CHAPTER XVIII

SYMMETRIC POLYNOMIALS

83. Fundamental Conceptions. Σ and *S* Functions.

DEFINITION 1. *A polynomial $F(x_1, \cdots x_n)$ is said to be* **symmetric** *if it is unchanged by any interchange of the variables $(x_1, \cdots x_n)$.*

It is not necessary, however, to consider all the possible permutations of the variables in order to show that a polynomial is symmetric. If we can show that it is unchanged by the interchange of *every pair* of the variables, this is sufficient, for any arrangement $(x_a, x_b, \cdots x_k)$ may be obtained from $(x_1, x_2, \cdots x_n)$ by interchanging the x's in pairs. Thus, if $a \neq 1$, interchange x_a with x_1; then interchange the second letter in the arrangement thus obtained with x_2; and so on. Hence we have the following theorem:

THEOREM 1. *A necessary and sufficient condition for a polynomial to be symmetric is that it be unchanged by every interchange of two variables.*

A special class of symmetric polynomials of much importance are the Σ-functions, defined as follows:

DEFINITION 2. *Σ before any term means the sum of this term and of all the similar ones obtained from it by interchanging the subscripts.*

Thus, for example,

$$\Sigma x_1^\alpha \equiv x_1^\alpha + x_2^\alpha + \cdots + x_n^\alpha,$$

$$\begin{aligned} \Sigma x_1^\alpha x_2^\beta \equiv\ & x_1^\alpha x_2^\beta + x_1^\alpha x_3^\beta + \cdots + x_1^\alpha x_n^\beta \\ & + x_2^\alpha x_1^\beta + x_2^\alpha x_3^\beta + \cdots + x_2^\alpha x_n^\beta \qquad (\alpha \neq \beta) \\ & + \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ & + x_n^\alpha x_1^\beta + x_n^\alpha x_2^\beta + \cdots + x_n^\alpha x_{n-1}^\beta, \end{aligned}$$

$$\begin{aligned} \Sigma x_1^\alpha x_2^\alpha \equiv\ & x_1^\alpha x_2^\alpha + x_1^\alpha x_3^\alpha + \cdots + x_1^\alpha x_n^\alpha \\ & \qquad + x_2^\alpha x_3^\alpha + \cdots + x_2^\alpha x_n^\alpha \\ & \qquad\qquad + \cdot \quad \cdot \quad \cdot \quad \cdot \\ & \qquad\qquad\qquad + x_{n-1}^\alpha x_n^\alpha. \end{aligned}$$

It is clearly immaterial in what order the exponents $\alpha, \beta, \cdots$ are written. Thus, $\Sigma x_1^\alpha x_2^\beta x_3^\gamma \equiv \Sigma x_1^\beta x_2^\gamma x_3^\alpha$.

If we consider any term of a symmetric polynomial, it is evident that the polynomial must contain all the terms obtained from this one by interchanging the x's. This aggregate of terms is merely a constant multiple of one of the Σ's just defined. In the same way it is clear that all the other terms of the symmetric polynomial must arrange themselves in groups each of which is a constant multiple of a Σ. That is,

THEOREM 2. *Every symmetric polynomial is a linear combination with constant coefficients of a certain number of Σ's.*

Among these Σ's the simplest are the sums of powers of the x's. For the sake of brevity the notation is used:

$$S_k \equiv \Sigma x_1^k \equiv x_1^k + x_2^k + \cdots + x_n^k \qquad (k = 1, 2, \cdots).$$

It is sometimes convenient to write $S_0 = n$.

THEOREM 3. *Any symmetric polynomial in the x's can be expressed as a polynomial in a certain number of the S's.*

Since every symmetric polynomial is a linear combination of a certain number of Σ's, in order to prove our theorem we have only to show that every Σ can be expressed as a polynomial in the S's. Now

$$S_\alpha \equiv x_1^\alpha + x_2^\alpha + \cdots + x_n^\alpha,$$
$$S_\beta \equiv x_1^\beta + x_2^\beta + \cdots + x_n^\beta.$$

Hence, if $\alpha \neq \beta$,

$$\begin{aligned} S_\alpha S_\beta & \equiv x_1^{\alpha+\beta} + x_2^{\alpha+\beta} + \cdots + x_n^{\alpha+\beta} + x_1^\alpha x_2^\beta + x_1^\alpha x_3^\beta + \cdots \\ & \equiv S_{\alpha+\beta} + \Sigma x_1^\alpha x_2^\beta. \end{aligned}$$

From this we get the formula:

(1) $$\Sigma x_1^\alpha x_2^\beta = S_\alpha S_\beta - S_{\alpha+\beta} \qquad (\alpha \neq \beta).$$

If $\alpha = \beta$, we have

$$\begin{aligned} S_\alpha^2 & \equiv x_1^{2\alpha} + x_2^{2\alpha} + \cdots + x_n^{2\alpha} + 2 x_1^\alpha x_2^\alpha + 2 x_1^\alpha x_3^\alpha + \cdots \\ & \equiv S_{2\alpha} + 2\, \Sigma x_1^\alpha x_2^\alpha. \end{aligned}$$

Hence

(2) $$\Sigma x_1^\alpha x_2^\alpha \equiv \tfrac{1}{2}(S_\alpha^2 - S_{2\alpha}).$$

Similarly, by multiplying $\Sigma x_1^\alpha x_2^\beta$ by S_γ, we get the following formulæ where the three integers α, β, γ are supposed to be distinct:

(3) $$\Sigma x_1^\alpha x_2^\beta x_3^\gamma \equiv S_\alpha S_\beta S_\gamma - S_{\alpha+\beta} S_\gamma - S_{\alpha+\gamma} S_\beta - S_{\beta+\gamma} S_\alpha + 2 S_{\alpha+\beta+\gamma},$$

(4) $$\Sigma x_1^\alpha x_2^\alpha x_3^\gamma \equiv \tfrac{1}{2}(S_\alpha^2 S_\gamma - S_{2\alpha} S_\gamma - 2 S_{\alpha+\gamma} S_\alpha + 2 S_{2\alpha+\gamma}),$$

(5) $$\Sigma x_1^\alpha x_2^\alpha x_3^\alpha \equiv \tfrac{1}{6}(S_\alpha^3 - 3 S_{2\alpha} S_\alpha + 2 S_{3\alpha}).$$

R

The proof indicated in these two special cases may be extended to the general case as follows:

If we multiply together the two symmetric polynomials

$$(6) \qquad \Sigma x_1^\alpha x_2^\beta \cdots x_k^\kappa, \qquad S_\lambda \equiv \Sigma x_1^\lambda, \qquad (k < n)$$

we get terms of various sorts which are readily seen to be all contained in one or the other of the following polynomials, each of these polynomials being actually represented:

$$(7) \quad \Sigma x_1^{\alpha+\lambda} x_2^\beta \cdots x_k^\kappa,\ \Sigma x_1^\alpha x_2^{\beta+\lambda} \cdots x_k^\kappa,\ \cdots\cdots\ \Sigma x_1^\alpha x_2^\beta \cdots x_k^{\kappa+\lambda},\ \Sigma x_1^\alpha x_2^\beta \cdots x_k^\kappa x_{k+1}^\lambda.$$

Consequently, since the product of the two polynomials (6) is symmetric, it must have the form

$$c_1 \Sigma x_1^{\alpha+\lambda} x_2^\beta \cdots x_k^\kappa + c_2 \Sigma x_1^\alpha x_2^{\beta+\lambda} \cdots x_k^\kappa + \cdots\cdots + c_k \Sigma x_1^\alpha x_2^\beta \cdots x_k^{\kappa+\lambda} + c_{k+1} \Sigma x_1^\alpha x_2^\beta \cdots x_k^\kappa x_{k+1}^\lambda,$$

where $c_1, \cdots c_{k+1}$ are positive integers.

Transposing, we may write

$$\Sigma x_1^\alpha x_2^\beta \cdots x_{k+1}^\lambda \equiv \frac{1}{c_{k+1}}[\Sigma x_1^\alpha x_2^\beta \cdots x_k^\kappa \cdot \Sigma x_1^\lambda - c_1 \Sigma x_1^{\alpha+\lambda} x_2^\beta \cdots x_k^\kappa - c_2 \Sigma x_1^\alpha x_2^{\beta+\lambda} \cdots x_k^\kappa - \cdots\cdots - c_k \Sigma x_1^\alpha x_2^\beta \cdots x_k^{\kappa+\lambda}].$$

Hence, if our theorem is true for $\Sigma x_1^\alpha \cdots x_k^\kappa$, it is also true for $\Sigma x_1^\alpha \cdots x_{k+1}^\lambda$. But we know it is true for $k = 1$ (by definition of the S's), hence it is true for $k = 2$, hence for $k = 3$, and so on. Thus our theorem is completely proved.

84. Elementary Symmetric Functions. The notation $\Sigma x_1^\alpha x_2^\beta \cdots x_n^\nu$ may be used to represent *any* Σ in n variables. If $\beta = \gamma = \cdots = \nu = 0$, this becomes Σx_1^α or S_α; if $\gamma = \cdots = \nu = 0$, it becomes $\Sigma x_1^\alpha x_2^\beta$; and so on.

Let us now consider $\Sigma x_1^\alpha x_2^\beta \cdots x_n^\nu$ where $\alpha, \beta, \cdots \nu$, are all 0 or 1. The following n cases arise:

$$\begin{array}{lll}
\alpha = 1, & \beta = \gamma = \cdots = \nu = 0, & \Sigma x_1, \\
\alpha = \beta = 1, & \gamma = \cdots = \nu = 0, & \Sigma x_1 x_2, \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
\alpha = \beta = \cdots = \mu = 1, & \nu = 0, & \Sigma x_1 x_2 \cdots x_{n-1}, \\
\alpha = \beta = \cdots = \nu = 1, & & x_1 x_2 \cdots x_n.
\end{array}$$

The extreme case $\alpha = \beta = \cdots = \nu = 0$ is of no interest. We will represent these n symmetric polynomials by $p_1, p_2, \cdots p_n$, respectively. They are called the *elementary symmetric functions*.

THEOREM 1. *Any symmetric polynomial in the x's may be expressed as a polynomial in the p's.*

Since any symmetric polynomial in the x's may be expressed as a polynomial in the S's, it is sufficient to show that every S may be expressed as a polynomial in the p's.

Let us introduce a new variable x and consider the polynomial

$$f(x;\, x_1, x_2, \cdots x_n) \equiv (x - x_1)(x - x_2) \cdots (x - x_n)$$
$$\equiv x^n - p_1 x^{n-1} + p_2 x^{n-2} - \cdots + (-1)^n p_n.$$

Using the factored form of f, we may write

$$\frac{\partial f}{\partial x} \equiv \frac{f}{x - x_1} + \frac{f}{x - x_2} + \cdots + \frac{f}{x - x_n}.$$

Since f vanishes identically when $x = x_i$, we may write

$$f \equiv (x^n - x_i^n) - p_1(x^{n-1} - x_i^{n-1}) + \cdots.$$

Accordingly,

$$\frac{f}{x - x_i} \equiv x^{n-1} + (x_i - p_1)x^{n-2} + (x_i^2 - p_1 x_i + p_2)x^{n-3} + \cdots,$$

$$\frac{\partial f}{\partial x} \equiv nx^{n-1} + (S_1 - np_1)x^{n-2} + (S_2 - p_1 S_1 + np_2)x^{n-3} + \cdots.$$

On the other hand, we have

$$\frac{\partial f}{\partial x} \equiv nx^{n-1} - (n-1)p_1 x^{n-2} + (n-2)p_2 x^{n-3} - \cdots.$$

Hence, equating the coefficients of like powers of x in these two expressions, we have

$$\begin{cases}
S_1 - np_1 \equiv -(n-1)p_1, \\
S_2 - p_1 S_1 + np_2 \equiv (n-2)p_2, \\
\cdots\cdots\cdots \\
S_{n-1} - p_1 S_{n-2} + p_2 S_{n-3} - \cdots + (-1)^{n-1} np_{n-1} \equiv (-1)^{n-1} p_{n-1},
\end{cases}$$

or

$$(1) \begin{cases}
S_1 - p_1 \equiv 0, \\
S_2 - p_1 S_1 + 2p_2 \equiv 0, \\
\cdots\cdots\cdots \\
S_{n-1} - p_1 S_{n-2} + p_2 S_{n-3} - \cdots + (-1)^{n-1}(n-1)p_{n-1} \equiv 0.
\end{cases}$$

Now consider the identities

$$x_i^n - p_1 x_i^{n-1} + p_2 x_i^{n-2} - \cdots + (-1)^n p_n \equiv 0 \qquad (i = 1, 2, \cdots n).$$

Multiplying these identities by $x_1^{k-n}, \cdots x_n^{k-n}$ respectively and adding the results, we have

$$(2) \qquad S_k - p_1S_{k-1} + p_2S_{k-2} - \cdots + (-1)^n p_n S_{k-n} \equiv 0 \quad (k = n, n+1, \cdots).$$

Formulæ (1) and (2) are known as *Newton's Formulæ.* By means of them we can compute in succession the values of $S_1, S_2, \cdots$ as polynomials in the p's:

$$(3) \qquad \begin{cases} S_1 \equiv p_1, \\ S_2 \equiv p_1^2 - 2p_2, \\ S_3 \equiv p_1^3 - 3p_1p_2 + 3p_3, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{cases}$$

Thus our theorem is proved.

It will be noted that Newton's formulæ (1) cannot be obtained from (2) by giving to k values less than n. The necessity for two different sets of formulæ may, however, be avoided by introducing the notation
$$p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv 0.$$

Then all of Newton's formulæ may be included in the following form:

$$(4) \qquad S_k - p_1S_{k-1} + \cdots + (-1)^{k-1}p_{k-1}S_1 + (-1)^k kp_k \equiv 0 \quad (k = 1, 2, \cdots).$$

Using this notation, we see that the explicit formulæ (3) for expressing the S's in terms of the p's are wholly independent of the number n of the x's.

Since the formulæ referred to in the last section for expressing the Σ's in terms of the S's are also independent of n, we have established

THEOREM 2. *If we introduce the notation* $p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv 0$ *and use Newton's Formulæ in the form* (4), *the formula for expressing any* Σ *as a polynomial in the* p*'s is independent of the number* n *of the* x*'s.*

When we have k polynomials in n variables

$$f_1(x_1, \cdots x_n), f_2(x_1, \cdots x_n), \cdots f_k(x_1, \cdots x_n),$$

we say that there exists a *rational relation* between them when, and only when, a polynomial in k variables

$$F(z_1, \cdots z_k)$$

exists which is not identically zero, but which becomes identically zero as a polynomial in the x's when each z is replaced by the corresponding f,
$$F(f_1, \cdots f_k) \equiv 0.$$

THEOREM 3. *There exists no rational relation between the elementary symmetric functions in* n *variables* $p_1, \cdots p_n$.

For let $F(z_1, \cdots z_n)$ be any polynomial in n variables which is not identically zero, and let $(a_1, \cdots a_n)$ be a point at which this polynomial does not vanish. Determine $(x_1, \cdots x_n)$ as the roots of the equation

$$x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n = 0.$$

For these values of the x's, the p's have the values $a_1, \cdots a_n$, and therefore $F(p_1, \cdots p_n)$ does not vanish for these x's, and is consequently not identically zero as a polynomial in the x_i's. Thus our theorem is proved.

COROLLARY. *There is only one way in which a symmetric polynomial in* $(x_1, \cdots x_n)$ *can be expressed as a polynomial in the elementary symmetric functions* $p_1, \cdots p_n$.

For if f is a symmetric polynomial, and if we had two expressions for it,

$$f(x_1, \cdots x_n) \equiv \phi_1(p_1, \cdots p_n),$$
$$f(x_1, \cdots x_n) \equiv \phi_2(p_1, \cdots p_n),$$

then by subtracting these identities from one another we should have as an identity in the x's,

$$\phi_1(p_1, \cdots p_n) - \phi_2(p_1, \cdots p_n) \equiv 0.$$

This, however, would give us a rational relation between the p's, unless
$$\phi_1(z_1, \cdots z_n) \equiv \phi_2(z_1, \cdots z_n).$$

Thus we see that the two expressions for f are really the same.

EXERCISES

1. Obtain the expressions for the following symmetric polynomials in terms of the elementary symmetric functions:

$$\Sigma x_1^2 x_2, \qquad \Sigma x_1^2 x_2^2, \qquad \Sigma x_1^2 x_2^2 x_3.$$

2. Prove that every symmetric polynomial in $(x_1, \cdots x_n)$ can be expressed in one, and only one, way as a polynomial in $S_1, \cdots S_n$.

85. The Weights and Degrees of Symmetric Polynomials. We will attach to each of the elementary symmetric functions p_i a weight equal to its subscript, cf. § 79.

THEOREM 1. *A homogeneous symmetric polynomial of degree* m *in the* x*'s, when expressed in terms of the* p*'s, is isobaric of weight* m.

Let

(1) $$f(x_1, x_2, \cdots x_n) \equiv \phi(p_1, p_2, \cdots p_n)$$

be such a polynomial. Since p_1 is a homogeneous polynomial of the first degree in the x's, p_2 of the second, etc., any term of ϕ, when written in the x's, must be a homogeneous polynomial of degree equal to the original weight of the term. Thus, for example, the term $6\, p_1^2 p_2 p_3^3$ whose weight is 13, when written in the x's will be a homogeneous polynomial of degree 13. Accordingly an isobaric group of terms when expressed in terms of the x's will, since by Theorem 3, § 84, it cannot reduce identically to zero, be homogeneous of the same degree as its original weight. If then ϕ were not isobaric, f would not be homogeneous, and our theorem is proved.

COROLLARY. *If f is non-homogeneous and of the mth degree, ϕ is non-isobaric and of weight m.*

THEOREM 2. *A symmetric polynomial in $(x_1, \cdots x_n)$, when written in terms of the elementary symmetric functions $p_1, \cdots p_n$, will be of the same degree in the p's as it was at first in **any one** of the x's.*

Let f be the symmetric polynomial, and write

$$f(x_1, x_2, \cdots x_n) \equiv \phi(p_1, p_2, \cdots p_n),$$

and suppose f is of degree m in x_1 (and therefore, on account of the symmetry, in any one of the x's), and that ϕ is of degree μ in the p's. We wish to prove that $m = \mu$. Since the p's are of the first degree in x_1, it is clear that $m \leqq \mu$.

If ϕ is non-homogeneous, we can break it up into the sum of a number of homogeneous polynomials by grouping together all the terms of like degree. Each of these homogeneous polynomials in the p's can be expressed (by substituting for the p's their values in terms of the x's) as a symmetric polynomial in the x's. If our theorem were established in the case in which the polynomial in the p's is homogeneous, its truth in the general case would then follow at once.

Let us then assume that ϕ is a homogeneous polynomial. The theorem is obviously true when $n = 1$, since then $p_1 \equiv -x_1$. It will therefore be completely proved by the method of mathematical induction if, assuming it to hold when the number of x's is $1, 2, \cdots n-1$, we can prove that it holds when the number of x's is n.

For this purpose let us first assume that p_n is not a factor of every term of ϕ. Then $\phi(p_1, \cdots p_{n-1}, 0)$ is not identically zero but is still a homogeneous polynomial of degree μ in $(p_1, \cdots p_{n-1})$. Now let $x_n = 0$. This makes $p_n = 0$, and gives the identity

(2) $$f(x_1, \cdots x_{n-1}, 0) \equiv \phi(p_1' \cdots p_{n-1}', 0),$$

where $p_1', \cdots p_{n-1}'$ are the elementary symmetric functions of $(x_1, \cdots x_{n-1})$, and $f(x_1, \cdots x_{n-1}, 0)$ is a symmetric polynomial of degree m_1 in x_1, where $m_1 \leqq m$. From the assumption that our theorem holds when the number of x's is $n-1$, we infer from (2) that $\mu = m_1 \leqq m$; and since we saw above that μ cannot be less than m, we infer that $\mu = m$, as was to be proved.

There remains merely the case to be considered in which p_n is a factor of every term of ϕ. Let p_n^k be the highest power of p_n which occurs as a factor in ϕ. Then

$$\phi(p_1, \cdots p_n) \equiv p_n^k \phi_1(p_1, \cdots p_n),$$

where ϕ_1 is a polynomial of degree $\mu - k$. Putting in for the p's their values in terms of the x's, we get

(3) $$f(x_1, \cdots x_n) \equiv x_1^k x_2^k \cdots x_n^k f_1(x_1, \cdots x_n),$$

where

(4) $$f_1(x_1, \cdots x_n) \equiv \phi_1(p_1, \cdots p_n).$$

From (3) we see that f_1 is of degree $m - k$ in x_1, and from (4), since ϕ_1 does not contain p_n as a factor, that the degrees of f_1 in x_1, and of ϕ_1 in the p's are equal,

$$m - k = \mu - k.$$

From which we see that $m = \mu$, as was to be proved.

The two theorems of this section are not only of theoretical importance, they may also be put to the direct practical use of facilitating the computation of the values of symmetric polynomials in terms of the p's.

In order to illustrate this, let us consider the symmetric function

$$f(x_1, \cdots x_n) \equiv \Sigma x_1^2 x_2 x_3.$$

Since f is homogeneous of the fourth degree in the x's, it will, by Theorem 1, be isobaric of weight 4 in the p's. Since it is of the second degree in x_1, it will, by Theorem 2, be of the second degree in the p's. Hence

$$\Sigma x_1^2 x_2 x_3 \equiv A p_1 p_3 + B p_2^2 + C p_4, \tag{5}$$

where A, B, and C are independent of the number n (Theorem 2, § 84), and may be determined by the ordinary method of undetermined coefficients.

Take $n = 3$, so that $p_4 = 0$. Letting $x_1 = 0$, $x_2 = x_3 = 1$, we have $p_1 = 2$, $p_2 = 1$, $p_3 = 0$. Substituting these values in (5), we find $B = 0$.

Letting $x_1 = -1$, $x_2 = x_3 = 1$, we have $p_1 = 1$, $p_2 = -1$, $p_3 = -1$, which gives $A = 1$.

Now let $$n = 4, x_1 = x_2 = x_3 = x_4 = 1.$$

From this we find $p_1 = 4$, $p_2 = 6$, $p_3 = 4$, $p_4 = 1$.

Substituting this in (5) gives $C = -4$. Hence

$$\Sigma x_1^2 x_2 x_3 \equiv p_1 p_3 - 4 p_4.$$

EXERCISES

1. The symmetric function

$$f(x_1, \cdots x_n) \equiv \Sigma x_1^2 x_2 x_3 + \Sigma x_1^2 x_2^2 + \Sigma x_1 x_2 x_3 x_4$$

is homogeneous of the fourth degree in the x's, and is of the second degree in x_1; hence, when written in terms of the p's, it will have the same form, $A p_1 p_3 + B p_2^2 + C p_4$, as the above example. Compute the values of A, B, and C.

2. If $f(x_1, x_2, x_3) \equiv (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$, show that

$$f(x_1, x_2, x_3) \equiv -27 p_3^2 - 4 p_2^3 + 18 p_1 p_2 p_3 - 4 p_1^3 p_3 + p_1^2 p_2^2.$$

86. The Resultant and the Discriminant of Two Polynomials in One Variable. Let

$$\begin{aligned} f(x) &\equiv x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \\ &\equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \\ \phi(x) &\equiv x^m + b_1 x^{m-1} + b_2 x^{m-2} + \cdots + b_m \\ &\equiv (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m), \end{aligned}$$

be two polynomials in x, and consider the product of the mn factors

$$\left\{ \begin{array}{l} (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \cdots (\alpha_1 - \beta_m) \\ (\alpha_2 - \beta_1)(\alpha_2 - \beta_2) \cdots (\alpha_2 - \beta_m) \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ (\alpha_n - \beta_1)(\alpha_n - \beta_2) \cdots (\alpha_n - \beta_m). \end{array} \right. \tag{1}$$

This product vanishes when, and only when, at least one of the α's is equal to one of the β's. Its vanishing therefore gives a necessary and sufficient condition that f and ϕ have a common factor. Moreover, the product (1), being a symmetrical polynomial in the α's and also in the β's, can be expressed as a polynomial in the elementary symmetric functions of the α's and β's, and therefore as a polynomial in the a's and b's. This will be still more evident if we notice that the product (1) may be written

$$\phi(\alpha_1)\phi(\alpha_2) \cdots \phi(\alpha_n).$$

In this form it is a symmetric polynomial in the α's whose coefficients are polynomials in the b's, and it remains merely to bring in the a's in place of the α's.

We thus see that the product (1) may be expressed as a polynomial $F(a_1, \cdots a_n;\ b_1, \cdots b_m)$ in the a's and b's whose vanishing gives a necessary and sufficient condition that f and ϕ have a common factor. In § 68 we also found a polynomial in the a's and b's whose vanishing gives a necessary and sufficient condition that f and ϕ have a common factor, namely the resultant R of f and ϕ.

We will now identify these two polynomials by means of the following theorem:

THEOREM 1. *The product* (1) *differs from the resultant R of f and ϕ only by a constant factor, and the resultant is an irreducible polynomial in the a's and b's.*

In order to prove this theorem we will first show that this product (1), which we will call $F(a_1, \cdots a_n;\ b_1, \cdots b_m)$, is irreducible. This may be done as follows: Suppose F is reducible, and let
$F(a_1, \cdots a_n;\ b_1, \cdots b_m) \equiv F_1(a_1, \cdots a_n;\ b_1, \cdots b_m)\, F_2(a_1, \cdots a_n;\ b_1, \cdots b_m)$, where F_1 and F_2 are polynomials neither of which is a constant. Then, since the a's and b's are symmetric polynomials in the α's and β's, F_1 and F_2 may be expressed as symmetric polynomials ϕ_1 and ϕ_2 in the α's and β's, and we may write

$$\phi_1(\alpha_1, \cdots \alpha_n;\ \beta_1, \cdots \beta_m)\, \phi_2(\alpha_1, \cdots \alpha_n;\ \beta_1, \cdots \beta_m)$$
$$\equiv \left\{ \begin{array}{l} (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \cdots (\alpha_1 - \beta_m) \\ (\alpha_2 - \beta_1)(\alpha_2 - \beta_2) \cdots (\alpha_2 - \beta_m) \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ (\alpha_n - \beta_1)(\alpha_n - \beta_2) \cdots (\alpha_n - \beta_m). \end{array} \right.$$

The factors on the right-hand side of this identity being irreducible, we see that ϕ_1 must be composed of some of these binomial factors and ϕ_2 of the others. This, however, is impossible, since neither ϕ_1 nor ϕ_2 would be symmetric. Hence F is irreducible.

Now, since $F=0$ is a necessary and sufficient condition for $f(x)$ and $\phi(x)$ to have a common factor, and $R=0$ is the same, any set of values of the a's and b's which make $F=0$ will also make $R=0$. Hence by the theorem for $n+m$ variables analogous to Theorem 7, § 76, F is a factor of R. Also, since F is a symmetric polynomial in the α's and β's of degree m in each of the α's and n in each of the β's, by Theorem 2, § 85, it must be of degree m in the a's and n in the b's. But R is of degree not greater than m in the a's and n in the b's, as is at once obvious from a glance at the determinant in § 68. Hence F, being a factor of R, and of degree not lower than R, can differ from it only by a constant factor. Thus our theorem is proved.

Let us turn now to the question: Under what conditions does the polynomial $f(x)$ have a multiple linear factor? Using the same notation as above, we see that the vanishing of the product

$$\left.\begin{array}{r}(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_n)\\ (\alpha_2-\alpha_3)\cdots(\alpha_2-\alpha_n)\\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ (\alpha_{n-1}-\alpha_n)\end{array}\right\}\equiv P(\alpha_1,\cdots\alpha_n)$$

is a necessary and sufficient condition for this. P is not symmetric in the α's, since an interchange of two subscripts changes P into $-P$. If, however, we consider P^2 in place of P, we have a symmetric polynominal, which can therefore be expressed as a polynomial in the a's,

$$[P(\alpha_1,\cdots\alpha_n)]^2\equiv F(a_1,\cdots a_n).$$

Moreover, $F=0$ is also a necessary and sufficient condition that $f(x)$ have a multiple linear factor.

On the other hand, it is easily seen that $f(x)$ has a multiple linear factor when and only when $f(x)$ and $f'(x)$ have a common linear factor. A necessary and sufficient condition for $f(x)$ to have a multiple linear factor is therefore the vanishing of the resultant of $f(x)$ and $f'(x)$. This resultant we will call the discriminant Δ of $f(x)$. It is obviously a polynomial in the coefficients of f.

THEOREM 2. *The polynomials F and Δ differ only by a constant factor, and are irreducible.*

The proof of this theorem is similar to the proof of Theorem 1, and is left to the reader.

EXERCISES

1. Compute by the use of symmetric functions the product (1) for the two polynomials

$$x^2+a_1x+a_2,$$
$$x^2+b_1x+b_2,$$

and compare the result with the resultant obtained in determinant form.

2. Verify Theorem 2 by comparing the result of Exercise 2, § 85, with the discriminant in determinant form of the polynomial

$$x^3+a_1x^2+a_2x+a_3.$$