Galois Theories of Commutative Rings and Differential Fields

by

Andy R. Magid

Theorem (Fundamental Theorem). *Let F be a field and let $E \supseteq F$ be a finite, normal, separable field extension. Let $G = Aut_F(E)$ be the group of field automorphisms of E fixing F. Then G is a finite group and there is a bijection between the the set of subgroups of G, and the set of subfields of E containing F, under which a subgroup H corresponds to the subfield E^H of E fixed element–wise by H and the subfield K corresponds to the subgroup $Aut_K(E)$of G which fixes each element of K.*

Theorem. *Let $E \supseteq F$ be a finite, normal, separable field extension. Let $G = Aut_F(E)$ and let $C(G, E)$ be the ring of E valued functions on G. Then the map*

$$\Phi : E \otimes_F E \to C(G, E) \qquad \text{by} \qquad \Phi(a \otimes b)(\sigma) = a\sigma(b)$$

is a ring ismorphism.

Consequently,

1. *$E^G = F$; and*

2. *If $H \leq G$ and $E^H = F$ then $H = G$*

Theorem (Fundamental Theorm in Tensor Product Form). *Let $E \supseteq F$ be a finite, normal, separable field extension. Then there is a bijection between the set of intermediate fields K between F and E, and the set of (isomorphism classes of) quotient E-algebras $E \otimes_F E \to B$ which satisfy*

$E \otimes_F E \to B$ factors through the multiplication map $E \otimes_F E \to E$

There is a (necessarily unique) map $\kappa : B \to B$ such that the following diagram commutes:

$$\begin{tikzcd}
E \otimes_F E \arrow[r, "i"] \arrow[d] & E \otimes_F E \arrow[d] \\
B \arrow[r, "\kappa"] & B
\end{tikzcd}$$

where i is induced from $a \otimes b \mapsto b \otimes a$;

There is a (necessarily unique) map $\Delta : B \to B \otimes_E B$ *such that the following diagram commutes:*

$$\begin{tikzcd}
E \otimes_F E \arrow[r, "D"] \arrow[d] & (E \otimes_F E) \otimes_E (E \otimes_F E) \arrow[d] \\
B \arrow[r, "\Delta"] & B \otimes_E B
\end{tikzcd}$$

where the top map D *is induced from* $a \otimes b \mapsto (a \otimes 1) \otimes (1 \otimes b)$*.*

The intermediate field K *leads to the quotient algebra* $E \otimes_K E$ *and the quotient algebra* B *leads to the field* K *which the kernel of the map* $\partial_B : E \to B$ *given by* $a \mapsto a \otimes 1 - 1 \otimes a$ *followed by the quotient map.*

Definition 1. *An* equivalence relation *on an object X in the category $\mathcal{S}$ of sets is a subobject of $X \times_{\mathfrak{f}} X$ represented by the injection $r : R \to X \times_{\mathfrak{f}} X$ plus maps d and t such that*

1. *The diagonal map $\Delta : X \to X \times_{\mathfrak{f}} X$ factors through $R \to X \times_{\mathfrak{f}} X$ via a map $d : X \to R$ with $rd = \Delta$ (reflexive)*

2. *If $\sigma : X \times_{\mathfrak{f}} X \to X \times_{\mathfrak{f}} X$ is the interchange of factors map, then both $\sigma r : R \to X \times_{\mathfrak{f}} X$ and $r : R \to X \times_{\mathfrak{f}} X$ represent the same subobject: that is, there is an isomorphism $s : R \to R$ such that $sr = \sigma r$ (symmetric)*

3. *If*

   $$\tau : (X \times_{\mathfrak{f}} X)X_{p_2,p_1}(X \times_{\mathfrak{f}} X) \to X \times_{\mathfrak{f}} X$$

   is the map induced from the morphisms

   $$X \times_{\mathfrak{f}} X \rightrightarrows X$$

by projection onto the factors, and

$(r, r) : R \times_{p_2 r, p_1 r} R \to (X \times_{\mathfrak{f}} X) X_{p_2, p_1} (X \times_{\mathfrak{f}} X)$

is the induced map on the fibre products then $R \to X \times_{\mathfrak{f}} X$ factors through $\tau(r, r)$ via a map

$$t : R \to R \times_{p_2 r, p_1 r} R$$

with $\tau(r, r)t = r$. (transitive)

Simplify: replace subobject map $r : R \to X \times_{\mathfrak{f}} X$ by the pair of maps $R \rightrightarrows X$ compose r with the projection p_i on the factors of the fibre product. Then the equivalence relation is a tuple

$$(R \rightrightarrows X, d : X \to R, s : R \to R, t : R \to R \times_{p_2 r, p_1 r} R).$$

Definition 2. *A* quotient X/R *of object* X *in the category* $\mathcal{S}$ *of sets by an equivalence* R *on* X *is a quotient object of* X *represented by a surjection* $p : X \to X/R$ *such that*

1. *The maps* $R \rightrightarrows X/R$ *by* pp_ir, $i = 1, 2$ *coincide.*

2. *If* $q : X \to Y$ *is any map such that* $qp_1r = qp_2r$ *then there is a map* $\overline{q} : X/R \to Y$ *such that* $q = \overline{q}p$.

$E \supseteq F$ is a field extension, equivalence relation on $\mathsf{Alg}_F(E,\cdot)$ is a subfunctor of

$$\mathsf{Alg}_F(E,\cdot) \times_{\mathfrak{f}} \mathsf{Alg}_F(E,\cdot) \cong \mathsf{Alg}_F(E \otimes_F E,\cdot)$$

Representable by an algebra B: given by surjection $E \otimes_F E \to B$ (specified by the pair of maps $E \rightrightarrows B$, using the injections $E \rightrightarrows E \otimes_F E$ of the tensor product)

The conditions the surjection must satisfy to give an equivalence relation then translate into maps and diagrams involving B, this pair of maps, and the maps $B \to E$ (corresponding to d), $B \to B$ (corresponding to s), and $B \otimes_E B \to B$ (corresponding to t). These maps, and the conditions they meet, are identical to the ones identified above in the tensor product form of the Fundamental Theorem (where the maps corresponding to s and t were termed κ and Δ respectively).

The quotient of the equivalence relation represented by B (if it exists) is a difference cokernel of $R \rightrightarrows X$; if it is representable, it would be represented by the difference kernel of the corresponding maps $E \rightrightarrows B$. The corresponding maps are induced by the injections into the tensor product followed by the projection on B and the difference kernel of these is precisely the kernel of the map ∂_B of the tensor product form of the Fundamental Theorem.

In other words, the Fundamental theorem in tensor product form, after passage to the category of set–valued functors, is precisely the (functorialized) correspondence between equivalence relations and quotients. Notice what has happened: the deep Fundamental Theorem of Galois Theory of Fields (in tensor product form) translates into the transparent correspondence between equivalence relations and quotients on sets.

F denotes a differential field of characteristic zero with derivation $D = D_F$ and algebraically closed field of constants C.

$E \supset F$ is a *Picard–Vessiot*, or *Differential Galois* extension for an order n monic linear homogeneous differential operator

$$L = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y^{(1)} + a_0 Y$$

$a_i \in F$ if

1. E is a differential field extension of F generated over F by $V = \{y \in E \mid L(y) = 0\}$

2. The constants of E are those of F ("no new constants")

3. $\dim_C(V) = n$ ("full set of solutions")

$E \supset F$ is an *infinite Picard–Vessiot extension* if it is a union of Picard–Vessiot extensions of F.

$\exists$ differential Galois theory for infinite Picard–Vessiot extensions due to Kovavcic: Pro-algebraic groups and the Galois theory of differential fields, *Amer. J. Math.* **95** (1973), pages 507–536.

Fundamental Theorem for Infinite Picard–Vessiot Extensions Let $E \supset F$ be an infinite Picard–Vessiot extension. Then $G = G(E/F)$ has a canonical structure of proaffine group and there is a one-one lattice inverting correspondence between differential subfields K, $E \supset K \supset F$, and Zariski closed subgroups H of G given by $K \mapsto G(E/K)$ and $H \mapsto K^H$. If K is itself an infinite Picard–Vessiot extension, then the restriction map $G \to G(K/F)$ is a surjection with kernel $G(E/K)$. If H is normal in G, then K^H is an infinite Picard–Vessiot extension.

Theorem 1. *There is an infinite Picard–Vessiot extension E_0 of F which contains an isomorphic copy of every Picard–Vessiot extension of F and is the unique (up to isomorphism) infinite Picard–Vessiot extension of F with this property.*

complete *Picard–Vessiot Compositum*

Differential automorphisms of the base field lift to differential automorphisms of a Picard–Vessiot compositum. The Picard–Vessiot compositum of F can have proper Picard–Vessiot extensions, and hence a proper Picard–Vessiot compositum.

$K_0 = F$

If K_i has a proper Picard–Vessiot extension, then $K_{i+1} \supset K_i$ is a Picard–Vessiot compositum. (The chain $K_0 \subset K_1 \subset \ldots$ may be finite or infinite.)

Let K_∞ denote the union of the chain whether it is finite or infinite.

G_i, $i \leq \infty$, denotes the group of differential automorphisms of K_i over F

K_∞ has no proper Picard–Vessiot extensions.

G_∞ is differential automorphisms of K_∞ over F.

$G_\infty = \varprojlim G_i$, with the projection maps p_i : $G_\infty \to G_i$ surjective and given by restriction.

For $i < \infty$, the kernel of $G_{i+1} \to G_i$ is proaffine proalgebraic.

$\{e\} = \mathrm{Ker}(p_{i,i}) \subset \mathrm{Ker}(p_{i,i-1}) \cdots \subset \mathrm{Ker}(p_{i,0}) = G_i$ is normal series for G_i with proaffine proalgebraic layers.

EXAMPLES SHOW THAT THE GROUPS G_i NEED NOT THEMSELVES, HOWEVER, BE PROALGEBRAIC.

An element y of a differential extension $E \supset F$ will be called an *antiderivative* if $y' \in F$. $E \supset F$ will be called an *antiderivative extension* if there are elements $y_1, \ldots, y_n$ in E which differentially generate E over F and such that each y_i' belongs to the differential field generated over F by $y_1, \ldots, y_{i-1}$. If $n = 1$, the antiderivative extension will be called *simple*.

Facts: an antiderivative extension is generated as a field, and not just as a differential field, by the elements $y_1, \ldots, y_n$; a proper simple antiderivative extension without new constants is a Picard–Vessiot extension with differential Galois group the additive group $\mathbb{G}_a$; and therefore any antiderivative extension without new constants is a tower of $\mathbb{G}_a$ Picard–Vessiot extensions.

An antiderivative extension $K \supset F$ with no new constants is a Liouville extension and any Picard–Vessiot extension $E \supset F$ which embeds in $K \supset F$ is then seen to be itself an antiderivative extension with unipotent differntial Galois group. Conversely, a Picard–Vessiot extension with unipotent differential Galois group is seen to be an antiderivative extension, so that "Picard–Vessiott antiderivative extension" is the same as "differential Galois with unipotent differential Galois group".

Complete Picard–Vessiot antiderivative composita: an infinite Picard–Vessiot extension $K_0 \supset F$ such that K_0 is the union of its Picard–Vessiot subextensions with unipotent differential Galois group, and K_0 contains a copy of every Picard–Vessiot antiderivative extension of F.

Picard-Vessiot Antiderivative Closure (abbreviation: *PVAC*) of F.

Theorem 2. *let $E_0 \supset F$ be a complete Picard–Vessiot compositum, and let H be the minimal closed normal subgroup of $G(E_0/F)$ such that $G(E_0/F)/H$ is prounipotent. Then $K_0 = E_0^H$ is a Picard–Vessiot antiderivative closure of F, and any Picard–Vessiot antiderivative closure of F is isomorphic to K_0. If σ is any differential automorphism of F, there is a differential automorphism Σ of K_0 whose restriction to F is σ.*

Suppose that $K \supset F$ is a Picard–Vessiot antiderivative extension and

$$1 \to \mathbb{G}_a \to G \to G(K/F) \to 1$$

is an extension of unipotent groups. If there is a Picard–Vessiot extension $E \supset F$ containing K such that $G(E/F)$ is isomorphic to G so that the restriction $G(E/F) \to G(K/F)$ is equivalent to the given map $G \to G(K/F)$ then we will say that E *solves the lifting problem* for $G \to G(K/F)$. F has the *lifting property* with respect to extensions of unipotents by $\mathbb{G}_a$ (or just lifting property) if every lifting problem has a solution.

Theorem 3. $\mathbb{C}(t)$ *has the lifting property with respect to extensions of unipotents.*

$\mathbb{C}(t)$ has the further property that every unipotent algebraic group over $\mathbb{C}$, in fact every connected algebraic group, appears as the differential Galois group of a Picard–Vessiot extension of $\mathbb{C}(t)$. A field F with this property is said to have the *(unipotent) inverse Galois property*.

If F is any field with the lifting property, by taking a Picard–Vessiot antiderivative closure $E_0 \supset F$ and applying the Fundamental Theorem to $G(E_0/F)$ we can conclude a lifting property for this prounipotent group:

Proposition 1. *Let F have the lifting property with respect to prounipotent extensions. Let E_0 be a Picard–Vessiot antiderivative closure of F. Suppose that*

$$1 \to \mathbb{G}_a \to G \to \overline{G} \to 1$$

is an exact sequence of unipotent groups. In addition, suppose there is a surjection $G(E_0/F) \to \overline{G}$. Then it lifts to a homomorphism $G(E_0/F) \to G$.

Proposition 2. *Let U be a prounipotent group over the algebraically closed characteristic zero field k, and suppose that for every extension of k unipotent groups*

$$1 \to \mathbb{G}_a \to G \to \overline{G} \to 1$$

such that there is a surjection $U \to \overline{G}$ there is a lifting of the surjection to $U \to G$. Then U is free prounipotent.

Theorem 4. *Let E_0 be a Picard–Vessiot antiderivative closure of the rational function field $F = \mathbb{C}(t)$. then the differential Galois group $G(E_0/F)$ is a free prounipotent group.*

Defined groups H_i for the tower of Picard–Vessiot antiderivative closures of $\mathbb{C}(t)$.

EPIMORPHISM $H_2 \to H_1$ DOESN'T SPLIT!