Roots of topology

Tobias Shin

Abstract

These are notes for a talk in the Graduate Student Seminar at Stony Brook. We discuss polynomials, covering spaces, and Galois theory, and how they all relate through the unifying concept of "resolvent degree", following Farb and Wolfson[1]. We will also see how this concept relates Hilbert's 13th problem (among others) to classical enumerative problems in algebraic geometry, such as 27 lines on a smooth cubic, 28 bitangents on a planar quartic, etc.

Algebraic functions and roots of topology

First, a historial note: the motivation for the concept of the fundamental group comes from studying differential equations on the complex plane (i.e., the theory of Riemann surfaces); namely, in the study of the monodromy of multi-valued complex functions. Consider for example, the path integral $\int 1/z$ around the punctured plane. This is nonzero and in fact, its value changes by multiples of $2\pi i$ based on how many times you wind around the puncture. This behavior arises since the path integral of this particular function is multivalued; it is only well defined as a function up to branch cuts. In a similar spirit, we can consider the function $\sqrt{z}$ which, as we go around the punctured plane once, sends a specified value to its negative.

More specifically, suppose we have a *branched covering space* $\pi : Y \to X$, i.e., a map and a pair of spaces such that away from a nowhere dense subset of X, called the *branched locus of* X, we have that π is a covering map. Given such a branched covering, we can define a *monodromy action* of the fundamental group on the fiber as follows: fix a basepoint $x \in X - X^{br}$ away from the branched locus, a point $\tilde{x}$ in the fiber over x, and a loop γ based at x. Lift the loop to a path in the covering and consider its endpoint, which is generally another point in the fiber, denoted $\gamma \cdot \tilde{x}$. This describes an action of $\pi_1(X - X^{br}, x)$ on the fiber of the branched cover away from the branched locus, as in ordinary covering space theory. The image of the homomorphism $\pi_1(X - X^{br}, x) \to S_n$ where S_n denotes the symmetric group on n points, acting on the n points of the fiber, is called the *monodromy group*. We allow n to be infinite. The idea is that the fundamental group is *permuting* the points of the fiber.

Example. For the path integral $\int 1/z$ above, we have the (genuine) cover $\pi : \widetilde{\mathbb{C}^*} \to \mathbb{C}^*$ where π is vertical projection, visualized as projecting an infinite helicoid sitting above the punctured plane, obtained from gluing along all the different branch cuts of the logarithm. As one winds once around a loop, one returns to the fiber but by an addition of $2\pi i$. Since this is an action on the universal cover, the action is free. The monodromy group in this example is then precisely $\mathbb{Z}$.

Example. For the function $\sqrt{z}$, we can consider the function $z \mapsto z^2$, viewed as a branching of $\mathbb{CP}^1 \to \mathbb{CP}^1$ with 0 and ∞ as its two branch points. Thus, removing the two points, we have a two-fold covering map $\mathbb{C}^* \to \mathbb{C}^*$. The monodromy representation is then a homomorphism $\mathbb{Z} \to \mathbb{Z}/2$. As observed above, the action is nontrivial; winding around a loop sends a point in the fiber to the other point in the fiber. The monodromy group is then precisely $\mathbb{Z}/2$.

Example. One can also check that the monodromy group of $\mathbb{CP}^1 \xrightarrow{z \mapsto z^d} \mathbb{CP}^1$ is $\mathbb{Z}/d$. This is due to the fact that the action merely multiplies by the d-th roots of unity.

The above analysis regarding $\sqrt{z}$ also shows that one *cannot globally find a section of the branched cover* $\mathbb{CP}^1 \xrightarrow{z \mapsto z^2} \mathbb{CP}^1$. This would be tantamount to expressing $\sqrt{z}$ globally on $\mathbb{C}$; one can also prove this by looking at the induced maps on the fundamental groups; if there were a global section, we would have that the induced map of the covering surjects onto the fundamental group of the base. But the map is exactly $1 \mapsto 2$ from $\mathbb{Z}$ to $\mathbb{Z}$.

The problem of determining when a given branched cover has a global section or not has its roots in classical algebraic geometry, although often not explicitly so. For example, suppose given a polynomial, we want to find its roots. We can reformulate this in terms of covers: define Roots_n as ordered tuples of complex numbers in $\mathbb{C}$, i.e. $\mathbb{C}^n$, and define Poly_n as monic polynomials, i.e., ordered tuples of complex numbers $(a_1, ..., a_n)$ where the a_i represent the *coefficients* of the polynomial $z^n + a_1 z^{n-1} + ... + a_n$, which is also equal to $\mathbb{C}^n$. So far, nothing seems interesting.

However, consider the following *Viete map* $\Phi : \text{Roots}_n \to \text{Poly}_n$ sending the tuple $(r_1, ..., r_n)$ to $(-\sum r_i, \sum r_i r_j, ..., (-1)^n r_1 ... r_n)$ i.e., we send the roots of a polynomial to that polynomial using the fact that the coefficients of a given polynomial are *the elementary symmetric functions in the roots*. Since the Viete map is defined in terms of symmetric functions, it is S_n-equivariant and so descends to a map $\mathbb{C}^n/S_n \to \mathbb{C}^n$. This map is actually an isomorphism of algebraic varieties (note this is not true for $\mathbb{R}$). After identifying Poly_n with $\mathbb{C}^n/S_n$ we see that the Viete map $\Phi : \text{Roots}_n \simeq \mathbb{C}^n \to \text{Poly}_n \simeq \mathbb{C}^n/S_n$ is an $n!$-sheeted branched covering map, where the branching locus is exactly the set of polynomials with *multiple roots*, called the *discriminant locus*. A fiber away from the branching locus will exactly be all $n!$ permutations of the n distinct roots; a fiber over the branching locus will have fewer permutations, depending on the multiplicity of the roots. The Viete map is exactly a covering away from the branched locus, as the determinant of its Jacobian is exactly Δ_n^2 where $\Delta_n(a_1, ..., a_n)$ is the discriminant for a degree n polynomial, which vanishes iff there is a multiple root. In general, there is no global section for this branched cover; it is difficult to find the roots of a given generic polynomial, based on its coefficients alone.

To make things simpler, we can consider an intermediate covering $\text{Roots}_n \to \widetilde{\text{Poly}_n} \to \text{Poly}_n$ where $\widetilde{\text{Poly}_n}$ denotes all pairs (p, λ) where p is a polynomial and λ is one of its roots, and the map from Roots_n equips the polynomial with whichever root is in the first coordinate, i.e., sends the tuple $(r_1, ..., r_n)$ to $((-\sum r_i, \sum r_i r_j, ..., (-1)^n r_1 ... r_n), r_1)$. The map $\widetilde{\text{Poly}_n} \to \text{Poly}_n$ where one simply forgets the root is a n-sheeted branched covering, where the n points in a generic fiber are precisely the n distinct roots.

Although generally we may not be able to find a global section, we may still be able to express the solutions of a polynomial in terms of *radicals* of the coefficients of the polynomial. This would be equivalent to finding a *tower* of branched coverings of our given branched cover, such that we know roughly that each piece in the tower behaves "like" the map $z \mapsto z^d$ above. We would formalize this in the sense of pullbacks of branched coverings. This motivates the following definition:

Definition. *We say that we can* solve an arbitrary degree n polynomial in radicals *if there is a tower of branched covers* $X_r \to ... \to X_0 \subset \text{Poly}_n$ *such that* X_0 *is open and dense, and* $X_r \to \text{Poly}_n$ *factors through a branched covering* $X_r \to \widetilde{\text{Poly}_n}$ *and where each* $X_{i+1} \to X_i$ *is a pullback from a branched covering* $\mathbb{CP}^1 \xrightarrow{z \mapsto z^{d_i}} \mathbb{CP}^1$*, with the* X_i*'s complex algebraic varieties.*

The fact that we are pulling back from $\mathbb{CP}^1$, a 1-dimensional complex variety, means solving by radicals is a process involving only 1 parameter at a time.

Example. Let us construct such a tower for $\widetilde{\mathrm{Poly}_2} \to \mathrm{Poly}_2$. Let $X_0 = \mathrm{Poly}_2$ and let $X_1 = \{(b, c, \delta) \mid b^2 - 4c = \delta^2\} \subset \mathbb{C}^3$. Then we have

$$\begin{array}{ccc} X_1 & \longrightarrow & \widetilde{\mathrm{Poly}_2} \\ & \searrow & \downarrow \\ & & X_0 = \mathrm{Poly}_2 \end{array}$$

where the horizontal arrow sends (b, c, δ) to $((b, c), (-b+\delta)/2)$ and the diagonal arrow sends (b, c, δ) to (b, c). We also have that

$$\begin{array}{ccc} X_1 & \longrightarrow & \mathbb{CP}^1 \\ \downarrow & & \downarrow \\ X_0 & \longrightarrow & \mathbb{CP}^1 \end{array}$$

is a pullback diagram, where the vertical map on the right is the branched cover $z \mapsto z^2$ and the map on the left is the diagonal map above. The top horizontal map sends (b, c, δ) to δ and the bottom horizontal map sends (b, c) to $b^2 - 4c$ so that the whole diagram commutes. We have just proved

Theorem. *(Babylonians) There is a formula in radicals for the roots of a general quadratic.*

The above definition should remind you of the situation in Galois theory where one wants to find a tower of field extensions in order to say that an element is expressible in radicals. In fact, we have the following dictionary between topology/geometry and algebra:

Top/Geo	Alg
birational class of X	$\simeq$ class of $\mathbb{C}(X)$
dimension of X	$\mathrm{trdeg}_{\mathbb{C}}\mathbb{C}(X)$
branched cover $Y \to X$	field extension $\mathbb{C}(Y)/\mathbb{C}(X)$
$\mathrm{Mon}(Y \xrightarrow{\text{normal}} X)$	$\mathrm{Gal}(\mathbb{C}(Y)/\mathbb{C}(X))$

In other words, we may apply Galois theory to sufficiently nice branched coverings. The above dictionary implies that a tower of branched coverings is equivalent to a tower of subgroups of the monodromy group. We may then use the monodromy group to deduce whether certain branched coverings have intermediate coverings that behave like radical covers, and therefore deduce whether certain polynomials have roots expressible in radicals of their coefficients.

Theorem. *(Cardano, del Ferro, Tartaglia, 1545) There is a formula in radicals for the roots of a general cubic.*

Exercise. Construct a sequence of towers for Cardano's cubic formula.

Theorem. *(Cardano, Ferrari, 1545) There is a formula in radicals for the roots of a general quartic.*

Theorem. *(Abel, Ruffini, 1824) There is* no *formula in radicals for the roots of a general quintic or higher degree polynomial.*

Remark. Arnol'd has a proof of the above statement using the perspective of branched coverings above. In it, he supposes for contradiction that a tower of branched covers exist. He then realizes that the monodromy group of the last cover over the base is solvable and surjects onto the monodromy group of $\widetilde{\text{Poly}_n} \to \text{Poly}_n$. However, the monodromy representation of this cover is a map $\pi_1(\text{Poly}_n - \Delta_n) \to S_n$ where Δ_n is the discriminant locus. We have that $\text{Poly}_n - \Delta_n$ is homeomorphic to UConf_n the *configuration space of n unordered points in* $\mathbb{C}$ which is a $K(B_n, 1)$ where B_n is the *Braid group on n strands*; the monodromy representation is exactly the map that sends a strand to the induced permutation on the n points, which is surjective. The monodromy group is then exactly S_n. But this is not solvable for $n \geq 5$.

The above results are all classical well-known theorems that most of us encounter in undergraduate algebra classes. However what is less well-known is the following:

Theorem. *(Bring, 1786) There* is *a formula for the roots of a general quintic, in square roots, cube roots, fifth roots, and the* Bring radical *defined as* $\sqrt[\text{br}]{a} = \{z \mid z^5 + az + 1 = 0\}$.

The Bring radical is an example of an *algebraic function*. An *algebraic function of degree n in m variables* is an assignment $\Phi(a_1, ..., a_m) = \{z \in \mathbb{C} | p_0(\vec{a})z^n + ... + p_n(\vec{a}) = 0\}$ where the p_i are polynomials in the variables a_j. Note that the degree refers to the power of z. One should think of these algebraic functions as multi-valued functions similar to radicals, with the values being unordered.

Example. The Bring radical above. Radicals and d-th roots. These are algebraic functions in 1 variable.

Example. The *universal quadratic* $U_2(a, b, c) = \{z \mid az^2 + bz + c = 0\}$ is an algebraic function in 3 variables. The *universal n-valued polynomial* $U_n(a_0, ..., a_n) = \{z \mid a_n z^n + ... + a_0 = 0\}$ is an algebraic function in $(n + 1)$-variables.

In other words, we can move away from the solvable/unsolvable-in-radicals dichotomy and extend the question of expressing roots in radicals to general algebraic functions. Following Bring, we can now ask the following question: how hard is it to obtain a formula in *algebraic functions* for the roots of a polynomial? One can formalize this as asking, how many *variables* in the algebraic functions does one need? Mimicking the definition for solving in radicals, we come to the following concept introduced by Brauer in 1975.

Resolvent degree

Definition. *The* resolvent degree *of a branched cover* $Y \to X$ *denoted* $RD(Y \to X)$ *is the minimum* d *such that there is a tower of branched covers* $X_r \to ... \to X_0 \subset X$ *such that* $X_r \to X$ *factors through a branched cover* $X_r \to Y$ *and such that, for each* i *we have* $X_i \to X_{i-1}$ *is a pullback from a branched cover* $\widetilde{Z}_i \to Z_i$ *with dimension* Z_i *at most* d.

The resolvent degree of the branched cover of the space of polynomials can be interpreted as the minimum d for which there is a formula in algebraic functions of at most d variables for the roots of a polynomial in terms of its coefficients.

Theorem. *(Hamilton, Tschirnhaus, 1836) Any degree 6 polynomial can be reduced via radicals to* $Q(z) = z^6 + az^2 + bz + 1$. *Any degree 7 polynomial can be reduced via radicals to* $Q(z) = z^7 + az^3 + bz^2 + cz + 1$. *Any degree 8 polynomial can be reduced via radicals to* $Q(z) = z^8 + az^4 + bz^3 + cz^2 + dz + 1$.

Transformations of coordinates that reduce the number of parameters of a polynomial are generally called *Tschirnhaus transformations*. The above theorem then implies that the number of variables needed to express roots in algebraic functions for a degree 6, 7, 8 resp. polynomial is at most 2, 3, and 4 respectively. Hilbert conjectures one cannot do better, which is what precisely motivated Brauer in defining resolvent degree in the first place.

Conjecture. *(Hilbert's sextic conjecture)* $RD(\widetilde{\text{Poly}_6} \to \text{Poly}_6) = 2$.

Conjecture. *(Hilbert's 13th problem)* $RD(\widetilde{\text{Poly}_7} \to \text{Poly}_7) = 3$.

Conjecture. *(Hilbert's octic conjecture)* $RD(\widetilde{\text{Poly}_8} \to \text{Poly}_8) = 4$.

Historically, much work has been done on finding upper bounds on resolvent degree, including theorems of Tschirnhaus (1683), Bring (1786), Hamilton (1836), Sylvester (1887), Klein (1888), Hilbert (1927), and Segre (1945). There are *currently no known lower bounds*. The best general upper bound was given by Brauer, who proved for $n \geq 4$ and fixed r that resolvent degree of the branched cover for degree n polynomials is $\leq n - r$ for $n \geq (r-1)! + 1$.

Note that resolvent degree was defined for arbitrary branched covers. Besides being used to study the reduction of parameters problem, one can also apply it to certain incidence varieties from algebraic geometry.

Example. Consider $\mathcal{H}_{3,3}$ the parameter space of cubic surfaces in $\mathbb{P}^3$ and $\mathcal{H}_{3,3}(1)$ the space of pairs (S, L) where S is a smooth cubic surface and $L \subset S$ is a line i.e., the zero set of two linear functions in two variables. We can consider the map $\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ that simply forgets the line on the cubic surface. One checks that this map is a proper smooth submersion away from the singular cubics, and therefore, by Ehresmann's lemma, is a locally trivial fibration. This immediately implies that every smooth cubic is diffeomorphic to one another and that the above is a branched covering, with branched locus the union of the discriminant loci in each variable. Considering the Fermat cubic $X^3 + Y^3 + W^3 + Z^3$, we can count that there are exactly 27 lines on it, and thus exactly 27 lines on a smooth cubic surface. However, given a smooth cubic surface, can one find an explicit line on it? That is, given the polynomial that determines the cubic surface, can one find a formula in algebraic functions of its coefficients for the polynomial equations that determine the lines?

Theorem. *(Harris) There is no formula in radicals in the coefficients of a smooth cubic S for a line on it. Given 3 skew (disjoint) lines $L_1, L_2, L_3 \subset S$, there* is *a formula in radicals for the other 24, in terms of coefficients of S* and *coefficients of the three lines. Given only 2 skew lines, there is no such formula in radicals.*

Proof sketch. We consider the tower of branched covers $\mathcal{H}_{3,3}(27) \to \mathcal{H}^{skew}_{3,3}(3) \to \mathcal{H}^{skew}_{3,3}(2) \to \mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ and only somewhat sketch the first statement. It turns out that the monodromy group of the cover $\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ is $W(E_6)$ the *Weyl group* of E_6, which is known to be not solvable.

The resolvent degree of $\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ is not known. However, what is known is the following:

Theorem. *(Farb-Wolfson)* $RD(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)) = RD(\widetilde{\text{Poly}_5} \to \text{Poly}_5) = 1$. *Moreover* $RD(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}) = RD(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1))$ *where $\mathcal{H}_{4,2}$ is the parameter space of smooth planar quartics in $\mathbb{CP}^2$ and the incidence varieties are those planar quartics with bitangents equipped (i.e., lines that are tangent to the planar quartic at two points).*

To conclude, the notion of resolvent degree unifies a vast number of algebro-geometric problems under one general concept. It allows one to formalize how difficult it is to find a formula for a solution to an equation in algebraic functions, and can be viewed through the lens of topology, enumerative algebraic geometry, and Galois theory, and there are still many questions left unanswered.

Some open questions include:

Conjecture. *Prove that* $RD(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}) = 3$.

Question. *From Harris's theorem above, there is a formula in radicals for 27 lines on a smooth cubic given 3 skew lines. Write down this formula.*

Conjecture. *Prove that resolvent degree for the branched cover of polynomials equipped with a root over the space of polynomials goes to* ∞ *as* $n \to \infty$.

Conjecture. *(Arnol'd-Shimura) Give a single example of a branched cover whose resolvent degree is strictly bigger than 1.*

References

[1] Farb, B., and Wolfson, J. "Resolvent degree, Hilbert's 13th problem, and geometry." https://www.arxiv.org/abs/1803.04063. Retrieved September 3, 2018, from the arXiv database.