Last time:

"Torsor theorem":

- R PV-ring $/F$ $\rightsquigarrow$ $X \in \mathrm{Aff}_F$ corresponding to R
- $G = \mathrm{Gal}^{\partial}(R/F)$ $\rightsquigarrow$ $G_F \in \mathrm{Aff}_F$ corresponding to $\mathcal{O}(G) \otimes_K F$

$\rightsquigarrow$ right-action: $\gamma : X \times G_F \longrightarrow X$ in Aff_F

and: $X \times G_F \xrightarrow[\cong]{(\gamma,\, \pi_X)} X \times X$

isomorphism

i.e., X is a G_F-torsor.

in particular, B F-algebra: $X(B) \times G_F(B) \xrightarrow{\cong} X(B) \times X(B)$

§6. The ∂-Galois correspondence

In ordinary Galois theory, for any given finite Galois extension E/F, we have

$$\left\{ \begin{array}{c} F \subseteq M \subseteq E \\ \text{intermediate} \\ \text{fields} \end{array} \right\} \cong \left\{ \begin{array}{c} H \leq \mathrm{Gal}(E/F) \\ \text{subgroups} \end{array} \right\}^{op}$$

We establish the analog in ∂-Galois theory:

Theorem 6.1. Let E/F Picard-Vessiot extension. Then there is bijective correspondence

$$\left\{ \begin{array}{c} F \subseteq M \subseteq E \\ \text{intermediate} \\ \partial\text{-fields} \end{array} \right\} \cong \left\{ \begin{array}{c} H \leq \mathrm{Gal}^{\partial}(E/F) \\ \text{Zariski-closed} \\ \text{subgroups} \end{array} \right\}^{op}$$

$$M \longmapsto \mathrm{Gal}^{\partial}(E/M)$$

$$E^{H} \longleftarrow H$$

<u>Proof</u>: We need to show:

(1) $M = E^{\mathrm{Gal}^\partial(E/M)}$, for $F \subseteq M \subseteq E$,

(2) $H = \mathrm{Gal}^\partial(E/E^H)$, for $H \subseteq \mathrm{Gal}^\partial(E/F)$ $\mathfrak{z}$-closed.

To show (1), we may assume $F = M$ and show
$F = E^G$ for $G = \mathrm{Gal}^\partial(E/F)$.

To this end, let $R \subseteq E$ PV ring so that
$E = \mathrm{Quot}(R)$. Let $\frac{b}{c} \in E \setminus F$, $b, c \in R$ and consider the element $d := b \otimes c - c \otimes b \in R \otimes_F R$.

We have $\overset{(!)}{d \neq 0}$ and, since $R \otimes_F R$ is reduced (Lemma 5.2), d is not nilpotent. Therefore (!),
$R \otimes_F R[\frac{1}{d}] \neq 0$. Let $J \trianglelefteq R \otimes_F R[\frac{1}{d}]$ maximal ∂-ideal.

$$R \xrightarrow{\ \varphi\ } (R \otimes_F R[\tfrac{1}{d}])/J \xleftarrow{\ \psi\ } R$$
$$r \longmapsto r \otimes 1 \qquad 1 \otimes r \longleftarrow\!\shortmid\ r$$

Then, since R ∂-simple, φ and ψ are injective and, for $R = F\langle Y, Y^{-1}\rangle$, $\varphi(Y) = \psi(Y) \cdot C$ with $C \in GL(n, K)$ so that $\mathrm{im}\,\varphi = \mathrm{im}\,\psi$.

Thus, we have

$$R \xrightarrow[\varphi]{\cong} \operatorname{im}\varphi = \operatorname{im}\psi \xleftarrow[\psi]{\cong} R$$

and obtain

$$\sigma := \psi^{-1} \circ \varphi \quad \in \operatorname{Gal}^{\partial}(R/F)$$

with

$$\psi \circ \sigma = \varphi \, . \qquad (*)$$

The image of d in $R \otimes_F R[\frac{1}{d}]/J$ is

$$\varphi(b) \cdot \psi(c) - \varphi(c) \cdot \psi(b)$$

and since this image is nonzero (d is invertible), we have

$$\varphi(b)\psi(c) \neq \varphi(c) \cdot \psi(b)$$

$$\overset{(*)}{\Rightarrow} \psi(\sigma(b))\psi(c) \neq \psi(\sigma(c))\psi(b)$$

$$\Rightarrow \psi(\sigma(b)c) \neq \psi(\sigma(c)b)$$

$$\Rightarrow \quad \sigma(b)c \neq \sigma(c)b$$

$$\Rightarrow \quad \sigma\left(\frac{b}{c}\right) \neq \frac{b}{c}$$

Therefore $\frac{b}{c} \notin E^G$ so that $E^G = F$.

We show (2): For this, we prove the stronger statement: For any abstract subgroup $H \leq \mathrm{Gal}^{\partial}(E/F)$ with $F = E^H$, we have

$$\overline{H} = \mathrm{Gal}^{\partial}(E/F).$$

We show this by contradiction. Suppose $H \leq \mathrm{Gal}^{\partial}(E/F)$ with $F = E^H$ but $\overline{H} \subsetneq \mathrm{Gal}^{\partial}(E/F) =: G$.

Then there exists $f \in K[z_{i,j} \mid 1 \leq i,j \leq n] \xrightarrow{\pi} \mathcal{O}(G)$

$$f|_H = 0, \text{ but } f|_G \neq 0.$$

Let $Y \in GL(n, E)$ generating fundamental matrix for E/F. Let $X = (X_{i,j})_{1 \leq i,j \leq n}$ formal variables and consider the polynomial

$$P(X) = f(Y^{-1}X) \in E[X_{i,j} \mid 1 \leq i,j \leq n]$$

$$\left.\begin{array}{l}\text{Then we have, for every } \sigma \in H: \ P(\sigma(Y)) = 0 \text{ but} \\ \text{there exists } \sigma' \in G: \ P(\sigma'(Y)) \neq 0.\end{array}\right\} (*)$$

We now choose a polynomial $P_0 \in E[X_{i,j}]$ which satisfies $(*)$ and has a minimal number of nonzero monomial terms.

Wlog, we may assume that one of the coefficients of P_0 is 1. Now, we denote by P_0^τ the polynomial obtained by applying $\tau \in H$ to all coefficients of P_0. Then $P_0 - P_0^\tau$ has fewer monomial terms than P_0 and satisfies, for $\sigma \in H$, $(P_0 - P_0^\tau)(\sigma Y) = 0$, since

$$P_0^\tau(\sigma Y) = \tau(P_0(\underbrace{\tau^{-1}\sigma}_{\in H} Y)) = 0.$$

Thus, by minimality, we have

$$(P_0 - P_0^\tau)(\sigma(Y)) = 0 \qquad \forall \underline{\sigma \in G}.$$

Now, if $P_0 - P_0^\tau \neq 0$, then we may find $a \in E$ such that

$$P_0 - a(P_0 - P_0^\tau)$$

satisfies $(*)$ but has fewer monomial terms than P_0 ↯. $\Rightarrow P_0 = P_0^\tau \quad \forall \tau \in H$.

But this implies that P_0 has coefficients in $E^H = F$. But then, for $\sigma \in G$, we have

$$P_0(\sigma Y) = \sigma(P_0(Y)) = \sigma(\underbrace{P_0(id(Y))}_{0}) = 0. \quad ↯. \quad \square$$

Remark: In ordinary Galois theory:

$$H \trianglelefteq \underset{G}{\mathrm{Gal}}(E/F) \text{ normal}$$

$$\Rightarrow E^H/F \text{ Galois with } \mathrm{Gal}(E^H/F) \cong G/H$$

We thus expect a ∂-analog:

$$H \trianglelefteq \mathrm{Gal}^{\partial}(E/F) \text{ normal} + Z\text{-closed}$$

$$\Rightarrow E^H/F \text{ PV-extension with } \mathrm{Gal}^{\partial}(E^H/F) \cong G/H.$$

This is true but requires some preliminaries before we can prove it!

§7. Linearizations and quotients of linear algebraic groups

Our two main goals in this section will be to show:

1. Every linear algebraic group G over a field k is isomorphic to a Zariski-closed subgroup of $GL(n,k)$.
2. Given $H \trianglelefteq G$ normal Z-closed subgroup, then G/H admits a canonical structure of linear algebraic group.

Let G linear algebraic group $/ k$ and V affine k-variety. We say V is a <u>G-variety</u> if G acts on V and the action map

$$G \times V \longrightarrow V, \quad (g,x) \longmapsto g \cdot x$$

is a morphism in Var_k. If V is a G-variety then G acts on the coordinate ring $\mathcal{O}(G)$ as follows:

For $g \in G$ and $\varphi \in \mathcal{O}(V)$:

$$g \cdot \varphi(x) = \varphi(g^{-1} \cdot x) \qquad \left(\overset{(!)}{\Rightarrow} g \cdot \varphi \in \mathcal{O}(V) \right)$$

Any linear algebraic group G is a G-variety via

1. $G \times G \longrightarrow G$, $(g,x) \longmapsto gx$ "left transl."
2. $G \times G \longrightarrow G$, $(g,x) \longmapsto xg^{-1}$ "right transl."

Proposition 7.1. Let G linear algebraic group and V a G-variety. Let $A \subseteq \mathcal{O}(V)$ be a f.d. sub k-vector space of $\mathcal{O}(V)$. Then:

(1) There exists a f.d. subspace $B \subseteq \mathcal{O}(V)$ such that $A \subseteq B$ and B is stable under the action of G on $\mathcal{O}(V)$: $g \in G$, $f \in B \Rightarrow g \cdot f \in B$.

(2) A is stable under the action of G iff $\varphi^* A \subseteq \mathcal{O}(G) \otimes_k A$ where

$$\varphi : G \times V \longrightarrow V, \ (g,x) \longmapsto g^{-1} \cdot x \quad . \ (*)$$

Proof

(1) Suffices to assume $\dim_k A = 1$, since every f.d. vector space is a finite sum of 1-dim subspaces so that we may take the sum of the corresponding B's.

So let $A = \langle f \rangle$ with $f \in \mathcal{O}(V)$.

We write

$$\varphi^* f = \sum_{i=1}^{n} h_i \otimes f_i \quad \in \mathcal{O}(G) \otimes \mathcal{O}(V)$$

where φ is as defined in $(*)$.

Then, for $g \in G$, we have

$$\begin{aligned} g.f(x) &= f(g^{-1}.x) = f \circ \varphi(g, x) = \\ &= \varphi^* f(g, x) \\ &= \sum_{i=1}^{n} h_i(g) \cdot f_i(x) \end{aligned}$$

$$\Rightarrow g.f \overset{(+)}{=} \sum_{i=1}^{n} h_i(g) \cdot f_i \quad \subseteq \quad \overbrace{\langle \{ f_i \mid 1 \leq i \leq n \} \rangle}^{\text{f.d. } k\text{-vector space}} \leq \mathcal{O}(V)$$

$\Downarrow$

Thus: $B := \langle \{ g.f \mid g \in G \} \rangle$ f.d. k-v.s.

which is also G-stable (!).

(2) If $\varphi^* f \in \mathcal{O}(G) \otimes A$, then the functions $\{f_i\}$ from above can be chosen to lie in A so that $(+)$ shows that $f \in A \Rightarrow g.f \in A$.

Vice versa, assume that A is G-stable, let $\{f_i\}$ be a k-basis of A and extend to a k-basis

$$\{f_i\} \cup \{r_j\}$$

of $\mathcal{O}(V)$. Then for $f \in A$, we have

$$\varphi^* f = \sum_{i=1}^{n} h_i \otimes f_i + \cancel{\sum \lambda_j \otimes r_j} \in \mathcal{O}(G) \otimes_k \mathcal{O}(V)$$

Then, for $g \in G$, we have

$$g.f = \sum h_i(g) f_i + \underbrace{\sum \lambda_j(g) r_j}_{0} \overset{!}{\in} A$$

$$\Rightarrow \lambda_j = 0$$

$$\Rightarrow \varphi^* f \in \mathcal{O}(G) \otimes A. \qquad \square$$

Theorem 7.3. Let G linear algebraic group. Then there exists $n \in \mathbb{N}$ such that G is isomorphic to a Zariski-closed subgroup of $GL(n, k)$.

Proof. We let G act on G via right translation

$$G \times G \to G, \quad (g, x) \mapsto xg^{-1}$$

and consider the corresponding G-action on $\mathcal{O}(G)$.

We choose generators

$$f_1, \ldots, f_n \in \mathcal{O}(G)$$

of $\mathcal{O}(G)$ as a k-algebra. By Prop. 7.2, we may assume that $\{f_i\}$ form the k-basis of the (finite-dimensional) G-stable sub vectorspace $\underbrace{\langle \{f_i\} \rangle}_{B} \leq \mathcal{O}(G)$.

With respect to the map $\varphi : G \times G \to G, \ (g, x) \longmapsto g^{-1} \cdot x = xg$ from Prop. 7.2, we have

$$\varphi^* f_i = \sum_{j=1}^{n} r_{ij} \otimes f_j \in \mathcal{O}(G) \otimes B$$

so that

$$g \cdot f_i = f_i(g^{-1} \cdot -) = f_i \circ \varphi(g, -) =$$
$$= \varphi^* f_i(g, -)$$
$$= \sum_{j=1}^{n} r_{ij}(g) f_j \, .$$

In particular, the matrix $(r_{ij}(g))_{1 \le i,j \le n} \in k^{n \times n}$ represents the k-linear map

$$B \longrightarrow B, \quad f \longmapsto g \cdot f$$

in terms of the k-basis $\{f_i\}$ of B.
Therefore, the functions $r_{ij} \in \mathcal{O}(G)$ determine a morphism

$$r : G \longrightarrow GL(n, k), \quad g \longmapsto (r_{ij}(g))_{1 \le i,j \le n}$$

of linear algebraic groups with

$$r^* : \underbrace{\mathcal{O}(GL(n,k))}_{k[x_{ij}, \frac{1}{\det(x)}]} \longrightarrow \mathcal{O}(G), \quad x_{ij} \longmapsto r_{ij} \, .$$

Further, the morphism r^* is surjective, since

$$f_i(x) = \varphi^* f_i(x, e) = \sum_{j=1}^{n} r_{ij}(x) \cdot f_j(e)$$

So that

$$f_i = \sum_{j=1}^{n} r_{i,j} \cdot f_j(e) \quad \in \quad \operatorname{im} r^* .$$

Since by assumption $\{f_i\}$ generate $\mathcal{O}(G)$ as a k-algebra, r^* is surjective.

$\Rightarrow \quad \mathcal{O}(G) \cong \mathcal{O}(GL(n,k))/I$ where $I = \ker(r^*)$

so that the morphism r defines a isomorphism of G with the subgroup $V(I) \subseteq GL(n,k)$:

$$\mathcal{O}(G) \xleftarrow{\cong} \mathcal{O}(GL(n,k))/I \twoheadleftarrow \mathcal{O}(GL(n,k))$$

$$G \xrightarrow{\cong} \underbrace{\operatorname{im} r = V(I)}_{\text{Zariski-closed subgroup.}} \hookrightarrow GL(n,k)$$

$\square$.