The Galois Group of a Picard-Vessiot Extension, Part 2.

Phyllis J. Cassidy
Smith College
and
The City College of CUNY
pcassidy1@nyc.rr.com

1 Linear algebraic groups.

Let V be a closed subset of $GL(n)$, and let $C\left[\gamma, \frac{1}{\det \gamma}\right]$ be its coordinate ring.

We have the short exact sequence:

$$0 \longrightarrow \mathfrak{a} \rightarrow C\left[X, \frac{1}{\det X}\right] \stackrel{\varphi}{\rightarrow} C\left[\gamma, \frac{1}{\det \gamma}\right] \rightarrow 0, \quad \varphi(X) = \gamma, \quad \varphi\left(\frac{1}{\det X}\right) = \frac{1}{\det \gamma}.$$

A subgroup G of $GL(n)$ that is also a closed subset is called a *closed subgroup* (*linear algebraic group*).

$GL(1)$ is denoted by $\mathbb{G}_{\mathrm{m}}$

A subgroup G of $\mathbb{G}_{\mathrm{m}}$ is closed if and only if there is a polynomial F in $C[X]$, X an indeterminate, such that $G = V(F)$.

G is the finite set of roots of a polynomial in 1 indeterminate.

The proper subgroups of $\mathbb{G}_{\mathrm{m}}$ are finite groups: the groups of m^{th} roots of unity.

Other examples:

1. The *special linear group* $SL(n) = \{c \in GL(n) : \det c = 1\}$.

2. The *upper triangular group* $T(n) = \{c \in GL(n) : c_{ij} = 0, \quad i > j\}$.

3. The *upper triangular unipotent group* $U(n) = \{c \in T(n) : c_{ii} = 1, i = 1, \ldots, n\}$.

4. The *diagonal group* $D(n) = \{c \in GL(n) : c_{ij} = 0, i \neq j\}$.

5. The *orthogonal group* $O(n) = \{c \in GL(n) : c^t c = 1_n\}$, 1_n the $n \times n$ identity matrix.The *special orthogonal group* $SO(n) = O(n) \cap SL(n)$.

6. A closed subgroup of $GL(2n)$ is the *symplectic group* $SP(2n) = \{c \in GL(2n) : c^t j c = 1_{2n}\}$, where

$$j = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}.$$

These are some of the so-called *classical groups*.

Recall: Let V be a closed subset of $GL(n)$, and W be a closed subset of $GL(m)$.

Let $C\left[\gamma, \frac{1}{\det \gamma}\right]$ be the coordinate ring of V, and $C\left[\varsigma, \frac{1}{\det \varsigma}\right]$ be the coordinate ring of W.

$C\left[\gamma, \frac{1}{\det \gamma}\right] \otimes_C C\left[\varsigma, \frac{1}{\det \varsigma}\right]$ is the coordinate ring of $V \times W$.

Therefore, if G and G' are linear algebraic groups, then $G \times G'$ is a linear algebraic group.

Let G be a closed subgroup of $GL(n)$. The following maps are morphisms of affine varieties:

The *multiplication map*

$$\mu : G \times G \to G, \quad , (a, b) \longmapsto ab;$$

the *left* and *right multiplication maps*

$$\begin{aligned} \lambda_a &: c \longmapsto ac \\ \rho_a &: c \longmapsto ca, \qquad a, c \in G, \end{aligned}$$

and the *inversion map* $\iota : G \to G$ sending $c \longmapsto c^{-1}$.The left and right multiplication maps, and the inversion map are homeomorphisms ot the algebraic variety G.

In particular, λ_a^* and ρ_a^* are C-algebra automorphisms of $C[G]$.

$$R = C[G] = C\left[\gamma, \tfrac{1}{\det \gamma}\right] \text{ is a } \textit{Hopf algebra.}$$

We have the following C-algebra homomorphisms:

$$\textit{comultiplication } \mu^* : R \to R \otimes_C R, \text{ sending } \gamma_{ij} \text{ to } \sum_{k=1}^{n} \gamma_{ik} \otimes \gamma.$$

$$\gamma \longmapsto \gamma \otimes \gamma.$$

$$\textit{augmentation } \epsilon : R \to C, \text{ sending } f \text{ to } f(1_n).$$

$$\gamma \longmapsto 1_n$$

$$\textit{antipode } \iota^* : R \to R, \text{ sending } \gamma_{ij} \text{ to } (\gamma^{-1})_{ij}.$$

We also have the algebra multiplication map $m : R \otimes_C R \to R$, sending $f \otimes g$ to fg.

The commutative diagrams expressing associativity, the properties of the identity element and inverses have their counterparts in the Hopf algebra.

$$\begin{array}{ccccccc} G & \times & G & \times & G & \xrightarrow{\mu \times id} & G & \times & G \\ & id \times \mu & \downarrow & & & & \downarrow & \mu & \\ & & G & \times & G & \xrightarrow{\mu} & G & & \end{array} \qquad \begin{array}{ccccccc} R & \otimes & R & \otimes & R & \xleftarrow{\mu^* \otimes id} & R & \otimes & R \\ & id \otimes \mu^* & \uparrow & & & & \uparrow & \mu^* & \\ & & R & \otimes & R & \xleftarrow{\mu^*} & R & & \end{array}$$

$$(id, 1) \quad \begin{array}{ccccc} G & & \xrightarrow{(1,id)} & G & \times & G \\ \downarrow & & \searrow id & & \downarrow & \mu \\ G \times G & & \xrightarrow{\mu} & & G & \end{array} \qquad m \circ (id \otimes \epsilon) \quad \begin{array}{ccccc} R & & \xleftarrow{m \circ (\epsilon \otimes id)} & R & \otimes & R \\ \uparrow & & \nwarrow id & & \uparrow & \mu^* \\ R \otimes R & & \xleftarrow{\mu^*} & & R & \end{array}$$

$$(id, \iota) \quad \begin{array}{ccccc} G & & \xrightarrow{(\iota,id)} & G & \times & G \\ \downarrow & & \searrow id & & \downarrow & \mu \\ G \times G & & \xrightarrow{\mu} & & G & \end{array} \qquad m \circ (id \otimes \iota^*) \quad \begin{array}{ccccc} R & & \xleftarrow{m \circ (\iota^* \otimes id)} & R & \otimes & R \\ \uparrow & & \nwarrow id & & \uparrow & \mu^* \\ R \otimes R & & \xleftarrow{\mu^*} & & R & \end{array}$$

Let G be a closed subgroup of $GL(n)$.

A morphism φ of algebraic varieties that is a homomorphism of algebraic groups

is called a *morphism of algebraic groups*.

Example 1 *1. The map* $\det : GL(n) \to \mathbb{G}_m$ *is a surjective morphism of algebraic groups, with kernel* $SL(n)$.

2. Let G *be a closed subgroup of* $GL(n)$*, and let* $A \in G$*. The group automorphism*

$$\tau_A : Z \longmapsto AZA^{-1}$$

(conjugation by A*) is an algebraic group automorphism.*

Proposition 2 *Let* G *be a closed subgroup of* $GL(n)$*, and, let* H *be a subgroup of* G*.*

Let U *and* V *be open dense subgroups of* G*.*

1. $G = UV$.
2. $\overline{H}$ *is a subgroup of* G.
3. *If* H *contains a dense open subset of* $\overline{H}$ *then* $H = \overline{H}$.

Proof. *We use the fact that the inversion, and left and right multiplication maps are homeomorphisms of the affinevariety* G.

Since λ_x *and inversion are homeomorphisms of affine varieties,*

if $x \in G$*,* xV^{-1} *is a dense open subgroup of* G*. Therefore,* $U \cap xV^{-1}$ *is nonempty. Let* $u = xv^{-1}$ *be in the intersection. Then,* $x = uv$.

So, we have established 1.

Since inversion is a homeomorphism of affine varieties, $\overline{H}^{-1} = \overline{H^{-1}} = \overline{H}$. *So,* $\overline{H}$ *is closed under inversion.*

Now, let $x \in H$. *Since* λ_x *is a homeomorphism of affine varieties,* $x\overline{H} = \overline{xH} = \overline{H}$. *Therefore,* $H\overline{H} \subseteq \overline{H}$. *Let* $x \in \overline{H}$. *Since* ρ_x *is a homeomorphism of affine varieties,* $\overline{H}x = \overline{Hx} \subseteq \overline{H}$. *Therefore,* $\overline{HH} \subseteq \overline{H}$.

So, we have established 2.

Let $U \subseteq H$ *be a dense open subset of* $\overline{H}$. *By* 2, $\overline{H}$ *is a closed subgroup of* G. *Therefore,* $\overline{H} = UU \subseteq H$.

So, we have established 3. ■

Proposition 3 *Let* $\varphi : G \to G'$ *be a morphism of algebraic groups. Then, the kernel of* φ *is a normal closed subgroup of* G,

and the image of φ *is a closed subgroup of* G'.

Proof. *By Corollary 20 (Chevalley),* $\varphi(G)$ *contains a dense open subgroup of* $\overline{\varphi(G)}$.

By Part 2 *of the previous proposition,* $\overline{\varphi(G)}$ *is a closed subgroup of* G'.

Therefore, by Part 3, $\varphi(G) = \overline{\varphi(G)}$. *Clearly, the kernel of* φ *is closed.* ■

Proposition 4 *1. The connected component* G^0 *of* G *containing the identity matrix* 1_n

is a closed normal subgroup of G *of finite index in* G.

Its cosets are the connected components (and irreducible components) of G.

2. Every closed subgroup of G of finite index in G contains G^0.

Proof. *We turn to the proof of part 1. Let a be in G^0.*

The left multiplication morphism $\lambda_{a^{-1}}$ permutes the connected components of G.

Since $\lambda_{a^{-1}}\left(G^0\right)$ contains 1_n, $\lambda_{a^{-1}}(G^0) = G^0$. Similarly, $\iota(G^0) = \left(G^0\right)^{-1} = G^0$.

It follows that G^0 is a closed subgroup of G. Furthermore, if $a \in G$, $\tau_a(G^0) =$

G^0.
Thus, G^0 is a normal closed subgroup of G.

Since left multiplication is a homeomorphism of affine varieties,

the left cosets of G^0 are connected components of G.

Let G^i be a connected component of G, and let $a \in G^i$.

Then, $\lambda_{a^{-1}}(G^i) = G^0$, and $G^i = \lambda_a(G^0)$. So, every connected component is a left coset of G^0.

We now show that the connected components are the irreducible components of G.

Let V and W be irreducible components containing 1_n.

The multiplication morphism $\mu : V \times W \to G$ has image the product VW.

Therefore, VW and $\overline{VW}$ are irreducible. $V \subseteq \overline{VW}$ and $W \subseteq \overline{VW}$. Therefore, $V = W = \overline{VW}$.

So, there is a unique irreducible component containing the identity matrix, and it is closed under multiplication.

$\iota(V)$ is closed and irreducible, and contains 1_n. So, $\iota\,(V) \subseteq V$.

The unique irreducible component containing the identity matrix is a closed subgroup of G.

For the same reasons, it is a normal subgroup of G.

It is easy to see that the irreducible components are mutually disjoint, and equal the left cosets of V.

G^0 is a union of irreducible components of G.

Since they are mutually disjoint and finite in number, they are both open and closed in G^0.

Since G^0 is connected, there is a unique irreducible component of G contained in G^0.

G^0 is irreducible, and equals V. Thus, every connected component of G is irreducible.

We turn now to part 2.

Let H be a closed subgroup of G of finite index in G.

Then H^0 is contained in G^0. Let $a \in G^0$. aH^0 is a left coset of H^0 in G.

Therefore, the index of H^0 in G^0 is $\leq$ the index of H^0 in G. So, H^0 has finite index in G^0.

Therefore, H^0 is both open and closed in G^0. Thus, $H^0 = G^0$, and $H \supseteq G^0$. ■

Corollary 5 *A linear algebraic group is connected if and only if it equals its identity component.*

1.1 The commutator subgroup of a linear algebraic group

Let V be an irreducible closed subset of $\mathbb{A}^n$.

$$\dim V := \text{tr deg}_C\, C(V)$$

Lemma 6 *Let V and W be irreducible closed subsets of $\mathbb{A}^n$, with $W \subseteq V$.*

1. $\dim W \leq \dim V$;
2. *If W is a proper subset of V, then* $\dim W < \dim V$.

Proof. *Write $C[V] = C[\gamma_1, \ldots, \gamma_n]$ and let $\mathfrak{p}$ be the defining ideal of W in $C[V]$.*

Write $C[W] = C[\varsigma_1, \ldots \zeta_n]$, where ς_i is the residue class of $\gamma_i \bmod \mathfrak{p}$.

Spose $\varsigma_1, \ldots \varsigma_d$ is a transcendence basis over C of $C[W]$.

Then, $\gamma_1, \ldots \gamma_d$ are algebraically independent over C. So, we have established 1.

Suppose $\dim V = \dim W = d$, *but $V \neq W$. Then there exists $f \in \mathfrak{p}$, $f \neq 0$.*

f is algebraic over $C(\gamma_1, \ldots, \gamma_d)$. Therefore, there exists $H \neq 0$ in the polynomial ring $C[\gamma_1, \ldots, \gamma_d, T] = C[\gamma_1, \ldots, \gamma_d][T]$ such that $H(f) = 0$.

WOLOG, we can assume that H is irreducible over $C(\gamma_1, \ldots, \gamma_d)$, and, therefore, $T \nmid H$.

$$\begin{aligned} H &= a_m(\gamma_1, \ldots, \gamma_d)T^m + \ldots + a_0(\gamma_1, \ldots, \gamma_d) \\ H(0) &= a_0(\gamma_1, \ldots, \gamma_d) \neq 0. \end{aligned}$$

Let $\varphi : C[\gamma_1, \ldots, \gamma_n] \to C[\zeta_1, \ldots, \zeta_n]$ be the surjective C-homomorphismwith

kernel $\mathfrak{p}$. Then, $0 = \varphi(H(f)) = H(\varphi(f)) = H(0) = a_0(\zeta_1, \ldots .\zeta_d)$, which contradicts the algebraic independence of $\zeta_1, \ldots, \zeta_d$. ∎

Proposition 7 *Let G be a closed subgroup of $GL(n)$,*

and let $(V_i)_{i\in I}$ be a family of irreducible closed subsets of $GL(n)$.

Let $\varphi_i : V_i \to G$ be a morphism Suppose each $W_i = \varphi_i(V_i)$ contains the identity matrix.

Let H be the smallest closed subgroup of G containing the subsets W_i, $i \in I$.

1. *H is connected.*

2. *There exists an integer $k > 0$ and $j = (j_1, \ldots, j_k) \in I^k$ and $\epsilon(j_h) = \pm 1$, $h = 1, \ldots, k$, such that $H = W_{j_1}^{\epsilon(j_1)} \cdots W_{j_k}^{\epsilon(j_k)}$.*

Proof. *We can ensure that for each $i \in I$, $\exists j \in I$ such that $V_i^{-1} = V_j$, and $\varphi_j\left(x_i^{-1}\right) = (\varphi_i(x_i))^{-1}$.*
Thus, $W_i^{-1} = W_j$.

$\forall\ k \in \mathbb{Z}_{>0}$, and $\forall j = (j_1, \ldots, j_k) \in I^k$, set $W_j = W_{j_1} \cdots W_{j_k}$.

Then, since the variety $V_{j_1} \times \cdots \times V_{j_k}$ is irreducible,

and the mapping $V_{j_1} \times \cdots \times V_{j_k} \to G$, sending $(x_{j_1}, \ldots, x_{j_k})$ to $\varphi(x_{j_1}) \cdots \varphi(x_{j_k})$ is a morphism of affine varieties,

W_j and $\overline{W_j}$ are irreducible.

It follows from Chevalley's Theorem that W_j contains an open dense subset of $\overline{W_j}$.

Clearly, $W_j W_k \subseteq W_{(j,k)}$.
We now repeat the argument used in the proof of part 2 of Proposition 2.to show that

$\overline{W_j}\ \overline{W_k} \subseteq \overline{W}\,(j,k)$.

Choose j such that $\dim \overline{W_j}$ is maximal.

$\forall k\ \overline{W_j} \subseteq \overline{W_j}\ \overline{W_k} \subseteq \overline{W}\,(j,k)$ By Lemma 6, $\overline{W}\,(j,k) = \overline{W_j}$, and, thus $\overline{W_k} \subseteq \overline{W_j}$ $\forall k$.

Moreover, since $\overline{W_j}\ \overline{W_j} \subseteq \overline{W}_{(j,j)} = \overline{W_j}$, $\overline{W_j}$ is closed under multiplication.

Taking $W_k = W_j^{-1}$, $\overline{W_j}^{-1} = \overline{W_j^{-1}}$.

Since it contains the identity matrix, $\overline{W_j}$ is a subgroup of G.

Since W_j contains an open dense subset of $\overline{W_j}$, it follows from part 3 of Proposition 2 that $\overline{W_j} = H$ is an irreducible closed subgroup of G.

It follows that H is connected by Proposition 3. ■

Corollary 8 *Let $(G_i)_{i\in I}$ be a family of closed connected subgroups of a closed subgroup G of $GL(n)$.*

Then, the subgroup generated by the family is closed and connected.

Let G be a group, and let H and K be subgroups of G.
(H, K) is the subgroup generated by all commutators $hkh^{-1}k^{-1}$,
$h \in H, k \in K$.
(G, G) is the *commutator subgroup* of G.

Corollary 9 *If H and K are closed subgroups of a closed subgroup G of $GL(n)$,*

one of which is connected, then (H, K) is connected.

Proof. *Set the indexing set I of the proposition equal to K,*

and for each index i, set $V_i = H$. Define, $\varphi_i(x) = xix^{-1}i^{-1}$, $x \in H$.

φ_i is a morphism from V_i into G. Then, (H, K) is the subgroup of G generated by H and K.

By Proposition 2, part 2, $\overline{(H, K)}$ is a subgroup of G. By Proposition 7, part 1, $\overline{(H, K)}$ is irreducible, hence connected, since H is irreducible.

A similar argument justifies the conclusion when K is connected. ■

Corollary 10 *The commutator subgroup of a connected linear algebraic group is closed and connected.*

Remark 11 *It is also true that the commutator subgroup of any linear algebraic group is closed, but, it is more difficult to establish.*

Remark 12 *Replace C by a differentially closed (constrainedly closed) Δ-field. The differential algebraic subgroups of $GL(n)$ are varieties defined by differential ideals in $C\left\{X, \frac{1}{\det X}\right\}$. Such ideals define the* Kolchin topology. *The commutator group of a differential algebraic group need not be Kolchin closed.*

1.2 The Jordan decomposition of an invertible matrix:

Let $a \in GL(n, C), C$ algebraically closed. Then, there is a matrix $b \in GL(n, C)$ such that bab^{-1} is in *Jordan normal form*:This matrix has square blocks along the diagonal. The diagonal entries are the eigenvalues of a – one eigenvalue for each block. The size of the jth block is the algebraic multiplicity of the

eigenvalue (its multiplicity as a root of the characteristic equation.)

$$\begin{pmatrix} \begin{pmatrix} a_1 & 1 & \dots & & 0 \\ & a_1 & 1 & & \\ & & \ddots & \ddots & \\ & & & a_1 & 1 \\ 0 & & & & a_1 \end{pmatrix} & & & & \\ & \ddots & & 0 & \\ & & & & \begin{pmatrix} a_p & 1 & \dots & & 0 \\ & a_p & 1 & & \\ & & \ddots & \ddots & \\ & & & a_p & 1 \\ 0 & & & & a_p \end{pmatrix} \end{pmatrix}.$$

$$bab^{-1} = su,$$

where s is a diagonal matrix whose diagonal entries are the eigenvalues of a, and u is upper triangular unipotent. Moreover,

$$su = us.$$

$$s = \begin{pmatrix} \begin{pmatrix} a_1 & & \dots & & 0 \\ & a_1 & & & \\ & & \ddots & \ddots & \\ & & & a_1 & \\ 0 & & & & a_1 \end{pmatrix} & & & \\ & \ddots & & \\ & & \begin{pmatrix} a_p & & \dots & & 0 \\ & a_p & & & \\ & & \ddots & \ddots & \\ & & & a_p & \\ 0 & & & & a_p \end{pmatrix} \end{pmatrix}$$

$$u = \begin{pmatrix} \begin{pmatrix} 1 & \frac{1}{a_1} & \dots & & 0 \\ & 1 & \frac{1}{a_1} & & \\ & & \ddots & \ddots & \\ & & & 1 & \frac{1}{a_1} \\ 0 & & & & 1 \end{pmatrix} & & & \\ & \ddots & & \\ & & \begin{pmatrix} 1 & \frac{1}{a_p} & \dots & & 0 \\ & 1 & \frac{1}{a_p} & & \\ & & \ddots & \ddots & \\ & & & 1 & \frac{1}{a_p} \\ 0 & & & & 1 \end{pmatrix} \end{pmatrix}.$$

1.2.1 The semisimple and unipotent parts of an invertible matrix

In general, a diagonalizable invertible matrix is called *semisimple.*

An invertible matrix u is called *unipotent* if $u-1_n$ is nilpotent, *i.e.*, some positive integer power equals 0.

Equivalently, the eigenvalues of u all equal 1.

For example, here is the general upper triangular 5×5 unipotent matrix.

$$u = \begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & a_{15} \\ 0 & 1 & a_{23} & a_{24} & a_{25} \\ 0 & 0 & 1 & a_{34} & a_{35} \\ 0 & 0 & 0 & 1 & a_{45} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Proposition 13 *(Springer, Linear Algebraic Groups, section 2.4) Every $n \times n$ matrix a in $GL(n, C)$, C algebraically closed, can be written uniquely*

$$a = su,$$

s semisimple, u unipotent, $su = us$, where $su = us$.

Theorem 14 *(Kolchin, On Certain Concepts in the Theory of Algebraic Matric Groups, 1948)*

Let G be a commutative linear algebraic group.

1. *The sets G_s and G_u of semisimple and unipotent matrices in G are closed subgroups.*

2. *The product map $G_s \times G_u \to G$ is an isomorphism of linear algebraic groups.*

Call G_{s} the *semisimple part* of G, and G_{u} the *unipotent part* of G.

Corollary 15 *Every commutative linear algebraic group is the direct product of its semisimple and unipotent parts.*

Remark 16 *A diagonalizable connected commutative linear algebraic group is called a* torus. *Every torus is isomorphic to $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$*

Let $\mathbb{G}_a$ be the additive group of the field C.

$\mathbb{G}_a$ has the natural linear representation as the commutative unipotent group

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \qquad a \in C \right\}.$$

Every unipotent linear algebraic group is isomorphic to $\mathbb{G}_a \times \cdots \times \mathbb{G}_a$.

So, every connected commutative linear algebraic group is isomorphic to

$$(\underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{\longleftarrow k \longrightarrow}) \times (\underbrace{\mathbb{G}_a \times \cdots \times \mathbb{G}_a}_{\longleftarrow l \rightarrow}),$$

where $k + l = \dim G$.

Suppose C is a differentially closed ordinary differential field. A differential algebraic group is defined by a radical differential ideal. If E is the elliptic curve with affine Legendre equation

$$y^2 = x(x-1)(x-t), t \in C,$$

where the derivation operator is $\frac{d}{dt}$, the differential algebraic subgroup structure on E is exactly the same as the differential algebraic subgroup structure on $\mathbb{G}_m$ .. (A. Buium, "Geometry of differential polynomial functions I: Algebraic groups," 1993.)

2 The linear algebraic group structure on the Galois group of a Picard-Vessiot extension.

Recall: K is an ordinary Δ-field of characteristic 0. The field C of constants of K is algebraically closed.

We fix a matrix $A \in M(n, K)$ and a Picard-Vessiot extension $L = K(\alpha)$ for A.

α is called a *fundamental matrix for* A.

$$\alpha' = A\alpha.$$

Gal is the Galois group of L over K.

$$c : \mathrm{Gal} \to GL(n, C), \qquad c(\sigma) = \alpha^{-1}\sigma\alpha.$$

c is an *injective homomorphism of groups.*

The Picard-Vessiot ring P:

$$\begin{aligned} P &= K\left[\alpha, \frac{1}{\det \alpha}\right] \\ D &= (P \otimes_K P)^{\Delta} = C\left[\gamma, \frac{1}{\det \gamma}\right], \qquad \gamma = \alpha^{-1} \otimes \alpha. \\ P \otimes_K P &= (P \otimes_K 1)\left[\gamma, \frac{1}{\det \gamma}\right]. \\ 1 \otimes \alpha &= (\alpha \otimes 1)\,\gamma. \end{aligned}$$

Jerry showed (Proposition 26) that the Δ-P-homomorphism

$$P \otimes_C D \to P \otimes_K P, \qquad a \otimes d \longmapsto (a \otimes 1)d$$

is a Δ-P- isomorphism.

Lemma 17 *$P \otimes_K P$ is reduced.*

Proof. *Zariski and Samuel, Commutative Algebra, Vol. I, Theorem 39, p. 195.*

This book contains an excellent study of tensor products of algebras over fields.

■

Let X be an $n \times n$ matrix of indeterminates. Define a surjective C-homomorphism

$$\varphi : C\left[X, \frac{1}{\det X}\right] \to C\left[\gamma, \frac{1}{\det \gamma}\right], \qquad X \longmapsto \gamma, \qquad \frac{1}{\det X} \longmapsto \frac{1}{\det \gamma}.$$

Set $\mathfrak{a} = \ker \varphi$. Since $C\left[\gamma, \frac{1}{\det \gamma}\right]$ is a subring of $P \otimes_K P$, it is reduced.

Thus, $\mathfrak{a}$ is a radical ideal.

We identify $C\left[\gamma, \frac{1}{\det \gamma}\right]$ with $C\left[V(\mathfrak{a})\right]$.

Proposition 18 *If $\sigma \in Gal$, $c(\sigma) \in V(\mathfrak{a})$.*

Proof. *Define a Δ-K-homomorphism*

$$\overline{\sigma} : P \otimes_K P \to P$$

by

$$\overline{\sigma}(a \otimes b) = a\sigma b.$$

Then,

$$\overline{\sigma}(\gamma) = \overline{\sigma}(\alpha^{-1} \otimes \alpha) = \alpha^{-1}\sigma\alpha = c(\sigma).$$

Also,

$$\overline{\sigma}\left(\frac{1}{\det \gamma}\right) = \frac{1}{\det \overline{\sigma}\gamma} = \frac{1}{\det c(\sigma)}.$$

Define a C-homomorphism $\chi_\sigma : C\left[\gamma, \frac{1}{\det \gamma}\right] \to C$ by

$$\chi_\sigma(\gamma) = c(\sigma), \qquad \chi_\sigma\left(\frac{1}{\det \gamma}\right) = \frac{1}{\det c(\sigma)}.$$

By Lemma 26, Part I, which identifies $V(\mathfrak{a})$ with $Hom_C\left(C\left[\gamma, \frac{1}{\det \gamma}\right], C\right)$, $c(\sigma) \in V(\mathfrak{a})$. ■

Proposition 19 *The injective group homomorphism $c : Gal \to V(\mathfrak{a})$ is surjective.*

Proof. *Let $c \in V(\mathfrak{a})$. c defines the evaluation homomorphism, which is a Δ-C-homomorphism:*

$$\chi_c : D = C\left[\gamma, \frac{1}{\det \gamma}\right] \to C, \qquad \left(\gamma, \frac{1}{\det \gamma}\right) \longmapsto \left(c, \frac{1}{\det c}\right).$$

The homomorphism

$$f : P \otimes_C D \to P \otimes_K P, \qquad a \otimes d \longmapsto (a \otimes 1)\, d$$

is a Δ-P-isomorphism.

Let $\pi_2 : P \to P \otimes_K P$ be the mapping $a \longmapsto 1 \otimes a$.

Define $\sigma : P \to P$ by

$$P \xrightarrow{\pi_2} P \otimes_K P \xrightarrow{f^{-1}} P \otimes_C D \xrightarrow{id \otimes \chi} P \otimes_C C \xrightarrow{mult} P.$$

We equip P with the structure of Δ-K-algebra, $P \otimes_K P$ and $P \otimes_C D$,and $P \otimes_C C$

with the structure of (left) Δ-P-algebra, by defining

$$a\,(b \otimes c) = ab \otimes c = (a \otimes 1)\,(b \otimes c).$$

Note: π_2 is a Δ-K-homomorphism,

f^{-1} is a Δ-P-homomorphism, hence is a Δ-K-homomorphism,

$id \otimes \chi$ is a Δ-P-homomorphism, hence is a Δ-K-homomorphism,

mult is a Δ-P-homomorphism, hence is a Δ-K-homomorphism.

So, σ is a Δ-K-homomorphism from P to P.

Since P is Δ-simple*, and σ is clearly not the* 0 *map, σ is* injective.

Recall that $P = K\left[\alpha, \frac{1}{\det \alpha}\right]$. What is the effect of σ on α?

$$\sigma : \alpha \longmapsto 1_n \otimes_K \alpha = (\alpha \otimes_K 1_n)\,\gamma \longmapsto \alpha \otimes_C \gamma \longmapsto \alpha \otimes_C c \longmapsto \alpha c.$$

$$\sigma : \det \alpha \longmapsto \frac{1}{\det \alpha} \frac{1}{\det c}$$

Thus,

$$\sigma\,(P) = K\left[\alpha c, \frac{1}{\det \alpha} \frac{1}{\det c}\right].$$

Since c is in $GL\,(n, C) \subseteq GL(n, K)$, σ is clearly surjective.

So, σ is a Δ-K-automorphism of P, and extends uniquely to an element σ of Gal.

Since $\sigma\,(\alpha) = \alpha c$,

$$c = \alpha^{-1}\sigma\alpha = c\,(\sigma)\,.$$

■

So, we defined on Gal the linear algebraic group structure defined on its image $G = V\,(\mathfrak{a})$ in $GL(n, C)$
This group structure depends on the choice of the fundamental matrix α for the differential equation

$$Y' = AY$$

that generates the Picard-Vessiot extension. Spose

$$L = K\,(\beta)\,, \qquad \beta' = A\beta$$

Then, there exists a matrix $c \in GL(n, C)$ with

$$\beta = \alpha c.$$

Therefore,

$$\begin{aligned} c_\beta\,(\sigma) &= \beta^{-1}\sigma\beta \\ &= c^{-1}\alpha^{-1}\sigma\beta \\ &= c^{-1}\left(\alpha^{-1}\sigma\alpha\right)c \\ &= c^{-1}c_\alpha\,(\sigma)\,c. \end{aligned}$$

So, the linear representations of Gal are conjugate.

Summary 20 *Let* $L = K(\alpha)$, *where* $\alpha \in GL(n, L)$, *and* $\alpha' = A\alpha$, $A \in M(n, K)$.

Assume L *is a Picard-Vessiot extension for* A.

Let C *be the algebraically closed field of constants of* K.

Then, $L^{\Delta} = C$.

Let $P = K\left[\alpha, \frac{1}{\det \alpha}\right]$ *be the associated Picard-Vessiot ring.*

Then, $P \otimes_K P = P \otimes_C C\left[\gamma, \frac{1}{\det \gamma}\right]$, *where* $\gamma = \alpha^{-1} \otimes \alpha$.

$D = C\left[\gamma, \frac{1}{\det \gamma}\right]$ *is the field of constants of* $P \otimes_K P$.

D *is the coordinate ring of the representation of* Gal *as a linear algebraic group.*

The group isomorphism $c : Gal \to GL(n, C)$

associates with the K*-automorphism* σ *of* L *the matrix* $c(\sigma) = \alpha^{-1}\sigma\alpha$.

$D = C\left[\gamma, \frac{1}{\det \gamma}\right]$ *has the structure of a Hopf algebra over* C,

with comultiplication, antipode, and counit induced by the group operations on the Galois group.