Notes for 14 March (Thursday)

1 The road so far...

1. Proved the Chinese Remainder and the Lagrange interpolation theorems.
2. Constructed $\mathbb{C}$ out of $\mathbb{R}[x]$. Stated the fundamental theorem of algebra.
3. Defined algebraic and transcendental numbers. Stated Lindmann-Weierstrass.
4. Defined symmetric and elementary symmetric polynomials.

2 Symmetric polynomials

Examples :

1. $p_k(x_1, x_2 \ldots) = x_1^k + x_2^k + \ldots + x_n^k$ are called power sums.
2. $\Pi_{1 \leq i \leq j \leq n}(X_i - X_j)^2$.

The most important theorem in the theory of symmetric polynomials is the fundamental theorem :

Theorem 1. *Every symmetric polynomial $f(x_1, \ldots, x_n)$ can be written uniquely as a polynomial of the elementary symmetric polynomials $e_k(x)$, i.e., $f(x_1, \ldots) = q(e_1(x), e_2(x), \ldots, e_n(x))$ where $q \in R[y_1, y_2, \ldots, y_n]$ is unique.*

Before we prove this theorem, here is another definition : A homogeneous polynomial $p(x_1, x_2 \ldots, x_n)$ is one such that the degree of every term is the same where $deg(x_1^{r_1} x_2^{r_2} \ldots)$ is defined as $r_1 + r_2 + \ldots$. A term of p is defined recursively as a term of $a_k(x_1, \ldots, x_{n-1})$ times x_n^k where $p(x) = \sum a_k(x_1, \ldots, x_{n-1}) x_n^k$. Every term is of the form $a_I x_1^{i_1} x_2^{i_2} \ldots$ (inductively proven). Firstly,

Theorem 2. *Every polynomial can be uniquely written as a sum of homogeneous polynomials. Every symmetric polynomial can be be uniquely written as a sum of homogeneous symmetric polynomials.*

This will be given as a HW problem. Now we prove the fundamental theorem of symmetric polynomials. We leave some of the proof as a HW. This proof is standard (one resource is Wikipedia.)

Proof. Without loss of generality, we may assume that our polynomial is a homogeneous symmetric polynomial. We use double induction on n and the degree d (after fixing n). For $n = 1$, every polynomial is symmetric. Assume truth for $1, 2 \ldots, n-1$. For n we shall induct on the degree d. For $d = 1$, we are done trivially. Assume truth for $1, 2 \ldots, d-1$.

Every such $p(x_1, \ldots, x_n) = P_{lac}(x_1, \ldots, x_n) + x_1 x_2 \ldots x_n q$ where p_{lac} (the lacunary part) is defined as the sum of terms that do not contain at least one of the x_j. Since p is symmetric, p_{lac} is determined by only those terms that do not contain x_n. Therefore p_{lac} is determined by $p(x_1, \ldots, x_{n-1}, 0)$ which is a symmetric polynomial in fewer variables and hence equal to $\tilde{q}(e_{1,n-1}, e_{2,n-1}, \ldots, e_{n-1,n-1})$. Now the polynomial $r(x_1, \ldots, x_n) = \tilde{q}(e_{1,n}, e_{2,n} \ldots, e_{n-1,n})$ is a symmetric polynomial in n variables of degree $n-1$ such that $r(x_1, \ldots, x_{n-1}, 0) = p(x_1, \ldots, x_{n-1}, 0)$. Therefore, $r_{lac} = p_{lac}$. Now $P - R = e_n Q$ where Q is a homogeneous symmetric polynomial of smaller degree and hence by the induction hypothesis we are done with existence.
Uniqueness is similar and given as HW. □

An example of this is as follows : We want to express $x_1^3 + x_2^3 + x_3^3$ in terms of elementary symmetric polynomials. This is already in the lacunary form. So take $x_1^3 + x_2^3$. Now consider $(x_1 + x_2)^3 - (x_1^3 + x_2^3) = 3x_1 x_2 (x_1 + x_2)$. Therefore consider $(x_1 + x_2 + x_3)^3 - 3(x_1 x_2 + x_2 x_3 + x_3 x_1)(x_1 + x_2 + x_3) - x_1^3 - x_2^3 - x_3^3 = -3x_1 x_2 x_3$. So we are done.

3 Cubics, Quartics, Quintics, etc

Suppose we want to solve $x^3 + bx^2 + cx + d = 0$. Here is Lagrange's method for it : Let x_1, x_2, x_3 be the roots. Consider the quantity $t = x_1 + \omega x_2 + \omega^2 x_3$ where ω is a primitive cube root of unity, i.e., $1, \omega, \omega^2$ are the cube roots. There are 6 possible values $t_1, t_2, \ldots, t_6$ of this expression depending on the order of x_1, x_2, x_3. The t_i are the roots of the 6th order polynomial $p = (x - t_1)(x - t_2) \ldots = 0$. This polynomial's coefficients are symmetric in t_i and hence in x_i. Therefore, in principle, they can be written using the elementary symmetric polynomials in x_i, i.e., in terms of b, c, d. Note that if we choose an ordering, then $t_1, \omega t_1, \omega^2 t_1, t_2, \omega t_2, \omega^2 t_2$ are the six roots where $t_1 = x_1 + \omega x_2 + \omega^2 x_3$ and $t_2 = x_2 + \omega x_1 + \omega^2 x_3$. Now $p = (x^3 - t_1^3)(x^3 - t_2^3) = 0$. This is a quadratic in x^3 whose coefficients can in principle be written using b, c, d and hence t_1, t_2 can be solved for in terms of b, c, d. Therefore x_1, x_2, x_3 can be recovered. In modern terms, the variables $t_0 = x_1 + x_2 + x_3, t_1 = x_1 + \omega x_2 + \omega^2 x_3$, $t_2 = x_2 + \omega x_1 + \omega^2 x_2$ are said to be the discrete Fourier transform of x_1, x_2, x_3.