Topic: Symmetric Polynomials.

Recall that for any ring R and any symbol "x" we define a ring of formal polynomial expressions:

$$R[x] = \left\{ f(x) = \sum_{k\geq 0} a_k x^k \; : \; a_k \in R \right\}.$$

If x_1, x_2 are two symbols, we define the ring $R[x_1, x_2]$ by induction:

$$R[x_1, x_2] = \left(R[x_1]\right)[x_2]$$

$$= \left\{ \sum_{k\geq 0} f_k(x_1)\, x_2^k \; : \; f_k(x_1) \in R[x_2] \right\}$$

$$\left[\text{Say } f_k(x_1) = \sum_{l \geq 0} a_{kl}\, x_1^l \right]$$

$$= \left\{ \sum_{\substack{k\geq 0 \\ l \geq 0}} a_{kl}\, x_1^l x_2^k \; ; \; a_{kl} \in R \right\}$$

Cute notation:

$$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} = \overline{x}^{\overline{k}}$$

where $\overline{x} = (x_1, \dots, x_n)$, $\overline{k} = (k_1, k_2, \dots, k_n)$

Then multivariable polynomial looks like

$$f(\bar{x}) = \sum_{\bar{k} \in \mathbb{N}^n} a_{\bar{k}} \bar{x}^{\bar{k}}, \quad a_{\bar{k}} \in R$$

What about "degree"? We need to define an ordering on the set of exponent vectors $\mathbb{N}^n$.

Def: Lexicographic ordering.
(Dictionary)

$(i_1, \dots, i_n) > (j_1, \dots, j_n)$ if $i_1 = j_1$, $i_2 = j_2$,

$\dots$ $i_k = j_k$, $i_{k+1} > j_{k+1}$ for some k.

In the first place where they differ, i is larger than j.

e.g. $(0,0,0) < (0,0,1) < (0,0,12)$

$< (0,1,3) <$ etc...

Definition: Given $f(\bar{x}) = f(x_1, \dots, x_n)$ we define

$\deg(f)$ = lex-highest exponent vector that occurs.

e.g. $\deg\left(\underset{(1,0,0)}{2x_1} + \underset{(2,1,0)}{3x_1^2 x_2^1} - \underset{(1,1,5)}{\tfrac{1}{2} x_1 x_2 x_3^5} \right)$

$= (2,1,0)$

Nice Property of Degree: If ring of coefficients is an integral domain ($ab = 0 \Rightarrow a = 0$ or $b = 0$) then for all $f, g \in R[x_1, \dots, x_n]$ we have

$$\deg(fg) = \deg(f) + \deg(g)$$

addition of vectors!

Proof: If $f(\bar{x}) = a\bar{x}^{\bar{m}}$ + Lower terms
$g(\bar{x}) = b\bar{x}^{\bar{n}}$ + Lower terms

then $f(\bar{x})g(\bar{x}) = ab\,\bar{x}^{\bar{m}+\bar{n}}$ + Lower terms. ///

e.g. $\underset{(1,1)}{x_1 x_2} + \underset{(1,0)}{x_1} + \underset{(0,1)}{x_2}) (\underset{(2,0)}{x_1^2} + \underset{(1,1)}{x_1 x_2})$

$= x_1^3 x_2^1$ + lower terms

$(3,1) = (1,1) + (2,0)$

Why do we care?

we say $S(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ is symmetric if for all $i<j$,

$$S(\dots, x_i, \dots, x_j, \dots) = S(\dots, x_j, \dots, x_i, \dots)$$

e.g. The elementary symmetric polynomials $e_1, e_2, \dots, e_n \in R[x_1, \dots, x_n]$ are defined as

$$e_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n$$
$$e_2(x_1, \dots, x_n) = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n$$
$$e_3(x_1, \dots, x_n) = x_1 x_2 x_3 + \dots + x_{n-2} x_{n-1} x_n$$
$$\vdots \qquad = \sum_{i<j<k} x_i x_j x_k$$
$$e_n(x_1, \dots, x_n) = x_1 x_2 \cdots x_n .$$

Alternatively:

$$(y-x_1)(y-x_2)\cdots(y-x_n)$$
$$= y^n - e_1 y^{n-1} + e_2 y^{n-2} - \cdots + (-1)^n e_n .$$

$\deg(e_1) = ?$

$$\deg(\underbrace{x_1}_{(1,0,0,\dots,0)} + x_2 + \cdots + x_n) = (1,0,0,\dots,0)$$

$\deg(e_2) =$

$$\deg(\underbrace{x_1 x_2}_{(1,1,0,\dots,0)} + \cdots) = (1,1,0,\dots,0)$$

$$\deg(e_k) = (\underbrace{1,1,\dots,1}_{k \text{ times}}, \underbrace{0,\dots,0}_{n-k \text{ times}}).$$

Fundamental Theorem of Sym. Polys.
(FTSP)

Let $\mathbb{F}$ be a field. For any sym. polynomial $S(x_1,\dots,x_n) \in \mathbb{F}[x_1,\dots,x_n]$, there exists a (possibly) nonsymmetric polynomial $N(x_1,\dots,x_n) \in \mathbb{F}[x_1,\dots,x_n]$ such that

$$S(x_1,\dots,x_2) = N(e_1,e_2,\dots,e_n)$$
$$= N(e_1(x_1\dots,x_n), e_2(x_1,\dots,x_n), \dots, e_n(x_1,\dots,x_n)).$$

Proof is a "division algorithm" due to Waring (1770). Perfected by Gauss (1815).

<u>Proof</u>: Let $\deg(S) = (i_1, i_2, \dots, i_n)$, so

$$S = c x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} + \text{lower terms.}$$

I claim $i_1 \geq i_2 \geq i_3 \geq \dots \geq i_n$. Indeed, if we had $i_k < i_{k+1}$ for some k, then by <u>symmetry</u> the term

$$c x_1^{i_1} \cdots x_k^{i_{k+1}} x_{k+1}^{i_k} \cdots x_n^{i_n}$$

also occurs in S. But this exponent vector is lex-higher! Contradiction.

Next observe that

$$\deg\left(c e_1^{i_1-i_2} e_2^{i_2-i_3} \cdots e_{n-1}^{i_{n-1}-i_n} e_n^{i_n}\right)$$
$$= (i_1-i_2)\cancel{\deg(e_1)}(1,0,\dots,0)$$
$$+(i_2-i_3)\cancel{\deg(e_2)}(1,1,0\dots0$$

$$\vdots$$
$$+ (i_{n-1} - i_n)\, \cancel{\deg(e_{n-1})}\, (1,1,\dots,1,0)$$
$$+ i_n\, \cancel{\deg(e_n)}\, (1,1,\dots,1)$$
$$= (i_1, i_2, i_3, \dots, i_n) = \deg(S).$$

This implies that

$$S'(x_1,\dots,x_n) := S(x_1,\dots,x_n) - c\, e_1^{i_1-i_2} \cdots e_n^{i_n}$$

is a symmetric polynomial of <u>strictly lower degree</u> than S. By induction

$$S' = N'(e_1,\dots,e_n) \text{ for some } N' \in \mathbb{F}[x_1,\dots,x_n].$$

Finally:

$$S = c\, e_1^{i_1-i_2} \cdots e_n^{i_n} + N'(e_1,\dots,e_n)$$
$$= N(e_1,\dots,e_n)$$

for the polynomial

$$N(x_1,\dots,x_n) = c\, x_1^{i_1-i_2} \cdots x_n^{i_n} + N'(x_1,\dots,x_n).$$ QED.

Example:
$$e_1 = r+s+t$$
$$e_2 = rs+rt+st$$
$$e_3 = rst.$$

Observe $\Delta = (r-s)^2 (r-t)^2 (s-t)^2$

is symmetric in r, s, t. By FTSP we can express

Δ = some polynomial expression in e_1, e_2, e_3.

Algorithm:

$$\deg(\Delta) = 2\deg(r-s) + 2\deg(r-t) + 2\deg(s-t)$$
$$= (2,0,0) + (2,0,0) + (0,2,0)$$
$$= (4,2,0)$$

$$\Delta = r^4 s^2 + \text{lower terms.}$$

$$\deg(e_1^2 e_2^2) = 2\deg(e_1) + 2\deg(e_2)$$
$$= (2,0,0) + (2,2,0)$$
$$= (4,2,0)$$

$$e_1^2 e_2^2 = r^4 s^2 + \text{lower terms}$$

Same leading term!

Next, my computer tells me that

$$\Delta - e_1^2 e_2^2 = -4 r^4 s t + \text{lower terms}$$

Observe also that

$$-4e_1^3 e_3 = -4e_1^{4-1} e_2^{1-1} e_3^1$$

$$= -4r^4 st + \text{lower terms.}$$

Next, my computer tells me that

$$(\Delta - e_1^2 e_2^2) - (-4e_1^3 e_3)$$

$$= -4r^3 s^3 + \text{lower terms.}$$

Note that the degree goes down at each step:

$$(4,2,0) > (4,1,1) > (3,3,0) > \cdots$$

Eventually this process must terminate with a nonzero constant (of degree $(0,0,0)$) or the zero polynomial.

In our expample there are 3 more steps (omitted). The final answer is

$$\Delta - e_1^2 e_2^2 + 4e_1^3 e_2 + 4e_2^2 - 18 e_1 e_2 e_3 + 27 e_3^2$$

$$= 0$$

and hence

$$\Delta = e_1^2 e_2^2 - 4e_1^3 e_3 - 4e_2^3 + 18 e_1 e_2 e_3 - 27 e_3^2 .$$

This is the formula for the "discriminant of the cubic polynomial"

$$x^3 - e_1 x^2 + e_2 x - e_3 = (x-r)(x-s)(x-t).$$

No one should ever memorize this formula, but you should know that such a formula exists because of the F.T.S.P..

The F.T.S.P. was well known in the 1700s (Lagrange regarded it as "common knowledge").

Next time we will use it to get a better understanding of Laplace's (1795) proof of the F.T.A.