The Fundamental Theorem of Galois Theory

Phyllis J. Cassidy
Smith College
and
The City College of CUNY
pcassidy1@nyc.rr.com
The Fundamental Theorem of Galois Theory, Part I

Let $K$ be an ordinary differential field with algebraically closed field $C$ of constants,

and let $L$ be a Picard-Vessiot extension of $K$. Write

$$L = K(\alpha), \quad \alpha \in GL(n, L),$$
$$\alpha' = A\alpha, \quad A \in M(n, K),$$
$$L^\Delta = C.$$

$Gal(L/K)$: the group of $\Delta$-$K$-automorphisms of $L$.

Let $M$ be a $\Delta$-subfield of $L$ containing $K$. We call $M$ an intermediate differential field.

Then,

$$L = M(\alpha)$$
$$\alpha' = A\alpha, \quad A \in M(n, M).$$
$$L^\Delta = C.$$

So, $L$ is a Picard-Vessiot extension of $M$ for $A$, with fundamental matrix $\alpha$.

Recall:

$$P = K\left[\alpha, \frac{1}{\det \alpha}\right]$$

is the Picard-Vessiot ring associated with $L$, and that it is $\Delta$-simple.

The tensor product $P \otimes_K P$ is reduced.

Recall, also, the mapping $c$:

$$c : Gal(L/K) \to GL(n, C)$$
$$\sigma \mapsto c(\sigma) = \alpha^{-1} \sigma \alpha.$$ 

The image of $c$ is a closed subgroup of $GL(n, C)$. 

2
The defining ideal of \( c(G) \) is the kernel \( a \) of the surjective homomorphism
\[
C \left[ X, \frac{1}{\det X} \right] \longrightarrow C \left[ \gamma, \frac{1}{\det \gamma} \right], \quad X \mapsto \gamma, \quad \frac{1}{\det X} \mapsto \frac{1}{\det \gamma}
\]
where \( D = C \left[ \gamma, \frac{1}{\det \gamma} \right] = (P \otimes_K P)^\Delta \).

Let \( H \) be a subgroup of \( \text{Gal}(L/K) \).

\( H \) is closed if \( c(H) \) is closed.

Let \( M \) be an intermediate differential field. \( \text{Gal}(L/M) \) is a closed subgroup of \( \text{Gal}(L/K) \).

Let \( H \) be a closed subgroup of \( \text{Gal}(L/K) \).

\[
L^H = \{ a \in L : \forall \sigma \in H \quad \sigma a = a \}.
\]
Clearly, \( L^H \) is a \( \Delta \)-subfield of \( L \) containing \( K \).

We want to prove the following theorem:

**Theorem 1** Let \( \mathcal{I} = \mathcal{I}(L/K) \) be the set of intermediate differential fields, and order \( \mathcal{I} \) by inclusion.

Let \( \mathcal{G} \) be the set of closed subgroups of \( \text{Gal}(L/K) \), also ordered by inclusion.

Then, the maps
\[
\Phi : \mathcal{I} \rightarrow \mathcal{G}, \quad M \mapsto \text{Gal}(L/M)
\]
and
\[
\Psi : \mathcal{G} \rightarrow \mathcal{I}, \quad H \mapsto L^H,
\]
are inclusion reversing and inverse to one another.

Adam proved that a maximal \( \Delta \)-ideal is prime. We need a slightly more general result.

**Lemma 2** Let \( R \) be a \( \Delta-K \)-algebra, and let \( f \in R, \ f \neq 0 \).

1. Let \( \mathfrak{m} \) be a radical \( \Delta \)-ideal that is a maximal \( \Delta \)-ideal of \( R \) with respect to the exclusion of all non-negative powers of \( f \). Then, \( \mathfrak{m} \) is prime.
2. If \( R \) is finitely generated over \( K \), then \((qf(R/m))^\Delta = C\).

**Proof.** Set \( S = R/m \). Let \( \pi : R \to S \) be the quotient homomorphism.

Since \( m \) is radical, \( S \) is reduced. Thus, the multiplicative set in \( S \) generated by \( \pi(f) \) does not contain 0.

So, \( T = S_{\pi(f)} \) is not the 0 ring.

Let \( j : S \to T \) be the canonical homomorphism. We show that \( T \) is \( \Delta \)-simple.

\( S = R/m \). Let \( \pi : R \to S \) be the quotient homomorphism. \( T = S_{\pi(f)} \)

Let \( a \) be a proper nonzero \( \Delta \)-ideal of \( T \).

Let \( a_0 = j^{-1}(a) \). \( a = j(a_0) \cdot T \neq 0 \). Thus, \( a_0 \neq (0) \).

Therefore, \( \pi^{-1}(a_0) \) properly contains \( m \).

It follows that there exists a nonnegative integer \( e \) such that \( f^e \in \pi^{-1}(a_0) \).

Therefore, \( (\pi(f))^e \in a_0 \). So, \( 1 \in a = j(a_0) \cdot T \). Thus, \( T \) is \( \Delta \)-simple.

Since \( (0) \) is a maximal \( \Delta \)-ideal, it is prime, and, therefore \( T \) is an integral domain.

We now show that \( \ker j = (0) \). Suppose not.

Then, \( \pi^{-1}(\ker j) \) is a \( \Delta \)-ideal of \( R \) properly containing \( m \).

It follows that there exists a nonnegative integer \( e \) such that \( (\pi(f))^e \in \ker j \).

Therefore, \( 1 = 0 \) in \( T \).

So, \( j \) is injective, which implies that \( S \) is an integral domain, and \( m \) is prime.

This establishes the first statement.

If \( R \) is finitely generated over \( K \), then, so are \( S \) and \( T \).

Since \( T \) is \( \Delta \)-simple, \((qf(T))^\Delta = C \) (Jerry’s Talk I, Proposition 6).

Thus,

\[ C \subseteq (qf(S))^\Delta \subseteq (qf(T))^\Delta = C, \]

thus, establishing the second statement.
Lemma 3 (The existence of a moving automorphism) Let \( a \in L, a \notin K \).

Then, there exists \( \sigma \in \text{Gal} (L/K) \) with \( \sigma a \neq a \).

**Proof.** Write \( a = \frac{b}{c} \), with \( b, c \in P \), \( c \neq 0 \). Since \( a \notin K \), \( b \) and \( c \) are linearly independent over \( K \).

We complete \( \{b, c\} \) to a basis \( \Lambda \) of \( P \) over \( K \).

Then, \( \Lambda \otimes_K \Lambda \) is a basis of \( P \otimes_K P \) over \( K \). In particular, \( b \otimes c \) and \( c \otimes b \) are linearly independent over \( K \). In particular,

\[
f = b \otimes c - c \otimes b
\]

is not zero. By Lemma 16, \( P \otimes_K P \) is reduced. Therefore, no positive integer power of \( f \) is 0.

Let \( m \) be a radical \( \Delta \)-ideal of \( P \otimes_K P \) that is maximal among the \( \Delta \)-ideals excluding all non-negative powers of \( f \).

By Lemma 3, \( m \) is prime and

\[
S = (P \otimes_K P)/m
\]

has the property that

\[
(qf (S))^\Delta = C.
\]

Let

\[
j_1 : P \to P \otimes_K P \quad j_1(x) = x \otimes_K 1
\]

\[
j_2 : P \to P \otimes_K P \quad j_2(x) = 1 \otimes_K x
\]

and

\[
\pi : P \otimes_K P \to S
\]

be the canonical \( \Delta \)-K-homomorphisms. Note that

\[
j_1(\alpha) = \alpha \otimes_K 1
\]

\[
j_2(\alpha) = (\alpha \otimes_K 1) \gamma.
\]

Let \( k = 1, 2 \). Since \( P \) is \( \Delta \)-simple, the \( \Delta \)-K-homomorphism \( \pi \circ j_k \) is injective.

\( j = 1, 2 \).
Thus, \( \det (\pi (j_k(\alpha))) = \pi (j_k(\det \alpha)) \neq 0 \), and, therefore, \( \pi (j_k(\alpha)) \in GL(n, S) \). Also,

\[
(\pi (j_k(\alpha)))' = \pi (j_k(\alpha'))
= \pi (j_k(A\alpha))
= A\pi (j_k(\alpha)).
\]

So, both \( \pi (j_1(\alpha)) \) and \( \pi (j_2(\alpha)) \) are fundamental matrices for \( A \).

As a result, there exists a matrix \( d \in GL(n, S^\Delta) = GL(n, C) \) such that

\[
\pi (j_2(\alpha)) = \pi (j_1(\alpha)) d.
\]

It follows that

\[
\pi (j_1(P)) = \pi (j_2(P)) =: R.
\]

We now replace \( S \) with \( R \).

For \( k = 1, 2 \), \( \pi \circ j_k \) is a \( \Delta \)-\( K \)-isomorphism from \( P \) onto \( R \).

Therefore, we may define

\[
\sigma : P \to P, \quad \sigma = (\pi \circ j_1)^{-1} \circ (\pi \circ j_2).
\]

Clearly, \( \sigma \) is a \( \Delta \)-\( K \)-automorphism of \( P \), and, extends uniquely to an element of \( Gal(L/K) \).

\[
\sigma \alpha = (\pi \circ j_1)^{-1}(\pi(j_2(\alpha))
= (\pi \circ j_1)^{-1}(\pi(j_1(\alpha))d)
= \alpha d.
\]

In particular, \( d = c(\sigma) \).

We want to show that for

\[
a = \frac{b}{c},
\]

\( \sigma a \neq a \). Suppose \( a - \sigma a = 0 \). Then,

\[
0 = \frac{b}{c} - \frac{\sigma b}{\sigma c}
= b\sigma c - \sigma b
= (\pi \circ j_1)(b)(\pi \circ j_1)(\sigma c) - (\pi \circ j_1)(c)(\pi \circ j_1)(\sigma b)
= (\pi \circ j_1)(b)(\pi \circ j_2)(c) - (\pi \circ j_1)(c)(\pi \circ j_2)(b)
= \pi(b \otimes_K 1)\pi(1 \otimes_K c) - \pi(c \otimes_K 1)\pi(1 \otimes_K b)
= \pi(b \otimes_K c - c \otimes_K b)
= \pi(f).
\]

This contradicts the hypothesis that \( f \notin \ker \pi \). Therefore, \( \sigma a \neq a \).
\( \mathcal{I} \) is the set of intermediate Δ-fields of \( L/K \).

\( \mathfrak{G} \) is the set of closed subgroups of \( \text{Gal}(L/K) \).

\[
\Phi : \mathcal{I} \to \mathfrak{G}, \quad M \mapsto \text{Gal}(L/M)
\]

\[
\Psi : \mathfrak{G} \to \mathcal{I}, \quad H \mapsto L^H,
\]

**Lemma 4** Let \( M \in \mathcal{I} \). Then,

\[
\Psi(\Phi(M)) = M.
\]

**Proof.** We want to show: The fixed field of \( \text{Gal}(L/M) \) is \( M \).

Evidently,

\[
M \subseteq L^{\text{Gal}(L/M)}.
\]

By Lemma 4,

\[
L^{\text{Gal}(L/M)} \subseteq M.
\]

Thus, \( M = L^{\text{Gal}(L/M)} \). ■

\[
\sigma : P \otimes_K P \to P, \quad a \otimes_K b \mapsto a\sigma b.
\]

\[
\overline{\sigma \gamma} = \overline{\sigma}(\alpha^{-1} \otimes_K \alpha) = \alpha^{-1} \sigma \alpha = c(\sigma).
\]

Let \( a \) be the defining ideal in \( K \left[ X, \frac{1}{\det X} \right] \) of \( c(\text{Gal}(L/K)) \).

Let \( H \subseteq \text{Gal}(L/K) \) be a closed subgroup.

\( \exists \) a radical ideal \( b \supseteq a \) in \( C \left[ X, \frac{1}{\det X} \right] \) such that

\[
\sigma \in H \iff F(c(\sigma)) = 0 \quad \forall F \in b.
\]
Lemma 5 If $L^H = K$, then, $b = a$, i.e., $H = \text{Gal}(L/K)$.

**Proof.** Suppose $b \neq a$. Let $F \in b$, $F \notin a$. $F(\gamma) \in C\left[\gamma, \frac{1}{\det \gamma}\right] \subseteq P \otimes_K P$, and $F(\gamma) \neq 0$.

However, $\forall \sigma \in H$, since $F$ has coefficients in the fixed field $K$ of $H$,

$$\sigma(F(\gamma)) = F(\sigma \gamma) = F(\epsilon(\sigma)) = 0.$$ 

$F(\gamma) \in C\left[\gamma, \frac{1}{\det \gamma}\right] \subseteq P \otimes_K P$.

$F(\gamma) \neq 0$, but, $\forall \sigma \in H$, $\sigma(F(\gamma)) = 0$.

Let $w \in P \otimes_K P$. Write

$$w = \sum_{i=1}^{d} a_i \otimes_K b_i, \quad a_i, b_i \in P,$$

with $d$ smallest. Choose $w$ such that

1. $w \neq 0$, but, $\forall \sigma \in H$, $\sigma w = 0$.

2. No element of $P \otimes_K P$ satisfying 1 has a representation with less than $d$ terms as a sum of tensors.

In particular, $a_1, \ldots, a_d$ are linearly independent over $K$, as are $b_1, \ldots, b_d$.

Since $P \otimes_K 1$ and $1 \otimes_K P$ are linearly disjoint over $K$, it follows that

$$1 \otimes_K b_1, \ldots, 1 \otimes_K b_d$$

are linearly independent over $P \otimes_K 1$, and

$$a_1 \otimes_K 1, \ldots, a_d \otimes_K 1$$

are linearly independent over $1 \otimes_K P$.  

8
Let $\tau \in H$, and set

$$w_\tau = \sum_{i=1}^{d} \tau a_i \otimes_K b_i.$$ 

We claim that $w_\tau \neq 0$.

Suppose $w_\tau = 0$. Since $1 \otimes_K b_1, \ldots, 1 \otimes_K b_d$ are linearly independent over $P \otimes_K 1$,

$$0 = \tau a_1 = \cdots = \tau a_d.$$

Since $\tau$ is injective, $a_1 = \cdots = a_d = 0$.

So, $w_\tau \neq 0$. We now show that $\forall \sigma \in H$, $\sigma w_\tau = 0$.

$$\begin{align*}
\sigma w_\tau &= \sum_{i=1}^{d} \tau a_i \sigma b_i \\
&= \tau \left( \sum_{i=1}^{d} a_i \tau^{-1} \sigma b_i \right) \\
&= \tau \left( \tau^{-1} \sigma (w) \right) \\
&= \tau (0) \\
&= 0,
\end{align*}$$

since $\tau^{-1} \sigma \in H$. 

Let
\[
z_\tau = (a_d \otimes_K 1) w_\tau - (\tau a_d \otimes_K 1) w
\]
\[
= (a_d \otimes_K 1) \sum_{i=1}^{d} \tau a_i \otimes_K b_i - (\tau a_d \otimes_K 1) \sum_{i=1}^{d} a_i \otimes_K b_i
\]
\[
= \sum_{i=1}^{d} (a_d \tau a_i - \tau a_d a_i) \otimes_K b_i
\]
\[
= \sum_{i=1}^{d-1} (a_d \tau a_i - \tau a_d a_i) \otimes_K b_i.
\]
If \(z_\tau = 0\), then, for \(i = 1, \ldots, d-1\), \(a_d \tau a_i - \tau a_d a_i = 0\).

Suppose \(z_\tau = 0\).

For \(i = 1, \ldots, d-1\), \(a_d \tau a_i - \tau a_d a_i = 0\). Since \(a_d \neq 0\), we have
\[
\forall \tau \in H, \quad \tau \left( \frac{a_i}{a_d} \right) = \frac{a_i}{a_d}.
\]

Therefore, since the fixed field of \(H\) is \(K\), there exists \(f \in K\) such that
\[
a_d = fa_i.
\]

This contradicts the linear independence over \(K\) of \(a_1, \ldots, a_d\).

So, \(z_\tau \neq 0\). We now show that \(\forall \sigma \in H, \sigma z_\tau = 0\).

\[
\sigma z_\tau = (a_d \otimes_K 1) \sigma w_\tau - (\tau a_d \otimes_K 1) \sigma w
\]
\[
= (a_d \otimes_K 1) \cdot 0 - (\tau a_d \otimes_K 1) \cdot 0
\]
\[
= 0.
\]

This contradicts the choice of \(w\), and proves the lemma. ■

Lemma 6 If \(H \in \mathfrak{G}\), then, \(\Phi(\Psi(H)) = H\).

Proof. \(\Phi(\Psi(H)) = \text{Gal}(L/L^H)\). By Lemma 6, \(\text{Gal}(L/L^H) = H\). ■

This ends the proof of the fundamental theorem of Galois theory, Part I.
Corollary 7 Let $H$ be a subgroup of $\text{Gal}(L/K)$ such that the fixed field of $H$ is $K$. Then, $H$ is dense in $\text{Gal}(L/K)$.

Remark 8 In particular, $A \in M(n, \mathbb{C}(x))$, and, if the differential equation

$$y' = Ay$$

is Fuchsian, then, its monodromy group is dense in $\text{Gal}(L/K)$.

Theorem 9 (The Fundamental Theorem of Galois Theory, Part II) Let $L$ be a Picard-Vessiot extension of $K$.

1. Let $H \in \mathcal{G}$. Then, $H$ is a normal subgroup of $G = \text{Gal}(L/K)$ if and only if $\forall \sigma \in G$, $\sigma(L^H) \subseteq L^H$. If $H$ is a normal subgroup of $G$, the restriction map

$$G \to \text{Gal}(L^H/K) \quad \sigma \mapsto \sigma | L^H,$$

is surjective, and has kernel $H$. Moreover, $L^H$ is a Picard-Vessiot extension of $K$, and $\text{Gal}(L^H/K)$ is isomorphic to the quotient group $G/H$.

2. Let $G^0$ be the identity component of $G$. Then, $L^{G^0}$ is a finite Galois extension of $K$, and $\text{Gal}(L^{G^0}/K) \cong G/G^0$ is its algebraic Galois group.

Corollary 10 $\text{Gal}(L/K)$ is connected if and only if $K$ is algebraically closed in $L$. 
