbb{R}$ not a field, just a ring

If $\alpha$ is algebraic, $F(\alpha)$ is a field

Define $F(\alpha) :=$ minimal subfield of $E$ containing $F$ and $\alpha$

Remark Why should "smallest subfield with some property" exist?
Look at all subfields of $E$ with that property
Clearly non-empty set of subfields of $E$ (contains $E$)
$\cap$ of fields is a field so $\cap$ of subfields is a subfield
For "smallest" to exist, suffices for property to be preserved

by intersections.

**How does $F(\alpha)$ look ?**

- If $\alpha$ alg $\longrightarrow$ $F(\alpha) = F(x)$
- If $\alpha$ transcendental $\longrightarrow$ $\frac{f(\alpha)}{g(\alpha)} \in E$ for some $g(\alpha) \neq 0$

(since $\alpha$ not a solution of poly)

$F(\alpha) \cong F(x) = \{ \frac{f}{g} , f, g \in F(x) \}$ (ring of rational fcts)

$F(\alpha)$ is really big.

Given extension $K \subset L$, $u \in L$ algebraic

$\mathrm{Im}(K(x) \longrightarrow L) \subseteq L$

- Integral Domain
- $\cong K(x)/p(x)$ , $p$ minimal poly of $u$

So, $p(x)$ prime (irreducible) and maximal $\longrightarrow$ field

$$\mathrm{Im}(K(x) \longrightarrow L) = K(u)$$
$$x \longmapsto u$$

$K \subset K(u) \subset L$

$[K(u) : K] = \deg(p) = \deg(u) < \infty$

**Lemma** $K \subset L$ extension of index $n < \infty$
If $u \in L$, then $u$ is algebraic of degree $\leq n$.
We have equality iff $u$ generates $L$ over $K$.

*proof* Look at the set $1, u, u^2, \dots, u^n$
Set has size $n+1$ $\longrightarrow$ to big to be a basis of $L$ as a $K$-vectorspace.
So, $\exists a_0, \dots, a_n \in K$ not all 0 such that
$a_0 1 + a_1 u + a_2 u^2 + \dots + a_n u^n = 0$.

Extension is algebraic if every element of codomain is algebraic over $K$.

**Corollary** $K \subset L$ is algebraic iff $L$ is ind-finite
i.e. $L$ is a union of finite dimensional extensions.

**Corollary** $K \subset E$ and $E \subset F$ are algebraic extensions
$\longrightarrow$ $K \subset F$ is algebraic.

**proof** Let $[E:K] = m$, $[F:E] = n$ $\quad m, n < \infty$
$F \cong E^n$ as vectorspaces over $E$
$E \cong K^m$ as vectorspaces over $K$
$\longrightarrow$ $F \cong (K^m)^n = K^{mn}$ as $K$-modules

**Example** $\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha} \in \underbrace{\mathbb{Q}(\sqrt{2},\sqrt{3})}_{\deg 4} \supseteq \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \supseteq \mathbb{Q}(\sqrt{3}) \supset \mathbb{Q}$
$1, \alpha, \alpha^2, \alpha^3, \alpha^4$ must be dependant
$1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}, 49+20\sqrt{6}$
find $\alpha^4 - 10\alpha^2 + 1 = 0 = f(\alpha)$

Then $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supseteq \mathbb{Q}(\alpha)$ but same degree
$\longrightarrow$ $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$

Since $\deg(f) = 4$, $f \leq 4$ roots.
Does $f$ factor completely in $\mathbb{Q}(\alpha)$? (splits)
Yes $\longrightarrow$ roots are $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $\sqrt{3}-\sqrt{2}$, $-(\sqrt{2}+\sqrt{3})$

**Definition** $F \subset E$ is a splitting field for $f(x) \in F(x)$ if $f$ splits in $E$ and not in any proper sub-extension

$\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$
↳ solves $x^3 - 2 = 0$ only one real solution
So $\mathbb{R}$ is not a splitting field for $x^3 = 2$

Let's work out a basis for $\mathbb{C}(x)$ as a $\mathbb{C}$-vectorspace.

Method of Partial Fractions

$\forall f(x), g(x) \in \mathbb{C}(x)$, where $g(x) = \prod_{i=1}^{n} (x - a_i)^{b_i}$

$g(x) \neq 0$

$$\frac{f(x)}{g(x)} = b(x) + \frac{c_{11}}{(x-a_1)^1} + \frac{c_{12}}{(x-a_2)^2} + \dots + \frac{c_{nd}}{(x-a_n)^d}$$

$$= b_0 + b_1 x + \dots + b_K x^K$$

$\mathbb{C}(x)$ has basis

$1, x, x^2, \dots$

$1/x, 1/x^2, 1/x^3, \dots$

$1/(x-1), 1/(x-1)^2, \dots$

$1/(x-\alpha), 1/(x-\alpha)^2, \dots \quad \forall \alpha \in \mathbb{C}$

So, $\dim_{\mathbb{C}} \mathbb{C}(x) = [\mathbb{C}(x) : \mathbb{C}] = {}^{\#}\mathbb{C} \cdot {}^{\#}\mathbb{N} >> {}^{\#}\mathbb{N}$

A finitely generated extension $F \subset E$ is algebraic iff finite.

$E = F(\alpha_1, \dots, \alpha_n) \quad n < \infty$

Pick $\alpha, \beta \in E$ both algebraic

$F(\alpha, \beta)$ = smallest subfield of $E$ containing $F, \alpha, \beta$

$F(\alpha) \subset F(\alpha, \beta)$ so $F(\alpha, \beta) = F(\alpha)(\beta)$

$\beta$ solves a poly in $F(x)$ so it solves a poly in $F(\alpha)(x)$

$\longrightarrow [F(\alpha, \beta) : F(\alpha)] \leq [F(\beta) : F] < \infty$

So, if $\alpha_1, \dots, \alpha_n$ all algebraic, then $F \subset F(\alpha_1, \dots, \alpha_n)$ is finite.

Corollary If $\alpha, \beta \neq 0$ both algebraic, then

- $\alpha + \beta$
- $\alpha - \beta$
- $\alpha\beta$
- $\alpha / \beta$

} all algebraic

$\longrightarrow \overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$

# Jan 10

$F = \mathbb{Q} \subset \mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha}) = E$

minimal polynomial of $\alpha$ is $f(x) = x^4 - 10x^2 + 1$
$E$ contains all roots of $f$

$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) \qquad \alpha_{1,2,3,4} = \{\pm\sqrt{2} \pm \sqrt{3}\}$
$\longrightarrow$ $f$ splits in $E$

$\nexists\, F' \subsetneq E$ such that $f$ splits in $F'$, so $E$ is a splitting field of $f$
$F''$

$= E$

**Example** $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) / \underbrace{(\alpha^3 - 10\alpha^2 - 1)}_{\text{only one real root}} \hookrightarrow \mathbb{R}$

$f$ does not split in $E$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, -\frac{1}{2} + \frac{\sqrt{3}}{2})$
roots of $x^3 - 2$ : $\sqrt[3]{2}$, $\sqrt[3]{2}\, e^{\frac{2\pi i}{3}}$, $\sqrt[3]{2}\, e^{\frac{-2\pi i}{3}}$

**Proposition** Splitting fields exist.
i.e. given $f \in F(x)$, $\exists\, E \supset F$ such that $f$ splits in $E$.
And if $\deg(f) = n$, $[E : F] = n!$

**proof**
1) if $f$ splits in $F$, done
2) else, choose $p(x)$ dividing $f$ primitive
look at $F \subset F_1 = F_0(\alpha) / p(\alpha)$
In $F_1$, $f(x) = (x-\alpha) f_1(x) \qquad \deg(f_1) < \deg(f_0)$
By induction on $\deg(f)$, $\exists F_1 \subset E$ splitting $f$.

**Theorem** Given $\varphi : F \xrightarrow{\sim} F'$ and $f(x) \in F(x)$.
Set $f' = \varphi(f)$ and splitting fields $F \overset{f}{\subset} E$ and $F' \overset{f'}{\subset} E'$

Then $\varphi$ extends into $\overline{\varphi} : E \xrightarrow{\sim} E'$

*proof*

1) if $f$ splits in $F : E = F$ and $f'$ splits in $F'$ so $E' = F'$
factor $f$ and apply $\varphi$ to factors

2) Choose $\alpha \in E$, root of $f$ not in $F$

$F \subset F(\alpha) \subset E$ | Let $p(x)$ be the minimal polynomial for $\alpha$

$\cong$ | $p(x) \mid f(x)$

$F(x)/p(x)$ | $p' = \varphi(p)$ $\quad p'(x) \mid f'(x)$

Then $E'$ splits $p'$ so take $\alpha' \in E'$ root of $p'$

$F' \subset F'(\alpha') \cong F'(x)/p'(x) \subset E$

$F(x)/p(x) \longrightarrow F'(x)/p'(x)$

$$[E : F(\alpha)] = \frac{[E : F]}{[F : F(\alpha)]} < [E : F] \qquad [F : F(\alpha)] > 1$$

By induction on deg $[E : F] < \infty$

$F(\alpha) \xrightarrow{\sim} F'(\alpha')$ extends to $E \xrightarrow{\sim} E'$

*Corollary* Splitting fields are unique up to iso

*proof* if $F \subset E$, $F \subset E'$ are two splitting fields for $f$,
then $id : F \xrightarrow{\sim} F$ extends to $E \xrightarrow{\sim} E'$

Jan 12

$K$ is <u>algebraically closed</u> if $\forall f \in K[x]$ has a root in $K$.

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

$\rightarrow$ $K$ called algebraic closure of $F$

Thm $\forall$ field has an algebraic closure

unique up to isomorphism

proof Consider the infinite polynomial ring

$F[\ldots, x_f, \ldots]$

where there is a generator $x_f$ $\forall f \in F[x]$

Let's look at ideal $I \subset F[\ldots, x_f, \ldots]$ generated by all of the $f(x_f)$ $\forall f \in F[x]$

$I = (\ldots f(x_f) \ldots)$

$I \neq (0)$

Is $I = (1)$? Or is $I \subseteq R$?

Suppose $I = (1)$. $\exists$ finite set of generators of $I$

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

and $g_1(x'_{f_1}) \cdots g_s(x'_{f_s})$ such that

$$1 = \sum_{i=1} g_i(x_f')$$

So, if $I = (1)$, then it would be true for finitely many polynomials.

$$\begin{array}{ccc} I \subset F[\ldots x_f \ldots] & = & R \\ \cup & & \cup \\ 1 \in I' = \text{finite} & & F[x_1, \ldots, x_r] = R^r \end{array}$$

Choose an extension $F \subset E$ in which the finite polys have roots

$\rightarrow$ choose roots

Thm $R' \longrightarrow E$
$xf \longmapsto$ choice of roots

$\rightsquigarrow$

So $I \neq (1)$
So, using choice : $I \subset M \subset R$

$\exists$ maximal ideal $M \subset R$

So, look at $R/M$ same field
In this field, $[xf] \in R/M$ will solve $f(xf) = 0$
because $I \subseteq M$

$F \subset K$ := all elts of $R/M$ algebraic over $F \subset R/M$

idea of proof
$R/I$ commutative ring freely built by adding a new root $\forall$ polynomial

$F = R \quad R/I = R(x$

Thm
$f \in F[x]$ is seperable iff it has no repeated roots in its splitting field

$x^2 + 1$ ✓
$x^2$ ×

Given $f$, let's look at splitting field $F \subset E$ and factor $f = \pi (x - a_i)^{d_i}$ in $E[x]$
all $a_i$'s distinct

$df = \dfrac{df(x)}{dx}$
$d(x^n) = nx^{n-1}$ extend linearly

$$d(f \cdot g) = df \cdot g + f \cdot dg$$

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

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

→ if $f$ has repeated root eg $d_i \geq 2$ for some $i$ then $f$ and $df$ have a common factor $(x - a_i)$

$f$ seperable iff $\gcd(f, df) = 1$

Euclidian Algorithm: $\gcd(f, df)$ calculable without leaving $F$

Example Suppose $f(x) \in F[x]$ is primitive over $F$
$\gcd(f, df)$

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

If $f$ is primitive then either
- $f$ is seperable
- $df$ is $0$
  possible in positive characteristic

Let $F \subset E$ be a field extension. The Galois Group of this extension $Gal(E/F) = \{$ field autos: $\varphi : E \to F$ st $\varphi_F = id \}$

Splitting fields have larger Galois gps than non-splitting fields.

Given $F \subset E$ and $G < Gal(E/F)$
Can look at fixed subfield $E^G = \{ e \in E \text{ st } ge = e \ \forall g \in G \}$

$E$
|
$F$

subgps of $\mathrm{Gal}(E/F)$ $\longrightarrow$ subextensions $F \subset K \subset E$

$\vee$

$G \longmapsto E^G$

$\mathrm{Gal}(E/K) \longleftarrow K$

$\mathrm{Gal}(E/F)$

$\cup$

$G \longrightarrow E^G$ fixed $\forall$ of $G$

$\cup$

$H \longrightarrow E^H$ fixed just for $H$

$\cup$

$\{1\} \longrightarrow E$

covariant map

In other words $G \longrightarrow E^G$ is an antimap of posets $\{\text{subgps of Gal}\} \longrightarrow \{\text{subfields of } E\}$

$\mathrm{Gal}(E/K) \longleftarrow K$

$\|$

autos of $E$ that fix $K$ $\quad \cap$

$\cup$

autos of $E$ that fix $L$ $\longleftarrow L$

$\cup \qquad \cap$

$\{1\} \longleftarrow E$

We have covariant maps

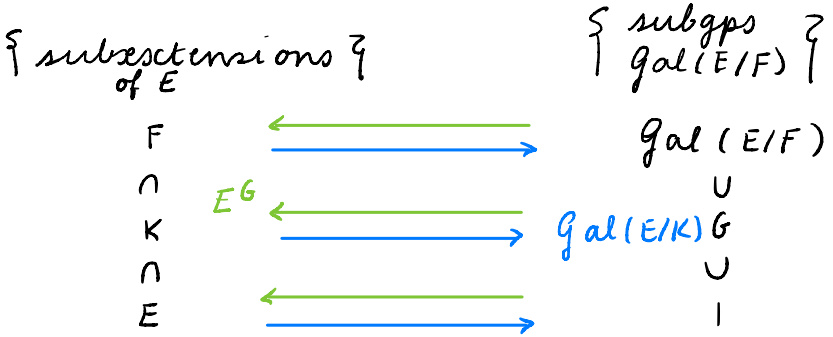
$\{\text{subgps } \mathrm{Gal}(E/F)\} \longrightarrow \{\text{subextensions of } F \subset E\}$

$\longleftarrow$

Jan 14

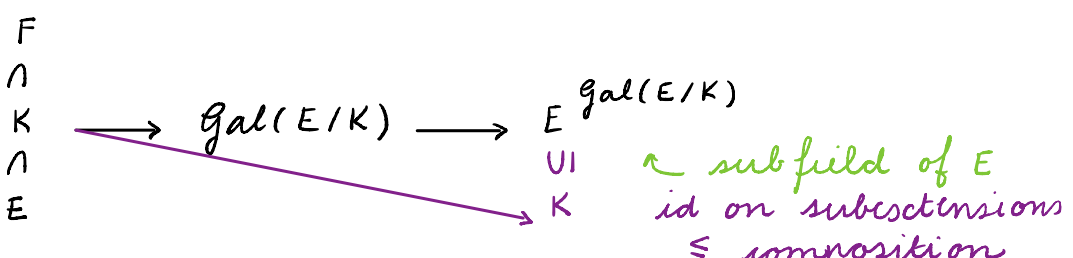
Given a field extension $F \hookrightarrow E$. Define $Gal(E/F) = \{\text{autos on } E, \text{ constant } F\}$

Then consider




Antimap: if $K \subseteq L$ then $Gal(E/L) \subseteq Gal(E/K)$
if $H \subseteq G$ then $E^G \subseteq E^H$

Start with




Maps of posets for posets. Posets are special types of categories.

map of poset ≡ functor

if $X, Y$ both posets, then

$maps(X,Y) := \{f : X \to Y \text{ st if } x_1 \leq x_2 \text{ then } f(x_1) \leq f(x_2)\}$

is again a poset where: $f_1 \leq f_2 \to f_1(x) \leq f_2(x)\ \forall x$

$$\begin{array}{ccccc} G & \longrightarrow & E^G & \longrightarrow & Gal(E/E^G) \\ \cap| & & & & \cup| \\ Gal(E/F) & & & & G \end{array}$$

Again, composition $\geq$ identity

**Def** Given two posets $X$ and $Y$, a <u>Galois Connection</u> between them is a pair of contravariant maps $f: X \rightleftarrows Y : g$ such that $id_Y \leq fg$ and $id_X \leq gf$

$$fgf = \underbrace{fg}_{\geq id_Y} \circ f \geq id_Y \circ f = f$$

$$f \circ \underbrace{gf}_{\geq id_X} \leq f \circ gf = f$$

$$fgf = f \qquad gfg = g$$

$$K \longrightarrow Gal(E/K) \longrightarrow E^{Gal(E/K)} \longrightarrow Gal(E/K)$$

$$= Gal(E/E^{Gal(E/K)})$$

Define $K \subseteq E$ is <u>Galois</u> if $K = E^{Gal(E/K)}$

$$\begin{array}{ccccccc} G & \longrightarrow & E^G & \longrightarrow & Gal(E/E^G) & \longrightarrow & E^{Gal(E/E^G)} \\ \cap| & & & & & & \\ Gal(E/F) & & & & & & \end{array}$$

**Prop** $\forall G \subseteq Gal(E/F)$, $E^G \subseteq E$ is <u>Galois</u>

# Remark about categories

Posets $\subseteq$ Categories $\leftarrow$ set of objects
given $x, y$ objects
there is a set ways for $x \leq y$
transitive: $x \leq y$, $y \leq z$
$\longrightarrow x \leq z$
"composition"

↑
set of
objects
notion of $\leq$
transitivity

---

Given categories $X, Y$, a <u>dual adjunction</u> is a pair of contravariant factors

$$f: X \leftrightarrows Y : g$$

and ways such that

$$id_Y \leq fg \qquad id_X \leq gf$$

such that the induced ways for $f \leq f$ and $g \leq g$ are the canonical "identity" ways

An adjunction is a pair of covariant factors
$id_Y \geq fg$ $id_X \leq gf$

$f$ = left adj $g$ = right adj
$g \vdash f$

<u>Remark</u>: Suppose $f: X \longrightarrow Y$ is a contravariant equivalence (of posets)

$\exists g: Y \longrightarrow X$ other contravariant map and isos
$fg = id_Y$ and $gf = id_X$

$\rightsquigarrow$ (contravariant) <u>equivalences</u> are examples of dual <u>adjunctions</u> <u>≡ galois correspondence</u>
≡ galois connection

$G = Gal(E/F)$

## Fundamental Theorem of Galois Theory

Suppose $F \subset E$ is finite and Galois.

1. Then, the Galois connection $\{\text{subexts of } E\} \leftrightarrows \{\text{subgroups of } Gal(E/F)\}$ is an equivalence. (anti) isomorphism of posets
In particular, every subext $K \subseteq E$ is Galois

2. $F \subset K$ is Galois iff $Gal(E/K) \subset Gal(E/F)$ is normal.
In which case, $Gal(K/F) =$ quotient group $Gal(E/F) \,/\, Gal(E/K)$

3. $|E:K| = \#\, Gal(E/K)$
$|K:F| = \#$ coset space $Gal(E/F) \,/\, Gal(E/K)$

Jan 17

Remark Given any Galois connection $f: X \leftrightarrows Y : g$ of posets, $x \in X$ is closed if $x = gf(x)$

$F \subset K \subset E \longrightarrow K$ is closed iff $K \subset E$ is Galois

$\{x \le gf(x),\ y \le fg(y)\ \forall x \in X, \forall y \in Y\}$

In the case of infinite Galois extensions $F \subset E$:
- every intermediate $K$ is indeed closed
- $Gal(E/F)$ has a natural topology and the closed subgps are the closed subgps

Lemma Suppose $F \subset E$ any field extension

| | | |
|---|---|---|
| $F$ | $Gal(E/F)$ | Then, $[Gal(E/K) : Gal(E/L)]$ |
| $\cap$ | $\cup$ | $\le [L:K] \in \mathbb{N} \cup \{\infty\}$ |
| $K$ | $Gal(E/K)$ | |
| $\cap$ | $\cup$ | |
| $L$ | $Gal(E/L)$ | $[Gal(E/K) : Gal(E/L)]$ |
| $\cap$ | $\cup$ | $= \dfrac{\#\, Gal(E/K)}{\#\, Gal(E/L)}$ |
| $E$ | $Gal(E/E) = \{1\}$ | |

## proof

Trivial: $[L:K] = \infty$ $\qquad$ $[L:K] = 1$

We induct on $n := [L:K]$

Pick $u \in L \setminus K$. Let $p(x) \in K[x]$ its minimal poly.
$k := \deg(u)$

Then $\overbrace{K \subset K[u] \subset L}^{n}$
$\underbrace{\qquad}_{k} \quad \underbrace{\qquad}_{n/k < n}$

If $n/k > 1$, then $n > k$ and true by induction.
Because if given $H \subset I \subset J$ inclusion of gps, then
$[J:H] = [J:I] : [I:H]$

Only case left to consider is $L = K[u]$

$$\frac{\#\,Gal(E/K)}{\#\,Gal(E/L)} \overset{\text{WTS}}{\leq} n = k$$

Given $\tau \in Gal(E/K)$ representing coset $[\tau]$.
Look at $\tau \circ u \in E$. Again solves $p(x)$.

If $[\tau] = [\tau']$ then $\tau = \tau' \circ \sigma$, $\sigma \in Gal(E/L)$

$\tau \cdot u = \tau' \circ \sigma \circ u = \tau' \circ u$
$\longrightarrow$ we built a map $\dfrac{Gal(E/K)}{Gal(E/L)} \longrightarrow$ roots of $p$ in $E$

Show that $[\tau] \longmapsto \tau \circ u$ is an injection.

If $\tau \cdot u = \tau' \circ u$ then $\tau^{-1}(\tau') \circ u = u$
so $\tau^{-1}\tau'$ acts trivially on $K[u] = L$
so $\tau^{-1}\tau' \in Gal(E/L)$ so $[\tau] = [\tau']$

**Lemma** For any $F \subset E$ with Galois group $G$

| | | |
|---|---|---|
| $E^G$ | $G$ | $[E^H : E^J] \leq [J : H]$ |
| $\cap$ | $\cup$ | |
| $E^J$ | $J$ | |
| $\cap$ | $\cup$ | |
| $E^H$ | $H$ | |
| $\cap$ | $\cup$ | |
| $E$ | $1$ | |

**Corollary** If $F \subset K \subset L \subset E$ and $K$ is closed and $K \subset L$ finite, then $L$ is closed.
If $\mathrm{Gal}(E/F) \supset J \supset H \supset 1$ and $H$ is closed and $H \subset J$ finite, then $J$ is closed.

*proof idea* $K \rightsquigarrow K$

$L \rightsquigarrow \geq L$ because Galois connection

$\leq L$ because lower index of $K \subset L$

---

Given $F \subset K \subset E$, $K$ is <u>stable</u> in $F \subset E$ if $\mathrm{Gal}(E/F)$ preserves $K$ as a set.
$\forall \tau \in \mathrm{Gal}(E/F), \tau(K) = K$

**Lemma** If $K$ is stable then $\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F)$ is normal.
. If $J \subset \mathrm{Gal}(E/F)$ is normal, then $F \subset E^J \subset E$ is stable

If $F \subset K \subset E$ and $F \subset E$ is Galois and $K$ stable then $F \subset K$ is Galois.

*Idea* If $K$ stable,
$\exists$ map $\mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(K/F)$
namely "restrict to $K$"

Jan 19

If given $F \subset K \subset E$ with $F \subset E$ Galois then $F \subset K$ Galois iff $\text{Gal}(E/K) \subset \text{Gal}(E/F)$ is normal
$\text{Gal}(K/F) =$ quotient group $\text{Gal}(E/F) \,/\, \text{Gal}(E/K)$

Recall an algebraic extension $F \subset E$ is splitting if any irreducible poly over $F$ with a root in $E$, splits completely in $E$.

$F \subset E$ is seperable if $\forall$ irreducible poly in $F$ with a root in $E$ is seperable (its roots in $E$ are distinct)

Thm $F \subset E$ algebraic is Galois iff splitting and seperable

proof
$\longrightarrow$ algebraic + Galois $\Rightarrow$ splitting and seperable

Let $F \subset E$ Galois and $u \in E$ and $p(x) \in F(x)$ minimal polynomial.
Let $u_1, \dots, u_r$ be distinct roots of $p$ in $E$.

WTS $p(x) = \underbrace{(x-u_1)(x-u_2)\dots(x-u_r)}_{q(x)}$ in $E(x)$

Certainly $q(x)$ divides $p(x)$ over $E$.

$\text{Gal}(E/F)$ acts as permutations of $\{u_1, \dots, u_r\}$.
i.e. if $\tau \in \text{Gal}(E/F)$ the $\tau \cdot u_i$ will be a root of $\tau \cdot p(x) = p(x)$

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

So it fixes all coefficients and since $F \subset E$ was Galois, $q(x) \in F(x)$

{ Euclid if $q(x)$ divides $p(x)$ in $E(x)$ then it does so in $F(x)$. }

But we assumed $p$ irreducible so $q = p$.

---

## Proof of Fundamental Theorem of Galois Theory

Let $F \subset K \subset E$ with $F \subset E$ Galois + algebraic

Recall $K$ is stable if $Gal(E/F)$ fixes $K$ as a set

Then, we get restriction map

$$Gal(E/F) \xrightarrow{res_K} Gal(K/F)$$

$\ker(res_K) = Gal(E/K)$

WTS . $K$ is stable iff $F \subset K$ Galois (a)
. $res_K$ is surjective (b)

(a)

$\leftarrow$ $F \subset K$ Galois then it is splitting and separable so any $u \in K$ and $\tau \in Gal(E/F)$.
Then $\tau . u$ solves same minimal poly as $u$. Since $K$ is splitting $\tau . u \in K$.

$\rightarrow$ Trivial since assumed $F \subset E$ Galois.

(b) $Gal(E/F) \xrightarrow{res_K} Gal(K/F)$

In the case $F \subset E$ finite:

$F \subset K \subset E$ all Galois $\rightarrow$ $\#\ Gal(E/K) = [E:K]$
$\#\ Gal(E/F) = [E:F]$
$\#\ Gal(K/F) = [K:F]$

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

So, $\#Gal(K/F) = \dfrac{\#\, Gal(E/F)}{\#\, Gal(E/K)}$

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

General Case

$F \subset K \subset E$ all Galois

WTS any $\tau : K \xrightarrow{\sim} K$ extends to $E$ but $E$ is splitting over $K$ (because its Galois)

But we know isos extend to splitting fields.

$K \subset E_1 \subset E_2 \subset E_3 \ldots \subset E = \bigcup_{K=1}^{\infty} E_K$

each $E_i$ finite splitting extension

$\tau \rightsquigarrow \tau_1 \rightsquigarrow \tau_2 \rightsquigarrow \ldots$ define $\tau_\infty : E \longrightarrow E$

by if $u \in E$ then $u \in$ some $E_K$ so $\tau_\infty \cdot u = \tau_K \cdot u$.

So Far Given any $F \subset E$, Galois connection

subexts of $F \subset E$ $\longrightarrow$ subgps of $Gal(E/F)$

$\longleftarrow$

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

 $= id$

If $F \subset E$ is also finite

 $= id$

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

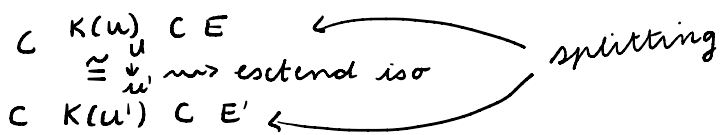
$\leftarrow$ If $F \subset E$ is algebraic, splitting and seperable then Galois.

WTS if $u \in E \setminus F$ then $\exists \tau \in Gal(E/F)$ st $\tau . u \neq u$.

$u \in E \setminus F$ so $u$ is algebraic, let $p(x) \in F(x)$ its minimal polynomial.

Observe since $u \notin F$, $deg(p) > 1$
Since $E$ is splitting, $p$ splits over $E$
Since $E$ is seperable, roots of $p$ are all different.
$\longrightarrow$ $\exists u' \in E$ also solving $p$
$\neq u$

So, look at




So, we built $\tau : E \longrightarrow E$ st $\tau|_F = id$ but $\tau . u = u'$.