

Galois Theory - 5122GALO6Y

Yoav Eshel

February 3, 2021

Contents

1	Introduction	2
2	Symmetric Polynomials	2
3	Exercises	4
3.1	Symmetric Polynomial	4
3.2	Field Extensions	6
3.3	Finite Fields	6
3.4	Separable and Normal Extensions	6

1 Introduction

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

$$f(T) = T^n + \cdots + a_1T + a_0 \in \mathbb{Q}[T].$$

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 $\text{Gal}(f)$. Not a very useful definition:

Definition. Let $\sigma : \mathbb{C} \rightarrow \mathbb{C}$ 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 $\text{Gal}(f) \subset S_n$. In other words we have a group action

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

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

$\text{Gal}(f) \subset S_n$ is transitive subgroup if and only if f is irreducible (what is a transitive subgroup?). Review group actions

2 Symmetric Polynomials

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

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

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. This is the main point of Symmetric polynomials. Fact: $\sqrt{\Delta_f} \in \mathbb{Q} \iff \text{Gal}(f) \subset A_n$. We will prove this later on.

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

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

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 subset of symmetric polynomials by $R^{S_n} \subset R$ which is a subring.

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

$$\begin{aligned} f^{\text{univ}}(T) &:= (T - X_1) \cdots (T - X_n) \\ &= T^n - (X_1 + \cdots + X_n)T^{n-1} + (X_1X_2 + X_1X_3 + \cdots)T^{n-2} + \\ &\quad \cdots + (-1)^n(X_1 \cdots X_n). \end{aligned}$$

Then *elementary symmetric polynomials* s_1, \dots, 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*

$$\begin{aligned} \Phi : \mathbb{Z}[Y_1, \dots, Y_n] &\rightarrow R^{S_n} \\ Y_i &\mapsto s_i \end{aligned}$$

is an isomorphism of rings.

3 Exercises

3.1 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

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

Thus

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

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

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

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

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

Exercise 14.21

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

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

$$\begin{aligned} s_1^4 &= \left(\sum_n T_1 \right)^4 \\ &= \sum_n T_1^4 + 4 \sum_n T_1^3 T_2 + 12 \sum_n T_1^2 T_2 T_3 + 6 \sum_n T_1^2 T_2^2 + 24 \sum_n T_1 T_2 T_3 T_4. \end{aligned}$$

To understand how the coefficients of the sum are obtained, consider the number of ways the T_i can be arranged. For example, $T_1^4 = T_1 T_1 T_1 T_1$ can only be arranged in 1 way but $T_1^2 T_2 T_3 = T_1 T_1 T_2 T_3$ can be arranged in $\frac{4!}{2} = 12$ ways (where we divided by 2 since the two T_1 can be swapped in any given arrangement). Then

$$s_1^2 s_2 = \left(\sum_n T_1 \right)^2 s_2 = \left(\sum_n T_1^2 + 2 \sum_n T_1 T_2 \right) s_2 = \sum_n T_1^3 T_2 + \sum_n T_1^2 T_2 T_3 + 2 s_2^2.$$

So far we have

$$\begin{aligned} p_4 &= s_1^4 - 4 \left(s_1^2 s_2 - 2 s_2^2 - \sum_n T_1^2 T_2 T_3 \right) - 12 \sum_n T_1^2 T_2 T_3 - 6 \sum_n T_1^2 T_2^2 - 24 \sum_n T_1 T_2 T_3 T_4 \\ &= s_1^4 - 4 s_1^2 s_2 + 8 s_2^2 - 24 s_4 - 6 \sum_n T_1^2 T_2^2 - 8 \sum_n T_1^2 T_2 T_3. \end{aligned}$$

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

$$s_2^2 = \left(\sum_n T_1 T_2 \right)^2 = \sum_n T_1^2 T_2^2 + 2 \sum_n T_1^2 T_2 T_3 + 6 \sum_n T_1 T_2 T_3 T_4.$$

Finding the coefficients here is slightly trickier since s_2 contains pairs not all arrangements are allowed. For example, $T_1^2 T_2^2$ can only come from the pair $T_1 T_2$. On the other hand $T_1 T_2 T_3 T_4$ can come from $T_1 T_2$ and $T_3 T_4$ or $T_1 T_4$ and $T_2 T_3$ 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 $T_1 T_2 T_3 T_4$. Hence

$$\begin{aligned} p_4 &= s_1^4 - 4 s_1^2 s_2 + 8 s_2^2 - 24 s_4 - 6 \left(s_2^2 - 2 \sum_n T_1^2 T_2 T_3 - 6 s_4 \right) - 8 \sum_n T_1^2 T_2 T_3 \\ &= s_1^4 - 4 s_1^2 s_2 + 2 s_2^2 + 12 s_4 + 4 \sum_n T_1^2 T_2 T_3. \end{aligned}$$

Using Exercise 14.10 we get

$$\begin{aligned} p_4 &= s_1^4 - 4 s_1^2 s_2 + 2 s_2^2 + 12 s_4 + 4(s_1 s_3 - 4 s_4) \\ &= s_1^4 - 4 s_1^2 s_2 + 2 s_2^2 - 4 s_4 + 4 s_1 s_3 \end{aligned}$$

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.

□

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.

3.2 Field Extensions

3.3 Finite Fields

3.4 Separable and Normal Extensions