**Summaries, April 28 and 30**

**symmetric functions**

The symmettric group $G = S_n$ of permutations of $n$ elements operates on the ring of polynomials $F[u_1, ..., u_n]$ in $n$ variables, by permuting the variables:

$$[\sigma f](u_1, ..., u_n) = f(u_{\sigma 1}, ..., u_{\sigma n})$$

A polynomial $f$ is *symmetric* if $\sigma f = f$ for all $\sigma$ in $G$. The *elementary symmetric polynomials* are:

$s_1 = u_1 + \cdots + u_n$,
$s_2 = u_1u_2 + \cdots = \sum_{i<j} u_iu_j$,
$s_3 = u_1u_2u_3 + \cdots = \sum_{i<j<k} u_iu_ju_k$,

...

$s_n = u_1u_2 \cdots u_n$.

They are the coefficients of the polynomial $P(x)$ that has $u_1, ..., u_n$ as its roots:

$$(x - u_1)(x - u_2) \cdots (x - u_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_n$$

Notice that the signs alternate and that the indices go from 1 to $n$.

**Theorem 1.** (Symmetric Functions Theorem) Every symmetric polynomial can we written, in a unique way, as a polynomial in the elementrary symmetric functions.

**Example 1.** Here $n = 2$. The polynomial $u_1^2 + u_2^2$ is symmetric, and $u - 1^2 + u_2 = s_1^2 - 2s_2$, where $s_1u_1 + u_2$ and $s_2 = u_1u_2$. The same formula works for the sum of any number of squares:

$$u_1^2 + u_2^2 + \cdots + u_n^2 = s_1^2 - 2s_2$$

where here $s_1, s_2$ are the elementary smmetric functions in $n$ variables.

**Example 2.** Let $n = 3$, and let $f(u_1, u_2, u_3) = u_1^2u_2 + u_2^2u_1 + \cdots$. The dots indicate that one takes all pairs of distinct indices. We call such an expression an *orbit sum* because the sum runs through the orbit of $u_1^2u_2$. There are 6 terms in the sum.

We'll use a systematic method to write $f$ as a polynmial in $s_1 = u_1 + u_2 + u_3$, $s_2 = u_1u_2 + u_1u_3 + u_2u_3$, $s_3 = u_1u_2u_3$.

According to the theorem, $f$ is a polynomial in $s_1, s_2, s_3$. The terms in $f$ have total degree $e$, so the monomials in $s_i$ that appear must have total degree 3 as well. Then $f = as_1^3 + bs_1s_2 + cs_3$ for some scalars $a, b, c$.

We set $u_3 = 0$, obtaining a polynomial $f^\circ(u_1u_2) = f(u_2, u_2, 0) = u_1^2u_2 + u_2^2u_1$, and we denote the elementary symmetric polynomials in two variables by $s_1^\circ = u_1 + u_2$ and $s_2^\circ = u_1u_2$. They are obtained by setting $u_3 = 0$ in $s_1, s_2$. Setting $u_3 = 0$ in $s_3$ gives $s_3^\circ = 0$. We note that $f^\circ$ is symmetric in $u_1, u_2$, and that $f^\circ = s_1^\circ s_2^\circ$.

On the other hand, setting $u_3 = 0$ is a homomorphism, so $f^\circ$ is also equal to $as_1^{\circ 3} + bs_1^\circ s_2^\circ + cs_3 = as_1^\circ + bs_2^\circ$. Therefore $a = 0$, $b = 1$, and $f = s_1s_2 + cs_3$.

A simple way to determine the last coefficient $c$ is to set $u_1 = u_2 = u_3 = 1$. This amounts to counting monomials in the equation $f = s_1s_2 + cs_3$. The result is $6 = 3 \cdot 3 + c\dot{1}$. So $c = -3$, and $f = s_1s_2 - 3s_3$.

One can do the same thing with four variables. The orbit sum $u_1^2u_2 + \cdots$ has 12 terms. To write it as a polynomial in $s_1, s_2, s_3, s_4$ we can use only monoimals in the $s_i$ whose total degree is 3. Therefore the elementary symmetric function $s_4$ cannot be used, and $f = as_1^3 + bs_1s_2 + cs_3$ for some scalars $a, b, c$. When we set $u_4 = 0$, we ge the symmetric polynomial in $u_1, u_2, u_3$ that we analyzed above. Therefore $a, b, c = 0, 1, -3$. The formula $f = s_1s_2 - 3s_3$ is valid for any number of variables $n \geq 3$. □

**proof of the Symmetric Functions Theorem**

The proof is by a double induction, on the number of variables and on the degree of the symmetric polynomial. We follow the method of Example 2. Let $g(u_1, ..., u_n)$ be a symmetric polynomial, and let

$g^\circ(u_1, ..., u_{n-1}) = g(u_1, ..., u_{n-1}, 0)$. Also, let $s_i^\circ$ be defined similarly, for $i = 1, ..., n-1$. By induction on $n$, we may assume that $g^\circ$ is a polynomial in $s_1^\circ, ..., s_{n-1}^\circ$, say

$$g^\circ(u_1, ..., u_{n-1}) = G(s_1^\circ, ..., s_{n-1}^\circ)$$

We inspect the polynomial $Q(u_1, ..., u_n) = f(u_1, ..., u_n) - G(s_1, ..., s_{n-1})$, with $s_i = s_i(u_1, ..., u_n)$. This is a symmetric polynomial. Since substituting $u_n = 0$ is a homomorphism, $Q(u_1, ..., u_{n-1}, 0) = 0$. Therefore $q$ is divisible by $u_n$, and since it is symmetric, $Q$ is divisible by $u_i$ for every $i = 1, ..., n$, and therefore $Q$ is divisible by $s_n$. Let $h(u_1, ..., u_n) = Q/s_n = (g - G)/s_n$. This is a symmetric polynomial whose degree is less than the degree of $g$. So by induction on degree, we may assume that it is a polynomial in the elementary symmetric functions: $h(u) = H(s_1, ..., s_n)$. Then $g = G + s_n H$. □

**Corollary 1.** Let $f(x) = x^n - a_1 x^{n-1} + \cdots \pm a_n$ be a polynomial with coefficients in $F$. Suppose that $f$ splits completely in a field extension $K$, with roots $\alpha_1, ..., \alpha_n$. If $g(u_1, ..., u_n)$ is a symmetric polynomial in $F[u]$, then $g(\alpha_1, ..., \alpha_n)$ is an element of $F$.

For example, $\alpha_1^3 + \alpha_2^3 + \cdots + \alpha_n^3$ is in $F$.

**proof of Corollary 1** The coefficients of $f$ are $a_i = s_i(\alpha_1, ..., \alpha_n)$. They are elements of $F$. By the Symmetric Functions Theorem, $g(u)$ can be written as a polynomial $G(s_1, ..., s_n)$ in the elementary symmetric functions, with coefficients in $F$. Then $g(\alpha) = G(s_1(\alpha), ..., s_n(\alpha)) = G(a_1, ..., a_n)$ is in $F$. □

**Definition.** Let $f(x)$ be a polynomial with coefficients in a field $F$. A *splitting field* $K$ of $f$ is a field extension with these properties:

• $f(x)$ splits completely in $K$, say with roots $\alpha_1, ..., \alpha_n$, and

• the extension $K$ is generated by the roots of $f$ $K = F[\alpha_1, ..., \alpha_n]$. Thus every element of $K$ can be written as a polynomial in $\alpha_1, ..., \alpha_n$ with coefficients in $F$.

The next amazing theorem is probably the most important application of the Symmetric Functions Theorem.

**Theorem 2.** Let $f(x)$ be a polynomial in $F[x]$, and let $K$ be a splitting field of $f$. If an irreducible polynomial $g(x)$ in $F[x]$ has a root $\beta_1$ in $K$, then $g(x)$ splits completely in $K$.

**proof** There is a field extension $L$ of $K$ in which $g$ splits completely, and there is a polynomial $p_1(u_1, ..., u_n)$ in $F[u_1, ..., u_n]$ such that $\beta_1 = p_1(\alpha_1, ..., \alpha_n)$. Let $p_1(u), ..., p_k(u)$ be the orbit of $p_1(u)$ for the operation of the symmetric group $S_n$ on $F[u_1, ..., u_n]$. (We don't know $k$. It could be as large as $n!$.) Let $\beta_j = p_j(\alpha_1, ..., \alpha_n)$. The roots of our polynomial $g(x)$ will be among the elements $\beta_j$, but which of those elements are roots depends on the particular case.

Let $h(x)$ be the polynomial $(x - \beta_1) \cdots (x - \beta_k)$ with roots $\beta_1, ..., \beta_k$. Its coefficients are the elementary symmetric functions in the roots. But these symmetric functions aren't the elementary symmetric functions in $u_1, ..., u_n$. To keep things straight, we introduce new variables $w_1, ..., w_k$, and we call the elementary symmetric functions in these variables $s'_j(w) = s'_j(w_1, ..., w_k)$. So $s'_1 = w_1 + \cdots + w_k$, etc. Then

$$h(x) = (x - \beta_1) \cdots (x - \beta_k) = x^k - s'_1(\beta)x^{k-1} - s'_2(\beta)x^{k-2} + \cdots \pm s'_k(\beta)$$

We'll show that $h(x)$ as coefficients in $F$. Suppose that is proved. Then $g(x)$ and $h(x)$ both have $\beta_1$ as root, so they aren't relatively prime elements of$F[x]$. Since $g(x)$ is irreducible, it generates the ideal of all polynomials with root $\beta_1$. So $g$ divides $h$. Then, since $h$ splits completly in $K$, so does $g$. The proof will be complete.

**Lemma.** If $q(w_1, ..., w_k)$ is a symmetric polynomial in $w_1, ..., w_k$, then $q(\beta_1, ..., \beta_k)$ is an element of $F$.

**proof** Let $p_1(u), ..., p_k(u)$ be the orbit of $p_1(u)$ for the operation of the symmetric group, as above, and let $q(w_1, ..., w_k)$ be a symmetric polynomial in $w$. Then $q(p_1(u), ..., p_k(u))$ will be a symmetric polynomial in $u_1, ..., u_n$. This is easy to see: A permutation of $u_1, ..., u_n$ permutes the orbit $p_1(u), ..., p_k(u)$, and therefore fixes the symmetric polynomial $q(p_1, ..., p_k)$.

This being so, $q(p_1(u), ..., p_k(u))$ can be written as a polynomial in the elementary symmetric functions $s_1(u), ..., s_n(u)$, say $q(p(u)) = Q(s_1(u), ..., s_n(u))$. Then $q(\beta_1, ..., \beta_k) = q(p_1(\alpha), ..., p_k(\alpha)) = Q(s_1(\alpha), ..., s_n(\alpha))$ is in $F$ because $\alpha_i$ and $s_i(\alpha)$ are elements of $F$. □

Now to prove that $h(x)$ has coeffiients in $F$, we apply the lemma to the elementary symmetric functions $s'_j(w_1, ..., w_k)$. It tells us that the coefficients $s'_j(\beta_1, ..., \beta_k)$ of $h$ are elements of $F$. □