# Crash course in Galois theory (continued...)

Let $\mathbb{E}/\mathbb{F}$ be a field extension of degree $d$. By finite dimensionality, one can show that

$$\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n) \quad \mathbb{F}\text{-rational expressions}$$
$$= \mathbb{F}[\alpha_1, \ldots, \alpha_n] \quad \mathbb{F}\text{-polynomial expressions.}$$

We say that $\mathbb{E}/\mathbb{F}$ is <u>normal</u> if the polynomial

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in \mathbb{E}[x]$$

actually has coefficients in $\mathbb{F}$, i.e., the following elements of $\mathbb{E}$ are actually in $\mathbb{F}$:

$$e_1 = \alpha_1 + \cdots + \alpha_n,$$
$$e_2 = \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n,$$
$$\vdots$$
$$e_n = \alpha_1\alpha_2\cdots\alpha_n.$$

[In this case we say that $\mathbb{E}$ is a (or the) splitting field of $f(x) \in \mathbb{F}[x]$.]

Now let $G = Gal(\mathbb{E}/\mathbb{F})$ be the group of ring automorphisms $\varphi: \mathbb{E} \to \mathbb{E}$ fixing the elements of $\mathbb{F}$ (i.e., $\varphi(a) = a$ for all $a \in \mathbb{F}$).

Note that $G$ acts on the set of generators $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ i.e. the set of roots of $f(x)$. Indeed since $f(x)$ has coefficients in $\mathbb{F}$ we have

$$\varphi(f(\beta)) = f(\varphi(\beta)) \text{ for all } \beta \in \mathbb{E},$$

so that for any $i$ we have

$$f(\alpha_i) = 0$$

$$\varphi(f(\alpha_i)) = \varphi(0)$$

$$f(\varphi(\alpha_i)) = 0$$

$$\Longrightarrow \varphi(\alpha_i) = \alpha_j$$

for some $j$.

Now we have an important theorem.

Arithmetic Connectedness Theorem:

If $f$ is an irreducible polynomial then $G$ acts transitively on the roots $\alpha_1, \dots, \alpha_n$.

Proof: Suppose not, i.e., suppose that there is a $G$-orbit not equal to the full set $\{\alpha_1, \dots, \alpha_n\}$.

Say: $\{\varphi(\alpha_1) : \varphi \in G\} = \{\alpha_1, \dots, \alpha_m\}$

for some $m < n$. Now define

$$g(x) = (x-\alpha_1)\cdots(x-\alpha_m) \in \mathbb{E}[x]$$

$$h(x) = (x-\alpha_{m+1})\cdots(x-\alpha_n) \in \mathbb{E}[x],$$

and note that $f(x) = g(x)h(x)$.

If we can show that in fact

$$g(x), h(x) \in \mathbb{F}[x]$$

then we will have the desired contradiction.

Expand $g(x) = x^m - a_1 x^{m-1} + \cdots \pm a_m$

where $a_1 = \alpha_1 + \cdots + \alpha_m$,

$\vdots$

$a_m = \alpha_1 \alpha_2 \cdots \alpha_m$.

By assumption, each coefficient $a_i$ is fixed by each element of $G$.

So what?

Now the hard part:

One can show that $\mathbb{E}^G = \mathbb{F}$, where

$$\mathbb{E}^G := \{ \alpha \in \mathbb{E} : \varphi(\alpha) = \alpha \ \forall \ \varphi \in G \}$$

and it follows that $a_1, \cdots, a_m \in \mathbb{F}$, hence $g(x) \in \mathbb{F}[x]$ as desired.

Similarly, $h(x) \in \mathbb{F}[x]$. //

Remark: The statement $\mathbb{E}^G = \mathbb{F}$ is hard to prove. Indeed, I wasted several hours today trying to find a nice proof that would fit in one lecture. Oh well...

[Galois is famous for a reason!]

What does Galois theory have to do with algebraic curves?

Analytic Connectedness Theorem:

IF $f(x,y) \in \mathbb{C}[x,y]$ is irreducible then the curve $C = V(f) \subseteq \mathbb{C}^2$ is connected in the usual topology (i.e. the Euclidean topology on $\mathbb{C}^2 = \mathbb{R}^4$.)

[I will follow the ideas from Griffiths, Intro. to Alg. Curves.]

Start: Recall that the projection

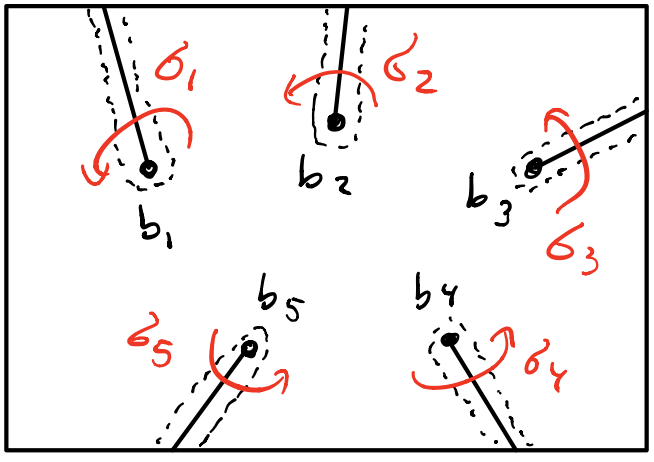
$$\begin{aligned} C &\longrightarrow \mathbb{C} \\ (x,y) &\longmapsto x \end{aligned}$$

has finitely many brach points:

$$\Delta(\pi) = \{x \in \mathbb{C} : \#\pi^{-1}(x) < d\}$$
$$= \{b_1, b_2, \ldots, b_r\}$$

Choose non-intersecting rays from the branch points to $\infty$, and delete them:

$\mathbb{C}' =$



Above each point $x \in \mathbb{C} - \Delta$ there are $d$ distinct points

$$p_i = (x, y_i) \in C, \quad i = 1, \dots, d.$$

And each complex number $y_i(x) \in \mathbb{C}$ is locally a holomorphic function of $x$. Since $\mathbb{C}'$ is simply-connected, it is a standard fact ("Riemann's monodromy theorem") that each germ $y_i(x)$ extends uniquely to a holomorphic function $y_i : \mathbb{C}' \to \mathbb{C}$.

Next we consider how the curve is connected. Fix basepoint $x_0 \in \mathbb{C}$ and a labeling $y_1(x_0), \dots, y_d(x_0)$. The curve $C - \pi^{-1}(\text{rays})$ decomposes into $d$ sheets, $\mathbb{C}_1', \mathbb{C}_2', \dots, \mathbb{C}_d'$, with $(x_0, y_i(x_0)) \in \mathbb{C}_i'$, each

biholomorphic to $\mathbb{C}'$. We can describe how the sheets are connected at the cuts by giving $r$ permutations $\sigma_1, \sigma_2, \ldots, \sigma_r \in S_d$:

If we start at a point on $\mathbb{C}_i'$ and proceed counterclockwise around $b_j$ then we end up on the sheet $\mathbb{C}'_{\sigma_j(i)}$.

Consider the function $y_i : \mathbb{C}_i' \to \mathbb{C}$. If we analytically continue $y_i$ across the $j$th branch cut onto the $\sigma_j(i)$th branch then $y_i$ becomes $y_{\sigma_j(i)}$.

[Indeed, the property $f(x, y_i(x)) = 0$ is preserved by small movements of $x$.]

Let $G = \langle \sigma_1, \sigma_2, \ldots, \sigma_r \rangle \subseteq S_d$ be the group generated by the permutations.

Idea: $G$ is the "Galois group" of the covering space $\pi : C \to \mathbb{C}$.

Observe: $C$ is connected $\Leftrightarrow$ $G$ acts transitively on the sheets.

We will use these ideas to show that the curve is connected.

Proof: Given that $f(x,y) \in \mathbb{C}[x,y]$ is irreducible. Assume for cont. that the curve $C$ is not connected, i.e., $\exists$ a $G$-orbit of sheets that is not the full set of sheets.

Say: $\{\varphi(C_1') : \varphi \in G\} = \{C_1', \dots, C_m'\}$ with $m < d$. For each fixed $x$ in $\mathbb{C}'$ we will define

$$g(x,y) = (y - y_1(x)) \cdots (y - y_m(x)) \in \mathbb{C}[y]$$

$$h(x,y) = (y - y_{m+1}(x)) \cdots (y - y_d(x)) \in \mathbb{C}[y].$$

so that

$$F(x,y) = g(x,y)h(x,y) \in \mathbb{C}[y].$$

As $x$ varies, we know that the coefficients of $F(x,y)$ are polynomial functions of $x$, hence $F(x,y) \in \mathbb{C}[x,y]$.

What about the coefficients of

$$g(x,y), h(x,y) \in \mathbb{C}[y] \; ?$$

By assumption, $G$ permutes the coefficients of $g, h \in \mathbb{C}[y]$, so that the coefficients extend uniquely to holomorphic functions

$$\mathbb{C} - \Delta \to \mathbb{C},$$

i.e. the coefficients are well-defined on the branch cuts.

Now the Hard Part!

If we can show that each coefficient is actually a polynomial function

then we will have

$$f(x,y) = g(x,y)\,h(x,y)$$

with $g, h \in \mathbb{C}[x,y]$, contradicting the fact that $f$ is irreducible.

To see this, note that each coefficient is holomorphic on the non-simply-connected domain $\mathbb{C} - \Delta$.

- Since each coefficient is bounded near each point of $\Delta$, it extends uniquely ("Riemann extension") to a holomorphic function $\mathbb{C} \to \mathbb{C}$.

- Since each coefficient has "polynomial growth" it must in fact be a polynomial.

QED

[ Concept of a "meromorphic function"... ]