Galois embedding of algebraic variety and some of its application

Hisao YOSHIHARA

Niigata University

October 24, 2017

The purpose of this talk is

1. to introduce the notion of Galois embedding
2. and to show its application to curves and surfaces.

Preliminary remark 1

First I explain a preliminary remark.
I have been having an interest in field theory. Suppose K is a field finitely generated over a field k. If the extension K/k is algebraic, then there are effective methods for the study, for example, degree, Galois theory etc. However if not, then there are no suitable ones (I think). How to study the extension K/k? We take a purely transcendental extension as starting point. Let n be the transcendental degree. In this case, we pay attention to a maximal rational subfield K_m, which has the following properties:

Preliminary remark 2

The properties are

1. K_m is an intermediate field between K and k,
2. and purely trans. ext. of k with the trans. degree n,
3. there is no field between K and K_m.
   Then, we consider the algebraic extension K/K_m
   However, there is an inconvenient point.
   In fact, even if $n = 1$ and $K = k(x)$, there are many maximal rational subfields:
   $k(x^2),\ k(x^3), \ldots,\ k(x^p), \ldots$ (p is a prime number)

Preliminary remark 3

So, we use the notion: the degree of irrationality, which is defined as follows:
$\min \{ \ [K : K_m] \ | \ K_m$ is a maximal rational subfield. $\}$
We denote this number by $\mathrm{irr}(K/k)$ or $\mathrm{irr}(K)$.
Clearly this number is a birational invariant.
K is rational if and only if $\mathrm{irr}(K) = 1$.
Maximal rational subfield F with $[K : F] = \mathrm{irr}(K)$ is called g-maximal rational subfield.
For example, for the elliptic function field
$k(x, y), \ y^2 = x^3 + ax + b, \ 4a^3 + 27b^2 \neq 0$
$\mathrm{irr}(k(x, y)) = 2$ and $k(x)$ is a g-maximal rational subfield,
$k(y)$ is a maximal rational field but not a g-maximal one.

Preliminary remark 4

By the way, $\mathrm{irr}(k(x,y)) \neq 1$ is closely connected with the integrabillity $\int y\, dx$, where $f(x,y) = 0$ and $f(x,y) \in k[x,y]$.
If $x^2 + y^2 = 1$, then $\mathrm{irr}(k(x,y)) = 1$ and

$$\int \frac{1}{\sqrt{1-x^2}}\, dx = \sin^{-1} x$$

However, if $x^3 + y^2 = 1$, then $\mathrm{irr}(k(x,y)) = 2$ and

$$\int \frac{1}{\sqrt{1-x^3}}\, dx$$

cannot be expressed by elementary functions.
It needs higher functions, elliptic functions.

Preliminary remark 5

I mention one more fact
An extension L/K corresponds to a surjective morphism
$f : V \longrightarrow W$,
where V and W are algebraic varieties
with function fields L and K, respectively.
If the extension is algebraic, then the morphism is a covering.
Moreover, if the extension is Galois, then the covering is Galois.
So, we can ”see” field extension by the mapping between varieties.
For example, for the elliptic function field $k(x, y)$, the extension $k(x, y)/k(x)$ corresponds to
the double covering $E \longrightarrow \mathbb{P}^1$, where E is an elliptic curve.

Preliminary remark 6

I explain the motive of this research.
Roughly speaking, algebraic variety is a realization of algebra.
Commutative ring R is nothing but the scheme Spec(R).
So, we can study algebra by variety, and vice versa.
Let's look at an example (Lüroth Theorem)
Let k be an infinite field and x transcendental over k,
If F is a subfield of $k(x)$ and is trans. over k, then F is also a purely trans. extension of k.
The proof is rather complicated if we use algebra.

Preliminary remark 7

However, if we use geometry, the proof is very clear.
We have only to consider the regular 1-form.
By the way, the similar assertion for two dimensional case, which is called Castelnuovo-Enriques Theorem, is too hard to to prove by only algebra.
It can be proved by using the criterion of rationality of algebraic surface S:
$\mathrm{H}^0(S,\ \mathcal{O}(2K_S)) = \mathrm{H}^1(S,\ \mathcal{O}) = 0$

Galois Point 1

Example

Before proceeding to the definition, we mention the notion of Galois point for plane curve.
The notion of Galois embedding is a generalization of Galois point.
Let k be a ground field, which is assumed to be an algebraically closed field with characteristic zero.
Let C be a smooth plane curve of degree d.
Take a point $P \in \mathbb{P}^2$ and consider the projection π_P from P to $\mathbb{P}^1$, i.e., $\pi_P : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$.
Restricting π_P onto C, we get a surjective morphism $\pi : C \longrightarrow \mathbb{P}^1$.

Galois Point 2

Example

This induces an extension of fields $k(C)/k(\pi^*(\mathbb{P}^1))$ of degree $d-1$ or d, corresponding to $P \in C$ and $P \notin C$, respectively.
We notice that $k(\pi^*(\mathbb{P}^1))$ is a maximal rational subfield.
If we take P in C, then $k(\pi^*(\mathbb{P}^1))$ becomes a g-maximal rational subfield.
If the extension is Galois, we call P is a Galois point,
or if the covering $\pi : C \longrightarrow \mathbb{P}^1$ is Galois, so is called P.
Such a point is a very special one.
If we take a general point for C, then it is not a Galois point.
If P is a Galois point, then the Galois group Gal$(k(C)/k(\mathbb{P}^1))$ is the cyclic group of order $d-1$ or d.

Galois Point 3

Example

If P is a general point, then the Galois group of the Galois closure is a full symmetric group.
In general it is difficult to determine the Galois group.
Note that in case k has a positive characteristic, there are big differences in the results.

Galois embedding 1

Now we treat varieties not necessarily in the projective spaces.
I make preparations for the definition.
k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) \geq 0$
later we will assume $k = \mathbb{C}$.
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding assoc. with $|D|$
where $N + 1 = \dim \mathrm{H}^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$ s.t.
$\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow \mathbb{P}^n$: projection with the center W

Galois embedding 2

$\pi = \pi_W \cdot f : V \longrightarrow \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(\mathbb{P}^n)$: function field of $\mathbb{P}^n$
$\pi^* : K_0 \hookrightarrow K$: finite extension, $d := \deg \pi^* = \deg f(V) = D^n$
The structure of this extension depends on W.
K_W : Galois closure of K/K_0 (in case separable ext.)
$G_W := \mathrm{Gal}(K_W/K_0)$
V_W : K_W-normalization of V

Galois embedding 3

Definition

We call G_W the Galois group at W
and V_W the Galois closure variety at W.
If K/K_0 is Galois,
we call f and W a Galois embedding and Galois subspace respectively.
In case $\dim W = 0$ and 1
W is said to be a Galois point and line, respectively.

Galois embedding 4

Definition

V is said to have a Galois embedding
if there exists a very ample divisor D
s.t. the embedding assoc. with $|D|$ has a Galois subspace.

In this case we say that (V, D) defines a Galois embedding.

Remark

It may happen that there exist several Galois subspaces for $f_D(V)$.

Remark

Remark

G_W is isomorphic to the monodromy group of the covering $\pi : V \longrightarrow \mathbb{P}^n$.

Remark

If W is general for $f_D(V)$, then G_W is isomorphic to the full symmetric group of degree d.

So, we consider for non-general W.

Basic result 1

Hereafter we assume W is a Galois subspace.

Proposition

There exists an injective representation $\alpha : G_W \hookrightarrow Aut(V)$.

Corollary

If $Aut(V)$ *is trivial, then* V *has no Galois embedding.*

Proposition

We have another injective representation $\beta : G_W \hookrightarrow PGL(N, k)$.

Basic result 2

Proposition

We have $V/G_W \cong \mathbb{P}^n$.
The projection $\pi : V \longrightarrow \mathbb{P}^n$ *turns out a finite morphism.*
In particular, the fixed loci of G_W *consists of divisors.*

Criterion

Theorem

(V, D) defines a Galois embedding iff

1. *There exists a subgroup G of $\mathrm{Aut}(V)$ with $|G| = D^n$.*
2. *There exists a G-invariant linear subspace $\mathcal{L}$ of $\mathrm{H}^0(V, \mathcal{O}(D))$ of dimension $n+1$ such that, for any $\sigma \in G$, the restriction $\sigma^*|_{\mathcal{L}}$ is a multiple of the identity.*
3. *The linear system $\mathcal{L}$ has no base points.*

Problem

There are lots of problems, let's take up typical ones:

Problem

1. *Find the structure of* G_W.
2. *How is the structure of* V *which has a Galois embedding?*
3. *How is the divisor class of* D *which defines a Galois embedding?*
4. *Find the arrangement of Galois subspaces for* $f(V)$.
5. *What is the Galois closure variety* V_W?

Example 1

Example

Let us examine the Galois embedding for elliptic curves E:
(i) $\deg D = 3$ case:
E has a Galois embedding iff $j(E) = 0$.
$G \cong Z_3$, there exists three Galois points.
In other words, let C be a smooth plane cubic.
Assume $P \in \mathbb{P}^2 \setminus C$ and consider the projection π with the center P to $\mathbb{P}^1$.
Then, π induces a Galois extension $k(C)/k(\pi^*(\mathbb{P}^1))$, or Galois covering
$\pi|_C : C \longrightarrow \mathbb{P}^1$ iff P is a Galois point.

Example 2

Example

The C has a Galois point iff $j(C) = 0$,
it is projectively equivalent to the Fermat cubic :
$X^3 + Y^3 + Z^3 = 0$.
There are three Galois points: $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$.
If we use Weierstrass normal form, C is given by
$Y^2Z = 4X^3 + Z^3$ and
the Galois points are $(1; 0 : 0)$, $(0 : \sqrt{-3} : 1)$
and $(0 : -\sqrt{-3} : 1)$

Example 3

Example

(ii) $\deg D = 4$ case:

$|D|$ defines always a Galois embedding.

$f_D(E) = C \subset \mathbb{P}^3$ has six Galois lines

the six lines form a tetrahedron (as in the next page):

$G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

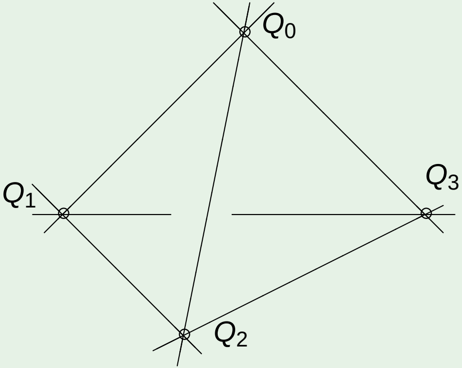
If $j(E) = 12^3$, there exist eight Z_4-lines in addition.

In this case the arrangement of Galois lines is very complicated.

Galois lines

Example

Galois lines for a space elliptic curve ($j(E) \neq 12^3$).



Example 4

Example

In other words, let C be a smooth genus-one curve in the projective three space $\mathbb{P}^3$.
Then C has 6 Galois lines ℓ_i $(i = 1, \ldots, 6)$
i.e., the projection with the center ℓ_i to $\mathbb{P}^1$
induces a Galois covering $C \longrightarrow \mathbb{P}^1$
with the Galois group G.
(iii) If $\deg D = 5$, E has no Galois embeddings.
(iv) For any $\deg D$, we can find the possibility of G,
however it is difficult to determine the arrangement of Galois subspaces.

Example 5

Example

Abelian variety of dimension two is called abelian surface.
Suppose an abelian surface A has a Galois embedding.
Then, we can find all possible analytic representations of G.
in particular,

they are not commutative,

A is isogenous to $E \times E$.

The least number N such that A has a Galois embedding into $\mathbb{P}^N$ is seven.

All such surfaces can be determined.

PS

For the details, please refer to
J. Algebra 226, 239, 264, 287, 320, 321, 323 and others listed in our website
http://hyoshihara.web.fc2.com/
In this site about 70 open questions are asked.