## Lecture 7 : Symmetric Polynomials II

---

### Objectives

(1) Discriminant in terms of power-sum symmetric polynomials.
(2) Discriminant of a cubic.
(3) Existence of a splitting field of a polynomial.
(4) Fundamental theorem of algebra via symmetric polynomials.

**Key words and phrases:** Discriminant of a polynomial, splitting field, fundamental theorem of algebra.

---

**Discriminant of a polynomial:** We discuss a method to calculate the discriminant of a polynomial by employing Newton's identities.

**Definition 7.1.** *Let $u_1, u_2, \ldots, u_n, x$ be indeterminate and*

$$f(x) = (x - u_1)(x - u_2)\ldots(x - u_n).$$

*The discriminant of $f(x)$ is the symmetric function*

$$disc\,(f(x)) = \Pi_{i<j}(u_i - u_j)^2$$

It is clear that $f(x)$ has a repeated root if and only if disc $(f) = 0$. Since disc $(f)$ is a symmetric polynomial with integer coefficients, by the fundamental theorem for symmetric polynomials, there exists a polynomial $g(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$ such that disc $(f) = g(\sigma_1, \sigma_2 \ldots, \sigma_n)$. The van der Monde matrix

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2 & \cdots & u_n \\ u_1^2 & u_2^2 & \cdots & u_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ u_1^{n-1} & u_2^{n-1} & \cdots & u_n^{n-1} \end{bmatrix}$$

has determinant $\det M = \Pi_{i>j}(u_i - u_j)$. Hence

$$\text{disc }(f) = \det(MM^t) = \begin{vmatrix} n & w_1 & w_2 & \cdots & w_{n-1} \\ w_1 & w_2 & w_3 & \cdots & w_n \\ w_2 & w_3 & w_4 & \cdots & w_{n+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ w_{n-1} & w_n & w_{n+1} & \cdots & w_{2n-2} \end{vmatrix}.$$

**Example 7.2.** Using Newton's identities, we calculate the discriminant of the polynomial $p(x) = x^3 + px + q$. We have $\sigma_1 = 0, \sigma_2 = p, \sigma_3 = -q$ and

$$MM^t = \begin{bmatrix} 3 & w_1 & w_2 \\ w_1 & w_2 & w_3 \\ w_2 & w_3 & w_4 \end{bmatrix}$$

Newton's identities in this case are

$$\begin{aligned} w_1 &= \sigma_1 = 0 \\ w_2 &= \sigma_1^2 - 2\sigma_2 = -2p \\ w_3 &= \sigma_1 w_2 - \sigma_2 w_1 + 3\sigma_3 = -3q \\ w_4 &= \sigma_1 w_3 - \sigma_2 w_2 + \sigma_3 w_1 = 2p^2 \end{aligned}$$

Therefore

$$\text{disc }(f) = \det MM^t = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -4p^3 - 27q^2.$$

In this section we construct a field extension $K/F$ which contains all the roots of a given polynomial $f(x) \in F[x]$. For simplicity, we want $K$ to be the smallest field containing $F$ with respect to this property.

**Definition 7.3.** *Let $F$ be a field and $f(x) \in F[x]$ be a monic polynomial of degree $n$. A field $K \supseteq F$ is called a* **splitting field of** $f(x)$ **over** $F$ *if there exist $r_1, r_2, \ldots, r_n \in K$ so that $f(x) = (x - r_1)\ldots(x - r_n)$ and $K = F(r_1, r_2, \ldots, r_n)$.*

**Example 7.4.** (i) Let $f(x) = x^2 + ax + b \in F[x]$. If $f(x)$ is reducible then $F$ is a splitting field of $f(x)$. If $f(x)$ is irreducible then $(f(x))$ is a maximal ideal of $F[x]$. Hence $F(x)/(f(x)) \simeq F(r)$ is a field, where $r = x + (f(x))$. If

$s$ is another root of $f(x)$, then $s + r = -a$, so $s = -a - r \in F(r)$. Hence $F(r)$ is a splitting field of $f(x)$ over $F$.

(ii) Consider the irreducible polynomial $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Let $r = x + (f(x)) \in \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_2(r)$. Since $[\mathbb{F}_2(r) : \mathbb{F}_2] = 3$, $\mathbb{F}_2(r)$ has 8 elements. A basis of the $\mathbb{F}_2-$vector space $\mathbb{F}_2(r)$ is $\{1, r, r^2\}$. Hence

$$\mathbb{F}_2(r) = \{0, 1, r, r^2, 1 + r, 1 + r^2, r + r^2, 1 + r + r^2\}$$

and we have the relation $r^3 = 1+r$. Check that $f(r^2) = f(r^4) = 0$. Therefore

$$x^3 + x + 1 = (x + r)(x + r^2)(x + r^4).$$

Thus $\mathbb{F}_r(r)$ is a splitting field of $x^3 + x + 1$ over $\mathbb{F}_2$.

We will later see that if $f(x) \in \mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field with $q$ elements, then $\mathbb{F}_q[x]/(f(x))$ is a splitting field of $f(x)$, if $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$.

**Existence of Splitting field**

**Theorem 7.5.** *Let $F$ be a field. Then any polynomial $f(x) \in F[x]$ of positive degree has a splitting field.*

*Proof.* Apply induction on $\deg f$. If $\deg f = 1$ then $F$ is the splitting field of $f$ over $F$. Suppose $\deg f > 1$. If $f(x)$ splits as a product of linear factors in $F[x]$ then $F$ is the splitting field of $f(x)$ over $F$. Suppose $g(x)$ is an irreducible factor of $f(x)$ with $\deg g \geq 2$. Then $r = x + (g(x)) \in K := F[x]/(g(x))$ is a root of $g(x)$ and hence of $f(x)$. Since $f(x) = (x - r)h(x)$ for some $h(x) \in K[x]$ and $\deg h(x) < \deg f(x)$. By induction $h(x)$ has a splitting field $L$ over $K$. Let $r_2, r_3, \ldots, r_n \in L$ be the roots of $h(x)$. Then $L = K(r_2, r_3, \ldots, r_n) = F(r_1, r_2, \ldots, r_n)$ is the required splitting field. □

We end this section by presenting a proof of the fundamental theorem of algebra due to Gauss.

**Theorem 7.6** (**The Fundamental Theorem of Algebra).** *Every complex polynomial of positive degree has a complex root.*

*Proof.* We shall use the following facts:
(i) Every odd degree polynomial with real coefficients has a real root.

(ii) Every quadratic polynomial in $\mathbb{C}[x]$ has a complex root.
(iii) The fundamental theorem for symmetric polynomials.
(iv) Every polynomial $f(x)$ has a splitting field.

(i) This is a consequence of the Intermediate Value Theorem.

(ii) It is enough to show that complex numbers have a complex square root. Indeed, let $z = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$ and $(c + di)^2 = a + bi$. Then $c^2 - d^2 + 2cdi = a + bi$. Thus $a = c^2 - d^2$ and $b = 2cd$. Therefore

$$\begin{aligned} a^2 + b^2 &= (c^2 + d^2)^2 \\ c^2 + d^2 &= \sqrt{a^2 + b^2} \in \mathbb{R}. \end{aligned}$$

Therefore $c^2 = \frac{1}{2}[a + \sqrt{a^2 + b^2}] \geq 0$ and $d^2 = \frac{1}{2}[\sqrt{a^2 + b^2} - a] \geq 0$. Thus $c, d \in \mathbb{R}$.

The polynomial $g(x) = f(x)\bar{f}(x) \in \mathbb{R}[x]$. Here $\bar{f}$ denotes the polynomial whose coefficients are conjugates of the coefficients of $f(x)$. If $g(x)$ has a complex root $z$ then either $f(z) = 0$ or $\bar{f}(z) = 0$. If $\bar{f}(z) = 0$, then $f(\bar{z}) = 0$. Thus by replacing $f$ by $g$, we may assume that $f(x)$ is a monic polynomial with real coefficients.

Let $d = \deg f = 2^n q$, where $q$ is odd. We apply induction on $n$. If $n = 0$, then $f$ is a real odd degree polynomial, hence it has a real root. Now let $n \geq 1$. Let $K = \mathbb{C}(\alpha_1, \ldots, \alpha_2)$, be a splitting field of $f(x)$, over $\mathbb{C}$, where $\alpha_1, \ldots, \alpha_d$ are the roots of $f(x)$ in $K$. Consider the elements

$$y_{ij} = \alpha_i + \alpha_j + r\alpha_i\alpha_j,$$

where $r \in \mathbb{R}$ is fixed and $1 \leq i \leq j \leq d$. There are $\binom{d+1}{2}$ such pairs $(i, j)$. Hence

$$\deg h(x) = \prod_{1 \leq i \leq j \leq d} (x - y_{ij}) = \binom{d+1}{2} = 2^{n-1}q(d+1).$$

The coefficients of $h(x)$ are elementary symmetric polynomials in $y_{ij}$'s. So they are symmetric polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_d$. Hence they are polynomials in the coefficients of $f(x)$. Hence $h(x) \in \mathbb{R}[x]$. By induction on $n$, $h(x)$ has a complex root say $z_r$. Since all the roots of $h(x) \in K$ and $z_r \in \mathbb{C} \subseteq K$,

$$z_r = \alpha_{i(r)} + \alpha_{j(r)} + r\alpha_{i(r)}\alpha_{j(r)}$$

for some pair $(i(r), j(r))$ so that $1 \leq i(r) \leq j(r) \leq d$. Define

$$\varphi : \mathbb{R} \to \{(i,j) \mid 1 \leq i(r) \leq j(r) \leq d\} = P,\ \varphi(r) = (i(r), j(r)).$$

Since $\mathbb{R}$ is infinite and $P$ is finite, there exists $c \neq d \in \mathbb{R}$ such that $(i(c), j(c)) = (i(d), j(d)) := (a, b)$. Therefore,

$$z_c = \alpha_{i(c)} + \alpha_{j(c)} + r\alpha_{i(c)}\alpha_{j(c)} = \alpha_a + \alpha_b + c\alpha_a\alpha_b = z_d = \alpha_a + \alpha_b + d\alpha_a\alpha_b.$$

Therefore $(d-c)\alpha_a\alpha_b = z_d - z_c \in \mathbb{C}$. Hence $\alpha_a\alpha_b \in \mathbb{C}$ so that $\alpha_a + \alpha_b \in \mathbb{C}$. But $\alpha_a$ and $\alpha_b$ are roots of

$$x^2 - (\alpha_a + \alpha_b)x + \alpha_a\alpha_b \in \mathbb{C}[x].$$

Hence $\alpha_a, \alpha_b \in \mathbb{C}$. Therefore $f(x)$ has a complex root. $\square$