Last time $\mathbb{H}_0 := \{\text{quaternions } q \in \mathbb{H} \mid \overline{q} = -q\} \simeq \mathbb{R}^3$.

Theorem $\forall$ rotation in $\mathbb{R}^3 \simeq \mathbb{H}_0 = R_x$ for some $x \in \mathbb{H}^\times, N(x) = 1$ where $R_x(q) = xqx^{-1}, q \in \mathbb{H}_0$.

Corollary Let $u \in \mathbb{H}_0, N(u) = 1$ and $\theta \in \mathbb{R}$. Then $R_u(\theta) = R_x, x = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}u$.

Proof Check that: $\overline{u} = -u$.

$$\begin{aligned} N(x) = x\overline{x} &= \left(\cos\theta + \sin\frac{\theta}{2}u\right)\left(\cos\theta - \sin\frac{\theta}{2}u\right) \\ &= \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2}u^2. \end{aligned}$$

$1 = u\overline{u} = -u^2 \implies N(x) = \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1$.

If $u = \mathrm{i}$, we know that $R_u(\theta) = R_x$ for the x above. In general, $\exists$ rotation P in $\mathbb{H}_0 \simeq \mathbb{R}^3$ s.t. $P(\mathrm{i}) = u$.

Known: $R_u(\theta) = PR_{\mathrm{i}}(\theta)P^{-1} \overset{\text{Thm}}{=} R_y R_{\mathrm{i}}(\theta) R_{y^{-1}} = R_x$ where

$$\begin{aligned} x &= y\left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\mathrm{i}\right)y^{-1} \\ &= y\cos\frac{\theta}{2}y^{-1} + y\sin\frac{\theta}{2}\mathrm{i}y^{-1} \\ &= \cos\frac{\theta}{2} + \sin\frac{\theta}{2}y\mathrm{i}y^{-1} \\ &= \cos\frac{\theta}{2} + \sin\frac{\theta}{2}u \end{aligned}$$

since $y\mathrm{i}y^{-1} = R_y(\mathrm{i}) = P(\mathrm{i}) = u$. □

Remarks

1. $\{x \in \mathbb{H}^\times : N(x) = 1\} \overset{2:1}{\twoheadrightarrow} \{\text{rotations in } \mathbb{H}_0 \simeq \mathbb{R}^3\}$.
2. $R_u(\theta) = R_x$ where $x = e^{\psi u} = \sum_{n=0}^{\infty} \frac{\psi^n u^n}{n!} = \cos\psi + \sin\psi \cdot u, \psi := \frac{\theta}{2}$. Convergence can be achieved in $\mathbb{H} \simeq \mathbb{R}^4$, and the proof is same as the proof for $e^{\mathrm{i}\psi} = \cos\psi + \sin\psi \cdot \mathrm{i}$.

§ Symmetric Polynomials

Recall A **ring** is a set R with $+$(commutative), $\cdot, 0_R, 1_R$ with associativity, distributativity and some other properties. We denote the invertibles of R as $R^\times$. A **division ring** is a non-zero ring s.t. $R^\times = R \setminus \{0\}$. A **field** is a commutative division ring.

Examples $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, $\mathbb{H}$ is a division ring, $M_{n\times n}(\mathbb{F})$ is a ring for all fields $\mathbb{F}$, $R[x] := \{\text{polynomials } f = c_0 + c_1 X + \dots + c_n X^n \mid c_i \in R\}$ is a commutative ring when R is also a commutative ring. $R[X, Y, \dots] = \{\text{polynomials in } X, Y, \dots \text{ with coefficient} \in R\}$ is also a commutative ring.

Now we fix a field $\mathbb{F}$ and $n \in \mathbb{Z}_{\geq 1}$. Define $S_n = \left\{\text{permutations } \sigma : \{1, \dots, n\} \overset{1:1}{\to} \{1, \dots, n\}\right\}$. $\forall f \in \mathbb{F}[X_1, \dots, X_n], \forall \sigma \in S_n$, set $\sigma f := f\left(X_{\sigma(1)}, \dots, X_{\sigma(n)}\right) \in \mathbb{F}[X_1, \dots, X_n]$.

Then

$$\mathrm{id} \cdot f = f,$$
$$\forall \sigma, \tau \in S_n, (\sigma\tau)f = \sigma(\tau f),$$

$$\begin{aligned}\because \sigma(\tau(f))(X_1,...,X_n) &= (\tau f)\left(X_{\sigma(1)},...,X_{\sigma(n)}\right)\\ &= (\tau f)(Y_1,...,Y_n)\\ &= f\left(Y_{\tau(1)},...,Y_{\tau(n)}\right)\\ &= f\left(X_{\sigma\tau(1)},...,X_{\sigma\tau(n)}\right).\end{aligned}$$

Definition If $f \in \mathbb{F}[X_1,...,X_n]$ satisfies $\forall \sigma \in S_n, \sigma f = f$, we say f is a **symmetric polynomial**. All symmetric polynomials in $\mathbb{F}[X_1,...,X_n]$ are denoted as $\mathbb{F}[X_1,...,X_n]^{S_n} := \{\text{symmetric } f\}$.

Properties

1. Subring of $\mathbb{F}[X_1,...,X_n]$, since $\sigma(f+g) = \sigma f + \sigma g, \sigma(fg) = (\sigma f)(\sigma g), \sigma(1) = 1$.
2. $\mathbb{F}[X_1,...,X_n]^{S_n} \supset \mathbb{F} = \{\text{const polynomials}\}$.

$\Longrightarrow \mathbb{F}[X_1,...,X_n]^{S_n}$ is an $\mathbb{F}$-vector subspace of $F[X_1,...,X_n]$.

Examples

1. Power sum $p_k := X_1^k + ... + X_n^k, \quad k \geq 0$.
2. Elementary symmetric polynomials $e_k := \sum\limits_{1 \leq i_1 < ... < i_k \leq n} X_{i_1}...X_{i_k}, \quad \forall 1 \leq k \leq n$.

   Set $e_0 := 1$ to get $(Y+X_1)...(Y+X_n) = \underbrace{Y^n}_{=e^0 Y^n} + e_1 Y^{n-1} + ... + e_n$ where Y is another variable (**Vieta**).

$f \in \mathbb{F}[X_1,...,X_n], g_1...g_n \in \mathbb{F}[Y_1,...,Y_m]$, then evaluation function $f(g_1,...,g_n) \in \mathbb{F}[Y_1,...,Y_m]$.

Theorem (对称多项式基本定理, 存在性) $\forall f \in \mathbb{F}[X_1,...,X_n]^{S_n}, \exists g \in \mathbb{F}[X_1,...,X_n]$ s.t. $f = g(e_1,...,e_n)$.

$\forall f \in \mathbb{F}[X_1,...,X_n]$, write $f = \sum_{d \geq 0} f_d$,

$$f_d := \sum_{i_1+...+i_n=d} c_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n},$$

which is called the d-homogeneous part of f if $f = \sum_{i_1,...,i_n \geq 0} c_{i_1,...,i_n} X_1^{i_1},...,X_n^{i_n}$.

When $f = f_d$, we say f is **homogeneous** of degree d.

Lemma Let $f \in \mathbb{F}[X_1,...,X_n]^{S_n}$, then $f(X_1,...,X_{n-1},0) = 0 \Longleftrightarrow e_n \mid f$.

Proof $(\Longleftarrow)$ $0 = e_n(X_1,...,X_{n-1},0) \mid f(x_1,...,X_{n-1},0)$.

$(\Longrightarrow)$ $f = \sum c_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n}$. Now $f(X_1,...,X_{n-1},0) = \sum_{i_n=0} c_{i_1,...,0} X_1^{i_1}...X_{n-1}^{i_{n-1}} = 0$ implies $c_{i_1,...,i_n} \neq 0 \Longrightarrow i_n \geq 1$. Since f is symmetric, $c_{i_1,...,i_n} \neq 0 \Longrightarrow i_k \geq 1, \quad \forall k$. Hence $e_n \mid f$.□

Proof of Theorem Let $f \in \mathbb{F}[X_1,...,X_n]^{S_n}$. $\forall d \geq 0, f_d$ is symmetric $\Longrightarrow$ Reduce to the case $f = f_d$ for some d. $\forall g \in F[X_1,...,X_n]$, define its **weight**

$$\mathrm{wt}(g) := \begin{cases}\max\left\{\sum\limits_{k=1}^{n} k i_k \mid c_{i_1,...,i_n} \neq 0\right\}, & g \neq 0\\ -\infty, & g = 0.\end{cases}$$

To show: If $f = f_d$, then $\exists g$ s.t. $\mathrm{wt}(g) \le d$ and $f = g(e_1, ..., e_n)$.
Induction on $n + d$:

- If $d = 0$ i.e. $n + d = 1$, then $f \in \mathbb{F}$ and we can take $g = f, \mathrm{wt}(g) = 0/\infty$ when $f \neq 0/f = 0$, respectively.
- Assume $d \ge 1. \forall h \in \mathbb{F}[X_1, ..., X_n]$, define $h^\flat := h(X_1, ..., X_{n-1}, 0) \in \mathbb{F}[X_1, ..., X_{n-1}]$, and $d = 1$ gives elements in $\mathbb{F}$.
  h symmetric $\Longrightarrow h^\flat$ also symmetric in $n - 1$ variables. Hence $f^\flat$ is still homogeneous of degree d, and $e_i^\flat$ is the elementary symmetric polynomial with $n - 1$ variables.

  By induction $\exists g_1 \in \mathbb{F}[X_1, ..., X_{n-1}]$ s.t. $f^\flat = g\left(e_1^\flat, ..., e_n^\flat\right), \mathrm{wt}(g) \le d$.

  Observation $\deg g_1(e_1, ..., e_{n-1}) \le \mathrm{wt}(g_1) \le d$.

  Hence

  $$f_1 := f - g_1(e_1, ..., e_{n-1})$$

  with deg $\le d$ is symmetric (in n variables), and

  $$f_1^\flat = f^\flat - g_1\left(e_1^\flat, ..., e_{n-1}^\flat\right) = 0 \quad \overset{\text{Lem}}{\Longrightarrow} \quad e_n \mid f_1.$$

  Note that

  $$f_2 := \frac{f_1}{e_n} \in \mathbb{F}[X_1, ..., X_n]$$

  is symmetric and deg $f_2 \le d - n$. Write $f_2 = \sum_{d' \ge 0} f_{2,d'}$.

  By induction (applied to $\forall f_{2,d'}$) we get g_2 s.t. $f_2 = g_2(e_1, ..., e_n), \mathrm{wt}(g) \le d - n$.

  $$\begin{aligned} f &= f_1 + g_1(e_1, ..., e_{n-1}) \\ &= e_n f_2 + g_1(e_1, ..., e_{n-1}) \\ &= g(e_1, ..., e_n), \end{aligned}$$

  with $g = X_n g_2 + g_1$.

  Here $\mathrm{wt}(g) \le \max\{\mathrm{wt}(X_n g_2), \mathrm{wt}(g_1)\} \le d$. $\square$

Remark Can replace $\mathbb{F}$ by any commutative ring in the above since we did not use any division.

Theorem (对称多项式基本定理, 唯一性) $g_1(e_1, ..., e_n) = g_2(e_1, ..., e_n) \Longrightarrow g_1 = g_2$.

Proof $(g_1 - g_2)(e_1, ..., e_n) = 0$. Suffices to show: $g \in \mathbb{F}[X_1, ..., X_n]$,

$$\begin{aligned} g(e_1, ..., e_n) = 0 \quad &\Longrightarrow \quad g = 0 \\ \text{or} \qquad g \neq 0 \quad &\Longrightarrow \quad g(e_1, ..., e_n) \neq 0. \end{aligned}$$

The proof can be completed in the following steps:

1. May enlarge the field $\mathbb{F} \Longrightarrow$ may assume $\mathbb{F}$ is infinite, eg. $F \hookrightarrow F(t)$: real functions.
2. $\mathbb{F}$ infinite, $g \neq 0 \overset{\text{Fact}}{\Longrightarrow} \exists (y_1, ..., y_n) \in \mathbb{F}^n$ s.t. $g(y_1, ..., y_n) \neq 0$.
3. Consider $p := X^n - y_1 X^{n-1} + ... + (-1)^n y_n \in \mathbb{F}[X]$.
   $\exists$ extension of fields $F \hookrightarrow L$ s.t. p splits in L, i.e.

$$p = \prod_{i=1}^{n} (X - x_i) \Longrightarrow e_k(x_1, ..., x_n) = y_k, \quad \forall 1 \le k \le n.$$

Now set $X_i = x_i$ in step 3 above, then

$$g(e_1, ..., e_n) = g(y_1, ..., y_n) \neq 0 \quad \Longrightarrow \quad g(e_1, ..., e_n) \neq 0.$$

$\square$

Fact Let F : infinite field, $g \in \mathbb{F}[X_1, ..., X_n], g \neq 0$. Then $\exists (y_1, ..., y_n) \in \mathbb{F}^n, g(y_1, ..., y_n) \neq 0$.

Proof

- $n = 1$: g has at most $\deg g$ roots in F.
- $n > 1$: Let $g = \sum_{k \ge 0} g_k X_n^k \neq 0$, $g_k \in \mathbb{F}[X_1, ..., X_{n-1}] \Longrightarrow \exists k, g_k \neq 0$.

  By induction,

$$\begin{aligned} &\exists (y_1, ..., y_{n-1}), g_k(y_1, ..., y_{n-1}) \neq 0 \\ \Longrightarrow\ & g(y_1, ..., y_{n-1}, X_n) \in \mathbb{F}[X_n] \setminus \{0\} \\ \Longrightarrow\ & \exists y_n \in \mathbb{F}, g(y_1, ..., y_n) \neq 0. \quad (n = 1 \text{ case}) \end{aligned}$$

$\square$

Remark If $\mathbb{F}$ is a subfield of $\mathbb{C}$, we may work with $L = \mathbb{C}$.