Galois Theory - 5122GALO6Y

Yoav Eshel

February 15, 2021

Contents

1 Introduction

Galois theory is about studying Polynomials with coefficients in a field ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.). Let

$$f(T) = T^n + \cdots + a_1 T + a_0 \in \mathbb{Q}[T].$$

Then $f(T)$ splits completely in $\mathbb{C}[T]$ as

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n)$$

with $\alpha_1, \dots \alpha_n \in \mathbb{C}$ are the roots of f. Galois theory studies permutation of the the roots that preserve algebraic relations between these roots. The allowed permutation of the roots give rise to a group denoted Gal(f). The following definition of a Galois group does not require any background knowledge but is not very useful in practice.

Definition. *Let $\sigma : \mathbb{C} \to \mathbb{C}$ be a field automorphism and $\alpha \in \mathbb{C}$ a root of $F(T) \in \mathbb{Q}[T]$. Since $\sigma(1) = 1$ it follows that $\sigma(n) = n$ for all integers and so $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$ is the identity on $\mathbb{Q}$. Then*

$$\begin{aligned} f(\sigma(\alpha)) &= \sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(f(\alpha)) \\ &= 0. \end{aligned}$$

Then each automorphism σ is a permutation of the roots which is precisely the Galois group of the polynomial $Gal(f) \subset S_n$. In other words we have a group action

$$Aut(\mathbb{C}) \times \{\alpha_1, \dots, \alpha_n\} \to \{\alpha_1, \dots, \alpha_n\}$$

Then $Gal(f) := Im(\phi)$ where $\phi : Aut(\mathbb{C}) \to S_n$ mapping $\sigma \mapsto (\alpha_i \mapsto \sigma(\alpha_i))$

Gal$(f) \subset S_n$ is transitive subgroup (i.e. if its action on the set of roots is transitive) if and only if f is irreducible.

2 Symmetric Polynomials

Let $f = (T - \alpha_1) \cdots (T - \alpha_n) \in \mathbb{C}[T]$. Then its discriminant is defined as

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

When f is quadratic this definition coincides with the high-school definition of the discriminant. However in high school the discriminant is usually written in terms of the coefficients rather than the roots. One can rewrite the discriminant in terms of the coefficients using symmetric polynomials. An interesting property of the discriminant is that $\sqrt{\Delta_f} \in \mathbb{Q} \iff \text{Gal}(f) \subset A_n$, a proof of which will be given in the following sections.

Consider the ring $R = \mathbb{Z}[X_1, \ldots, X_n]$. If $\sigma \in S_n$ is a permutation then let

$$\sigma(X_i) := X_{\sigma(i)}$$

which extends to a group action of S_n on R. Then a polynomial is said to be *symmetric* if $\sigma(f) = f$ for all $\sigma \in S_n$. We denote the the subset of symmetric polynomials by $R^{S_n} \subset R$. Note that R^{S_n} is in fact a subring of R.

Define the *universal polynomial* $f^{\text{univ}} \in R[T]$ with roots $X_1, \ldots, X_n$ as

$$\begin{aligned} f^{\text{univ}}(T) :&= (T - X_1) \cdots (T - X_n) \\ &= T^n - (X_1 + \cdots + X_2)T^{n-1} + (X_1X_2 + X_1X_3 + \cdots)T^{n-1} + \\ &\quad \cdots + (-1)^n(X_1 \cdots X_n). \end{aligned}$$

Then the *elementary symmetric polynomials* $s_1, \ldots, s_n$ are the coefficients of f^{univ}. Every element in R^{S_n} is a combination of the elementary symmetric polynomials

Theorem 2.1. *The map*

$$\begin{aligned} \Phi : \mathbb{Z}[Y_1, \ldots, Y_n] &\to R^{S^n} \\ Y_i &\mapsto s_i \end{aligned}$$

is an isomorphism of rings.

To actually write a symmetric polynomial in terms of elementary symmetric polynomials we introduce some useful notation. We say a polynomial is ordered *lexicographically* if the monomial $T_1^{e^1} T_2^{e_2} \cdots T_n^{e_n}$ with the highest e_1 is in front. If two monomials have the same e_1, then we compare their e_2 and so on. Like a dictionary. If P is a symmetric polynomial in n variables, choose a single representative proceeded by the symbol $\sum_n$ to denote the sum over the monomials in the S_n orbit of the representative. Then for example

$$\begin{aligned} s_1 &= \sum_n T_1 \\ s_2 &= \sum_n T_1 T_2 \\ &\vdots \\ s_n &= \sum_n T_1 T_2 \cdots T_n = T_1 T_2 \cdots T_n. \end{aligned}$$

Now suppose P is a symmetric polynomial. To find its representation in terms of symmetric polynomials:

1. Let $a \cdot T_1^{e_1} T_2^{e_2} \cdots T_n^{e_n}$ be the the first term in P, lexicographically.
2. Form the monomial

$$M = s_1^{e_1 - e_2} s_2^{e_2 - e_1} \cdots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n}$$

3. Let $P_i = P - cM$.

4. Repeat steps (1)-(3) until $\deg P_i = 0$.

5. The we can solve for P and write it as a polynomial in the elementary symmetric polynomials.

The representation obtained through the algorithm above is unique.

The following theorem is useful when applying the algorithm above.

Theorem 2.2 (Orbit Stabilizer Theorem)**.** *Let G be a group acting on set S. For any $x \in S$ let $G_x = \{g \in G \mid g \cdot x = x\}$ denote the stabilizer of x, and let $G \cdot x = \{g \cdot x \mid g \in G\}$ denote the orbit of x. Then*

$$|G| = |G \cdot x||G_x|$$

Since S_n is acting on the set $\{T_1, \ldots, T_2\}$ we can find the number of elements in a given sum. Since $|S_n| = n!$ the orbit of an elementary is given by

$$\frac{n!}{\text{size of stabilizer}}$$

3 Exercises

Symmetric Polynomial

Exercise 14.10
Express the symmetric polynomials $\sum_n T_1^2 T_2$ and $\sum_n T_1^3 T_2$ in the elementary symmetric polynomials.

Solution. To get the polynomial $\sum_n T_1^2 T_2$ we start with

$$s_1 s_2 = \sum_n T_1 \sum_n T_1 T_2 = \sum_n T_1^2 T_2 + 3 \sum_n T_1 T_2 T_3 = \sum_n T_1^2 T_2 + 3s_3$$

Thus

$$\sum_n T_1^2 T_2 = s_1 s_2 - 3s_3$$

Similarly, to transform the polynomial $\sum_n T_1^3 T_2$ we start with

$$\begin{aligned} s_1^2 s_2 &= \left(\sum_n T_1 \right)^2 \sum_n T_1 T_2 \\ &= \left(\sum_n T_1^2 + 2 \sum_n T_1 T_2 \right) \sum_n T_1 T_2 \\ &= \sum_n T_1^2 \sum_n T_1 T_2 + 2s_2^2 \\ &= \sum_n T_1^3 T_2 + \sum_n T_1^2 T_2 T_3 + 2s_2^2. \end{aligned}$$

And since

$$s_1 s_3 = \sum_n T_1 \sum_n T_1 T_2 T_3 = \sum_n T_1^2 T_2 T_3 + 4 \sum_n T_1 T_2 T_3 T_4$$

it follows that $\sum_n T_1^2 T_2 T_3 = s_1 s_3 - 4s_4$ and so

$$\sum_n T_1^3 T_2 = s_1^2 s_2 - s_1 s_3 + 4s_4 - 2s_2^2$$

Exercise 14.14
Prove: For $n \in \mathbb{Z}_{>0}$, we have $\Delta(X^n + a) = (-1)^{\frac{1}{2}n(n-1)} n^n a^{n-1}$.

Proof. Let $f(X) = X^n + a$ and let α_i be its roots. Then $f'(X) = nX^{n-1}$ and

$$\Delta(f) = (-1)^{n(n-1)/2} R(f, f').$$

Let $f_1(X) = a$ and then $f \equiv f_1 \mod (f')$ since $f = f_1 + f' \cdot \left(\frac{1}{n}X\right)$. Simplifying the resultant we get

$$\begin{aligned} R(f, f') &= R(f', f) && \text{(Property 1)} \\ &= n^n R(f', f_1) && \text{(Property 3)} \\ &= n^n \cdot \left(n^0 \prod_{i=1}^{n-1} f_1(\alpha_i) \right) && \text{(Property 2)} \\ &= n^n a^{n-1} \end{aligned}$$

and the result follows. □

Exercise 14.15
Calculate the discriminant of the polynomial $f(X) = X^4 + pX + q \in \mathbb{Q}(p, q)[X]$.

Solution. Then $f'(X) = 4X^3 + p$ and so

$$f_1(X) = f - f' \cdot h = X^4 + pX + q + (4X^3 + p)(\frac{1}{4}X) = \frac{3p}{4}X + q.$$

Then the resultant is

$$\begin{aligned} R(f, f') &= R(f', f) && \text{(Property 1)} \\ &= 4^{4-1} R(f', f_1) && \text{(Property 3)} \\ &= 4^3 \left((-1)^{3 \cdot 1} R(f_1, f')\right) && \text{(Property 1)} \\ &= -4^3 \left(\left(\frac{3p}{4}\right)^3 \prod_{i=1}^{1} f'\left(\frac{-4q}{3p}\right) \right) && \text{(Property 2)} \\ &= -3^3 p^3 \left(4 \left(\frac{-4q}{3p}\right)^3 + p \right) \\ &= 4^4 q^3 - 3^3 p^4. \end{aligned}$$

Therefore the discriminant of f is

$$\Delta(f) = (-1)^{4 \cdot 3/2} R(f, f') = R(f, f') = 4^4 q^3 - 3^3 p^4.$$

Exercise 14.16
For every $n > 1$, determine an expression for the discriminant of the polynomial $f(X) = X^n + pX + q \in \mathbb{Q}(p, q)[X]$.

Solution. Let $f(X) = X^n + pX + q \in \mathbb{Q}(p, q)[X]$ for $n > 1$. Then $f'(X) = nX^{n-1} + p$ and $f \equiv f_1 \mod (f')$ where

$$f_1 = f - f' \cdot h = X^n + pX + q - \left(nX^{n-1} + p\right) \left(\frac{1}{n}X\right) = \frac{p(n-1)}{n}X + q.$$

The resultant of f and f' is given by

$$\begin{aligned}
R(f,f') &= R(f',f) && \text{(Property 1)}\\
&= n^{n-1}R(f',f_1) && \text{(Property 3)}\\
&= n^{n-1}\left((-1)^{n-1}R(f_1,f')\right) && \text{(Property 1)}\\
&= (-n)^{n-1}\left(\frac{p(n-1)}{n}\right)^{n-1}\prod_{i=1}^{1} f'\left(-\frac{nq}{(n-1)p}\right) && \text{(Property 2)}\\
&= (-1)^{n-1}p^{n-1}(n-1)^{n-1}\left(\frac{(-1)^{n-1}n^n q^{n-1}}{(n-1)^{n-1}p^{n-1}}+p\right)\\
&= n^n q^{n-1} + (-1)^{n-1}p^n(n-1)^{n-1}.
\end{aligned}$$

Hence the discriminant of f is

$$\Delta(f) = (-1)^{n(n-1)/2}R(f,f') = (-1)^{n(n-1)/2}\left(n^n q^{n-1} + (-1)^{n-1}p^n(n-1)^{n-1}\right)$$

Exercise 14.17
Let $f \in \mathbb{Z}[X]$ be a monic polynomial. Prove that the following are equivalent

1. $\Delta(f) \neq 0$.
2. The polynomial f has no double zeroes in $\mathbb{C}$.
3. The decomposition of f in $\mathbb{Q}[X]$ has no multiple prime factors.
4. The polynomial f and its derivative f' are relatively prime in $\mathbb{Q}[X]$.
5. The polynomial $f \mod p$ and $f' \mod p$ are relatively prime in $\mathbb{F}_p[X]$ for almost all prime numbers p.

Proof. Let $f \in \mathbb{Z}[X]$ be monic and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ it roots in $\mathbb{C}$.
(1) $\Rightarrow$ (2). Suppose that $\alpha_i = \alpha_j$ for some $i \neq j$. Then

$$\Delta(f) = \prod_{1\le i<j\le n}(\alpha_i - \alpha_j) = 0,$$

which is a contradiction. Therefore if f has non-zero discriminant it has no double zeroes in $\mathbb{C}$.
(2) $\Rightarrow$ (3).
(3) $\Rightarrow$ (4).
(4) $\Rightarrow$ (5). If f and f' are relatively prime in $\mathbb{Q}[X]$ then
(1) $\Rightarrow$ (1). □

Exercise 14.19
Let $f \in \mathbb{Q}[X]$ be a monic polynomial with $n = \deg(f)$ distinct complex roots. Prove: the sign of $\Delta(f)$ is equal to $(-1)^s$ where $2s$ is the number of non-real zeroes of f.

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be all the roots of f. Then each term $(\alpha_i - \alpha_j)^2$ in the discriminant falls into one of 3 cases

1. Both α_i and α_j are non-real. Then

   (a) If $\alpha_j = \overline{\alpha_i}$ then $\alpha_i - \alpha_j$ is purely complex and $(\alpha_i - \alpha_j)^2$ is negative.

   (b) If $\alpha_j \neq \overline{\alpha_i}$ then $\overline{\alpha_i}$ and $\overline{\alpha_j}$ are also roots of f and the term

   $$(\alpha_i - \alpha_j)^2(\overline{\alpha_i} - \overline{\alpha_j})^2 = \left((\overline{\alpha_i - \alpha_j})(\alpha_i - \alpha_j)\right)^2 = |\alpha_i - \alpha_j|^2$$

   is positive.

2. α_i is non-real and α_j is real. Then $\overline{\alpha_i}$ is a root of f and the term

   $$(\alpha_i - \alpha_j)^2(\overline{\alpha_i} - \alpha_j)^2 = |\alpha_i - \alpha_j|^2$$

   is positive.

3. Both α_i and α_j are real. Then $(\alpha_i - \alpha_j)^2$ is positive.

Since the only negative terms are of the form $(\alpha_i - \overline{\alpha_i})^2$ and there are $2s$ non-real roots the sign of the determinant is $(-1)^s$.

□

Exercise 14.20
Prove: $f(X) = X^3 + pX + q \in \mathbb{R}[X]$ has three (counted with multiplicity) real zeroes $\iff$ $4p^3 + 27q^{\leq}0$.

Proof. By Ex. 16 we know that $\Delta(f) = (-1)^3\left(3^3q^2 + 2^2p^3\right) = -27q^2 - 4p^3$. Let a, b and c be the roots of f. If $a, b, c \in \mathbb{R}$ then

$$-27q^2 - 4p^3 = \Delta(f) = (a-b)^2(a-c)^2(b-c)^2 \geq 0$$

and so $4p^3 + 27q^{\leq}0$.

Now suppose that $a = x + yi$ and $b = x - yi$ are complex conjugates and c is real. Then

$$\begin{aligned} -27q^2 - 4p^3 &= \Delta(f) \\ &= (a-b)^2(a-c)^2(b-c)^2 \\ &= -4y^2\left((a-c)(\overline{a-c})\right)^2 \\ &= -4y^2|a-c|^2 \\ &\leq 0. \end{aligned}$$

Hence $4p^3 + 27q^{\geq}0$ and the result follows by contraposition. □

Exercise 14.21
Express $p_4 = \sum_n T_1^4$ in elementary symmetric polynomials

Solution. Let $n \geq 4$. Starting with

$$\begin{aligned} s_1^4 &= \left(\sum_n T_1\right)^4 \\ &= \sum_n T_1^4 + 4\sum_n T_1^3T_2 + 12\sum_n T_1^2T_2T_3 + 6\sum_n T_1^2T_2^2 + 24\sum_n T_1T_2T_3T_4. \end{aligned}$$

To understand how to coefficients of the sum are obtained, consider the number of ways the T_i can be arranged. For example, $T_1^4 = T_1T_1T_1T_1$ can only be arranged in 1 way but $T_1^2T_2T_3 = T_1T_1T_2T_3$ can be arrange in $\frac{4!}{2} = 12$ ways (where we divided by 2 since the two T_1 can be swapped in any given arrangement). Then

$$s_1^2s_2 = \left(\sum_n T_1\right)^2 s_2 = \left(\sum_n T_1^2 + 2\sum_n T_1T_2\right) s_2 = \sum_n T_1^3T_2 + \sum_n T_1^2T_2T_3 + 2s_2^2.$$

So far we have

$$\begin{aligned} p_4 &= s_1^4 - 4\left(s_1^2s_2 - 2s_2^2 - \sum_n T_1^2T_2T_3\right) - 12\sum_n T_1^2T_2T_3 - 6\sum_n T_1^2T_2^2 - 24\sum_n T_1T_2T_3T_4 \\ &= s_1^4 - 4s_1^2s_2 + 8s_2^2 - 24s_4 - 6\sum_n T_1^2T_2^2 - 8\sum_n T_1^2T_2T_3. \end{aligned}$$

So continuing with $\sum_n T_1^2T_2^2$ we get

$$s_2^2 = \left(\sum_n T_1T_2\right)^2 = \sum_n T_1^2T_2^2 + 2\sum_n T_1^2T_2T_3 + 6\sum_n T_1T_2T_3T_4.$$

Finding the coefficients here is slightly trickier since s_2 contains pairs not all arrangements are allowed. For example, $T_1^2T_2^2$ can only come from the pair T_1T_2. On the other hand $T_1T_2T_3T_4$ can come from T_1T_2 and T_3T_4 or T_1T_4 and T_2T_3 and so on. We choose the first pair ($\binom{4}{2} = 6$ ways) which also fixes the second pair and so there are 6 ways to get $T_1T_2T_3T_4$. Hence

$$\begin{aligned} p_4 &= s_1^4 - 4s_1^2s_2 + 8s_2^2 - 24s_4 - 6\left(s_2^2 - 2\sum_n T_1^2T_2T_3 - 6s_4\right) - 8\sum_n T_1^2T_2T_3 \\ &= s_1^4 - 4s_1^2s_2 + 2s_2^2 + 12s_4 + 4\sum_n T_1^2T_2T_3. \end{aligned}$$

Using Exercise 14.10 we get

$$\begin{aligned} p_4 &= s_1^4 - 4s_1^2s_2 + 2s_2^2 + 12s_4 + 4(s_1s_3 - 4s_4) \\ &= s_1^4 - 4s_1^2s_2 + 2s_2^2 - 4s_4 + 4s_1s_3 \end{aligned}$$

Exercise 14.22
A rational function $f \in \mathbb{Q}[T_1, \dots, T_n]$ is called symmetric if it is invariant under all permutations of the variables T_i. Prove that every symmetric rational function is a rational function in the elementary symmetric functions.

Proof. Let $f \in \mathbb{Q}[T_1, \dots, T_n]$ be a symmetric rational function. Then $f = g/h$ for g, h polynomials. If h is a symmetric polynomial then $g = fh$ is symmetric as well. By the fundamental theorem of symmetric polynomial both g and h can be written in terms of elementary symmetric polynomials and we're done. If h is not symmetric, then let

$$\tilde{h} = \prod_{\sigma \in S_n \setminus \{e\}} \sigma(h)$$

and then $h\tilde{h}$ is symmetric so $f = \frac{g\tilde{h}}{h\tilde{h}}$ which is again the case above. □

Exercise 14.23
Write $\sum_n T_1^{-1}$ and $\sum_n T_1^{-2}$ as rational functions in $\mathbb{Q}[s_1, \dots, s_n]$

Solution. Starting with

$$\sum_n T_1^{-1} = \frac{1}{T_1} + \cdots + \frac{1}{T_n}.$$

We multiply by $1 = \frac{s_n}{s_n}$ and simplify

$$\begin{aligned}\frac{s_n}{s_n} \sum_n T_1^{-1} &= \frac{T_1 T_2 \cdots T_n}{T_1 T_2 \cdots T_n} \left(\frac{1}{T_1} + \cdots + \frac{1}{T_n} \right) \\ &= \frac{s_{n-1}}{s_n}\end{aligned}$$

For the second expression we present to approaches.

1. Observing that

$$\left(\sum_n T_1^{-1} \right)^2 = \sum_n T_1^{-2} + 2 \sum_n T_1^{-1} T_2^{-1}$$

we can write using the previous part

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2}{s_n^2} - 2 \sum_n T_1^{-1} T_2^{-1}$$

and multiplying by the second term by $\frac{s_n}{s_n}$ we get

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2}{s_n^2} - 2 \left(\frac{1}{T_1 T_2} + \cdots + \frac{1}{T_{n-1} T_n} \right) \frac{T_1 \cdots T_n}{T_1 \cdots T_n} = \frac{s_{n-1}^2}{s_n^2} - 2 \frac{s_{n-2}}{s_n}.$$

Hence $\sum_n T_1^{-2} = \frac{s_{n-1}^2 - 2 s_{n-2} s_n}{s_n^2}$.

2. The second approach is slightly more involved. We start by multiplying by 1 in a clever (but different) way

$$\left(\sum_n T_1^{-2}\right)\frac{s_n^2}{s_n^2} = \left(\frac{1}{T_1^2}+\cdots+\frac{1}{T_n^2}\right)\frac{T_1^2\cdots T_n^2}{T_1^2\cdots T_n^2} = \frac{\sum_n T_1^2\cdots T_{n-1}^2}{s_n^2}.$$

Then $\sum_n T_1^2\cdots T_{n-1}^2$ is obviously (condescending much?) a symmetric polynomial and so we can use our trusty algorithm. Starting with

$$\begin{aligned} s_1^{2-2}s_2^{2-2}\cdots s_{n-1}^{2-0} &= s_{n-1}^2 \\ &= \left(\sum_n T_1\cdots T_{n-1}\right)^2 \\ &= \sum_n T_1^2\cdots T_{n-1}^2 + 2\sum_n T_1^2\cdots T_{n-2}^2 T_{n-1}T_n. \end{aligned}$$

Moving to the second term

$$\begin{aligned} s_1^{2-2}\cdots s_{n-2}^{2-1}s_{n-1}^{1-1}s_n^1 &= s_{n-2}s_n \\ &= \left(\sum_n T_1\cdots T_{n-2}\right)T_1\cdots T_n \\ &= \sum_n T_1^2\cdots T_{n-2}^2 T_{n-1}T_n \end{aligned}$$

and it follows that

$$\sum_n T_1^2\cdots T_{n-1}^2 = s_{n-1}^2 - 2s_{n-2}s_n.$$

So we conclude that

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2 - 2s_{n-2}s_n}{s_n^2}$$

which is reassuring.

Note that in the first approach we stumbled upon something rather interesting:

$$\sum_n T_1^{-1}\cdots T_k^{-1} = \frac{s_{n-k}}{s_n}$$

the proof of which is left as an exercise to the reader.

Exercise 14.24

Field Extensions

Finite Fields

Separable and Normal Extensions