$$\begin{tikzcd}
 & \text{inseparables} \arrow[dr, "G"] & \\
K \arrow[ur, "\text{trivial}"] \arrow[rr, "G"] \arrow[dr, "G"'] & & L \\
 & \text{separables} \arrow[ur, "\text{trivial}"'] &
\end{tikzcd}$$

Jan 28

Theorem

$F \subset K \subset E$

→ if $F \subset K$ and $K \subset E$ $\overbrace{\text{alg and Galois}}^{1)\ \text{splitting} \quad 2)\ \text{separable}}$ then $F \subset E$ need not be Galois

An algebraic extension $F \subset E$ is normal if for any $u \in E$, the minimal polynomial of u over E splits completely over E.

Suppose $E = F(u_1, \dots, u_n)$. The minimal polynomials of these u_i's split completely, the $\forall u \in E$, the minimal polynomial of u over E splits completely in E.

proof Let f minimal polynomial of u.
Look at $F \subset F(u) \subset E \subset E(\dots)$
(on the homework)

This part of a pattern where if $E = F(u_1, \dots, u_n)$ and all the u_i's have some property, often, all $u \in E$ have that property.

Example

- If all u_i's are purely inseparable over F then $\forall u \in E$ is.

u_i is purely inseparable iff $Fr^N(u_i) \in F$ for large N.

If all u_i's are purely inseperable over F, then
$Fr^N E \subseteq F \qquad N >> 0$

- If $E = F(u_1, \dots, u_n)$ and all u_i's are seperable then $\forall u \in E$ is seperable.

proof Let f minimal polynomial of u
Let $u \in E$
$F \subset F(u) \subset E \subset K$ = splitting field of u_i's
We proved that $F \subset K$ is finite and Galois by counting sizes of various Galois group.
And, every element of a Galois exctension is seperable.

Seperable $\longleftrightarrow$ sub of Galois

Let $F \subset E$ algebraic

purely insep

$F \subset E^{insep}$ = {purely inseperables} $\subset E$

seperable

$F \subset E^{sep}$ = {purely seperable} $\subset E$

both fields and stable (we have restriction maps)

$Gal(E/F) \nearrow Gal(E^{sep}/F)$

$Gal(E/F) \searrow Gal(E^{insep}/F)$

Because these subfields are stable we get a left-exact sequence:
$\forall$ stable $F \subset K \subset E$

$$1 \longrightarrow Gal(E/K) \longrightarrow Gal(E/F) \longrightarrow Gal(K/F)$$

Recall: A sequence of groups $1 \longrightarrow N \longrightarrow G \longrightarrow K$ is left-exact, if $N \longrightarrow G$ is injective and $Im\, N = Ker(G \longrightarrow K)$

$Gal(E^{insep}/F)$ is trivial so
$Gal(E/E^{insep}) \longrightarrow Gal(E/F)$ is isomorphic.
In particular $E^{Gal(E/F)} \supset E^{insep}$.
Also, if $F \subset E$ is Galois, no inseperables.

$$\begin{array}{ccccccc} & \subset & E^{insep} = \{\text{purely inseperables}\} & \subset & & \subset & \\ F & \uparrow\text{purely insep} & & & K & \subset & E \\ & \subset & E^{sep} = \{\text{purely seperable}\} & \cup & & \cup & \\ & \uparrow\text{seperable} & & & & \uparrow\text{purely insep} & \end{array}$$

Theorem In the diagram
Let $K = E^{insep}E^{sep}$, then $E^{insep} \subset E$ is seperable iff $K = E$.

proof
$E^{insep} \subset K$ seperable $\longleftarrow$
$\longrightarrow$ if $E^{insep} \subset E$ is seperable then K is seperable
But $K \subset E$ is purely inseperable. Must have $K = E$

Theorem If $F \subset E$ is splitting, all subextensions are splitting:
$F \subset E^{sep}$, $F \subset E^{insep}$ splitting.
- $F \subset E^{sep}$ is Galois
- E^{insep} is Galois

If $F \subset E$ is normal, $Gal(E/E^{insep}) \longrightarrow Gal(E/F)$
$\longrightarrow Gal(E^{sep}/F)$
$\cong$ both and Galois

Jan 31

Suppose $K \subset L$ finite exstension

$K \subset$ maximal seperable subext $\subset L$
$\uparrow$ purely insep
$\downarrow$

automatically trivial
in char = 0
in char p, its
adjoining $\sqrt[p]{\ }$

Definition

A field K is <u>perfect</u> if every finite extension is seperable

Example

- char = 0
- finite
- algebraically close

Non Example

$\mathbb{F}_p(t)$

Lemma (corrolary?)

Let $K \subset L$ is finite and seperable, then there are only finitely many subextensions.

proof

Since L seperable, we can find a finite Galois extension $K \subset L \subset E$.

$$\underbrace{K \subset L \subset E}_{\text{Galois}}$$

$\# Gal(E/K) = [E:K] < \infty$

So, $K \subset E$ has only finitely many subextensions.

So $K \subset L$ too

Proposition

Let $K \subset L$ is finite and seperable, then $L = K(u)$ for some $u \in L$. This u is called <u>primitive</u>.

proof

Choose $u \in L$ such that $[K(u):K]$ is maximal.

Pick any $v \in L$. Look at the fields $K(u + av) \subset L$ for $a \in K$

(If $\#K < \infty$ do it directly)

So, $\exists a \neq b$ with $K(u + av) = K(u + bv)$

$u + av,\ u + bv \in K(u + av)$

$$v = \frac{(u + bv) - (u + av)}{(b - a)} \in \underset{\underset{K(u)}{\cup\!\!\mid}}{K(u + av)}$$

So u is as well.
It must be equal by maximality.

Choose an algebraic closure $\overline{K} \supset K$

$K \underset{\text{Galois}}{\subset} K^s \underset{\text{purely insep}}{\subset} \overline{K}$

K^s ← separable closure

for any $K \subset L$ finite and separable, $\exists K$-linear homomorphism $L \hookrightarrow K^s$

If $K \hookrightarrow L$ finite (not necessarily separable) $\exists K$-linear inclusion $L \hookrightarrow \overline{K}$

$$\mathrm{Gal}(\overline{K}/K) \cong \mathrm{Gal}(K^s/K) := \mathrm{Gal}^{abs}(K) = G$$

So for any separable $K \subset L$, if I pick $L \hookrightarrow \overline{K}$, then I get a subgroup of G. $J \subseteq G$

$$[L : K] = [J : G]$$

How does this subgroup depend on the choice of homomorphism $L \hookrightarrow \overline{K}$?

$$\begin{array}{ccc} L & \hookrightarrow & K^s = E \quad \text{original} \\ \cong\ \mathrm{id} & & \swarrow\ g \\ L & \hookrightarrow & E' = K^s \quad \text{different inclusion.} \end{array}$$

Given two inclusions, I can think of them as different extensions to splitting fields.
But, we know how to extend $\cong$'s to splitting fields.

$$L \; \begin{matrix} \xrightarrow{i} & \overline{K} \\ \xrightarrow{i'} & \overline{K} \end{matrix} \circlearrowleft g \quad \rightsquigarrow \quad \begin{matrix} J = Gal(\overline{K}/i(L)) = \{g \in G \text{ st } gi = i\} \\ J' = Gal(\overline{K}/i'(L)) = \{g \in G \text{ st } \underbrace{gi'}_{\gamma i} = i'\} \end{matrix}$$

$J' = J^\gamma$ conjugate the subgroup

$J \cong J'$ by $g \longmapsto \gamma g \gamma^{-1}$

On the other hand, if J, J' conjugate subgroups of G, then fields $(K^s)^J$ $(K^s)^{J'}$ are isos

Conclusion

The category of finite seperable extensions of K

- obj : field extensions $K \hookrightarrow L$ seperable and finite
- $\longrightarrow$: $\hom(K \hookrightarrow L, K \hookrightarrow L') = \hom_K(L, L')$
  the K-linear rings homomorphisms

There is a bijection of sets between the set

$$\{\text{iso classes of finite seperable extensions of } K\}$$
$$\cong$$
$$\{\text{conjugacy classes of finite subgroups of } G\}$$

Given $J \subset G \rightsquigarrow G/J = X$ sets of cosets,
Then G acts transitively on X by $g \triangleright hJ = ghJ$

On the other hand, if X is any finite set with a transitive G-action $G \times X \longrightarrow X$ and if pick $x_0 \in X$ reference element.

$$J = stab(x_0) = \{g \in G \text{ such that } gx_0 = x_0\}$$
$$[G \circlearrowright X] \cong [G \circlearrowright G/J]$$

iso of G-sets

unique such iso which takes $x_0 \longleftrightarrow [1] \in G/J$

If you choose a different reference point γx_0 for some γ, $stab(\gamma x_0) = J^\gamma$ conjugates subgroups

$\{$ finite subgroups of G up to conjugation $\}$

$\updownarrow$

$\{$ transitive finite G-sets up to isomorphism $\}$

There is a contravariant equivalence of categories
$\{$ finite separable extensions of $K \}$ $\qquad K \subset L$

$$\downarrow$$

$\{$ transitive finite G-sets $\}$ $\qquad G \circlearrowright \hom_K(L, K)$

$K \leq \hom_G(X, \bar{K}) \longrightarrow \underbrace{\text{set of functions } f : X \longrightarrow \bar{K} \text{ such that } f(gx) = g \cdot f(x)}$

$\uparrow$

Given G-set X $\qquad$ A commutative ring that contains K.

Given $K \subset \bar{K}$ the constant function $x \longmapsto a \ \forall x$ is indeed G-equivalent.

Feb 2

Fix a field $\mathbb{K}$.
Consider the category $\{$ com $\mathbb{K}$-algebra $\}$
Pick some "coreference" object R Ψ , $G := Aut_K(R)$
Get a contravariant functor
$\hom_{\text{com } K\text{-alg}}(-, R) : \{$ com K-alg $\} \longrightarrow \{ G$-sets $\}$
This functor has a (dual) adjoint

Given $X \circlearrowleft G$, write down $\hom_G(X, R) \in Com_K$

<u>Claim</u> These functors, $\hom_K(-, R)$:
$\underbrace{\{\text{com } K\text{-alg}\} \longrightarrow \{G\text{-sets}\}}$
are a dual adjunction. analogize to the Galois connections for subexts $K \hookrightarrow L$

A *dual adjunction* is a pair of contravariant functors $F : \mathcal{C} \rightleftarrows \mathcal{D} : G$ and natural transformat $\varphi : id_{\mathcal{C}} \Rightarrow GF$, $\psi : id_{\mathcal{D}} \Rightarrow FG$ such that

$$\begin{array}{ccc} F = F \circ id_{\mathcal{C}} & & G \\ \uparrow F(\varphi) & & \uparrow G(\psi) \\ FGF & & GFG \\ \uparrow \psi(F) & & \uparrow \varphi(G) \\ id \circ F = F & & G \end{array}$$

<u>Recall</u> a natural transformation $\varphi : id_{\mathcal{C}} \Rightarrow GF$
$\forall X \in \mathcal{C}$ an arrow $\varphi(X) : \underset{X}{\underset{\shortparallel}{id_{\mathcal{C}}(X)}} \longrightarrow GFX$

such that $\forall f : X \longrightarrow Y$

$$\begin{array}{ccc} id_{\mathcal{C}} X & \xrightarrow{\varphi_X} & GFX \\ {\scriptstyle id_{\mathcal{C}} f} \downarrow & & \downarrow {\scriptstyle GGf} \\ id_{\mathcal{C}} Y & \xrightarrow[\varphi_Y]{} & GFY \end{array}$$

Given this data, $F\varphi X = F(X \xrightarrow{\varphi_F} GFX)$
$FX \longleftarrow FGFX$

$F\varphi$ is a natural transformation $F \Leftarrow FGF$

<u>proof of claim</u>

To give you maps
$\forall A \in Com_K$ $\quad \underbrace{A \longrightarrow hom_G(hom_K(A, R), R)}_{\text{com alg map}}$

$$a \longmapsto ((f : A \to R) \longmapsto f(a))$$

$\forall X \in Set_G$ $\quad \underbrace{X \longrightarrow hom_K(hom_G(X, R), R)}_{G\text{-set map}}$

$$x \longmapsto \text{" evaluation at } x\text{"}$$

$$hom_K(A, R) \longrightarrow hom(hom(hom(A, R), R), R) \longrightarrow hom(A, R)$$
$$f \longmapsto$$

$$\text{Com } K\text{-alg} \xleftrightarrow{hom(-,R)} Set_G$$

How nice are these functors?
Are there equivalences of categories?
Maybe just on some subsets?
Do they play well with monoidal structures?

Given commutative K-alg A, B,

. I can build $A \oplus B$ ($\oplus$ not a direct sum op) + of underlying v-spaces

$$A \oplus B = (a, b),\ a \in A,\ b \in B$$

$(a, b) \cdot (a', b') = (aa', bb')$

. I can build $A \otimes B$ ($\otimes$ of underlying v-spaces)

$$A \otimes B = (a \otimes b),\ a \in A,\ b \in B$$

Make $A \otimes B$ into a com K-alg by declaring on pure tensors $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$

Given $X \circlearrowleft G$, $Y \circlearrowleft$

. I can build $X \sqcup Y$ disjoint union : elt of $X \sqcup Y$ either in X or Y

. I can build $X \times Y$ cartesian union : (x, y)

Remark

$\times$ is $\prod$ in Set

$\sqcup$ is $\amalg$ in Set

$\oplus$ is $\prod$ in Com_K

$\otimes$ is $\amalg$ in Com_K

$\mathrm{hom}_K(A \otimes B, R)$ $\longleftarrow$ given as an alg by $a \otimes 1$, $1 \otimes b$

Given any $f : A \to R$ and $g : B \to R$

$$f \otimes g : A \otimes B \longrightarrow R$$
$$a \otimes b \longmapsto f(a)g(b)$$

if f, g homs, so is $f \otimes g$

$\cong \mathrm{hom}(A, R) \times \mathrm{hom}(B, R)$

is of G-sets

$\mathrm{hom}_K(A \oplus B, R) \supset \mathrm{hom}(A, R) \amalg \mathrm{hom}(B, R)$

$\uparrow$ might not be iso *

linear map $A \longrightarrow A \oplus B$

$a \longmapsto (a, 0)$

not unital algebra

given $f : A \to R$ we can define $A \oplus B \longrightarrow R$

$(a, b) \longmapsto f(a)$

$g : B \to R$ $\quad A \oplus B \longrightarrow R$

$(a, b) \longmapsto g(b)$

* is iso if R has no zero-div (R a field)

$h((1,0))h((0,1)) = 0$ so either $(1,0) \longmapsto 0$

$(0,1) \longmapsto 0$

but $(1,0) + (0,1) = (1,1) \longmapsto 1$

For any R, $G := \mathrm{Aut}_K(R)$

$\mathrm{hom}(\_, R) : \mathrm{Com}_K \longrightarrow \mathrm{Set}_G$

1) has a dual adjoint

2) take $\otimes \longrightarrow \times$

3) if R field $\oplus \longrightarrow \sqcup$ (connectivity condition)

Compare Pick a topological space T

Get covariant functors

$$\begin{array}{ccc} & \mathrm{hom}_{top}(T, -) & \\ top & \longrightarrow & set \\ \prod & \longmapsto & \prod \quad \text{any } T \\ \coprod & \overset{?}{\longmapsto} & \coprod \end{array}$$

$$\mathrm{hom}(T, X \sqcup Y) \supset \mathrm{hom}(T, X) \sqcup \mathrm{hom}(T, Y)$$

$\uparrow$ iso iff T <u>connected</u>

Feb 7

Let's fix a ground field K, commutative algebra L

$\longrightarrow$ get a contravariant adjunction

$$\begin{array}{ccc} Com_K & \leftrightarrows & Set_G \\ \mathrm{hom}_K(-, L) & & \mathrm{hom}_G(\_, L) \end{array}$$

(think of this adjunction as version of Galois connection)

Side Remark A covariant adjunction

$$F : \mathcal{C} \leftrightarrows \mathcal{D} : G$$

and natural isomorphisms

$$\underbrace{\mathrm{hom}_{\mathcal{D}}(FC, D)}_{F \text{ is left adjoint}} \cong \underbrace{\mathrm{hom}_{\mathcal{C}}(C, GD)}_{G \text{ is right adjoint}}$$

$$\overset{F}{\mathrm{hom}_K(-, L)} : \overset{\mathcal{C}}{Com_K} \leftrightarrows \overset{\mathcal{D}}{Set_G} : \overset{G}{\mathrm{hom}_G(\_, L)}$$

We have the natural isomorphism:

$$\underbrace{\mathrm{hom}_{\mathcal{D}}(D, FC) = \mathrm{hom}_{\mathcal{C}}(C, GD)}_{\text{both on the right}}$$

Both sides are functions from a $\underset{com_K}{\text{ring}} \times \underset{G\text{-set}}{\text{set}} \longrightarrow L$

All maps are G-equivalent.

How do we make this adjunction into an equivalence?

Example

$\oplus \longmapsto \sqcup$ if L field

$\otimes \longmapsto \times$

$\times \longmapsto \otimes$

$\sqcup \longmapsto \oplus$

When does $\mathrm{Com}_K \longleftarrow \mathrm{Set}_G$ take one point G-set to K?

$$\hom_G(\{\cdot\}, L) = L^G$$

$\longrightarrow$ When $K \subset L$ is Galois

Example

What if $K = L$?

G is trivial.

$\mathrm{Com}_K \longleftarrow \mathrm{Set}$

$\underbrace{K\text{-valued fcts on } X}_{K(X)} \longleftarrow\!\shortmid \; X \quad x \longmapsto ev(x)$

$K(X) \longmapsto \hom_K(K(X), K)$, $\quad X \searrow \hom_K(K(X), K)$

Is this an isomorphism?

Yes when X is finite : $\#X < \infty$

$\longrightarrow$ then $K(X) = \bigoplus_{x \in X} K\,\delta(x)$ $\qquad \delta_{xy} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$ $\qquad \delta_x^2 = \delta_x$, $\quad 1 = \sum_{x \in X} \delta_x$

What if $\#X = \infty$?

If K finite $\longrightarrow$ NO

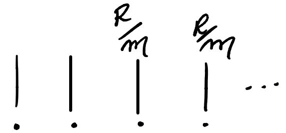
If K also infinite $\longrightarrow$ often is a iso

Any commutative has a max Spec.

$$\mathrm{maxspec}(R) = \{\text{maximal ideals of } R\} = \{\text{field quotients of } R\}$$

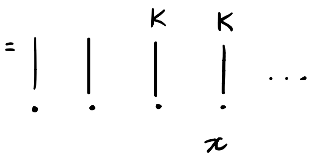
Given $\mathfrak{m} \in$ maxSpec, get field $R/\mathfrak{m}$

maxSpec :



If $R \in \mathrm{Com}_K$ then these fields contain K

max Spec $(K(X))$ =



$\mathfrak{m} = \mathrm{Ker}(ev(x))$

$\sqcup$ all points at ∞ : strictly nonempty if X infinite
the fields at ∞ are $\gg K$

$K = L$

$$\mathrm{Com}_K \longleftarrow \text{finite Set}$$
$$K(X) \longleftarrow\!\!\shortmid\; X$$

<u>Image</u>: those algebras $\cong \bigoplus_{x \in X} K$

$K \subset L$ Galois

$$\mathrm{Com}_K \longleftarrow \text{finite Set}_G$$
$$\hom_G(X, L) \longleftarrow\!\!\shortmid\; X$$
$$\longmapsto \hom_K(\hom_G(X, L), L)$$

If X finite, you end up back where you started.

(disjoint union of orbits)

Suppose X finite G-set.

$\hom_G(X, L)$

$\shortparallel$

$\bigoplus_{\text{orbits}}$ (version of single orbit)

$\uparrow$ fields

If X is a single orbit, then $\hom_G(X, L)$ is a field.

$\hom_G(X, L) = R$

Look at $R \otimes_K L$ $\cong$ $\dim_K(R)$ many copies of L

. when $K \subset L$ is finite

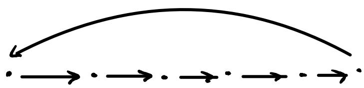
Then finiteSet$_G$ has a favorite element

$$\begin{array}{ccc} L & \longleftarrow & (G \circlearrowleft G) \\ \uparrow & & \uparrow \\ \mathrm{Com}_K & & \text{multiplication action} \end{array}$$

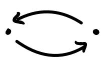
Take any G-set : $X \times G$ with diagonal G-action

$G = \mathbb{Z}/6$

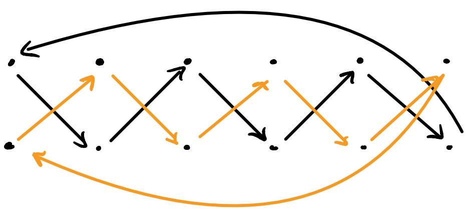
$G \circlearrowleft G$



$X = \mathbb{Z}/2$



$X \times G$



$X \times G \underset{\text{as } G\text{-sets}}{\cong} \# X$ copies of G

"separable and L-split"

$R \in \mathrm{Com}_K$ is the image of $\mathrm{Com}_K \longleftarrow \text{finiteSet}_G : \hom_G(-, L)$

iff $R \otimes_K L \cong \bigoplus_{\dim_K R} L$

$X \in \mathrm{Set}_G$ $\qquad X \xhookrightarrow[\text{diag}]{} X \times X$ $\qquad L^G(X) = \hom_G(X, L)$

$$\begin{tikzcd} L^G(X) \arrow[r, leftarrow, "\text{restrict}"'] \arrow[rrr, bend right, "\text{push forward diagonal}"'] & L^G(X \times X) \cong L^G(X) \otimes L^G(X) \arrow[l, bend left, "\text{mult}"] \end{tikzcd}$$

(not a ring map)

$f \longmapsto (x, y) := f(x)\,\delta(x = y)$

We just wrote down

$$\begin{tikzcd} R \otimes R \arrow[d, "\text{mult}"] \arrow[r] & \text{bimodule} \\ R \arrow[u, bend right, "\mu = \text{pushforward}"'] \arrow[r] & \text{bimodule} \end{tikzcd}$$

If I take $(a \otimes b) \in R \otimes R$, $c, d \in R$
$(a \otimes b)\, \mu(c) = \mu(acb)$

An algebra is separable if $m : R \times R$ has bimodule splitting

Feb 9

Fix K, pick $K \subset L$ algebraic and galois

$$\mathrm{Com}_K \underset{\hom_G(-, L)}{\overset{\hom_K(-, L)}{\rightleftarrows}} \mathrm{Set}_G$$

Image of $\leftarrow$ is the commutative algebras which split over L.

$$R \otimes_K L \cong \oplus L$$

If R is a field, and if $\exists R \hookrightarrow L$ then R is the essential image.

the connected
G - sets

<u>Remark</u> If $K \subset R$ field extension and $K \subset L$ is galois then $R \subset L$ iff $R \otimes_K L \cong \bigoplus_{[R:K]} L$

Every seperable field embeds into a Galois field.
Every split field splits under some base change.

If $K \hookrightarrow L$ field extension

$$\mathrm{Vect}_K \xrightarrow{\otimes_K L} \mathrm{Vect}_L$$

"base change"

$\otimes_K$ $\otimes_L$

this functor is symmetric
takes algebra $\longrightarrow$ algebra

Given $V \in \mathrm{Vect}_K$
$K^n = V \otimes_K L$
has an action given by $Gal(L/K) = G$
(not L-linear action)

$(V \otimes_K L)^G$ is another K vectorspace

If $K \hookrightarrow L$ is Galois, $(V \otimes_K L)^G = V$

Let $V \in \mathrm{Vect}_L$ and G its Galois group.
A <u>Galois twisted action</u> of G on V is
$\forall g \in G$, function $p(g) : V \longrightarrow V$

$p(gh) = p(g)p(h)$
additive : $p(g)(v+w) = p(g)v + p(g)w$
not L-linear.

Given $l \in L$, $p(g)(lv) = g(l)\,p(g)v$

$$
\begin{tikzcd}
\mathrm{Vect}_K \arrow[rr, "\otimes_K L"] \arrow[dr, "\otimes_K L"'] & & \mathrm{Vect}_L \\
& \mathrm{Vect}_L^G \arrow[ur] &
\end{tikzcd}
$$

Vect_L^G = L-vector space with twisted G-action

Galois Descent

If $K \subset L$ is Galois, is an equivalence of symmetric $\otimes$ of categories