# THE ALGEBRAIC THEORY OF MODULAR SYSTEMS

## Introduction

*Definition.* A modular system is an infinite aggregate of polynomials, or whole functions* of $n$ variables $x_1, x_2, \dots, x_n$, defined by the property that if $F, F_1, F_2$ belong to the system $F_1 + F_2$ and $AF$ also belong to the system, where $A$ is any polynomial in $x_1, x_2, \dots, x_n$.

Hence if $F_1, F_2, \dots, F_k$ belong to a modular system so also does $A_1F_1 + A_2F_2 + \dots + A_kF_k$, where $A_1, A_2, \dots, A_k$ are arbitrary polynomials.

Besides the algebraic or relative theory of modular systems there is a still more difficult and varied absolute theory. We shall only consider the latter theory in so far as it is necessary for the former.

In the algebraic theory polynomials such as $F$ and $aF$, where $a$ is a quantity not involving the variables, are not regarded as different polynomials, and any polynomial of degree zero is equivalent to 1. No restriction is placed on the coefficients of $F_1, F_2, \dots, F_k$ except in so far as they may involve arbitrary parameters $u_1, u_2, \dots$, in which case they are restricted to being rational functions of such parameters. The same restriction applies to the coefficients of the arbitrary polynomials $A_1, A_2, \dots, A_k$ above.

In the absolute theory the coefficients of $F_1, F_2, \dots, A_1, A_2, \dots$ are restricted to a domain of integrity, generally ordinary integers or whole functions of parameters $u_1, u_2, \dots$ with integral coefficients; and a polynomial of degree zero other than 1 or a unit is not equivalent to 1.

* We use the term *whole function* throughout the text (but not in the Note at the end) as equivalent to *polynomial* and as meaning a *whole rational function*.

*Definitions.* A modular system will be called a *module* (of polynomials).

Any polynomial $F$ belonging to a module $M$ is called a *member* (or element) of $M$.

According as we wish to denote that $F$ is a member of $M$ in the relative or absolute sense we shall write $F=0 \bmod M$, or $F \equiv 0 \bmod M$. The notation $F \equiv 0 \bmod M$ only comes into use in the sequel in connection with the Resultant.

A *basis* of a module $M$ is any set of members $F_1, F_2, \ldots, F_k$ such that every member of $M$ is of the form $X_1 F_1 + X_2 F_2 + \ldots + X_k F_k$, where $X_1, X_2, \ldots, X_k$ are polynomials.

*Every module of polynomials has a basis consisting of a finite number of members* (Hilbert's theorem, § 37).

The proof of this theorem is from first principles, and its truth will be assumed throughout.

The theory of modular systems is very incomplete and offers a wide field for research. The object of the algebraic theory is to discover those general properties of a module which will afford a means of answering the question whether a given polynomial is a member of a given module or not. Such a question in its simpler aspect is of importance in Geometry and in its general aspect is of importance in Algebra. The theory resembles Geometry in including a great variety of detached and disconnected theorems. As a branch of Algebra it may be regarded as a generalized theory of the solution of equations in several unknowns, and assumes that any given algebraic equation in one unknown can be completely solved. In order that a polynomial $F$ may be a member of a module $M$ whose basis $(F_1, F_2, \ldots, F_k)$ is given it is evident that $F$ must vanish for all finite solutions (whether finite or infinite in number) of the equations $F_1 = F_2 = \ldots = F_k = 0$. These conditions are *sufficient* if $M$ resolves into what are called *prime modules**; otherwise they are not sufficient, and $F$ must satisfy further conditions, also connected with the solutions, which may be difficult to express concretely. The first step is to find all the solutions of the equations $F_1 = F_2 = \ldots = F_k = 0$; and this is completely accomplished in the theories of the resultant and resolvent.

* Cayley and Salmon constantly assume this. Salmon also discusses particular cases of a number of important and suggestive problems connected with modular systems (Sa).

978-0-521-45562-6 - The Algebraic Theory of Modular Systems
F. S. Macaulay




## I. THE RESULTANT

**1.** The Resultant is defined in the first instance with respect to $n$ *homogeneous* polynomials $F_1, F_2, \ldots, F_n$ in $n$ variables, of degrees $l_1, l_2, \ldots, l_n$, each polynomial being complete in all its terms with literal coefficients, all different. The resultant of any $n$ given homogeneous polynomials in $n$ variables is the value which the resultant in the general case assumes for the given case. The resultant of $n$ given non-homogeneous polynomials in $n-1$ variables is the resultant of the corresponding homogeneous polynomials of the same degrees obtained by introducing a variable $x_0$ of homogeneity.

*Definitions.* An *elementary member* of the module $(F_1, F_2, \ldots, F_n)$ is any member of the type $\omega F_i$ $(i=1, 2, \ldots, n)$, where $\omega$ is any power product of $x_1, x_2, \ldots, x_n$. What is and what is not an elementary member depends on the basis chosen for the module.

The total number of elementary members of an assigned degree is evidently finite.

The diagram below represents the array of the coefficients of all elementary members of $(F_1, F_2, \ldots, F_n)$ of degree $t$, arranged under the power products $\omega_1^{(t)}, \omega_2^{(t)}, \ldots, \omega_\mu^{(t)}$ of degree $t$ $\left(\mu = \dfrac{|\underline{t+n-1}}{|\underline{t}\;|\underline{n-1}}\right)$:

$$\begin{array}{c|cccc|}
 & \omega_1^{(t)} & \omega_2^{(t)} & \ldots\ldots\ldots & \omega_\mu^{(t)} \\
\lambda_1 & a_1 & b_1 & \ldots\ldots\ldots & k_1 \\
\lambda_2 & a_2 & b_2 & \ldots\ldots\ldots & k_2 \\
 & \ldots & \ldots & \ldots\ldots\ldots & \ldots \\
\lambda_\rho & a_\rho & b_\rho & \ldots\ldots\ldots & k_\rho
\end{array}$$

Each row of the array, in association with $\omega_1^{(t)}, \omega_2^{(t)}, \ldots, \omega_\mu^{(t)}$, represents an elementary member of degree $t$; and the rows of the array corresponding to $F_i$ all consist of the same elements (the coefficients of $F_i$ and zeros) but in different columns.

Any member $F = X_1 F_1 + X_2 F_2 + \ldots + X_n F_n$ of degree $t$ is evidently a linear combination $\lambda_1\omega_1 F_1 + \lambda_2\omega_2 F_1 + \ldots + \lambda_p\omega_p F_i + \ldots + \lambda_\rho\omega_\rho F_n$ of elementary members of degree $t$, and is represented by the above array when bordered by $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ on the left, where $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ are the coefficients of $X_1, X_2, \ldots, X_n$, some of which may be zeros.

This bordered array also shows in a convenient way the whole coefficients of the terms of $F$, viz. $\Sigma\lambda a, \Sigma\lambda b, \ldots, \Sigma\lambda k$.

These remarks and definitions are equally applicable to any module $(F_1, F_2, \ldots, F_k)$ of homogeneous or non-homogeneous polynomials; but the following definition applies only to the particular module $(F_1, F_2, \ldots, F_n)$.

The *resultant* $R$ of $F_1, F_2, \ldots, F_n$ is the H.C.F. of the determinants of the above array for degree $t = l+1$, where $l = l_1 + l_2 + \ldots + l_n - n$. It will be shown (§ 7) that $R$ is homogeneous and of degree $l_1 l_2 \ldots l_n / l_i$ in the coefficients of $F_i$ $(i = 1, 2, \ldots, n)$.

## 2. Resultant of two homogeneous polynomials in two variables.

Let
$$F_1 = a_1 x_1^{l_1} + b_1 x_1^{l_1-1} x_2 + \ldots + k_1 x_2^{l_1},$$
$$F_2 = k_2 x_1^{l_2} + \ldots + a_2 x_2^{l_2},$$
$$l = l_1 + l_2 - 2.$$

The array of the coefficients of all elementary members of $(F_1, F_2)$ of degree $l+1$, viz. $x_1^{l_2-1}F_1, x_1^{l_2-2}x_2F_1, \ldots x_2^{l_2-1}F_1, x_1^{l_1-1}F_2, \ldots, x_2^{l_1-1}F_2$, has $l_2$ rows corresponding to $F_1$ and $l_1$ rows corresponding to $F_2$, and the same number $l_1 + l_2$ of rows in all as columns. The resultant $R$ is therefore the determinant of this array. The array is

$$\begin{array}{c|cccccc|l}
 & \omega_1^{(l+1)} & \omega_2^{(l+1)} & \ldots\ldots & \omega_{l_1+1}^{(l+1)} & \ldots\ldots & \omega_{l+2}^{(l+1)} & \\
\hline
\lambda_1 & a_1 & b_1 \ldots\ldots & k_1 & . & . & . & = x_1^{l_2-1} F_1 \\
\lambda_2 & . & a_1 & b_1 \ldots\ldots & k_1 & . & . & = x_1^{l_2-2} x_2 F_1 \\
 & & & & & & & \\
\lambda_{l_2} & . & . & a_1 & b_1 \ldots\ldots & \ldots & k_1 & = x_2^{l_2-1} F_1 \\
\lambda_{l_2+1} & k_2 \ldots\ldots & \ldots & a_2 & . & . & . & = x_1^{l_1-1} F_2 \\
 & . & k_2 \ldots\ldots & \ldots & a_2 & . & . & = x_1^{l_1-2} x_2 F_2 \\
 & & & & & & & \\
\lambda_{l+2} & . & . & k_2 & \ldots\ldots & \ldots & a_2 & = x_2^{l_1-1} F_2
\end{array}$$

On the right are written the elementary members which the rows represent. Thus, neglecting the left hand border, we may regard the diagram as a set of $l+2$ identical equations for

$$\omega_1^{(l+1)}, \quad \omega_2^{(l+1)}, \ldots, \omega_{l+2}^{(l+1)}.$$

Solving them we have

$$R\omega_i^{(l+1)} = A_{i1} F_1 + A_{i2} F_2 \quad (i = 1, 2, \ldots, l+2),$$

where $A_{i1}$, $A_{i2}$ are polynomials whose coefficients are whole functions of the coefficients of $F_1, F_2$. Hence

$$R\omega^{(l+1)} \equiv 0 \bmod (F_1, F_2),$$

where $\omega^{(l+1)}$ is any power product of $x_1$, $x_2$ of degree $l+1$. This expresses the first important property of $R$.

**3. Irreducibility of $R$.** The general expression for the resultant $R$ is irreducible in the sense that it cannot be resolved into two factors each of which is a whole function of the coefficients of $F_1$, $F_2$. When this has been proved it follows that any whole function of the coefficients of $F_1$, $F_2$ which vanishes as a consequence of $R$ vanishing must be divisible by $R$.

$R$ has a term $a_1^{l_2} a_2^{l_1}$ obtained from the diagonal of the determinant, and this is the only term of $R$ containing $a_2^{l_1}$. Also, when $a_1 = 0$, $R$ has a term $(-1)^{l_2} k_2 b_1^{l_2} a_2^{l_1-1}$, and this is the only term of $R$ containing $a_2^{l_1-1}$ when $a_1 = 0$. Hence, when $R$ is expanded in powers of $a_2$ to two terms, we have

$$R = a_1^{l_2} a_2^{l_1} + b a_2^{l_1-1} + \dots,$$

where $$b \equiv (-1)^{l_2} k_2 b_1^{l_2} \bmod a_1.$$

Hence if $R$ can be written as a product of two factors, we have

$$R = (a_1^{p_1} a_2^{p_2} + \dots)(a_1^{q_1} a_2^{q_2} + \dots),$$

where $p_1 + q_1 = l_2$ and $p_2 + q_2 = l_1$, and either $p_1$ or $q_1$ is zero; for otherwise the coefficient $b$ of $a_2^{l_1-1}$ would be zero or divisible by $a_1$, which is not the case. Hence one of the factors of $R$ is independent of the coefficients of $F_1$, since both factors must be homogeneous in the coefficients of $F_1$. Similarly one of the factors must be independent of the coefficients of $F_2$, i.e.

$$R = (a_1^{l_2} + \dots)(a_2^{l_1} + \dots) = a_1^{l_2} a_2^{l_1},$$

since the whole coefficient of $a_1^{l_2}$ in $R$ is $a_2^{l_1}$, and of $a_2^{l_1}$ is $a_1^{l_2}$. This is not true; hence $R$ is irreducible.

**4.** *The necessary and sufficient condition that the equations $F_1 = F_2 = 0$ may have a proper solution (i.e. a solution other than $x_1 = x_2 = 0$) is the vanishing of $R$.*

This is the fundamental property of the resultant. If the equations $F_1 = F_2 = 0$ have a solution other than $x_1 = x_2 = 0$ it follows from

$$R x_1^{l+1} \equiv 0 \bmod (F_1, F_2), \quad R x_2^{l+1} \equiv 0 \bmod (F_1, F_2),$$

that $R = 0$, by giving to $x_1$, $x_2$ the values (not both zero) which satisfy the equations $F_1 = F_2 = 0$.

Conversely if $R = 0$ we can choose $\lambda_1, \lambda_2, \dots, \lambda_{l+2}$ so that the sum of their products with the elements in each column of the determinant $R$ vanishes. Multiplying each sum by the power product corresponding to its column, and adding by rows, we have

$$(\lambda_1 x_1^{l_2-1} + \lambda_2 x_1^{l_2-2} x_2 + \dots + \lambda_{l_2} x_2^{l_2-1}) F_1 + (\lambda_{l_2+1} x_1^{l_1-1} + \dots + \lambda_{l+2} x_2^{l_1-1}) F_2 = 0,$$

where $\lambda_1, \lambda_2, \dots \lambda_{l+2}$ do not all vanish. Hence, since $\lambda_1 x_1^{l_2-1} + \dots$ is of less degree than $F_2$, $F_1$ must have a factor in common with $F_2$, and the equations $F_1 = F_2 = 0$ have a proper solution.

In the following article another proof is given which can be extended more easily to any number of variables.

**5.** When $R \neq 0$ there are $l+2$ linearly independent members of $(F_1, F_2)$ of degree $l+1$, and $l$ of degree $l$. When $R=0$ there are only $l+1$ linearly independent members of degree $l+1$ and still $l$ of degree $l$, i.e. in each case 1 less than the number of terms in a polynomial of degree $l+1$ and $l$ respectively. Hence there will be one and only one identical linear relation between the coefficients of the general member of $(F_1, F_2)$ whether of degree $l+1$ or $l$. Let this identical relation for degree $l+1$ be

$$c_{l+1,0}\, z_{l+1,0} + c_{l,1}\, z_{l,1} + \dots + c_{0,l+1}\, z_{0,l+1} = 0,$$

where $z_{i,j}$ denotes the coefficient of $x_1^i x_2^j$ in the general member of $(F_1, F_2)$ of degree $i+j$, and the $c_{i,j}$ are constants. Then, if $F$ is the general member

$$z_{l,0}\, x_1^l + z_{l-1,1}\, x_1^{l-1} x_2 + \dots + z_{0,l}\, x_2^l$$

of $(F_1, F_2)$ of degree $l$, $x_1 F$ is a member of degree $l+1$ whose coefficients must satisfy the relation above. Hence

$$c_{l+1,0}\, z_{l,0} + c_{l,1}\, z_{l-1,1} + \dots + c_{1,l}\, z_{0,l} = 0.$$

Similarly $$c_{l,1}\, z_{l,0} + c_{l-1,2}\, z_{l-1,1} + \dots + c_{0,l+1}\, z_{0,l} = 0,$$

since $x_2 F$ is a member of $(F_1, F_2)$ of degree $l+1$. These two relations must be equivalent to one only, since only one identical relation exists for degree $l$. Hence we have

$$\frac{c_{l+1,0}}{c_{l,1}} = \frac{c_{l,1}}{c_{l-1,2}} = \dots = \frac{c_{1,l}}{c_{0,l+1}} = \frac{a_1}{a_2} \text{ (say)},$$

i.e. $c_{l+1,0}, c_{l,1}, \dots, c_{0,l+1}$ are proportional to $a_1^{l+1}, a_1^l a_2, \dots, a_2^{l+1}$. Hence the original identical relation may be written

$$z_{l+1,0}\, a_1^{l+1} + z_{l,1}\, a_1^l a_2 + \dots + z_{0,l+1}\, a_2^{l+1} = 0,$$

showing that the general member $z_{l+1,0}\, x_1^{l+1} + \dots$ of $(F_1, F_2)$ of degree $l+1$ vanishes when $x_1 = a_1$, $x_2 = a_2$, and that the equations $F_1 = F_2 = 0$ have the proper solution $(a_1, a_2)$. The theorem being thus proved true in general is assumed to be true in particular.

**6. Resultant of $n$ homogeneous polynomials in $n$ variables.**

The general theory of the resultant to be now given is exactly parallel to that already given for two variables, although it involves points of much greater difficulty as might be expected. Another method of exposition depending on a different definition of the resultant is given in (K, p. 260 ff.).

Let $F_1, F_2, \ldots, F_n$ be $n$ homogeneous polynomials of degrees $l_1, l_2, \ldots, l_n$ of which all the coefficients are different letters. In particular, let $a_1, a_2, \ldots, a_n$ be the coefficients of $x_1^{l_1}, x_2^{l_2}, \ldots, x_n^{l_n}$ in $F_1, F_2, \ldots, F_n$ respectively, and $c_1, c_2, \ldots, c_n$ the constant terms of $F_1, F_2, \ldots, F_n$ when $x_n$ is put equal to 1, so that $c_n = a_n$. Let

$$l = l_1 + l_2 + \ldots + l_n - n, \quad L = l_1 l_2 \ldots l_n, \quad L_1 = L/l_1, \quad L_2 = L/l_2, \ldots L_n = L/l_n.$$

The resultant $R$ of $F_1, F_2, \ldots, F_n$ has already been defined (§ 1) as the H.C.F. of the determinants of the array of the coefficients of all elementary members of $(F_1, F_2, \ldots, F_n)$ of degree $l+1$.

We shall first consider a particular determinant $D$ of the array, viz. that representing (§ 1) the polynomial

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-1)} F_n \text{ of degree } l+1,$$

where $X^{(i)}$ denotes a polynomial in which all terms divisible by $x_1^{l_1}$ or $x_2^{l_2} \ldots$ or $x_i^{l_i}$ are absent, which may be expressed by saying that $X^{(i)}$ is *reduced* in $x_1, x_2, \ldots, x_i$. The polynomial

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-1)} F_n$$

is represented by the bordered array

$$\begin{array}{c|cccc|l} & \omega_1^{(l+1)} & \omega_2^{(l+1)} & \ldots\ldots\ldots & \omega_\mu^{(l+1)} & \\ \hline \lambda_1 & a_1 & b_1 & \ldots\ldots\ldots & k_1 & = \omega_1 F_1 \\ \lambda_2 & a_2 & b_2 & \ldots\ldots\ldots & k_2 & = \omega_2 F_1 \\ & \ldots & \ldots & \ldots\ldots\ldots & \ldots & \\ \lambda_\mu & a_\mu & b_\mu & \ldots\ldots\ldots & k_\mu & = \omega_\mu F_n \end{array}$$

where $\omega_1^{(l+1)}, \omega_2^{(l+1)}, \ldots, \omega_\mu^{(l+1)}$ are all the power products of $x_1, x_2, \ldots, x_n$ of degree $l+1$, and $\lambda_1, \lambda_2, \ldots, \lambda_\mu$ are the coefficients of $X^{(0)}, X^{(1)}, \ldots, X^{(n-1)}$. That this array has the same number $\mu$ of rows as columns is seen from the fact that *one and only one of the elements* $a_1, a_2, \ldots, a_n$* *(the coefficients of* $x_1^{l_1}, x_2^{l_2}, \ldots, x_n^{l_n}$ *in* $F_1, F_2, \ldots, F_n$*) occurs in each row and each column.* This is evident as regards the rows. To prove

* These are not the same as the $a_1, a_2, \ldots, a_n$ in the first column of the array. The latter should be represented by some other symbols.

that the same is true of the columns, we notice firstly that there is no power product $\omega^{(l+1)}$ of degree $l+1$ reduced in all the variables, for the highest power product of this kind is $x_1^{l_1-1} x_2^{l_2-1} \dots x_n^{l_n-1}$ which is of degree $l < l+1$; and secondly, if we put every coefficient of $F_1, F_2, \dots, F_n$, except only $a_1, a_2, \dots, a_n$, equal to zero, the diagram will represent the polynomial

$$X^{(0)} a_1 x_1^{l_1} + X^{(1)} a_2 x_2^{l_2} + \dots + X^{(n-1)} a_n x_n^{l_n},$$

in which each power product $\omega^{(l+1)}$ occurs once and once only, so that one and only one element $a_1, a_2, \dots, a_n$ occurs in each column of $D$.

*Thus $D$ when expanded has a term* $\pm a_1^{\mu_1} a_2^{\mu_2} \dots a_n^{\mu_n}$, where $\mu_i$ is the number of terms in $X^{(i-1)}$, and by saying that the coefficient of this term in $D$ is to be $+1$ we remove any ambiguity as to the sign of $D$. Also it is to be noted that *$D$ vanishes when $c_1, c_2, \dots, c_n$ all vanish*, for the column of $D$ corresponding to $x_n^{l+1}$ contains no elements other than $c_1, c_2, \dots, c_n$ and zeros.

Regarding the diagram as giving $\mu$ identical equations for

$$\omega_1^{(l+1)}, \omega_2^{(l+1)}, \dots, \omega_\mu^{(l+1)},$$

and solving, we have

$$D\omega^{(l+1)} \equiv 0 \bmod (F_1, F_2, \dots, F_n),$$

where $\omega^{(l+1)}$ is any power product of $x_1, x_2, \dots, x_n$ of degree $l+1$. It can be proved that the factors of $D$ other than $R$ can be divided out of this congruence equation, so that

$$R\omega^{(l+1)} \equiv 0 \bmod (F_1, F_2, \dots, F_n);$$

but this will not be assumed in what follows*.

**7.** The number of rows in $D$ corresponding to $F_n$ is the number of terms in $X^{(n-1)}$. But $X^{(n-1)}$ is of degree $l+1-l_n$ or

$$(l_1 - 1) + (l_2 - 1) + \dots + (l_{n-1} - 1),$$

and its terms consist of all the power products in

$$(1 + x_1 + \dots + x_1^{l_1-1}) \dots (1 + x_{n-1} + \dots + x_{n-1}^{l_{n-1}-1})$$

each multiplied by a power of $x_n$; hence the number of the terms is $l_1 l_2 \dots l_{n-1} = L_n$. Thus $D$ is homogeneous and of degree $L_n$ in the

* No proof of this has been published so far as I know. It can be proved that if $A$ is any whole function of the coefficients of $F_1, F_2, \dots, F_n$ not divisible by $R$, and $AF \equiv 0 \bmod (F_1, F_2, \dots, F_n)$, then $F \equiv 0 \bmod (F_1, F_2, \dots, F_n)$. Hence from $D\omega^{(l+1)} \equiv 0 \bmod (F_1, F_2, \dots, F_n)$ we have $R\omega^{(l+1)} \equiv 0 \bmod (F_1, F_2, \dots, F_n)$. The condition that $A$ is not divisible by $R$ is not needed if $F$ is of degree $\leqslant l$.

coefficients of $F_n$, and homogeneous and of degree $> L_i$ in the coefficients of $F_i$ $(i = 1, 2, \ldots, n-1)$. It follows that $R$, which is a factor of $D$, is at most of degree $L_n$ in the coefficients of $F_n$. We shall prove that $R$ is of this degree, and consequently of degree $L_i$ in the coefficients of $F_i$.

Let $D'$ be any other non-vanishing determinant of the array, viz.

$$\begin{array}{c|cccc|} & \omega_1^{(l+1)} & \omega_2^{(l+1)} & \ldots\ldots & \omega_\mu^{(l+1)} \\ \hline \alpha_1 & a_1' & b_1' & \ldots\ldots & k_1' \\ \alpha_2 & a_2' & b_2' & \ldots\ldots & k_2' \\ & \ldots & \ldots & \ldots & \ldots \\ \alpha_\mu & a_\mu' & b_\mu' & \ldots\ldots & k_\mu' \end{array}$$

This represents the polynomial $A_1 F_1 + A_2 F_2 + \ldots + A_n F_n$, in which $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the (arbitrarily chosen) coefficients of $A_1, A_2, \ldots, A_n$ which are not zeros. Choose $\lambda_1, \lambda_2, \ldots, \lambda_\mu$ in the previous diagram so that we have identically

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-1)} F_n = A_1 F_1 + A_2 F_2 + \ldots + A_n F_n.$$

This gives, by equating coefficients of power products on both sides,

$$\Sigma \lambda a = \Sigma \alpha a', \quad \Sigma \lambda b = \Sigma \alpha b', \ \ldots, \quad \Sigma \lambda k = \Sigma \alpha k'$$

as equations for $\lambda_1, \lambda_2, \ldots, \lambda_\mu$; and they have a unique solution, since $D$ does not vanish.

Let $\binom{\lambda}{\alpha}$ denote the determinant of the substitution corresponding to the solution of the above equations for $\lambda_1, \lambda_2, \ldots, \lambda_\mu$ as linear functions of $\alpha_1, \alpha_2, \ldots, \alpha_\mu$. Then if we put

$$\Sigma \lambda a = \Sigma \alpha a' = \lambda_1', \ \Sigma \lambda b = \Sigma \alpha b' = \lambda_2', \ \ldots, \ \Sigma \lambda k = \Sigma \alpha k' = \lambda_\mu'$$

we have

$$\binom{\lambda'}{\lambda} = D, \quad \binom{\lambda'}{\alpha} = D', \text{ and } \binom{\lambda'}{\lambda}\binom{\lambda}{\alpha} = \binom{\lambda'}{\alpha}, \quad \text{i.e. } D\binom{\lambda}{\alpha} = D',$$

by the rule of successive substitutions, or the rule for multiplying determinants. Hence

$$\frac{D'}{D} = \binom{\lambda}{\alpha}.$$

Now we can find the solution for $\lambda_1, \lambda_2, \ldots, \lambda_\mu$, or the solution of

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-1)} F_n = A_1 F_1 + A_2 F_2 + \ldots + A_n F_n,$$

in the following way. First solve the equation

$$Y^{(0)} F_1 + Y^{(1)} F_2 + \ldots + Y^{(n-2)} F_{n-1} + X^{(n-1)} = A_n$$

for the unknowns $Y^{(0)}, Y^{(1)}, \ldots, Y^{(n-2)}, X^{(n-1)}$. This equation has a unique solution, since the more particular equation

$$Y^{(0)} x_1^{l_1} + Y^{(1)} x_2^{l_2} + \ldots + Y^{(n-2)} x_{n-1}^{l_{n-1}} + X^{(n-1)} = A_n$$

has a unique solution (for any given polynomial $A_n$ can be expressed in one and only one way in the form on the left) and shows that the number of the coefficients of $Y^{(0)}, Y^{(1)}, \ldots, Y^{(n-2)}, X^{(n-1)}$ is equal to the number of equations they have to satisfy.

Substituting the value thus found for $X^{(n-1)}$ in the equation

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-1)} F_n = A_1 F_1 + A_2 F_2 + \ldots + A_n F_n,$$

it becomes

$$X^{(0)} F_1 + X^{(1)} F_2 + \ldots + X^{(n-2)} F_{n-1}$$
$$= (A_1 + Y^{(0)} F_n) F_1 + \ldots + (A_{n-1} + Y^{(n-2)} F_n) F_{n-1},$$

where $Y^{(0)}, Y^{(1)}, \ldots, Y^{(n-2)}$ have been found. Next solve the equation

$$Z^{(0)} F_1 + Z^{(1)} F_2 + \ldots + Z^{(n-3)} F_{n-2} + X^{(n-2)} = A_{n-1} + Y^{(n-2)} F_n,$$

which has a unique solution for $Z^{(0)}, Z^{(1)}, \ldots, Z^{(n-3)}, X^{(n-2)}$. We can proceed in this way till $X^{(0)}, X^{(1)}, \ldots, X^{(n-1)}$, i.e. $\lambda_1, \lambda_2, \ldots, \lambda_\mu$, have all been found.

In this method of solving the unknowns on the left are associated with $F_1, F_2, \ldots, F_{n-1}$ only and not with $F_n$. Hence $\binom{\lambda}{a}$ is a rational function of the coefficients of $F_1, F_2, \ldots, F_n$ whose denominator is independent of the coefficients of $F_n$, and the same is therefore true of $\frac{D'}{D} = \binom{\lambda}{a}$. Hence every determinant $D'$ of the array has a factor in common with $D$ which is of degree $L_n$ in the coefficients of $F_n$. The resultant $R$, which is the H.C.F. of all the determinants $D'$, is therefore of degree $L_i$ in the coefficients of $F_i$ $(i = 1, 2, \ldots, n)$.

If we put $D = AR$, $A$ is called the *extraneous factor* of $D$. We have proved that $A$ is independent of the coefficients of $F_n$; and it is proved at the end of § 8 that $A$ depends only on the coefficients of $(F_1, F_2, \ldots, F_{n-1})_{x_n=0}$.

**8. Properties of the Resultant.** Since $D$ has a term $a_1^{\mu_1} \ldots a_n^{\mu_n}$ (§ 6) *$R$ has a term $a_1^{L_1} a_2^{L_2} \ldots a_n^{L_n}$.* This is called the *leading term* of $R$.

Since $D$ *vanishes when* $c_1, c_2, \ldots, c_n$ *all vanish* (§ 6) *the same is true of $R$*; for $D = AR$ and $A$ is independent of $c_1, c_2, \ldots, c_n$.

*The extraneous factor $A$ of $D$ is a minor of $D$, viz. the minor obtained by omitting all the columns of $D$ corresponding to power*