MA 454: Honors Galois Theory Notes

Lecturer: Ilya Shredkov
Transcribed by Josh Park

Spring 2025

Contents

Lecture 1

1 Introduction

1.1 Polynomials

Since ancient times, people have been interested in *polynomial equations*:

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \quad (n \geq 1), \tag{1}$$

where the coefficients a_i are in, say, $\mathbb{R}$. It was Évariste Galois (1811-1832) who characterized (1) that are *solvable by radicals*, transforming elementary algebra to higher algebra.

The case $n = 1$ is a trivial. If $n = 2$, we have get the general quadratic equation:

$$ax^2 + bx + c = 0 \quad (a \neq 0).$$

We can make the substitution $x = y - \frac{b}{2a}$, which gives us

$$y^2 = \frac{b^2 - 4ac}{4a^2} := \frac{D}{4a} \iff y = \pm\frac{\sqrt{D}}{2a},$$

hence $x_{1,2} = \frac{-b\pm\sqrt{D}}{2a}$. Here, D is the *discriminant* of the polynomial $f(x) = ax^2 + bx + c$.

One can check that $D = (x_1 - x_2)^2 \cdot a^2$. More generally, if we have

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

then the discriminant is given by

$$D = D(f) = \prod_{i<j}(x_i - x_j)^2 \cdot a_0^{2n-2},$$

where $x_1, \ldots, x_n$ are the complex roots of $f(x) = 0$.

Example 1.1. Consider the cubic equation

$$f(x) = ax^3 + bx^2 + cx + d$$

where x_1, x_2, x_3 are solutions of f. Then,

$$D = (x_1 - x_2)^2 \cdot (x_1 - x_3)^2 \cdot (x_2 - x_3)^2 \cdot a^4$$

Why do we square? Consider the discriminant as a polynomial in $x_1, \ldots, x_n$:

$$D(x_1, \cdots, x_n) = \prod_{i<j}(x_i - x_j)^2.$$

Then, $D(x_1, \cdots, x_n)$ is a *symmetric* polynomial, e.g.

$$D(x_1, x_2) = (x_1 - x_2)^2 = D(x_2, x_1) = b^2 - 4ac.$$

Definition 1 (Elementary symmetric polynomials in $x_1, \ldots, x_n$)**.**

$$\begin{aligned}
\sigma_1 &= \sigma_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n \\
\sigma_2 &= \sigma_2(x_1, \ldots, x_n) = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
\sigma_k &= \sigma_n(x_1, \ldots, x_n) = \sum_{i_1<\ldots<i_k} x_{i_1} \cdots x_{i_k} \quad (\# \text{ of terms is } \binom{n}{k}) \\
&\vdots \\
\sigma_n &= \sigma_n(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i
\end{aligned}$$

If we consider the group S_n of all permutations on n symbols, then $\forall k, \forall w \in S_n$,

$$\sigma_k(x_1, \dots, x_n) = \sigma_k(x_{w(1)}, \dots, x_{w(n)}).$$

More generally,

Definition 2 (Symmetric function)**.** Let $\phi(x_1, \dots, x_n)$ be a function. Then ϕ is *symmetric* if $\forall$ permutations $\omega \in S_n$, $\phi(x_1, \dots, x_n) = \phi(x_{\omega(1)}, \dots, x_{\omega(n)})$.

Theorem 1.1. *For $\forall$ symmetric function ϕ $\exists!$ polynomial $P(t_1, \dots, t_n)$ such that $\phi(x_1, \dots, x_n) = P(\sigma_1, \dots, \sigma_n)$.*

Moreover, if ϕ is a polynomial with coefficients in a ring R ($\phi \in R[x]$) then $P \in R[x]$.

Example 1.2. Let $n = 2$, $\phi(x_1, x_2) = x_1^2 + x_2^2 = (x_1^2 + x_2^2)^2 - 2x_1x_2$.

Theorem 1.2 (Vieta Formula)**.**

$$\begin{aligned} x^n + a_1x^{n-1} + \ldots + a_n = (x - x_1) \cdots (x - x_n) \\ &= x^n - \sigma_1(x_1, \dots, x_n)x^{n-1} + \sigma_2(x_1, \dots, x_n)x^{n-2} + \cdots \\ &\quad + (-1)^n\sigma_n(x_1, \dots, x_n) \end{aligned}$$

Corollary 1. *If $f \in R[x]$ where R is a ring and $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, then $D(f) \in R[a_1, \dots, a_n]$. That is, the discriminant is a polynomial in $a_1, \dots, a_n$ with coefficients from R.*

1.2 Cubic polynomials

If $ax^3 + bx^2 + cx + d = 0$, then one solution is

$$\begin{aligned} x = &\sqrt[3]{-\frac{1}{2}\left(\frac{2b^3 - 9abc + 27a^2d}{27a^3}\right) + \sqrt{\left(\frac{1}{2}\left(\frac{2b^3 - 9abc + 27a^2d}{27a^3}\right)\right)^2 + \left(\frac{3ac - b^2}{9a^2}\right)^3}} \\ &+ \sqrt[3]{-\frac{1}{2}\left(\frac{2b^3 - 9abc + 27a^2d}{27a^3}\right) - \sqrt{\left(\frac{1}{2}\left(\frac{2b^3 - 9abc + 27a^2d}{27a^3}\right)\right)^2 + \left(\frac{3ac - b^2}{9a^2}\right)^3}}, \end{aligned}$$

and the other two have similar expressions. Obviously this is not practical. Suppose we modify our polynomial:

$$x^3 + Ax^2 + Bx + C = \left(\underbrace{x + \frac{A}{3}}_{y}\right)^3 + p\left(x + \frac{A}{3}\right) + q$$

for some p, q, so we can simply consider the equation $x^3 + px + q = 0$

$$\left(\underbrace{a + b}_{x}\right)^3 = 3ab(a + b) + a^3 + b^3$$
$$x^3 - 3abx - a^3 - b^3 = 0, \quad x_1 = a_b$$

$$x_1 + x_2 + x_3 = 0 \implies x_2 + x_3 = -a - b$$
$$x_1x_2 + x_1x_3 + x_2x_3 = a^3 + b^3 \implies x_2x_3 = \frac{a^3 + b^3}{x_1} = \frac{a^3 + b^3}{a + b} = a^2 - ab + b^2$$

Theorem 1.3 (Inverse Vieta Theorem)**.**

Example 1.3 (Root of unity). ε

Example 1.4. What about $x^3 + px + q = 0$?

1.3 Quadric Method

Let $f(x) = x^4 + ax^2 + bx + c = 0$.

1. If $b = 0$, it is simply a quadratic equation.
2. If $x^4 - g^2(x) = 0 \implies x^2 = g(x), x^2 = -g(x)$

$$
\begin{aligned}
f(x) &= \left(x^2 + \frac{y}{2}\right)^2 + (a-y)x^2 + bx + c - \left(\frac{y^2}{4}\right) \\
D &= b^2 - 4(a-y)(c - \frac{y^2}{4}) = 0
\end{aligned}
$$

Definition 3 (Ferrari's Resolvent). $y^3 - ay^2 - 4cy + 4ac - b^2 = 0$

$$
\begin{aligned}
g(x) &= Ax + B \\
0 = f(x) &= \left(x^2 + \frac{y}{2}\right)^2 - (Ax+B)^2 \\
&= \left(x^2 + \frac{y}{2} - Ax - B\right)\left(x^2 + \frac{y}{2} + Ax + B\right)
\end{aligned}
$$

$$
\begin{aligned}
x_1 + x_2 = A;\ x_1x_2 &= \frac{y}{2} - B \\
x_3 + x_4 = -A;\ x_3x_4 &= \frac{y}{2} + B
\end{aligned}
$$

$$
\begin{aligned}
x_1x_2 + x_3x_4 &= y_1 \\
x_1x_3 + x_2x_4 &= y_2 \\
x_1x_4 + x_2x_3 &= y_3 \\
x_1 + x_2 + x_3 + x_4 &= 0
\end{aligned}
$$

Suppose we have some quadric equation $f(x) = x^4 + ax^2 + bx + c$. Then we have unknown roots x_1, x_2, x_3, and x_4.

Claim 1. *y_1, y_2, y_3 are roots of a cubic equation*

$y_1 + y_2 + y_3 = \sigma_2(x_1, x_2, x_3, x_4) = a$
$\sigma_2(y_1, y_2, y_3) = \phi(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$

Example 1.5. Consider the polynomial $\phi(x_1, x_2, x_3, x_4) = x_1 + x_2 - x_3 - x_4$

$$
\begin{cases}
z_1 = (x_1 + x_2 - x_3 - x_4)^2 \\
z_2 = (x_1 - x_2 + x_3 - x_4)^2 \\
z_3 = (x_1 - x_2 - x_3 + x_4)^2
\end{cases}
$$