Galois Theory - 5122GALO6Y

Yoav Eshel

February 22, 2021

Contents

1 Summary

2 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 $\alpha_1, \ldots \alpha_n \in \mathbb{C}$ 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 $\mathrm{Gal}(f)$. 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
$$Aut(\mathbb{C}) \times \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$$
Then $Gal(f) := Im(\phi)$ where $\phi : Aut(\mathbb{C}) \to S_n$ mapping $\sigma \mapsto (\alpha_i \mapsto \sigma(\alpha_i))$

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

3 Symmetric Polynomials

A symmetric polynomial is a polynomial $F(X_1, X_2, \ldots, X_n)$ the is invariant under permutations of its variables. In other words
$$P(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})$$
for all $\sigma \in S_n$. Symmetric polynomials arise naturally in the study of the relation between the roots of a polynomial in one variable and its coefficients, since the coefficients can be given by polynomial expressions in the roots, and

all roots play a similar role in this setting. Let $f \in K(T)$ be a monic polynomial of degree n that splits completely in K. Then

$$f(T) = (T - X_1)(T - X_2)\cdots(T - X_n)$$

where X_i are the roots of f. Then

$$f(T) = T^n + s_1 T^{n-1} + \cdots + (-1)^n s_n$$

where

$$\begin{aligned}
s_1 &= X_1 + X_2 + \cdots + X_n \\
s_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\
&\vdots \\
s_n &= X_1X_2\cdots X_n
\end{aligned}$$

are called the *elementary symmetric polynomials* in $X_1, X_2, \dot{,} X_n$. Then the fundamental theorem of symmetric polynomials states that every symmetric polynomial can be written as a polynomial expression in the elementary symmetric polynomials.

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

$$\begin{aligned}
s_1 &= \sum_n T_1 \\
s_2 &= \sum_n T_1T_2 \\
&\vdots \\
s_n &= \sum_n T_1T_2\cdots T_n = T_1T_2\cdots T_n.
\end{aligned}$$

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 3.1 (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*

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

Wondering how it might be useful? Consider

$$s_1^4 = \left(\sum_n T_1\right)^4 = (T_1 + \cdots + T_n)(T_1 + \cdots + T_n)(T_1 + \cdots + T_n)(T_1 + \cdots + T_n).$$

After some thinking you might conclude that there are five possible representatives:

$$T_1^4, \quad T_1^3T_2, \quad T_1^2T_2^2, \quad T_1^2T_2T_3 \quad \text{and} \quad T_1T_2T_3T_4$$

(note the the degrees always add up to four). But what are the coefficients? That's when the orbit-stabilizer theorem comes to the rescue. Let the permutation group S_4 act on the set of indices by permuting them. Then the coefficients in front of $\sum_n T_1^4$ is the size of the orbit of $(1,1,1,1)$. Since every permutation in S_4 return the same sequence, the size of the orbit is $\frac{4!}{4!} = 1$. Then the coefficients in front of $\sum_n T_1^2T_2^2$ is the size of the orbit of $(1,1,2,2)$. The permutations that fix it are $(1),(12),(34)$ and $(12)(34)$. So the size of the stabilizer is 4 and the size of the orbit is $\frac{4!}{4} = 6$ Similarly, the coefficients in front of $\sum_n T_1^2T_2T_3$ is the size of the orbit of $(1,1,2,3)$. Since the stabilizer contains only the permutations that switches the 1s and fixes the other two elements (namely (1) and (12)) the size of the orbit is $\frac{4!}{2} = 12$. Lastly, the size of the orbit of $\sum_n T_1T_2T_3T_4$ is the 4! since there is no permutations (except the identity of course) that stabilizes it. We conclude that

$$s_1^4 = \sum_n T_1^4 + 6\sum_n T_1^2T_2^2 + 12\sum_n T_1^2T_2T_3 + 24\sum_n T_1T_2T_3T_4$$

4 Field Extensions

Prime Fields

Definition. *Let k be a field. Then the* ***prime field*** *in K is the intersection over all subfields of K*

Lemma 4.1. *Let K be a field of characteristic k. Then the prime field of K is $\mathbb{F}_p$ if $k = p$ and $\mathbb{Q}$ if $k = 0$.*

Algebraic and Transcendental Extensions

Let L/K be a field extensions. Then we say that $\alpha \in L$ is *algebraic* over K if there exists an $f \in K[x], f \neq 0$, such that $f(\alpha) = 0$. We say that α is *transcendental* over K if there exists no such f. The number of algebraic elements over $\mathbb{Q}$ in $\mathbb{C}$ is countable, so in fact $\mathbb{C}$ is mostly transcendental elements.

Theorem 4.2. *Let L/K be a field extension and take $\alpha \in L$. Then*

1. *If α is transcendental over k, then $K[\alpha] \simeq K[X]$*
2. *If α is algebraic over K then there exists $f \in K[X]$ monic and irreducible and*
$$K[X]/f \simeq K[\alpha] = K(\alpha)$$
and the degree of L over K is the degree of f.

Definition. *We say that an extension L/K is* ***algebraic*** *if $\forall \alpha \in L$, α is algebraic over K.*

Lemma 4.3. *If a field extension is finite then it is algebraic.*

The converse of this lemma does not hold.

5 Exercises

Symmetric Polynomial

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

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

$$s_1s_2 = \sum_n T_1 \sum_n T_1T_2 = \sum_n T_1^2T_2 + 3\sum_n T_1T_2T_3 = \sum_n T_1^2T_2 + 3s_3$$

Thus

$$\sum_n T_1^2T_2 = s_1s_2 - 3s_3$$

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

$$\begin{aligned}
s_1^2s_2 &= \left(\sum_n T_1\right)^2 \sum_n T_1T_2 \\
&= \left(\sum_n T_1^2 + 2\sum_n T_1T_2\right)\sum_n T_1T_2 \\
&= \sum_n T_1^2 \sum_n T_1T_2 + 2s_2^2 \\
&= \sum_n T_1^3T_2 + \sum_n T_1^2T_2T_3 + 2s_2^2.
\end{aligned}$$

And since

$$s_1s_3 = \sum_n T_1 \sum_n T_1T_2T_3 = \sum_n T_1^2T_2T_3 + 4\sum_n T_1T_2T_3T_4$$

it follows that $\sum_n T_1^2T_2T_3 = s_1s_3 - 4s_4$ and so

$$\sum_n T_1^3T_2 = s_1^2s_2 - s_1s_3 + 4s_4 - 2s_2^2$$

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

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 $f \in \mathbb{Q}[T_1, \ldots, T_n]$ 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 $f \in \mathbb{Q}[T_1, \ldots, T_n]$ 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. $\square$

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

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

Exercise 21.18
Let $K \subset L$ be an algebraic extension. For $\alpha, \beta \in L$ prove that we have

$$[K(\alpha,\beta):K] \leq [K(\alpha):K]\cdot[K(\beta):K]\,.$$

Show that equality does not always hold. Does equality always hold if $[K(\alpha):K]$ and $[K(\beta):K]$ are relatively prime?

Proof. Let f and g be the minimal polynomials of α and β (respectively) in $K[x]$ and f' be the minimal polynomial of α in $K(\beta)[x]$. If $\deg f' > \deg f$ then f is a lower degree polynomial in $K(\beta)[x]$ with $f(\alpha) = 0$ which is a contradiction. Hence $\deg f' \leq \deg f$ and so

$$\begin{aligned}[K(\alpha,\beta):K] &= [K(\alpha,\beta):K(\beta)]\cdot[K(\beta):K]\\ &= \deg f'\cdot\deg g\\ &\leq \deg f\cdot\deg g\\ &= [K(\alpha):K]\cdot[K(\beta):K]\,,\end{aligned}$$

as desired.

To show that equality does not always hold consider $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})$. Then $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$ but

$$[\mathbb{Q}(\sqrt{2},\sqrt[4]{2}):\mathbb{Q}] = 4\cdot[\mathbb{Q}(\sqrt{2},\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})] = 4 < 8$$

since $\left(\sqrt[4]{2}\right)^2 = \sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$

Lastly, suppose that $\deg f$ and $\deg g$ are relatively prime. Since

$$\begin{aligned}[K(\alpha,\beta):K] &= [K(\alpha,\beta),K(\alpha)]\cdot\deg f\\ &= [K(\alpha,\beta),K(\beta)]\cdot\deg g\end{aligned}$$

it follows that $[K(\alpha,\beta):K]$ is divisible by $\deg f$ and $\deg g$ and since they are relatively prime it is also divisible by $\deg f\cdot\deg g$. But we know that $[K(\alpha,\beta):K] \leq \deg f\cdot\deg g$ and so $[K(\alpha,\beta):K] = \deg f\cdot\deg g$. $\square$

Exercise 21.19
Let $K \subset K(\alpha)$ be an extension of odd degree. Prove that $K(\alpha^2) = K(\alpha)$.

Proof. Let f be the minimal polynomial of α in $K[x]$. Then $\deg f = 2n+1$ for some $n \in \mathbb{Z}_+$. Since $\alpha^2 \in K(\alpha)$ we get the tower $K(\alpha)/K\left(\alpha^2\right)/K$ and so

$$[K(\alpha):K] = \left[K(\alpha):K\left(\alpha^2\right)\right]\cdot\left[K\left(\alpha^2\right):K\right].$$

Let g be the minimal polynomial of α in $K\left(\alpha^2\right)$. Then $\deg g \leq 2$ since $x^2-\alpha^2 \in K\left(\alpha^2\right)$ is a polynomial with a root α. Since $[K(\alpha):K]$ is odd, it is not divisible by two and so $\deg g = 1$. Hence $\left[K(\alpha):K\left(\alpha^2\right)\right] = 1$ and it follows that $K(\alpha) = K\left(\alpha^2\right)$. $\square$

Exercise 21.23
Show that every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}\left(\sqrt{d}\right)$ with $d \in \mathbb{Z}$. For what d do we obtain the cyclotomic field $\mathbb{Q}(\zeta_3)$?

Proof. Let $K/\mathbb{Q}$ be a quadratic extension. Take $\alpha \in K \setminus \mathbb{Q}$. Then

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$$

and so

$$2 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \, [\mathbb{Q}(\alpha) : \mathbb{Q}] \, .$$

If $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$ then $\mathbb{Q}(\alpha) = \mathbb{Q}$ and so $\alpha \in \mathbb{Q}$, which contradicts our assumption. It follows that $[K : \mathbb{Q}(\alpha)] = 1$ and so $K = \mathbb{Q}(\alpha)$. Let

$$f(x) = x^2 + a_1 x + a_0 \in \mathbb{Q}[x]$$

be the minimal polynomial of α. Let $d = \frac{a_1^2}{4} - a_0 \in \mathbb{Q}$ and note that $a_0 = -\alpha a_1 - \alpha^2$. Then

$$\begin{aligned}
\sqrt{d} &= \sqrt{\frac{a_1^2}{4} - a_0} \\
&= \sqrt{\frac{a_1^2}{4} + a_1\alpha + \alpha^2} \\
&= \frac{a_1 + 2\alpha}{2}.
\end{aligned}$$

Hence $\sqrt{d} \in \mathbb{Q}(\alpha)$. By similar calculations we get $\alpha = \frac{2\sqrt{d} - a_1}{2} \in \mathbb{Q}(\sqrt{d})$. Hence $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. Of course, it is not yet the case the d is an integer. Suppose that $d = \frac{p}{q}$. Since $\sqrt{d} = \frac{1}{q^2}\sqrt{qp} \in \mathbb{Q}(\sqrt{qp})$ we have

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{qp})$$

with $qp \in \mathbb{Z}$ as desired. □

Exercise 21.24
Is every cubic extension of $\mathbb{Q}$ of the form $\mathbb{Q}\left(\sqrt[3]{d}\right)$ for some $d \in \mathbb{Q}$?

Solution. No.

Exercise 21.26
Let $M = \mathbb{Q}(\alpha) = \mathbb{Q}(1 + \sqrt{2} + \sqrt{3})$. Show that M is of degree 4 over $\mathbb{Q}$, determine the minimal polynomial and write $\sqrt{2}$ and $\sqrt{3}$ in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$. Also prove that the group $G = \mathrm{Aut}_{\mathbb{Q}}(M)$ is isomorphic to V_4 and that $f_{\mathbb{Q}}^{\alpha} = \prod_{\sigma \in G} X - \sigma(\alpha) \in \mathbb{Q}[X]$.

Solution. Let $\beta = \alpha - 1 = \sqrt{2} + \sqrt{3}$. Then clearly $M = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Let

$$\begin{aligned} f(x) &= (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \\ &= x^4 - 10x^2 + 1 \in \mathbb{Q}[x] \end{aligned}$$

and so $f(\beta) = 0$ by construction.

Is f the minimal polynomial of β in $\mathbb{Q}[x]$? It is if we can prove that $[M : \mathbb{Q}] = 4$. From

$$(\sqrt{2} + \sqrt{3})(\sqrt{3} - \sqrt{2}) = 1$$

It follows that $\beta^{-1} = \sqrt{3} - \sqrt{2}$. Therefore

$$\sqrt{2} = \frac{1}{2}(\beta - \beta^{-1}) \quad \text{and} \quad \sqrt{3} = \frac{1}{2}(\beta + \beta^{-1})$$

and so $M = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence we have the towers $M/\mathbb{Q}(\sqrt{2})/Q$ and $M/\mathbb{Q}(\sqrt{3})/Q$. Let $g(x) = x^2 - 3$. Suppose it is not the minimal polynomial of $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$. Then there exists $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ such that

$$0 = g(a + b\sqrt{2}) = a^2 + 2b^2 - 3 + 2ab\sqrt{2}.$$

But since

$$\begin{cases} a^2 + 2b^2 - 3 = 0 \\ 2ab = 0 \end{cases}$$

has no solutions it follows that no such element exists. Therefore g is the minimal polynomial of $\sqrt{3}$ and $[M : \mathbb{Q}(\sqrt{2})] = \deg g = 2$. Since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ in $\mathbb{Q}$ we conclude that

$$[M : \mathbb{Q}] = [M : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q})] = 4$$

and therefore f is the minimal polynomial of β.

Thus $f(x-1)$ is the minimal polynomial of α in $\mathbb{Q}$. From $f(\beta) = 0$ it follows that $1 = \beta(10\beta - \beta^3)$ and so $\beta^{-1} = 10\beta - \beta^3$. Hence

$$\sqrt{2} = \frac{1}{2}\left(\beta - \beta^{-1}\right) = \frac{1}{2}\left(\beta - 10\beta + \beta^3\right) = \frac{1}{2}\left(-9(\alpha - 1) + (\alpha - 1)^3\right)$$

and

$$\sqrt{3} = \frac{1}{2}\left(\beta + \beta^{-1}\right) = \frac{1}{2}\left(11(\alpha - 1) - (\alpha - 1)^3\right)$$

Let $G = \mathrm{Aut}(M)$ and take $\sigma \in G$. Then by definition $\sigma(1) = 1$ and it follows by induction and the properties of isomorphism that $\sigma(a) = a$ for all $a \in \mathbb{Z}$. Since $1 = \sigma(1) = \sigma(a \cdot a^{-1}) = \sigma(a) \cdot \sigma(a)^{-1} = a \cdot a^{-1}$ it also follows that $\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$. Hence σ restricted to $\mathbb{Q}$ is simply the identity map. Therefore σ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Since $0 = \sigma(0) = \sigma(\sqrt{2}^2 - 2) = \sigma(\sqrt{2})^2 - 2$ the only options are $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Similarly we conclude that $\sigma(\sqrt{3}) = \pm\sqrt{3}$. This gives four possible automorphism. Take $\sigma, \tau \in G$ such that $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(x) = x\ \forall x \in M \setminus \{\sqrt{2}\}$ and $\tau(\sqrt{3}) = -\sqrt{3}, \tau(x) = x$ $\forall x \in M \setminus \{\sqrt{3}\}$. Since

$$\sigma \circ \sigma = \tau \circ \tau = \sigma \circ \tau \circ \sigma \circ \tau = e$$

where e is the identity map it follows that G is isomorphic to V_4, the Klein four-group.

Lastly, consider

$$\begin{aligned}\tilde{f} &= \prod_{\sigma \in G} x - \sigma(\alpha)\\ &= (x - 1 - \sqrt{2} - \sqrt{3})(x - 1 + \sqrt{2} - \sqrt{3})(x - 1 - \sqrt{2} + \sqrt{3})\\ &\qquad (x - 1 + \sqrt{2} + \sqrt{3}).\end{aligned}$$

Hence $\tilde{f}(x) = f(x-1)$ which we already proved is the minimal polynomial of α in $\mathbb{Q}[x]$.

Exercise 21.29

Take $K = \mathbb{Q}(\alpha)$ with $f_{\mathbb{Q}}^{\alpha} = x^3 + 2x^2 + 1$.

1. Determine the inverse of $\alpha + 1$ in the basis $\{1, \alpha, \alpha^2\}$ of K over $\mathbb{Q}$.
2. Determine the minimal polynomial of α^2 over $\mathbb{Q}$.

Solution.

1. Since

$$\begin{aligned}0 &= \alpha^3 + 2\alpha^2 + 1\\ &= (\alpha + 1)(\alpha^2 + \alpha - 1) + 2.\end{aligned}$$

   It follows that $(\alpha + 1)^{-1} = -\frac{1}{2}(\alpha^2 + \alpha - 1)$.

2. From $\alpha^3 + 2\alpha^2 + 1 = 0$ it follows that $\alpha^3 = -2\alpha^2 - 1$. Squaring both sides we get that $\alpha^6 = 4\alpha^4 + 4\alpha^2 + 1$ or alternatively

$$\left(\alpha^2\right)^3 - 4\left(\alpha^2\right)^2 - 4\left(\alpha^2\right) - 1 = 0.$$

   By Ex. 19 we know that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$. Therefore the minimal polynomial of α^2 over $\mathbb{Q}$ has degree 3 and it follows that

$$f_{\mathbb{Q}}^{\alpha^2}(x) = x^3 - 4x^2 - 4x - 1.$$

Exercise 21.30

Define the cyclotomic field $\mathbb{Q}(\zeta_5)$ and let $\alpha = \zeta_5^2 + \zeta_5^3$.

1. Show that $\mathbb{Q}(\alpha)$ is a quadratic extension of $\mathbb{Q}$ and determine $f_{\mathbb{Q}}^{\alpha}$.

2. Prove: $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$

3. Prove: $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ and $\sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{8}}$

Proof.

1. The degree of the 5th cyclotomic polynomial

$$\Phi_5(x) = \prod_{\substack{1 \leq k \leq 5 \\ (k,5)=1}} \left(x - e^{\frac{2\pi k}{5} i}\right) = x^4 + x^3 + x^2 + x + 1$$

is 4 and since $\Phi_5 = f_{\mathbb{Q}}^{\zeta_5}$ it follows that $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Thus

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] \mid 4.$$

Note that $\zeta_5^3 = \frac{1}{\zeta_5^2} = \overline{\zeta_5^2}$. Hence $\alpha = \zeta_5^2 + \zeta_5^3 = \zeta_5^2 + \overline{\zeta_5^2} \in \mathbb{R}$ and so $\mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\zeta_5)$. Together with the fact that ζ_5 is a root of $x^3 + x^2 - \alpha \in \mathbb{Q}(\alpha)$ it follows that

$$1 < [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] \leq 3 \implies [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] = 2.$$

Finally, since $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\alpha)/\mathbb{Q}$ is a tower of fields and

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_5) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)]} = 2$$

it follows that $\mathbb{Q}(\alpha)$ is a quadratic extension.

Let $w = \zeta_5^2$. Then $\alpha = w + \frac{1}{w}$ and $\Phi_5(w) = 0$ by definition of Φ_5. Since $w \neq 0$ it follows that

$$\begin{aligned}
0 &= 1 + w + w^2 + w^3 + w^4 \\
0 &= \frac{1}{w^2} + \frac{1}{w} + 1 + w + w^2 \\
0 &= \left(w + \frac{1}{w}\right)^2 + w + \frac{1}{w} - 1 \\
0 &= \alpha^2 + \alpha - 1.
\end{aligned}$$

Since $x^2 + x - 1$ is monic polynomial of degree 2 we conclude that $f_{\mathbb{Q}}^{\alpha} = x^2 + x - 1$.

2. By construction α is a root of $x^2 + x - 1$ and so

$$\alpha \in \left\{ \frac{-1 \pm \sqrt{5}}{2} \right\}.$$

Since we can write α as polynomial in $\sqrt{5}$ and vice versa it follows that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

3. Let $\zeta_5 = e^{\frac{6\pi}{5}i}$. Then $w = \zeta_5^2 = e^{\frac{2\pi}{5}i}$ and

$$\cos\frac{2\pi}{5} = \frac{w+\overline{w}}{2} = \frac{\alpha}{2}.$$

Thus $2\cos\frac{2\pi}{5}$ is a root of f_Q^{α}. Since $\frac{2\pi}{5}$ is in the first quadrant, $\cos\frac{2\pi}{5}$ is positive and so

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

Therefore we also have

$$\begin{aligned}\sin\frac{2\pi}{5} &= \sqrt{1-\cos^2\frac{2\pi}{5}}\\ &= \sqrt{\frac{5+\sqrt{5}}{8}}.\end{aligned}$$

□

1. The degree of the pth cyclotomic polynomial is $\varphi(p) = p-1$ and so

$$4 = \deg\Phi_5 = [\mathbb{Q}(\zeta_5):\mathbb{Q}] = [\mathbb{Q}(\zeta_5):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]$$

Since ζ_5 is a root of $x^3+x^2-\alpha \in \mathbb{Q}(\alpha)[x]$ it follows that

$$[\mathbb{Q}(\zeta_5):\mathbb{Q}(\alpha)] \leq 3.$$

Thus the minimal polynomial of α over $\mathbb{Q}$ is of degree 2 or 4.

Let $f(x) = x^2+x-1 \in \mathbb{Q}[x]$. Then

$$\begin{aligned}f(\alpha) &= \alpha^2+\alpha-1\\ &= (\zeta_5^2+\zeta_5^3)^2+\zeta_5^2+\zeta_5^3-1\\ &= \zeta_5^4+2+\zeta_5^6+\zeta_5^2+\zeta_5^3-1 && \text{(Since } \zeta_5^5 = 1)\\ &= 1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_4^4.\end{aligned}$$

Since the 5th cyclotomic polynomial is given by

$$\Phi_5(x) = \prod_{\substack{1\leq k\leq 5\\(k,5)=1}}\left(x-e^{\frac{2\pi k}{5}i}\right) = x^4+x^3+x^2+x+1$$

and $\Phi_5(\zeta_5) = 0$ by definition it follows that $f(\alpha) = 0$. Since f is monic and of degree 2 it is the minimal polynomial of α over $\mathbb{Q}$. Hence $\mathbb{Q}(\alpha)$ is a quadratic extension.

2. Since α is a root of $f(x) = x^2+x-1$ and the roots of f are given by $\frac{-1\pm\sqrt{5}}{4}$ it follows that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

3. We know that

$$\frac{-1 \pm \sqrt{5}}{4} = \alpha = \zeta_5^2 + \zeta_5^3 = \cos\frac{4\pi k}{5} + \cos\frac{6\pi k}{5} + \left(\sin\frac{4\pi k}{5} + \sin\frac{6\pi k}{5}\right) i.$$

and since

$$\sin\frac{4\pi k}{5} + \sin\frac{6\pi k}{5} = 2\cos\frac{2\pi k}{10}\sin\pi k = 0, \quad k \in \mathbb{Z}$$

it follows that

$$\frac{-1 \pm \sqrt{5}}{4} = \cos\frac{4\pi k}{5} + \cos\frac{6\pi k}{5}.$$

Finite Fields

Separable and Normal Extensions