From last time

Descent 1 (Eq. of Cat's)

$$\begin{array}{c} E \\ |G \\ F \end{array}$$

$$\left[\text{Algebraic Structures} / F\right] \underset{S^G \leftarrow S}{\overset{S \mapsto S\otimes E}{\rightleftarrows}} \left[\begin{array}{l}\text{Alg. structures} / E \\ \text{w/ } G\text{-semilinear action}\end{array}\right]$$

Descent 2

$$\left\{\begin{array}{c}\text{twisted forms of } S \\ \text{w/r/to } E/F\end{array}\right\} \xleftrightarrow{\text{bijection}} H^1(G, \mathrm{Aut}(S\otimes E))$$

Connection between these:

$H^1(G, \mathrm{Aut}(S\otimes E))$ can be identified with G-semilinear actions on $S\otimes E$.

Example: H-Galois extensions (of rings)

Def An H-Galois extension of F is a commutative F-algebra E, together with an action of $H \hookrightarrow \mathrm{Aut}(E/F)$ such that

$$(E, H, 1) \longrightarrow \mathrm{End}_F(B) \text{ is an iso.}$$

Reminder: $(E, H, \lambda) = \coprod_{h \in H} E x_h$

w/ multiplication: $x_h x_k = x_{hk}$

$$x_h \lambda = h(\lambda) x_h$$

Remark
- This implies $E^H = F$

(hint: $Z(\mathrm{End}_F(E)) = Z(M_n(F)) = F$

& they're in center $\Leftrightarrow$ they commutes w/ all x_h's & E)

- also $|H| = \dim_F E$

Lemma E/F is H-Galois $\Longleftrightarrow$

$E \cong \bigtimes_{i=1}^{m} E_i$ w/ H transitively permuting factors E_i, and with

E_i/F an H_i-Galois field extension, where H_i = stabilizer of E_i, and where action on components can be identified w/ H/H_i

via $H/H_i \longrightarrow$ factors E_j

$$1 \longmapsto E_i$$

$$g \longmapsto gE_i$$

Pf $\Rightarrow$ As before, (from descent prank)

E is the unique simple $(E,H,1)$-module.

Consider $J(E)$ Jacobson radical, note

H acts as auts of E, so preserve $J(E)$

& $J(E)$ is a left E-module, H acts similarly

w/ respect to module structure

$$x \in J(E) \quad \lambda \in E \quad h \in H$$

$$h(\lambda x) = h(\lambda) h(x)$$

$\Rightarrow$ $J(E)$ is a $(E,H,1)$-submodule of E

$\Rightarrow$ $J(E) = 0$. $\Rightarrow$ E artin (f.d.), semisimple

$$E \cong \times E_i \qquad E_i \text{ simple rgs.}$$

$\Rightarrow$ E_i/F field extension.

$$E = \mathrm{End}_E(E) = \mathrm{End}_E(\oplus S_i)$$

$$= \begin{bmatrix} \boxed{\mathrm{End}_E(S_0) \quad \mathrm{Hom}(S_0,S_1)} & \cdots \\ & \ddots \end{bmatrix}$$

if $e_i \in E_i$ unit then claim e_i's are transitively permuted by H.

<u>Subclaim</u>: e_i's are exactly the primitive idempotents of E.

Idempotent: $f^2 = f$

primitive: $f = f_1 + f_2$ $f_i^2 = f_i$ then f_1 or $f_2 = f$

<u>Pf</u>: suppose $f \in E$ idempotent

$f = (f_1, \dots, f_m) \in \bigtimes_{i=1}^{m} E_i$

then each f_i idempotent $\Rightarrow$ $f_i = 0$ or e_i

$\Rightarrow$ $f = \sum$ some e_i's. $\square$.

Now H permutes these e_i's

& if $e_1, e_2, \dots, e_\ell$ is a complete H orbit

then $\sum_{i=1}^{\ell} e_i$ is in $\underset{F}{\overset{\shortparallel}{E^H}}$ & is idempotent

$\Rightarrow$ $\ell = m$, $\sum e_i = 1$ & action on e_i's is transitive.

Notice $E_i = E e_i$ $\Rightarrow$ $h(E) = h(E) h(e_i)$
$= E h(e_i)$

$= E\, e_{h(i)}$

$\Rightarrow H$ acts transitively on factors. $= E_{h(i)}$

if $H_1 =$ Stabilizer of E_1

then orbit stab $\Rightarrow$ action on ~~the~~ factors is same as H/H_1

& $H_i = \mathrm{Stab}(E_i) \Rightarrow H_i = \sigma_i H_1 \sigma_i^{-1}$ where

$\sigma_i(e_1) = e_i$

$H_i \sigma_i = \sigma_i H_1$ are all the left cosets of H_1

$$\bigcup \sigma_i H_1 = H$$

<u>Next:</u> E_1/F is H_1-Galois.

$\Leftarrow$ $E_1^{H_1} = F$

suppose $\lambda \in E_1^{H_1}$ then consider the orbit of λ under H.

$h \in H$, can write $h = \sigma_i h_1$

$h\lambda = \sigma_i h_1 \lambda = \sigma_i \lambda \Rightarrow \{\sigma_i \lambda\}$ orbit.

$\Rightarrow \sum \sigma_i \lambda$ is H-fixed $\in F$

$\sigma_i \lambda \in E_i$ $\qquad (\lambda, \sigma_2 \lambda, \sigma_3 \lambda \dots \quad) \in F$

$\lambda \in E_1$ $\qquad \lambda E_i \qquad \lambda \rightsquigarrow \lambda \cdot (1, 1, 1 \dots 1)$

$$= (\lambda, \lambda \dots, \lambda)$$

$\Rightarrow \lambda \in F.$ $\qquad \square$

<u>Example</u> $\quad K = \bigtimes_{h \in H} F = \bigtimes_{h \in H} F e_h$

has a natural H action. & is H-Galois.

$(K, H, 1) \xrightarrow{\sim} \mathrm{End}_F(K)$ ✓

Forms of this?

$K \otimes E \simeq K' \otimes E$

$$\begin{tikzcd}
 & & & E \\
 & K' & & \\
K & & & \\
 & F \arrow[ul, dash] \arrow[u, dash] \arrow[uuurr, dash, "G"'] & &
\end{tikzcd}$$

Answer: if E/F big enough, all H-Gal. exts are forms of this one.

why? if $\quad (K', H, 1) \xrightarrow{\sim} \mathrm{End}_F(K')$

same true for $(K' \otimes_F E, H, 1)$

$$A/_F \rightsquigarrow A \otimes E/_E$$

$$M_n(F) \rightsquigarrow M_n(E)$$

Choose E/F s.t. poly defines K'/F splits completely

$$CRT \Rightarrow K' \otimes E \cong \prod_{h \in H} E \quad ✓.$$

(Ident. factors / E.)

<u>Def</u> An H-algebra $/F$ is a commutative F-algebra w/ H acting as F-algebra automorphisms.

<u>Def</u> morphism of H algebras is an alg map commuting w/ H action.

<u>Remark</u>: If an H algebra K'/F is a form of $K = \prod_{h \in H} F$ then K'/F is H-Galois

why? consider the map

$$(K', H, 1) \longrightarrow \mathrm{End}_F(K')$$

then if $\otimes_F E$, this becomes an iso.

$\Rightarrow$ is an iso ✓.

Form of $K \longleftrightarrow$ H-Galois exts
(big E)

$\Rightarrow \left\{ \begin{array}{c} H\text{-Galois exts}/F \\ \text{forms of } K \text{ w/r/to} \\ E/F \end{array} \right\} \longleftrightarrow H^1(G, \mathrm{Aut}_E(K \otimes E))$

$\mathrm{Aut}_E(K \otimes E)$ $\qquad\qquad$ $\mathrm{Aut}_{H,F}(K)$

$$K = \bigtimes_{h \in H} F e_h$$

$\varphi : K \longrightarrow K$ $\quad$ H-alg map

$\varphi(e_1) = e_h$ $\quad$ but now, for $h' \in H$

$$\varphi(e_{h'}) = \varphi(h'(e_1)) = h' \varphi(e_1)$$
$$= h' e_h = e_{h'h}$$

So $\mathrm{Aut}_{H,F}(K) \longleftrightarrow H$

$$H \xrightarrow{\alpha} \mathrm{Aut}_{H,F}(K)$$

$$h \longmapsto \left[\begin{array}{l} e_1 \longmapsto e_h \\ e_{h'} \longmapsto e_{h'h} \end{array} \right]$$

$$\alpha(h_1 h_2)(e_1) = e_{h_1 h_2}$$

$$\alpha(h_1) \cdot \alpha(h_2)(e_1) = \alpha(h_1)\, e_{h_2}$$
$$= e_{h_2 h_1}$$

So could say $\mathrm{Aut}_{F,H}(K) = H^{op}$

H gp $\quad H^{op} \quad h_1 \cdot_{op} h_2 = h_2 h_1$

$$H \cong H^{op}.$$
$$h \mapsto h^{-1}$$

$$H \xrightarrow{\sim} \mathrm{Aut}_{F,H}(K)$$
$$h \longmapsto [e_1 \mapsto e_{h^{-1}}] \quad \checkmark$$

Conclusion:

$$H^1(G,H) = \frac{\text{cr}\cancel{\text{ossed}} \text{ hom } G \to H}{\text{eq. rel.}}$$

G acts trivially on H

$\updownarrow$

H-Galois exts
"split by E/F"

$\updownarrow$ $E \otimes K' \cong K$

$$a(gh) = a(g)\, g(a(h))$$
$$= a(g)\, a(h)$$

eq. rel $\quad a: G \to H \quad b\, a(g)\, g(b^{-1})$

$b \in H \quad b(a(g))\, b^{-1}$

$$H^1(G,H) = \mathrm{Hom}(G,H)/\sim \text{ conj by } H$$

$G \twoheadrightarrow H \qquad H \cong G/N$

$$\begin{array}{c} E \\ \big|\, N \\ K' \\ \big|\, G/N \cong H \\ F \end{array}$$

$G \twoheadrightarrow H_1 \hookrightarrow H$

$$\begin{array}{c} E \\ \big|\, G/N \\ K_1 \\ \big|\, H_1 \\ F \end{array}$$

$K' = \mathrm{Ind}_{H_1}^{H} K_1$

$\parallel$

spanned by symbols

f from

$h(x)$

$h \in H \quad x \in K_1$

$\big/ \sim$

$h_1(x) \leftrightarrow h_1 x$

$h_1 \in H_1$

Extensions

Given F. ~~Galois extension~~

given a G/N Galois extension of F

Q: Can we extend this to a G-Gal ext of F?

$\mathrm{Gal}(E/F) = \Gamma$ Gal ext.

Same question, for Gal. extensions split by E.

$$1 \to N \to G \to G/N \to 1$$

K a G/N ext split by $E \Rightarrow$ given by

$\varphi \in \mathrm{Hom}(\Gamma, G/N) \twoheadrightarrow H^1(\Gamma, G/N)$

$$\begin{tikzcd} & & & \Gamma \arrow[d, "\varphi"] \arrow[dl, dashed, "\tilde{\varphi}"'] & \\ 1 \arrow[r] & N \arrow[r] & G \arrow[r] & G/N \arrow[r] & 1 \end{tikzcd}$$

choose lifting $\tilde{\varphi}$, don't worry about whether or not it's a homomorphism.

Did we get lucky?

$$\tilde{\varphi}(\sigma\tau) \overset{?}{=} \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau)$$ eqn in G

true in G/N

$$\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau)\, a_{\sigma,\tau}$$

$a_{\sigma,\tau} \in N$.

If this doesn't work, change it:

$$\tilde{\tilde{\varphi}}(\sigma) = \tilde{\varphi}(\sigma)\, b_\sigma \qquad b_\sigma \in N$$

how does this change the $a_{\sigma,\tau}$?

$$\tilde{\tilde{\varphi}}(\sigma\tau) = \tilde{\varphi}(\sigma\tau)\, b_{\sigma\tau}$$
$$= \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau)\, a_{\sigma,\tau}\, b_{\sigma\tau}$$

$\overset{?}{=}$ super akward.

$$\overset{?}{=} \tilde{\tilde{\varphi}}(\sigma)\tilde{\tilde{\varphi}}(\tau) = \tilde{\varphi}(\sigma)\, b_\sigma\, \tilde{\varphi}(\tau)\, b_\tau$$

$\tilde{\varphi}(\text{stuff}) \in G \qquad b_?, a_{?,?} \in N$

Make an assumption (because we are kind of weak)

$N \subset Z(G)$

<u>Def</u> $1 \to N \to G \to G' \to 1$ is a <u>central</u> <u>extension</u> of G' by N

want $a_{\sigma,\tau} b_{\sigma\tau} \overset{?}{=} b_\sigma b_\tau$ all σ, τ

$a_{\sigma,\tau} = b_\sigma b_{\sigma\tau}^{-1} b_\tau$?

Need more info about $a_{\sigma,\tau}$.

Def was $\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau) a_{\sigma,\tau}$

$$\tilde{\varphi}(\sigma\tau\gamma) = \tilde{\varphi}(\sigma\tau)\tilde{\varphi}(\gamma) a_{\sigma\tau,\gamma}$$

$$= \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau) a_{\sigma,\tau} \tilde{\varphi}(\gamma) a_{\sigma\tau,\gamma}$$

$$= \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau)\tilde{\varphi}(\gamma) a_{\sigma,\tau} a_{\sigma\tau,\gamma}$$

$$\tilde{\varphi}(\sigma)\tilde{\varphi}(\tau\gamma) a_{\sigma,\tau\gamma}$$

$$= \tilde{\varphi}(\sigma)\tilde{\varphi}(\tau)\tilde{\varphi}(\gamma) a_{\tau,\gamma} a_{\sigma,\tau\gamma}$$

$$\Rightarrow \quad a_{\sigma,\tau} a_{\sigma\tau,\gamma} = a_{\tau,\gamma} a_{\sigma,\tau\gamma}$$

Def: $Z^2(\Gamma, N) =$ maps α from $\Gamma \times \Gamma \to N$

s.t. $\alpha(\sigma,\tau)\alpha(\sigma\tau,\gamma) = \alpha(\tau,\gamma)\alpha(\sigma,\tau\gamma)$

$$\alpha(\tau,\gamma)\alpha(\sigma\tau,\gamma)^{-1}\alpha(\sigma,\tau\gamma)\alpha(\sigma,\tau)^{-1} = 1$$

$$\left(\underset{\beta}{Z^1(\Gamma, N)} \qquad \sigma(\beta(\tau))\,\beta(\sigma\tau)^{-1}\beta(\sigma) = 1 \right)$$

$\tilde{\varphi}(\sigma)$ lift of $\varphi(\sigma)$

$$\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma)\,\tilde{\varphi}(\tau)\,a_{\sigma,\tau}$$

chge $\tilde{\tilde{\varphi}}(\sigma) = \tilde{\varphi}(\sigma)\,b_\sigma$

$$\tilde{\tilde{\varphi}}(\sigma\tau) = \tilde{\tilde{\varphi}}(\sigma)\,\tilde{\tilde{\varphi}}(\tau)\,\tilde{a}_{\sigma,\tau}$$

$$= \tilde{\varphi}(\sigma) b_\sigma\, \tilde{\varphi}(\tau) b_\tau\, \tilde{a}_{\sigma,\tau}$$

$$= \tilde{\varphi}(\sigma\tau)\, b_{\sigma\tau}$$

$$= \tilde{\varphi}(\sigma)\,\tilde{\varphi}(\tau)\,a_{\sigma,\tau}\,b_{\sigma\tau}$$

$$a_{\sigma,\tau}\,b_{\sigma\tau} = b_\sigma b_\tau\,\tilde{a}_{\sigma\tau}$$

$$\tilde{a}_{\sigma,\tau} = a_{\sigma,\tau}\,b_{\sigma\tau}\,b_\sigma^{-1}\,b_\tau^{-1}$$

Def: $B^2(\Gamma, N)$ are maps $\Gamma^2 \to N$ of form $\sigma,\tau \mapsto b_{\sigma\tau} b_\sigma^{-1} b_\tau^{-1}$ some $b_\sigma \in N$

$$H^2(\Gamma, N) \cong Z^2(\Gamma, N) / B^2(\Gamma, N)$$

tells us whether or not an extension is possible.

Where does H^2 "come from"

Division algebras!

Alternate interpretation of Z^2: Defining associative multiplication rules!

If $\begin{matrix} E \\ | \Gamma \\ F \end{matrix}$, $c : \Gamma^2 \to E^*$, can form "algebra" (E, Γ, c) by:

$$\coprod_{\sigma \in \Gamma} E x_\sigma$$

$$x_\sigma \lambda = \sigma(\lambda) x_\sigma$$

$$x_\sigma x_\tau = c(\sigma,\tau) x_{\sigma\tau}$$

Not usually associative.

but will be if: $x_\sigma(x_\tau x_\gamma) = (x_\sigma x_\tau) x_\gamma$ all σ, τ, γ.

$$x_\sigma(x_\tau x_\gamma) = x_\sigma\, c(\tau,\gamma)\, x_{\tau\gamma} = \sigma(c(\tau,\gamma))\, x_\sigma x_{\tau\gamma} = \sigma(c(\tau,\gamma))\, c(\sigma,\tau\gamma)\, x_{\sigma\tau\gamma}$$

$$(x_\sigma x_\tau) x_\gamma = c(\sigma,\tau)\, x_{\sigma\tau} x_\gamma = c(\sigma,\tau)\, c(\sigma\tau,\gamma)\, x_{\sigma\tau\gamma} \overset{?}{=} \sigma(c(\tau,\gamma))\, c(\sigma,\tau\gamma)\, x_{\sigma\tau\gamma}$$

want $\sigma(c(\tau,\gamma))\, c(\sigma,\tau\gamma) = c(\sigma,\tau)\, c(\sigma\tau,\gamma)$

" $\Gamma^2 \to E^*$ is a Noether-Factor set. "

In general, if Γ is a grp A an abelian grp w/ Γ-action, then a Noether factor set is a map $c: \Gamma^2 \to A$ s.t.

$$\sigma(c(\tau,\gamma))\, c(\sigma,\tau\gamma) = c(\sigma,\tau)\, c(\sigma\tau,\gamma)$$

Connection w/ $\mu_n \hookrightarrow E^*$

$\mathbb{Z}/n \subseteq F$ (have roots of unity)

$$c \longmapsto \mathbb{C} \longmapsto (E,\Gamma,c)$$

$$H^2(\Gamma, \mathbb{Z}/n) \longrightarrow H^2(\Gamma, E^*)$$

~~injective~~!

injective ~~when we go to infinite field thing.~~

ex: $\mathbb{Z}/2\mathbb{Z}$ $F = \mathbb{Q}$

$$(E,\Gamma,c) \simeq M_n(\mathbb{Q})$$

$\mathbb{Q} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$

$ij = -ji$ $i^2 = a \in \mathbb{Q}$ $j^2 = b \in \mathbb{Q}$

is a matrix alg $\iff$ equ $x^2 - ay^2 = b$ has a soln.