Galois theory, Advanced III, Spring 2024

Wenyuan Li

Given a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, **a root of** $f(x)$ is a solution to the polynomial equation $f(x) = 0$; in other words, a root of $f(x)$ is a number α so that $f(\alpha) = 0$.

We have seen how to solve cubic and quadratic equations using resolvents. The resolvent of an equation can be expressed in terms of the roots of the polynomial, and conversely, the roots of the polynomials can also be expressed in terms of the resolvents. This reduces the problem of solving the original equation into solving the resolvent equations.

1 Galois Resolvents

When the degree of the equation gets higher, the degree of the resolvent equation will become higher, making it more difficult to solve. Later, in around 1820, Abel and Galois showed that in fact a general polynomial equation of degree at least 5 is not **solvable by radicals**, which is a mathematically precise way to say that you can't find a formula like the quadratic formula to solve a polynomial like $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$!

Nevertheless, the idea of resolvents can be generalized and turn out to have a huge importance in Galois' work on solvability of polynomial equations. Here, we investigate cubic equations again to illustrate the notion of Galois resolvents.

We will use the notion of **rational functions**, which here mean the quotients of two polynomial functions. For a polynomial equation $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, a **Galois resolvent** $t = t(x_1, \ldots, x_n)$ is a polynomial of the roots $x_1, x_2, \ldots, x_n$ with coefficients in $\mathbb{Q}$ such that all the roots $x_1, x_2, \ldots, x_n$ can be written as a rational function of t and $a_{n-1}, a_{n-2}, \ldots, a_1$ and a_0 with coefficients in $\mathbb{Q}$.

(*Remark: In general, a rational function* $p(x)/q(x)$ *or* $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ *is only defined when the denominator is non-zero. For example, the domain of* $p(x)/q(x)$ *is the set of real or complex numbers* x *such that* $q(x) \neq 0$.)

1. For a quadratic equation $x^2 + q = 0$ with two roots x_1 and x_2, compute $x_1 + x_2$ and x_1x_2. For a cubic equation $x^3 + px + q = 0$ with roots x_1, x_2 and x_3, compute $x_1 + x_2 + x_3$, $x_1x_2 + x_2x_3 + x_1x_3$ and $x_1x_2x_3$.

2. For a quadratic equation $x^2 + q = 0$ with two roots x_1 and x_2, show that $t = x_1 - x_2$ is a Galois resolvent by writing x_1, x_2 as rational functions of t and q.

3. For a cubic equation $x^3 + px + q = 0$ with three roots x_1, x_2, x_3, show that

$$F(t, x_1) = (t - (x_1 - x_2))(t - (x_1 - x_3)) = 3x_1^2 - 3tx_1 + t^2 + p.$$

4. For a cubic equation $x^3 + px + q = 0$ with three roots x_1, x_2 and x_3, show that $t = x_1 - x_2$ is a Galois resolvent by writing x_1, x_2, x_3 as rational functions of t, p and q. In fact,

$$x_1 = \frac{t}{2} - \frac{3}{2}\left(\frac{q}{t+p}\right), \quad x_1 = -\frac{t}{2} - \frac{3}{2}\left(\frac{q}{t+p}\right), \quad x_3 = \frac{3q}{t^2+p}.$$

5. For a cubic equation with rational coefficients $x^3 + px + q = 0$ with three roots x_1, x_2 and x_3, suppose x_1, x_2, x_3 are not rational numbers. Show that $t = x_1 + x_2 + x_3$ is not a Galois resolvent.

6. For a cubic equation with rational coefficients $x^3 + px + q = 0$ with three roots x_1, x_2 and x_3, suppose x_1, x_2, x_3 are not rational numbers. Show that $t = x_1 + x_2$ is not a Galois resolvent (*Hint: since x_1 and x_2 are symmetric in all the expressions, they must be expressed as the same rational function in terms of t, p and q*).

For a general polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, we will now explain how to find the Galois resolvent in general.

For a general polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, let $t(x_1, x_2, \ldots, x_n)$ be a rational function of $x_1, x_2, \ldots, x_n$. For a permutation $\sigma \in S_n$, define $t_\sigma = t(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n})$ and consider the resolvent equation where X is the variable

$$F(X) = \prod_{\sigma \in S_n} (X - t_\sigma) = 0.$$

The Galois resolvent is a solution to the above equation, that is, $F(t) = 0$.

Recall the following theorem we learned from two weeks ago: Let $x_1, x_2, \ldots, x_n$ be solutions to the equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0.$$

Let $f(x_1, x_2, \ldots, x_n)$ be a symmetric polynomial in the variables $x_1, x_2, \ldots, x_n$, which means for any permutation $\sigma \in S_n$,

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n}).$$

Then $f(x_1, x_2, \ldots, x_n)$ can be expressed as a polynomial of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ (with coefficients in $\mathbb{Q}$).

7. Let x_1, x_2, x_3 be roots of the eqution $x^3 + a_2x^2 + a_1x + a_0 = 0$. Consider the symmetric polynomial $x_1^2 + x_2^2 + x_3^2$ and $x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1^2x_3 + x_2^2x_1 + x_3^2x_1$, express them as polynomials of a_2, a_1 and a_0.

8. For a general polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, let $t(x_1, x_2, \ldots, x_n)$ be a rational function of $x_1, x_2, \ldots, x_n$. Show that the coefficients of the resolvent equation $F(X) = \prod_{\sigma \in S_n}(X - t_\sigma) = 0$ are polynomials with coefficients expressed in terms of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$.

9. Let x_1, x_2, x_3 be roots of the eqution $x^3 + a_2x^2 + a_1x + a_0 = 0$. Consider the symmetric polynomial $x_1^2 + x_2^2$ and $x_1^2x_2 + x_2^2x_1$, express them as polynomials of a_2, a_1, a_0 and x_3.

For a general polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, let $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ be a rational function of the roots $x_1, x_2, \ldots, x_{n-1}, x_n$. For a permutation $\sigma \in S_{n-1}$ of the first $n-1$ elements, define

$$t_\sigma = t(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_{n-1}}, x_n)$$

and consider the equation where X is the variable

$$F_{n-1}(X, x_n) = \prod_{\sigma \in S_{n-1}} (X - t_\sigma) = 0.$$

10. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, show that $F_{n-1}(X, x_n)$ is a polynomial of X and x_n with coefficients expressed in terms of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$.

11. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, let $Y = x_n$ and consider the polynomial where X and Y are variables

$$F_{n-1}(X, Y) = \prod_{\sigma \in S_{n-1}} (X - t_\sigma).$$

$F_{n-1}(t, Y)$ can be viewed as a polynomial of Y whose coefficients are expressed in terms of $t = t(x_1, \ldots, x_n)$. Use Euclidean division to show that $Y - x_n$ is a factor of both $F_{n-1}(t, Y)$ and the original polynomial $f(Y)$.

12. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, show that for a permutation $\sigma' \in S_{n-1}$ of any $n-1$ elements and Y being the remaining element in the roots, the polynomials are equal:

$$F'_{n-1}(X, Y) = \prod_{\sigma \in S_{n-1}} (X - t_{\sigma'})$$

is equal to $F_{n-1}(X, Y)$ defined in Problem 11.

13. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, suppose for any $\sigma \in S_n$ that is not the identity permutation,

$$t_\sigma = t(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_{n-1}}, x_{\sigma_n}) \neq t(x_1, x_2, \ldots, x_{n-1}, x_n) = t.$$

Show that $F(t, x_i) \neq 0$ for any $1 \leq i \leq n-1$.

In the following problem, you will need to use the **Euclidean algorithm** for polyomials: let $f(x), g(x)$ be polynomials and $d(x)$ be their maximal common divisor, that is, the maximal degree monic polynomial (monic means the top degree coefficient is 1) that divides both $f(x)$ and $g(x)$. Then there are polynomials $a(x)$ and $b(x)$ such that

$$d(x) = a(x)f(x) + b(x)g(x).$$

14. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, suppose for any $\sigma \in S_n$ that is not the identity permutation, $t_\sigma \neq t$. Use the **Euclidean algorithm** to show that there are polynomials $a_t(Y), b_t(Y)$ whose coefficients are rational functions of t such that

$$Y - x_n = a_t(Y)f(Y) + b_t(Y)F_{n-1}(t, Y).$$

15. (**Galois' lemma**) For a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $t(x_1, x_2, \ldots, x_{n-1}, x_n)$ a rational function of the roots, suppose for any $\sigma \in S_n$ that is not the identity permutation, $t_\sigma \neq t$. Show that t is a Galois resolvent, that is, the roots $x_1, \ldots, x_n$ can be expressed as rational functions of t.

For a polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, we define the **discriminant** to be

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)^2.$$

16. For a polynomial equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, show that the discriminant is a polynomial of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$.

17. For a cubic equation $x^3 + px + q = 0$ with three roots x_1, x_2, x_3, show that

$$\Delta = -4p^3 - 27q^2.$$

18. For a cubic equation $x^3+px+q = 0$ with three roots x_1, x_2, x_3 and $t = x_1-x_2$, suppose Δ has a positive square root P. Show that the resolvent equation is

$$F(X) = (X^3 + 3pX + P)(X^3 + 3pX - P).$$

We say that a polynomial with $\mathbb{Q}$ coefficients $f(x)$ is **irreducible** over $\mathbb{Q}$ if it cannot be decomposed into a product of two polynomials with $\mathbb{Q}$ coefficients that have lower degrees.

19. For a cubic equation with $\mathbb{Q}$ coefficients $x^3 + px + q = 0$ with three roots x_1, x_2, x_3 and $t = x_1 - x_2$. Show that the resolvent equation is reducible if and only if Δ has a square root over $\mathbb{Q}$.

2 Galois Groups

Recall that a polynomial $f(x)$ with coefficients in $\mathbb{Q}$ is **irreducible over** $\mathbb{Q}$ if it cannot be further decomposed into products of two polynomials $f_1(x)f_2(x)$ of lower degrees with coefficients in $\mathbb{Q}$.

For a polynomial equation with $\mathbb{Q}$ coefficients $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, consider the resolvent equation $F(X)$ for a Galois resolvent t. We can decompose $F(X)$ into a product of irreducible polynomials $G_1(X) \ldots G_r(X)$ over $\mathbb{Q}$. Suppose $X - t$ is a factor of $G_1(X)$. Then we define the **Galois group** of $f(x)$ over $\mathbb{Q}$ to be the set of permutations σ such that $X - t_\sigma$ is a factor in $G_1(X)$.

(*Note that since t may not be rational, $X - t$ may not be a polynomial over $\mathbb{Q}$. However, the decomposition $F(X) = G_1(X) \ldots G_r(X)$ is over $\mathbb{Q}$.*)

20. For a polynomial equation with $\mathbb{Q}$ coefficients $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, let t be a Galois resolvent and $x_1 = \phi_1(t), x_2 = \phi_2(t), \ldots, x_n = \phi_n(t)$. Then for σ in the Galois group over $\mathbb{Q}$,

$$\phi_1(t_\sigma), \phi_2(t_\sigma), \ldots, \phi_n(t_\sigma)$$

is a permutation of the roots $x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n}$.

This means that the **Galois group** of a polynomial equation is the set of permutations of the roots that also permutes the roots of the Galois resolvent equation.

21. For a polynomial equation with $\mathbb{Q}$ coefficients $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with roots $x_1, x_2, \ldots, x_n$, let t be a Galois resolvent. Show that for any σ, σ' in the Galois group, $t_\sigma = t(x_{\sigma_1}, \ldots, x_{\sigma_n})$ and $t'_\sigma = t(x_{\sigma'_1}, \ldots, x_{\sigma'_n})$ only differ by another permutation of the roots τ in the Galois group. (*Hint: Use the fact that t_σ is also a rational function in t.*)

22. Use Problem 21 to show that the **Galois group** of a polynomial equation over $\mathbb{Q}$ is a group; in other words, if σ, τ are two permutations in the Galois group, then the composition of the two permutations $\sigma\tau$ and the inverse permutation σ^{-1} are both in the Galois group, and moreover, the identity permutation id is also in the Galois group.

23. Use Problem 21 to show that the Galois group of a polynomial equation over $\mathbb{Q}$ does not depend on the Galois resolvent we choose.

24. For a polynomial that is irreducible over $\mathbb{Q}$, show that the Galois group acts transitively on the roots, that is, for any two roots x_i and x_j, there is a permutation in the Galois group that sends x_i to x_j.

25. For a cubic equation with $\mathbb{Q}$ coefficients $f(x) = x^3 + px + q = 0$ with three roots x_1, x_2, x_3 and $t = x_1 - x_2$. Suppose $f(x)$ is irreducible. Show that the Galois group over $\mathbb{Q}$ is either all the 6 permutations or the 3 permutations given by $123, 231$ and 312, depending on whether Δ has a square root in $\mathbb{Q}$.

26. For the polynomial equation $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ where p is a prime, show that its roots are of the form $\alpha, \alpha^2, \ldots, \alpha^{p-1}$.

27. For the polynomial equation $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ where p is a prime, assuming it is irreducible over $\mathbb{Q}$, show that the Galois group has $p - 1$ elements given by powers of the single permutation $12 \ldots (p-2)(p-1)$.

(*We remark that* $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *where* p *is a prime is in fact always irreducible over* $\mathbb{Q}$*, although the proof requires some further technology.*)

3 Taking Radicals

Now, we will take a glimpse on Galois theory, which answers the question when a polynomial is solvable by radicals using information from the Galois group. Here, we define a polynomial $f(x)$ of degree n to be **solvable** if all the n roots of the polynomial can be expressed in terms of rational numbers and coefficients of the polynomial using addition, subtraction, multiplication, division, and extraction of roots.

For subsets $H \subset G \subset S_n$, we define H to be a subgroup in G if it is closed under taking inverses and compositions of permutations.

28. (**Lagrange's theorem**) Show that for a subgroup H of G, the number of elements $|H|$ is always a factor of the number of all elements $|G|$. The quotient $|S_n|/|G|$ is called the **index** of G in S_n.

For a subgroup $H \subset G \subset S_n$, define H to be a normal subgroup of G if it is also closed under conjugations, that is, for any $\sigma \in H$ and any $\tau \in G$, we have $\tau^{-1}\sigma\tau \in H$.

You may recall the following result we learned about permutations: Let σ and τ be permutations and the two-line notation for σ is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma_1 & \sigma_2 & \sigma_3 & \dots & \sigma_n \end{pmatrix}.$$

Then the two-line notation for $\tau^{-1}\sigma\tau$ is

$$\tau^{-1}\sigma\tau = \begin{pmatrix} \tau(1) & \tau(2) & \tau(3) & \dots & \tau(n) \\ \sigma_{\tau(1)} & \sigma_{\tau(2)} & \sigma_{\tau(3)} & \dots & \sigma_{\tau(n)} \end{pmatrix}.$$

29. Show that the Galois group of a polynomial $f(x)$ over $\mathbb{Q}$ is always a normal subgroup of the group of permutations S_n.

30. Let $r \in \mathbb{C}$ be a complex number and $\mathbb{Q}(r)$ be the set of numbers that can be expressed as a rational function of r with $\mathbb{Q}$ coefficients. Show that the Galois group of a polynomial $f(x)$ over $\mathbb{Q}(r)$ is a normal subgroup of the Galois group of $f(x)$ over $\mathbb{Q}$. Show that similar arguments work for $\mathbb{Q}(r_1, \dots, r_k)$, the set of numbers that can be expressed as a rational function of $r_1, \dots, r_k$ with $\mathbb{Q}$ coefficients.

31. Let $f(x) = x^2 - 2$. Compute the Galois group of $f(x)$ over $\mathbb{Q}$ and its Galois group over $\mathbb{Q}(\sqrt{2})$.

32. Let $f(x) = x^3 - 2$. Compute the Galois group of $f(x)$ over $\mathbb{Q}$ and its Galois group over $\mathbb{Q}(\sqrt[3]{2})$.

33. Let $f(x)$ be a degree n polynomial over $\mathbb{Q}$ and t be a Galois resolvent of $f(x)$ with Galois resolvent equation

$$F(X) = \prod_{\sigma \in S_n} (X - t_\sigma).$$

Let $G(X)$ is an irreducible factor of $F(X)$ over $\mathbb{Q}$ and $H_r(X)$ be an irreducible factor of $F(X)$ over $\mathbb{Q}(r)$ for some complex number r. Show that $H_r(X)$ divides $G(X)$.

34. Let p be a prime, and α be a p-th root of unity, meaning that $\alpha \neq 1$ but $\alpha^p = 1$. Let $r = \sqrt[p]{a}$ for some rational number a. Consider

$$h(X) = H_{\alpha r}(X) H_{\alpha^2 r}(X) \dots H_{\alpha^{p-1} r}(X).$$

Show that $h(X)$ is a polynomial over $\mathbb{Q}$ and $h(X)$ equals to a nonzero number times $G(X)$.

35. Let $f(x)$ be a degree n polynomial over $\mathbb{Q}$, p be a prime and α be a p-th root of unity. Prove that the Galois group of $f(x)$ over $\mathbb{Q}(\alpha, \sqrt[p]{a})$ is either the same as the Galois group over $\mathbb{Q}(\alpha)$, or a subgroup of index p.

36. Let $f(x)$ be a degree n polynomial over $\mathbb{Q}$, p be a prime and α be a p-th root of unity. Prove that the Galois group of $f(x)$ over $\mathbb{Q}(\alpha, \sqrt[p]{a})$ is either the same as the Galois group over $\mathbb{Q}(\alpha)$, or a **normal** subgroup of index p.

This shows that when solving the polynomial equation, taking the p-th root corresponds to going to an index p normal subgroup of the Galois group. Therefore, solving polynomial equations by radicals corresponds to successively taking normal subgroups of prime indices.

On the other hand, it turns out that for any normal subgroup of prime index, we can find an element so that by adding that element the Galois group exactly becomes the subgroup. This means that there is a correspondence between finding normal subgroups of Galois groups and adding radicals solving polynomial equations.