IV. THE INVERSE SYSTEM AND MODULAR EQUATIONS

57. A considerable number of the properties proved in this section are to be found in (M); but the introduction of the inverse system is new.

Definitions. The array of the coefficients of a complete linearly independent set of members of a module M of degree $\leqslant t$ arranged under the power products $\omega_1, \omega_2, \ldots, \omega_\mu$ of degree $\leqslant t$ is called the *dialytic array* of the module M for degree t.

The linear homogeneous equations of which this array is the array of the coefficients are called the *dialytic equations* of M for degree t.

Thus the dialytic equations of M for degree t are represented by equating all members of M of degree $\leqslant t$ to zero and regarding the power products of $x_1, x_2, \ldots, x_n$ as symbols for the unknowns.

The array inverse (§ 54) to the dialytic array of M for degree t is called the *inverse array* of M for degree t.

The linear homogeneous equations of which this array is the array of the coefficients are called the *modular equations* of M for degree t.

The modular equations for degree t are the equations which are identically satisfied by the coefficients of each and every member of M of degree $\leqslant t$. They may not be independent for members of degree $< t$ and they do not apply to members of degree $> t$ (see § 59).

The sum of the products of the elements in any row of the inverse array for degree t with the inverse power products $\omega_1^{-1}, \omega_2^{-1}, \ldots, \omega_\mu^{-1}$ is called an *inverse function* of M for degree t.

Thus the modular equations of M for degree t are represented by equating all the inverse functions of M for degree t to zero, taking each negative power product $(x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ as a symbol for "the coefficient of $x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$ in the general member of M of degree t."

We shall also say that a polynomial $F = \Sigma a_{p_1, \ldots, p_n} x_1^{p_1} \ldots x_n^{p_n}$ and a finite or infinite negative power series $E = \Sigma c_{q_1, \ldots, q_n} (x_1^{q_1} \ldots x_n^{q_n})^{-1}$ are inverse to one another if the constant term of the product FE vanishes, i.e. if $\Sigma a_{p_1, p_2, \ldots, p_n} c_{p_1, p_2, \ldots, p_n} = 0$. Thus any member of M of degree $\leqslant t$ and any inverse function of M for degree t are inverse to one another.

Any inverse function of M for degree t can be continued so as to become an inverse function of M for any higher degree (§ 59), and when continued indefinitely becomes an inverse function of M *without limitation in respect to degree.* If all coefficients after a certain stage become zero the inverse function terminates and is a finite negative power series. In the case of an H-module the inverse functions are homogeneous (§ 59) and therefore finite.

In order that a function may be an inverse function of M it is necessary and sufficient that it should be inverse to all members of M; hence if M contains M' any inverse function of M' is an inverse function of M. The whole system of inverse functions of M can therefore be resolved into primary systems corresponding to the primary modules of M. The inverse functions of a Noetherian primary module are all finite (§ 65) but not in general homogeneous. The inverse functions of a non-Noetherian primary module are all infinite power series (§ 65).

We shall regard *inverse function* and *modular equation* as convertible terms, and use that term in each case which seems best suited to the context.

A module is completely determined by its system of modular equations no less than by its system of members. The two systems are alternative representations of the module. Also the properties of the modular equations are very remarkable, and it is necessary to consider them in order to give a complete theory of modular systems.

As there is a one-one correspondence between the members of a module M of degree $\leqslant t$ and the members of the equivalent H-module of degree t, so there is a one-one correspondence between the modular equations of M *for* degree t and the modular equations of the members of the equivalent H-module of degree t. These last are called the modular equations of the H-module *of* (absolute) degree t.

58. Theorem. *The number of independent modular equations of degree t of an H-module $(F_1, F_2, \ldots, F_r)$ of rank r is the coefficient of x^t in*

$$(1-x^{l_1})(1-x^{l_2})\ldots(1-x^{l_r})(1-x)^{-n},$$

where $l_1, l_2, \ldots, l_r$ are the degrees of $F_1, F_2, \ldots, F_r$.

Since the whole number of linearly independent polynomials of degree t is the number of power products of degree t, or the coefficient of x^t in $(1-x)^{-n}$, the theorem will be proved if it is shown that the number $N(r, t)$ of linearly independent members of $(F_1, F_2, \ldots, F_r)$ of degree t is the coefficient of x^t in

$$\{1-(1-x^{l_1})(1-x^{l_2})\ldots(1-x^{l_r})\}(1-x)^{-n}.$$

This is easily seen to be true when $r=1$.

Since any member of $(F_1, F_2, \ldots, F_r)$ is a linear combination of elementary members, we have

$$N(r, t)=N(r-1, t)+\rho,$$

where ρ is the number of polynomials $\omega_1 F_r, \omega_2 F_r, \ldots, \omega_\rho F_r$ of degree t of which no linear combination is a member of $(F_1, F_2, \ldots, F_{r-1})$, or the number of power products $\omega_1, \omega_2, \ldots, \omega_\rho$ of degree $t-l_r$ of which no linear combination is a member of $(F_1, F_2, \ldots, F_{r-1})$, § 48. Hence

$$\rho+N(r-1, t-l_r)=\text{number of power products of degree } t-l_r$$
$$=\text{coefficient of } x^t \text{ in } x^{l_r}(1-x)^{-n};$$

and

$$N(r, t)=N(r-1, t)-N(r-1, t-l_r)+\text{coefficient of } x^t \text{ in } x^{l_r}(1-x)^{-n}.$$

Hence, assuming the theorem for $N(r-1, t)$, it follows that $N(r, t)$ is the coefficient of x^t in

$$\{1-(1-x^{l_1})\ldots(1-x^{l_{r-1}})\}(1-x)^{-n}(1-x^{l_r})+x^{l_r}(1-x)^{-n},$$

or in
$$\{1-(1-x^{l_1})\ldots(1-x^{l_{r-1}})(1-x^{l_r})\}(1-x)^{-n},$$

which proves the theorem.

This result is independent of the coefficients of $F_1, F_2, \ldots, F_r$; hence it follows that any member of $(F_1, F_2, \ldots, F_r)$ is expressible in one way only in the form

$$X^{(0)}F_1+X^{(1)}F_2+\ldots+X^{(r-1)}F_r,$$

where $X^{(i)}$ (as in §§ 6, 7) is a polynomial in which $x_1, x_2, \ldots, x_i$ occur only to powers as high as $x_1^{l_1-1}, \ldots, x_i^{l_i-1}$, the variables having been subjected to a substitution beforehand.

The theorem can be applied to any module $(F_1, F_2, \ldots, F_r)$ of rank r if $(F_1, F_2, \ldots, F_r)$ is an H-basis, i.e. if the H-module determined by the terms of highest degree in $F_1, F_2, \ldots, F_r$ is of rank r (§ 49). In this case *the number of independent modular equations for degree t is the coefficient of x^t in* $(1-x^{l_1})\ldots(1-x^{l_r})(1-x)^{-n-1}$. An important particular case is the following:

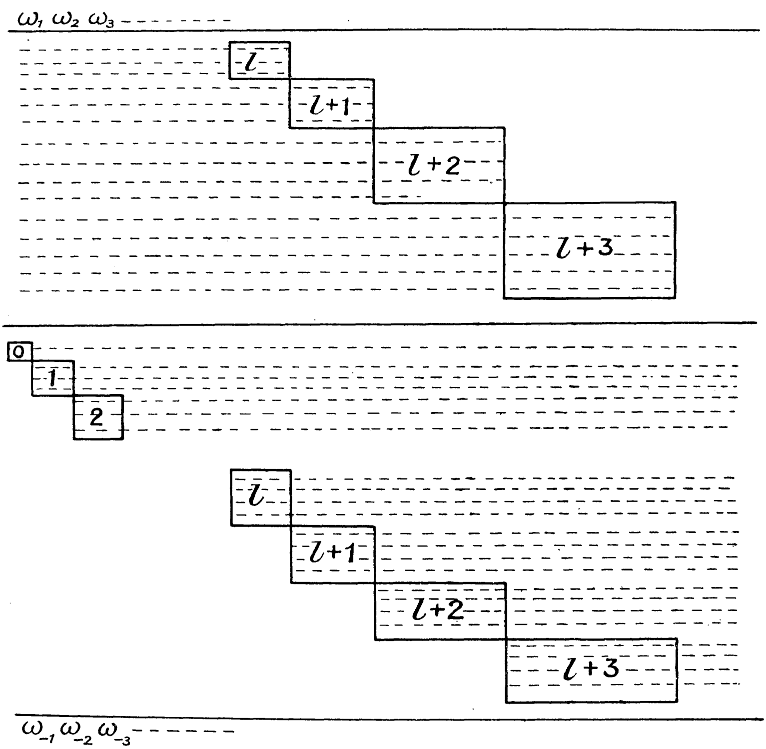
The number of independent modular equations of a module $(F_1, F_2, \ldots, F_n)$ of rank n such that the resultant of the terms of highest degree in $F_1, F_2, \ldots, F_n$ does not vanish is $l_1 l_2 \ldots l_n - 1$ for degree $l-1$, and $l_1 l_2 \ldots l_n$ for any degree $\geqslant l$, where

$$l=l_1+l_2+\ldots+l_n-n.$$

This is also true for any H-module $(F_1, F_2, \ldots, F_n)$ of rank n; but the number of modular equations *for* degree t will be the sum of the numbers of modular equations *of* all degrees $\leqslant t$, so that there is one modular equation of degree l and none of any degree $> l$.

59. *Any inverse function of M for any degree can be continued so as to give an inverse function of M for any higher degree.*

By carrying the continuation on indefinitely we obtain a power



series (finite or infinite) which is an inverse function of M for all degrees without limit.

Let $(F_1, F_2, \ldots, F_k)$ be an H-basis of M. Then any member F of M is a linear combination of elementary members $\omega_i F_j$ *no one of which is of higher degree than F.* Let l be the lowest degree of any member of M. Write down the dialytic array of M for degree l, viz. the array of the coefficients of such members of the H-basis as are of degree l. Their terms of degree l (corresponding to the compartment l of the diagram) are linearly independent, for if not there would be a member of M of degree $< l$, which is not the case. Next write down the rows of the array representing such members of the basis as are of degree $l+1$, and members obtained by multiplying members of degree l by $x_1, x_2, \ldots, x_n$, so as to obtain a complete set of members of degree $l+1$ linearly independent as regards their terms of degree $l+1$, these terms corresponding to the compartment $l+1$ of the diagram. Proceeding in the same way we can obtain the whole dialytic array for any degree.

To obtain the inverse array for the same degree first write down square compartments $0, 1, 2, \ldots, l-1$ with arbitrary elements corresponding to degrees $0, 1, 2, \ldots, l-1$, and then a compartment l inverse to the compartment l of the dialytic array. Each row of the compartments $0, 1, 2, \ldots, l-1$ can be continued so as to be inverse to the dialytic array for degree l, since the determinants of the compartment l do not all vanish. This completes the inverse array for degree l. All its rows can be continued so as to be inverse to the dialytic array for degree $l+1$, and a compartment $l+1$ of new rows can be added inverse to the compartment $l+1$ of the dialytic array. This completes the inverse array for degree $l+1$; and we can proceed in a similar way to obtain the inverse array for any degree.

This diagram or scheme for the dialytic and inverse arrays of a given module M will be often referred to. The ease with which it can be conceived mentally is due to the fact that it is obtained by working with an H-basis of M. Each pair of corresponding compartments $l+i$ form inverse arrays, and in combination form a square array, showing that the combined complete arrays for any degree have the same number of rows as columns. In the case of a module of rank n the compartments of the dialytic array eventually become square and *the total number of rows of the inverse array is finite.* To a square compartment in either array corresponds no compartment or rows of the other array. In the case of an H-module the compartments are the only parts of the arrays whose elements do not vanish, i.e. the inverse functions are homogeneous.

Definition. The negative power series represented by the rows of the inverse array *continued indefinitely* will be called the *members of the inverse system*, and $E_1, E_2, E_3, \ldots$ will be used to denote them, just as $F_1, F_2, F_3, \ldots$ denote members of the module.

The system inverse to (1) has no member. The system inverse to $(x_1, x_2, \ldots, x_n)$ has only one member $E=1$; and the modular equation $1=0$ signifies that the module contains the origin.

60. Properties of the Inverse System. Before attempting to show in what ways the inverse system may be simplified we consider its general properties.

Definition. If $E=\overset{\infty}{\Sigma} c_{p_1, p_2, \ldots, p_n}(x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ is a negative power series (no p_i negative), and A any polynomial, the part of the expanded product AE which consists of a negative power series will be denoted by $A.E$ and called the *A-derivate of E.* Thus

$$x_1 . (x_1 x_2)^{-1} = (x_2)^{-1}, \quad x_2^2 . (x_1 x_2)^{-1} = 0.$$

A negative power series $E=\overset{\infty}{\Sigma} c_{p_1, p_2, \ldots, p_n}(x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ is or is not an inverse function of a module M according as every member $F=\Sigma a_{p_1, p_2, \ldots, p_n} x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$ of M, or not every member of M, is inverse to it, i.e. according as every $\Sigma a_{p_1, p_2, \ldots, p_n} c_{p_1, p_2, \ldots, p_n} = 0$ or not. Suppose E an inverse function and F *any* member of M. Then $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} F = \Sigma a_{p_1, p_2, \ldots, p_n} x_1^{p_1+l_1} \ldots x_n^{p_n+l_n}$ is a member inverse to E; hence every $\Sigma a_{p_1, p_2, \ldots, p_n} c_{p_1+l_1, \ldots, p_n+l_n} = 0$, and

$$\Sigma c_{p_1+l_1, \ldots, p_n+l_n}(x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1},$$

or $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} . E$, is a member of the inverse system. *Hence if E is a member of the inverse system of M so also is $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} . E$, and if $E_1, E_2, \ldots, E_h$ are members so also is $A_1 . E_1 + A_2 . E_2 + \ldots + A_h . E_h$ a member, where $A_1, A_2, \ldots, A_h$ are arbitrary polynomials.*

In a slightly modified sense which will be explained later (§ 82) *the inverse system of any module M has a finite basis $[E_1, E_2, \ldots, E_h]$ such that any member of the inverse system is of the form*

$$X_1 . E_1 + X_2 . E_2 + \ldots + X_h . E_h,$$

where $X_1, X_2, \ldots, X_h$ are polynomials.

This theorem is evidently true in the important case in which the total number of linearly independent members of the inverse system is finite, viz. in the case of a module of rank n and in the case of a module of rank r when treated as a module in r variables only, or, in other words, in the case of a module which resolves into simple modules.

Regarding the inverse system as representing the modular equations of M we shall write $M=[E_1, E_2, \ldots, E_h]$ as well as $M=(F_1, F_2, \ldots, F_k)$. Here M is the L.C.M. of $[E_1]$, $[E_2]$, ..., $[E_h]$ and the G.C.M. of (F_1), (F_2), ..., (F_k).

Definition. A module M will be called a *principal system* if its inverse system has a basis consisting of a single member, i.e. if $M=[E]$.

A module of the principal class is a principal system (§ 72), but a principal system is not necessarily of the principal class. A principal system is however the residual of a module (F) with respect to any module of the principal class which contains, and is of the same rank as, the principal system (cf. § 62).

61. *The system inverse to $M=(F_1, F_2, \ldots, F_k)$ is the system whose F_i-derivates $(i=1, 2, \ldots, k)$ vanish identically.*

In other words, in order that E may be a member of the inverse system of M it is necessary and sufficient that $F_i \,.\, E$ $(i=1, 2, \ldots, k)$ should vanish identically. For if $E=\overset{\infty}{\Sigma} c_{q_1, q_2, \ldots, q_n}(x_1^{q_1} x_2^{q_2} \ldots x_n^{q_n})^{-1}$ is any member of the inverse system, and $F_i=\Sigma a_{p_1, p_2, \ldots, p_n} x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$, then

$$F_i \,.\, E=\sum_p a_{p_1, p_2, \ldots, p_n} \sum_q c_{p_1+q_1, \ldots, p_n+q_n}(x_1^{q_1} x_2^{q_2} \ldots x_n^{q_n})^{-1}$$

$$=\sum_q (x_1^{q_1} x_2^{q_2} \ldots x_n^{q_n})^{-1} \sum_p a_{p_1, p_2, \ldots, p_n} c_{p_1+q_1, \ldots, p_n+q_n}=0,$$

since every $\sum\limits_p a_{p_1, \ldots, p_n} c_{p_1+q_1, \ldots, p_n+q_n}$ vanishes ($x_1^{q_1} \ldots x_n^{q_n} F_i$ being inverse to E). Conversely if $F_i \,.\, E=0$, then $\sum\limits_p a_{p_1, \ldots, p_n} c_{p_1+q_1, \ldots, p_n+q_n}=0$, i.e. $x_1^{q_1} \ldots x_n^{q_n} F_i$ is inverse to E, and every member of M is inverse to E, i.e. E is a member of the inverse system.

Similarly if $M=[E_1, E_2, \ldots, E_h]$ the necessary and sufficient condition that F may be a member of M is that $F \,.\, E_j$ $(j=1, 2, \ldots, h)$ vanishes identically.

62. *The modular equations of $M/(F_1, F_2, \ldots, F_k)$ are the F_i-derivates of the modular equations of M, i.e.*

$$[E_1, E_2, \ldots, E_h]/(F_1, F_2, \ldots, F_k)=[\ldots, F_i \,.\, E_j, \ldots].$$

For the necessary and sufficient condition that F may be a member of the residual module is

$$FF_i=0 \bmod M \quad (i=1, 2, \ldots, k)$$

or $$FF_i \,.\, E_j = 0 \quad (i=1, 2, \ldots, k;\ j=1, 2, \ldots, h)$$
or $$F\,.\,(F_i\,.\,E_j)=0.$$
Hence $[\ldots, F_i\,.\,E_j, \ldots]$ is the residual module (§ 61).

63. *A system of negative power series with a finite basis $[E_1, E_2, \ldots, E_h]$ of such a nature that all derivates of $E_1, E_2, \ldots, E_h$ belong to the system is an inverse system of a module if E_i $(i=1, 2, \ldots, h)$ has an F_i-derivate which vanishes identically.*

For there are polynomials F such that the F-derivate of each of $E_1, E_2, \ldots, E_h$ vanishes identically, the product $F_1F_2\ldots F_h$ being one such polynomial. Also the whole aggregate of such polynomials F constitutes a module M; for if F belongs to the aggregate so does AF. Consider the dialytic and inverse arrays of M obtained as in § 59. Since every member of M is inverse to every member of $[E_1, E_2, \ldots, E_h]$ all members of the latter are represented in the inverse array. If any other power series are represented, viz. if there is a row of the inverse array which does not represent a member of $[E_1, E_2, \ldots, E_h]$, let it begin in the compartment $l+i$. Then if we omit this row we can add a row to the dialytic array representing a polynomial of degree $l+i$ inverse to all members of $[E_1, E_2, \ldots, E_h]$ but not a member of M. This is contrary to the fact that M is the whole aggregate of such polynomials. Hence the system inverse to M is $[E_1, E_2, \ldots, E_h]$.

Thus in order that $E=\overset{\infty}{\Sigma} c_{p_1, p_2, \ldots, p_n}(x_1^{p_1}x_2^{p_2}\ldots x_n^{p_n})^{-1}$ may represent a modular equation of a module it is necessary and sufficient that $c_{p_1, p_2, \ldots, p_n}$ should be a recurrent function of $p_1, p_2, \ldots, p_n$, that is, a function satisfying some recurrent relation

$$\sum_p a_{p_1, p_2, \ldots, p_n} c_{p_1+l_1, \ldots, p_n+l_n} = 0$$

for all positive integral values of $l_1, l_2, \ldots, l_n$, where the $a_{p_1, p_2, \ldots, p_n}$ are a set of fixed quantities finite in number. It may be that $c_{p_1, p_2, \ldots, p_n}$ satisfies several such recurrent relations not deducible from one another; but it is sufficient if it satisfies one.

64. *Transformation of the inverse system corresponding to a linear transformation of the modular system.*

If the variables in the modular system M are subjected to a linear non-homogeneous substitution with non-vanishing determinant by which M is transformed to M' it is required to find how the inverse system $[E_1, E_2, \ldots, E_h]$ is to be transformed so as to be inverse to M'.

In other words, if the negative power series E is inverse to the polynomial F it is required to find a power series E' inverse to the transformed polynomial F'. It will be shown that an E' exists which can be derived from E in a way depending only on the substitution and not on the polynomial F.

Let $F = \Sigma a_{p_1, \ldots, p_n} x_1^{p_1} \ldots x_n^{p_n}$, $F' = \Sigma a'_{q_1, \ldots, q_n} x_1'^{q_1} \ldots x_n'^{q_n}$, and let the coefficients $c_{p_1, p_2, \ldots, p_n}$ of E be represented symbolically by $c_1^{p_1} c_2^{p_2} \ldots c_n^{p_n}$. Then we have $E = \Sigma c_1^{p_1} \ldots c_n^{p_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1}$; and

$$\Sigma a_{p_1, p_2, \ldots, p_n} c_1^{p_1} c_2^{p_2} \ldots c_n^{p_n} = 0,$$

since E, F are inverse to one another. Let the inverse substitution be

$$x_i' = a'_{i1} x_1 + \ldots + a'_{in} x_n + a_i' \quad (i = 1, 2, \ldots, n).$$

Then $\Sigma a'_{q_1, \ldots, q_n} (a'_{11} x_1 + \ldots)^{q_1} \ldots (a'_{n1} x_1 + \ldots)^{q_n} = \Sigma a_{p_1, \ldots, p_n} x_1^{p_1} \ldots x_n^{p_n}$, and we have

$$\Sigma c_1^{p_1} \ldots c_n^{p_n} \times$$
$$\{\text{coeff. of } x_1^{p_1} \ldots x_n^{p_n} \text{ in } \Sigma a'_{q_1 \ldots q_n} (a'_{11} x_1 + \ldots)^{q_1} \ldots (a'_{n1} x_1 + \ldots)^{q_n}\} = 0,$$

i.e. $$\Sigma a'_{q_1 \ldots q_n} (a'_{11} c_1 + \ldots)^{q_1} \ldots (a'_{n1} c_1 + \ldots)^{q_n} = 0,$$

i.e. the power series $E' = \Sigma (a'_{11} c_1 + \ldots)^{q_1} \ldots (a'_{n1} c_1 + \ldots)^{q_n} (x_1^{q_1} \ldots x_n^{q_n})^{-1}$ is inverse to the polynomial $F' = \Sigma a'_{q_1, \ldots, q_n} x_1^{q_1} \ldots x_n^{q_n}$.

Hence the coefficient of $(x_1^{q_1} x_2^{q_2} \ldots x_n^{q_n})^{-1}$ in the transformed power series E' is

$$c'_{q_1, q_2, \ldots, q_n} = (a'_{11} c_1 + \ldots)^{q_1} (a'_{21} c_1 + \ldots)^{q_2} \ldots (a'_{n1} c_1 + \ldots)^{q_n},$$

where, after expanding the right-hand side, $c_1^{p_1} c_2^{p_2} \ldots c_n^{p_n}$ is to be put equal to $c_{p_1, p_2, \ldots, p_n}$, the coefficient of $(x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ in E. For such a transformation of F and E, when not inverse to one another, $\Sigma a_{p_1, p_2, \ldots, p_n} c_{p_1, p_2, \ldots, p_n}$ is an absolute invariant.

The most important transformation is that corresponding to a change of origin only. In this case, if

$$F = \Sigma a_{p_1 \ldots p_n} x_1^{p_1} \ldots x_n^{p_n} \quad \text{and} \quad E = \Sigma c_1^{p_1} \ldots c_n^{p_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1},$$

and the new origin is the point $(-a_1, -a_2, \ldots, -a_n)$,

then $$F' = \Sigma a_{p_1 \ldots p_n} (x_1 - a_1)^{p_1} \ldots (x_n - a_n)^{p_n}$$

and $$E' = \Sigma (c_1 + a_1)^{p_1} \ldots (c_n + a_n)^{p_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1}.$$

It is to be noticed that if E is a finite power series it nevertheless transforms into an infinite power series E'. In particular if $E = 1$

then $E' = \Sigma a_1^{p_1} \dots a_n^{p_n} (x_1^{p_1} x_2^{p_2} \dots x_n^{p_n})^{-1}$, the inverse function of $(x_1 - a_1, \dots, x_n - a_n)$.

For homogeneous substitutions another way of considering corresponding transformations of F and E can be given, which however *excludes a change of origin.* Represent E by

$$\overset{\infty}{\Sigma} c_{p_1, p_2, \dots, p_n} \frac{u_1^{p_1} u_2^{p_2} \dots u_n^{p_n}}{p_1!\, p_2! \dots p_n!}$$

instead of $\Sigma c_{p_1, p_2, \dots, p_n} (x_1^{p_1} \dots x_n^{p_n})^{-1}$, and let the new E be defined as inverse (or conjugate) to $F = \Sigma a_{p_1, p_2, \dots, p_n} x_1^{p_1} \dots x_n^{p_n}$ when the same relation $\Sigma a_{p_1, \dots, p_n} c_{p_1, \dots, p_n} = 0$ holds as before. Then for contragredient substitutions of $x_1, x_2, \dots, x_n$ and $u_1, u_2, \dots, u_n$ the polynomial F and power series E will always remain inverse (or conjugate) to one another if they are so originally. Also the members E of the inverse (or conjugate) system of a module M, when expressed in the new form above, are the power series with respect to which the members (of the basis) of the module M are apolar (§ 61).

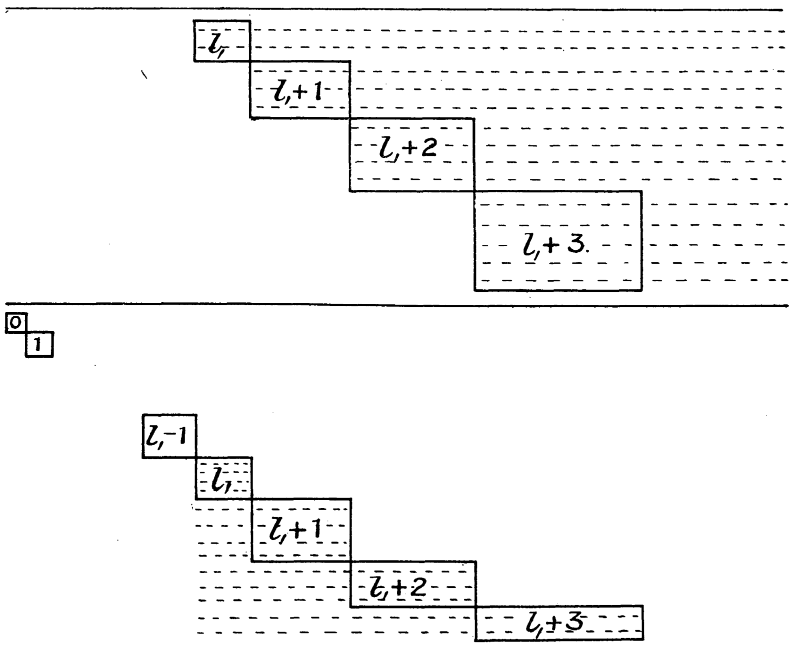
65. The Noetherian Equations of a Module. The modular equations $\Sigma c_{p_1, p_2, \dots, p_n} (x_1^{p_1} x_2^{p_2} \dots x_n^{p_n})^{-1} = 0$ of a module M for degree t are finite because they are only applicable to members of degree $\leqslant t$, and the coefficients $(x_1^{p_1} x_2^{p_2} \dots x_n^{p_n})^{-1}$ in the general member of degree t vanish when $p_1 + \dots + p_n > t$. A modular equation may however be finite in itself, i.e. every $c_{p_1, p_2, \dots, p_n}$ for which $p_1 + p_2 + \dots + p_n$ exceeds a certain fixed number l may vanish. If such an equation is applied to a polynomial of degree $> l$ it only affects the coefficients of terms of degree $\leqslant l$.

Definition. The *Noetherian equations* of a module are the modular equations which are finite in themselves.

There are no Noetherian equations if the module does not contain the origin. For if $E = 0$ is a Noetherian equation of absolute degree l, and ω^{-1} a power product of absolute degree l which is present in E, the derivate equation $\omega \,.\, E = 0$ is $1 = 0$, showing that the module contains the origin. *Every Noetherian equation has the equation* $1 = 0$ *as a derivate.*

On the other hand Noetherian equations always exist if the module contains the origin, for the equation $1 = 0$ exists, and so does the equation $\omega^{-1} = 0$, where ω is any power product of less degree than any term which occurs in any member of the module.

The whole system of Noetherian equations of a non-Noetherian module M forms only a part of the whole system of modular equations, and is exhibited by a scheme similar to but different from that of § 59, with which it should be compared. In this new scheme the rows of the dialytic array represent the members of the module arranged in order according to their *underdegree* (or degree of their lowest terms) instead of their degree (or degree of their highest terms). The first set of rows represents a complete set of members of underdegree l_1 which are linearly independent as regards their terms of degree l_1,



where l_1 is the lowest underdegree of any member of M. These are obtained from any basis of M, which need not be an H-basis. The next set of rows represents a complete set of members of underdegree l_1+1 which are linearly independent as regards their terms of degree l_1+1, obtained partly from the basis of M and partly from the set of members of underdegree l_1 by multiplying them by $x_1, x_2, \dots, x_n$; and similarly for succeeding sets. The compartments $l_1, l_1+1, \dots$ correspond to the terms of lowest degree in the successive sets.

To obtain the corresponding inverse (or Noetherian) array first insert square compartments $0, 1, 2, \ldots, l_1 - 1$ with arbitrary elements (or with elements 1 in the diagonal and the remaining elements zero) corresponding to degrees $0, 1, 2, \ldots, l_1 - 1$; and then a compartment l_1 inverse to the compartment l_1 of the dialytic array. This completes the array for degree l_1; all its rows are inverse to all members of M and represent Noetherian equations. Next insert a compartment $l_1 + 1$ inverse to the compartment $l_1 + 1$ of the dialytic array, and continue its rows backwards so as to be inverse to the first set of rows of the dialytic array. This completes the array for degree $l_1 + 1$; and we can proceed similarly to find in theory the whole of the Noetherian array.

The object of the diagram is merely to exhibit the whole system of Noetherian equations, which it evidently does. If F is a polynomial for which all the Noetherian equations for degree t are satisfied, then, up to and inclusive of its terms of degree t, F is a linear combination of members of the module of underdegree $\leqslant t$, i.e. F is expressible as far as degree t in the form $X_1F_1 + X_2F_2 + \ldots + X_kF_k$, where $X_1, X_2, \ldots, X_k$ are polynomials, and $F = 0 \bmod (M, O^{t+1})$. Consequently if F satisfies the whole system of Noetherian equations it is of the form $P_1F_1 + P_2F_2 + \ldots + P_kF_k$, where $P_1, P_2, \ldots, P_k$ are power series. Hence $FF_0 = 0 \bmod M$, where F_0 has a non-vanishing constant term (§ 56); and, if M is a Noetherian module, $F = 0 \bmod M$. *Hence the whole system of modular equations of a Noetherian module can be expressed as a system of Noetherian equations.*

66. Modular Equations of Simple Modules. If in the last article the rows of the compartment $l_1 + i$ of the dialytic array should be equal in number to the power products of degree $l_1 + i$ there will be no Noetherian equations of absolute degree $\geqslant l_1 + i$. In this case the Noetherian equations are finite in number and can be actually determined (at any rate in numerical examples). This can only happen when the module contains the origin as an isolated point, and the Noetherian equations are then the modular equations of the simple Noetherian module contained in the given module. The simple module itself is (M, O^{l_1+i}) and $l_1 + i$ is its characteristic number.

Thus the simple modules at isolated points of a given module M can all be found by moving the origin to each point in succession and finding its Noetherian equations and characteristic number.

Let M have a simple module at the point $(a_1, a_2, \ldots, a_n)$. Move the origin to the point and find the Noetherian equations. They will be represented by finite negative power series

$$E_1 = E_2 = \ldots = E_h = 0$$

and all derivates of the same. Also any such system represents a simple module at the origin; the fact that the coefficients of $E_1, E_2, \ldots, E_h$ are recurrent functions (§ 63) placing no restriction on them when finite in number. Let $E_i = \Sigma c_{p_1, p_2, \ldots, p_n} (x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ be of absolute degree $\gamma_i - 1$. Moving the origin back to its original position, that is, to the point $(-a_1, -a_2, \ldots, -a_n)$, the equation $E_i = 0$ becomes (§ 64)

$$\Sigma (c_1 + a_1)^{p_1} (c_2 + a_2)^{p_2} \ldots (c_n + a_n)^{p_n} (x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1} = 0,$$

where, after expanding $(c_1 + a_1)^{p_1} \ldots (c_n + a_n)^{p_n}$, each $c_1^{q_1} \ldots c_n^{q_n}$ is to be put equal to the known constant $c_{q_1, q_2, \ldots, q_n}$ which it represents. Also $c_{q_1, q_2, \ldots, q_n} = 0$ if $q_1 + q_2 + \ldots + q_n \geqslant \gamma_i$. Thus

$$(c_1 + a_1)^{p_1} (c_2 + a_2)^{p_2} \ldots (c_n + a_n)^{p_n} = \left(1 + \frac{c_1}{a_1}\right)^{p_1} \ldots \left(1 + \frac{c_n}{a_n}\right)^{p_n} a_1^{p_1} a_2^{p_2} \ldots a_n^{p_n}$$
$$= k_{p_1, p_2, \ldots, p_n} a_1^{p_1} a_2^{p_2} \ldots a_n^{p_n},$$

where $k_{p_1, p_2, \ldots, p_n}$ is a whole function of $p_1, p_2, \ldots, p_n$ of degree $\gamma_i - 1$.

Hence the modular equations of any simple module at the point $(a_1, a_2, \ldots, a_n)$ are represented by power series

$$\overset{\infty}{\Sigma} k_{p_1, p_2, \ldots, p_n} a_1^{p_1} a_2^{p_2} \ldots a_n^{p_n} (x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1} = 0$$

and their derivates, where $k_{p_1, p_2, \ldots, p_n}$ is a whole function of $p_1, p_2, \ldots, p_n$. Conversely any system of equations (finite in number) of this type with all their derivates is a system of modular equations of a simple module at the point $(a_1, a_2, \ldots, a_n)$.

The following is a consequence of the above. The general solution for the recurrent function $c_{p_1, p_2, \ldots, p_n}$ (§ 63) satisfying a set of recurrent equations $\sum_p a_{p_1, p_2, \ldots, p_n} c_{p_1 + l_1, \ldots, p_n + l_n} = 0$ for all positive integral values of $l_1, l_2, \ldots, l_n$, when the corresponding polynomials $\Sigma a_{p_1, p_2, \ldots, p_n} x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$ have only a finite number of points $(a_1, a_2, \ldots, a_n)$ in common, is $\Sigma A a_1^{p_1} a_2^{p_2} \ldots a_n^{p_n}$, where A is a whole function of $p_1, p_2, \ldots, p_n$ dependent on the point $(a_1, a_2, \ldots, a_n)$ and involving linear parameters. When the polynomials have an infinite number of points in common there can scarcely be said to be a general solution for $c_{p_1, p_2, \ldots, p_n}$.

Properties of Simple Modules

67. Theorem. *If the resultant of* $(F_1, F_2, \ldots, F_n)$ *does not vanish identically the number of Noetherian equations of any simple module of* $(F_1, F_2, \ldots, F_n)$ *is equal to the multiplicity of the corresponding solution of* $F_1 = F_2 = \ldots = F_n = 0$ *given by the resultant.*

This theorem is proved for the case $n = 2$ in (M_1, p. 388) and for the general case in (L, p. 98). Both proofs are very complicated; and a simpler proof is given here.

By the resultant of $(F_1, F_2, \ldots, F_n)$ we shall understand the resultant with respect to $x_1, x_2, \ldots, x_{n-1}$, viz. a polynomial in x_n, the variables having been subjected to a homogeneous linear substitution beforehand. Move the origin to any point of $(F_1, F_2, \ldots, F_n)$. Then, if x_n^C is the highest power of x_n which divides the resultant, C is the multiplicity of the solution of $F_1 = F_2 = \ldots = F_n = 0$ corresponding to the origin. Let Q be the whole simple module of $(F_1, F_2, \ldots, F_n)$ at the origin, and N the number of its modular equations. We have to prove that $C = N$.

Consider first the specially simple case in which the origin is not a singular point of the curve $(F_2, F_3, \ldots, F_n)$. The terms of the first degree in $F_2, F_3, \ldots, F_n$ are then linearly independent. For simplicity we may suppose them to be $x_2, x_3, \ldots, x_n$. Then F_1 can be modified by $F_2, F_3, \ldots, F_n$ so that its terms of lowest degree reduce to the single term x_1^p. Hence the modular equations of Q, or Noetherian equations of $(F_1, F_2, \ldots, F_n)$, are $x_1^{-p+1} = x_1^{-p+2} = \ldots = x_1^{-1} = 1 = 0$ (§ 65), so that $N = p$. Also the number of points of intersection of $F_1 = F_2 = \ldots = F_n = 0$ that coincide with the origin is p, so that $C = p$. Hence $C = N$.

Consider now the general case. Let $F_1', F_2', \ldots, F_n'$ be n polynomials whose coefficients are arbitrary except that they satisfy the N equations of Q. Then $(F_1, F_2, \ldots, F_n)$ and $(F_1', F_2', \ldots, F_n')$ have the same simple module Q at the origin, and the same N. It can be proved also that they have the same C. By the Lasker-Noether theorem (§ 56), since $(F_1, F_2, \ldots, F_n)$ and $(F_1', F_2', \ldots, F_n')$ have the same Noetherian equations, there exist polynomials $\phi_1, \phi_2, \ldots, \phi_n$ and $\phi_1', \phi_2', \ldots, \phi_n'$, none of which vanish at the origin, such that

$$\phi_i F_i = 0 \bmod (F_1', F_2', \ldots, F_n') \quad \text{and} \quad \phi_i' F_i' = 0 \bmod (F_1, F_2, \ldots, F_n).$$

Hence the module $(\phi_1 F_1, \phi_2 F_2, \ldots, \phi_n F_n)$ contains $(F_1', F_2', \ldots, F_n')$, and the resultant of the former is divisible by that of the latter (§ 11).

But the resultant of $(\phi_1 F_1, \phi_2 F_2, \ldots, \phi_n F_n)$ is the product of 2^n resultants of which one only, the resultant of $(F_1, F_2, \ldots, F_n)$, has x_n as a factor. Hence the resultant of $(F_1, F_2, \ldots, F_n)$ is divisible by as high a power of x_n as the resultant of $(F_1', F_2', \ldots, F_n')$, and *vice versa*; i.e. the two resultants are divisible by the same power of x_n.

Now the resultant of the terms of highest degree $l_1, l_2, \ldots, l_n$ in $F_1', F_2', \ldots, F_n'$ does not vanish, for the coefficients of these terms are absolutely arbitrary if $l_1, l_2, \ldots, l_n$ are all chosen as high as the characteristic number of Q. Hence the equations $F_1'=F_2'=\ldots=F_n'=0$ have no solutions at infinity, and the number of their finite solutions is $l_1 l_2 \ldots l_n$, taking multiplicity into account. Also the sum of the values of N for all the points of $(F_1', F_2', \ldots, F_n')$ is $l_1 l_2 \ldots l_n$ (end of § 58), i.e. is equal to the sum of the values of C. Also each point of $(F_1', F_2', \ldots, F_n')$ except the origin comes under the simple case considered above; for even if the curve $(F_2', F_3', \ldots, F_n')$ has any singular points other than the origin, F_1' does not pass through them, since the origin is the only fixed point of F_1'. Hence the values of C and N are equal at each point of $(F_1', F_2', \ldots, F_n')$ other than the origin, and are therefore also equal at the origin. This proves the theorem.

68. *Definitions.* The *multiplicity* of a simple module is the number of its independent Noetherian equations.

This number has a geometrical interpretation when the theory of the resultant is applicable; but in general it has only an algebraical interpretation.

The *multiplicity of a primary module* of rank r is the multiplicity of each of the simple modules into which it resolves when regarded as a module in r variables only.

Thus there are four important numbers in connection with any primary module, viz. the rank r, the order d, the characteristic number γ, and the multiplicity μ.

A primary module of rank r will be said to be of the *principal Noetherian class* if there is a module $(F_1, F_2, \ldots, F_r)$ of rank r which contains it and does not contain any primary module of greater multiplicity with the same spread. On moving the origin to any general point of the spread any member of the primary module will be of the form $P_1 F_1 + P_2 F_2 + \ldots + P_r F_r$, where $P_1, P_2, \ldots, P_r$ are power series.

In other words, the primary modules into which a module of the principal class resolves are said to be of the principal Noetherian class.

Any prime module is of the principal Noetherian class; but in general a primary module is such that any module of the principal class which contains it determines a primary module of greater multiplicity. For example, O^2 is of multiplicity $n+1$, but any module of the principal class of rank n containing O^2 contains a simple module at the origin of multiplicity 2^n at least.

If M is a module of rank n the number of its modular equations is finite and equal to the sum $\Sigma\mu$ of the multiplicities of its simple modules. In order that we may have $F=0 \bmod M$ the coefficients of F must satisfy the $\Sigma\mu$ equations (which will not be independent unless F is of sufficiently high degree). Any set of $\Sigma\mu$ linearly independent polynomials such that no linear combination of them is a member of M is called a *complete set of remainders* for M; and has the property that any polynomial F which is not a member of M is congruent mod M to a unique linear combination of the set of remainders. The simplest way of choosing a complete set of remainders is to take the polynomial 1 of degree 0, then as many power products of degree 1 as possible, then as many power products of degree 2 as possible, and so on, till a set of $\Sigma\mu$ power products has been obtained of which no linear combination is a member of M. We shall call any such set a *simple complete set* of remainders for M.

If $M=[E_1, E_2, \ldots, E_h]$ is a simple Noetherian module no member E of the system $[E_1, E_2, \ldots, E_h]$ can have the same coefficients (assumed real) as a member F of M; for if E and F had the same coefficients the sum of their squares would be zero. Hence if the members of the system $[E_1, E_2, \ldots, E_h]$ have their power products changed from negative to positive they will form a complete set of remainders for M.

69. *A Noetherian principal system $[E_1]$ is uniquely expressible as a system $[E]$ such that the polynomial F with the same coefficients as E is a member of the module $[E]/O$.*

Let $E_2, E_3, \ldots, E_\mu$ be a complete set of linearly independent derivates of E_1 all of less absolute degree than E_1, and let $F_1, F_2, \ldots, F_\mu$ be the polynomials having the same coefficients as $E_1, E_2, \ldots, E_\mu$. Then $E_2, E_3, \ldots, E_\mu$ are the members of the system

$$[E_1]/O=[x_1.E_1,\ x_2.E_1, \ldots, x_n.E_1];$$

and $F_2, F_3, \ldots, F_\mu$ is a complete set of remainders for the module $[E_1]/O$. Hence there is a unique F such that

$$F=F_1+\lambda_2 F_2+\ldots+\lambda_\mu F_\mu=0 \bmod [E_1]/O.$$

The member E of $[E_1]$ with the same coefficients as F is unique, and the system $[E]$ is the same as the system $[E_1]$. A homogeneous Noetherian equation is already in its unique form.

70. *If E is homogeneous and of absolute degree l the numbers of linearly independent derivates of E of degrees l' and $l-l'$ are equal.*

Let $E_1, E_2, \ldots, E_N$ be the members of the system $[E]$ of degree l', and $F_1, F_2, \ldots, F_L$ the members of the module $[E]$ of degree l', and $G_1, G_2, \ldots, G_N$ the polynomials which have the same coefficients as $E_1, E_2, \ldots, E_N$; so that $F_1, \ldots, F_L, G_1, \ldots, G_N$ form a complete set of linearly independent homogeneous polynomials of degree l'. Then the F_1-, F_2-, ..., F_L-derivates of E vanish identically, and the G_1-, G_2-, ..., G_N-derivates are the derivates of degree $l-l'$, and are linearly independent; otherwise some linear combination of $G_1, G_2, \ldots, G_N$ would be a member of the module $[E]$. Hence the numbers of derivates of E of degrees l' and $l-l'$ are equal.

71. *The modular equations of a simple module Q of the principal Noetherian class consist of a single equation $E=0$ and its derivates; that is, a simple module of the principal Noetherian class is a principal system* (M, p. 109).

Take the origin at the point of Q. Then the modular equations of Q are Noetherian, and the characteristic number γ of Q is 1 more than the absolute degree of the highest modular equation. Also since Q is of the principal Noetherian class it is the whole Noetherian module contained in a certain module $M=(F_1, F_2, \ldots, F_n)$ of rank n. By choosing the degrees $l_1, l_2, \ldots, l_n$ of $F_1, F_2, \ldots, F_n$ to be $\geqslant \gamma$ we may assume $(F_1, F_2, \ldots, F_n)$ to be an H-basis of M (§ 49).

Now if F is any polynomial of degree $l_1+l_2+\ldots+l_n-n-1$ such that $x_1F, x_2F, \ldots, x_nF$ are all members of M then F itself is a member. We prove this for 2 variables referring for the general proof to (M, p. 110). When $n=2$, we have

$$x_1F=A_1F_1+A_2F_2, \quad x_2F=B_1F_1+B_2F_2,$$

where A_1, B_1 are of degrees $\leqslant l_2-2$ and A_2, B_2 of degrees $\leqslant l_1-2$.

Hence $$x_2(A_1F_1+A_2F_2)=x_1(B_1F_1+B_2F_2),$$

or $$(x_2A_1-x_1B_1)F_1=(x_1B_2-x_2A_2)F_2,$$

or $$x_2A_1-x_1B_1=0=x_1B_2-x_2A_2,$$

since $x_2A_1-x_1B_1$ is of degree $<l_2$ and cannot be divisible by F_2. Hence A_1, A_2 are both divisible by x_1, and $F=0 \bmod (F_1, F_2)$.

Suppose $Q=[E_1, E_2, \ldots, E_h]$, where each E_i is relevant, that is, not a member of the system $[E_1, \ldots, E_{i-1}, E_{i+1}, \ldots, E_h]$. Then the conditions that $x_1F, x_2F, \ldots, x_nF$ are to be members of M require only that the coefficients of F should satisfy all the derivates of $E_1=E_2=\ldots=E_h=0$ (but not these equations themselves) and all the modular equations of the other simple modules of M; i.e. $l_1l_2\ldots l_n-h$ equations in all. But these conditions require $F=0 \bmod M$, or that the coefficients of F should satisfy all the $l_1l_2\ldots l_n$ modular equations of M, which are equivalent to $l_1l_2\ldots l_n-1$ independent equations as applied to F (§ 58). Hence the $l_1l_2\ldots l_n-h$ equations as applied to F are equivalent to no less than $l_1l_2\ldots l_n-1$ independent equations. Hence $h=1$, and $Q=[E_1]$.

The converse of this theorem, viz. that a simple principal system is of the principal Noetherian class, is true in the case of 2 variables (M_3), but not true in the case of more than 2 variables. Thus

$$[x_1^{-2}+x_2^{-2}+x_3^{-2}]=(x_1^2-x_2^2,\ x_1^2-x_3^2,\ x_2x_3,\ x_3x_1,\ x_1x_2)$$

is a principal system which is not of the principal Noetherian class.

72. *A module of the principal class of rank n is a principal system.* Let $[E_1], [E_2], \ldots, [E_a]$ be the simple modules into which the given module resolves, and $\gamma_1, \gamma_2, \ldots, \gamma_a$ the characteristic numbers, and $a_1, a_2, \ldots, a_a$ the x_1-coordinates of the points of $[E_1], [E_2], \ldots, [E_a]$. The given module $[E_1, E_2, \ldots, E_a]$ will be proved to be identical with $[E_1+E_2+\ldots+E_a]$.

Since x_1-a_i contains the spread of $[E_i]$, $(x_1-a_i)^{\gamma_i}$ is a member of the module $[E_i]$, § 32, and $(x_1-a_i)^{\gamma_i}.E_i$ vanishes identically (§ 61). Hence from the equation $E_1+E_2+\ldots+E_a=0$ we have

$$(x_1-a_2)^{\gamma_2}(x_1-a_3)^{\gamma_3}\ldots(x_1-a_a)^{\gamma_a}.E_1=0.$$

The operator on the left hand is a polynomial in x_1-a_1 in which the constant term does not vanish; hence if we apply the inverse operator $(x_1-a_2)^{-\gamma_2}\ldots(x_1-a_a)^{-\gamma_a}$ expanded in powers of (x_1-a_1) as far as $(x_1-a_1)^{\gamma_1-1}$ we shall obtain $E_1=0$; since $(x_1-a_1)^l.E_1$ vanishes identically when $l \geqslant \gamma_1$.

Hence E_1, and similarly $E_2, E_3, \ldots, E_a$, are all derivates of $E_1+E_2+\ldots+E_a$ and the given module $[E_1, E_2, \ldots, E_a]=[E_1+E_2+\ldots+E_a]$.

If M is a module of the principal class of rank r then $M^{(r)}$ and all its simple modules are principal systems. *Hence any module of the principal class, and its primary modules, are principal systems* (§ 82).

73. *If a simple module M_μ of multiplicity μ is a principal system $[E]$, and $M'_{\mu'}$ is a simple module of multiplicity μ' contained in M_μ, and $M_\mu/M'_{\mu'} = M''_{\mu''}$, then $M_\mu/M''_{\mu''} = M'_{\mu'}$, and $\mu' + \mu'' = \mu$* (M, p. 111).

The modular equations of $M_\mu/M'_{\mu'}$ are the F-derivates of $E=0$, where F is any member of $M'_{\mu'}$ (§ 62). Let $F_1, F_2, \ldots, F_{\mu'}$ be a complete set of remainders for $M'_{\mu'}$. To these can be added $F_{\mu'+1}, \ldots, F_\mu$ so that $F_1, F_2, \ldots, F_\mu$ is a complete set of remainders for M_μ. Also each of $F_{\mu'+1}, \ldots, F_\mu$ can be modified by a linear combination of $F_1, F_2, \ldots, F_{\mu'}$ so as to become a member of $M'_{\mu'}$; and we will suppose this to have been done. Then the $F_{\mu'+1}$-, …, F_μ-derivates of $E=0$ are modular equations of $M''_{\mu''}$, and are linearly independent, since no linear combination of $F_{\mu'+1}, \ldots, F_\mu$ is a member of M_μ. Also any other F-derivate of $E=0$, where F is a member of $M'_{\mu'}$, is dependent on the $\mu-\mu'$ equations already found, since

$$F = \lambda_1 F_1 + \lambda_2 F_2 + \ldots + \lambda_\mu F_\mu \bmod M_\mu,$$

which requires, since $F = 0 \bmod M'_{\mu'}$,

$$\lambda_1 F_1 + \lambda_2 F_2 + \ldots + \lambda_{\mu'} F_{\mu'} = 0 \bmod M'_{\mu'},$$

or

$$\lambda_1 = \lambda_2 = \ldots = \lambda_{\mu'} = 0.$$

Hence the F-derivate of $E=0$ is the $(\lambda_{\mu'+1}F_{\mu'+1} + \ldots + \lambda_\mu F_\mu)$-derivate, and the number of modular equations of $M''_{\mu''}$ is $\mu-\mu'$, i.e. $\mu = \mu' + \mu''$.

Also since $M'_{\mu'}M''_{\mu''}$ contains M_μ, $M'_{\mu'}$ contains $M_\mu/M''_{\mu''}$ which is of multiplicity $\mu - \mu'' = \mu'$. Hence $M'_{\mu'} = M_\mu/M''_{\mu''}$.

It is true in general for unmixed modules of the same rank that if M is a principal system containing M', and $M/M' = M''$, then M', M'' are mutually residual with respect to M (cf. § 24, Ex. ii).

In (M, p. 112) the opinion is expressed that if M_μ is any simple module of multiplicity μ, and $M'_{\mu'}$ any module contained in M_μ, then the multiplicity of $M_\mu/M'_{\mu'}$ cannot exceed $\mu-\mu'$. This is not correct, as the following example shows.

Example. Let

$$M_\mu = [E_1, E_2] = [(x_1x_3)^{-1} + (x_2x_4)^{-1}, (x_1x_5)^{-1} + (x_2x_6)^{-1}],$$

and

$$M'_{\mu'} = (x_1, x_2, O^2) = [x_3^{-1}, x_4^{-1}, x_5^{-1}, x_6^{-1}],$$

so that

$$\mu = 2+6+1 = 9, \quad \mu' = 4+1 = 5.$$

Then

$$M_\mu/M'_{\mu'} = [E_1, E_2]/(x_1, x_2) = [x_1 . E_1, x_2 . E_1, x_1 . E_2, x_2 . E_2]$$
$$= [x_3^{-1}, x_4^{-1}, x_5^{-1}, x_6^{-1}] = M'_{\mu'}.$$

Hence (since $M_\mu/M'_{\mu'} = M'_{\mu'}$) $M'_{\mu'}$ and $M'_{\mu'}$ are mutually residual with respect to M_μ; and the multiplicity of $M_\mu/M'_{\mu'}$ is $\mu' > \mu - \mu'$.

It can be proved that if M_μ is simple and contains $M'_{\mu'}$ the multiplicity of $M_\mu/M'_{\mu'}$ cannot exceed $1+\frac{1}{4}(\mu-\mu')^2$ or $\frac{3}{4}+\frac{1}{4}(\mu-\mu')^2$ according as $\mu-\mu'$ is even or odd.

74. *If a simple H-module M_μ of multiplicity μ is a principal system $[E]$ with characteristic number γ, and if $M'_{\mu'}$, $M''_{\mu''}$ are mutually residual with respect to M_μ, and μ_l, μ'_l, μ''_l are the numbers of linearly independent modular equations of M_μ, $M'_{\mu'}$, $M''_{\mu''}$ of degree l, then $\mu'_{l'}+\mu''_{l''}=\mu_{l'}=\mu_{l''}$, where $l'+l''=\gamma-1$* (M, p. 112).

Here E is homogeneous and of absolute degree $\gamma-1$; and we have already shown that $\mu_{l'}=\mu_{l''}$ (§ 70). The $\mu''_{l''}$ modular equations of $M''_{\mu''}$ of degree l'' are F'-derivates of $E=0$, where F' is a member of $M'_{\mu'}$ of degree l'. Hence $\mu''_{l''}$ is the number of members F' of $M'_{\mu'}$ of degree l' of which no linear combination is a member F of M_μ; for $F.E$ vanishes identically. There are $\mu_{l'}$ polynomials in all of degree l' of which no linear combination is a member of M_μ, and $\mu'_{l'}$ of these are such that no linear combination of them is a member of $M'_{\mu'}$, while the remainder $\mu_{l'}-\mu'_{l'}$ can be modified by the $\mu'_{l'}$ so as to be members of $M'_{\mu'}$. Hence

$$\mu''_{l''}=\mu_{l'}-\mu'_{l'}, \quad \text{or} \quad \mu'_{l'}+\mu''_{l''}=\mu_{l'}=\mu_{l''}.$$

Thus the values of μ''_l are known for all values of l in terms of the values of μ_l and μ'_l for all values of l.

75. *If M is any module of rank n in $x_1, x_2, \ldots, x_n$, and M_0 the equivalent H-module in $x_1, \ldots, x_n, x_0$, and μ_m the number of modular equations of $(M_0)_{x_0=0}$ of degree m, then the number of modular equations of M for degree m is*

$$H_m = 1+\mu_1+\mu_2+\ldots+\mu_m.$$

This is immediately seen by considering the scheme of § 59 carried as far as degree m. The number of rows in the compartments $0, 1, 2, \ldots, l-1$ of the inverse array is the number of power products of degree $\leqslant l-1$, and each such power product inverted represents a modular equation of $(M_0)_{x_0=0}$. This number is therefore $1+\mu_1+\mu_2+\ldots+\mu_{l-1}$. The numbers of rows in the succeeding compartments are $\mu_l, \mu_{l+1}, \ldots, \mu_m$; and H_m is the total number of rows, viz. $1+\mu_1+\mu_2+\ldots+\mu_m$.

Also the total number of modular equations of M, or the sum of the multiplicities of its simple modules, is equal to the multiplicity of $(M_0)_{x_0=0}$.

76. If M' is any module of rank n and μ' the sum of the multiplicities of its simple modules, we can choose n members $F_1, F_2, \ldots, F_n$ of M' such that the resultant of their terms of highest degree does not vanish. If then the sum of the multiplicities of the simple modules of $M=(F_1, F_2, \ldots, F_n)$ is μ the sum of the multiplicities of the simple modules of M/M' is $\mu-\mu'$ (§§ 71, 73), and if $M/M'=M''$ then $M/M''=M'$. The important point is that M' is unrestricted except that it is composed of simple modules. The simple modules of M are principal systems, but not those of M'. These remarks are intended to point out the generality of the following theorem.

If $(F_1, F_2, \ldots, F_n)$ is an H-basis of a module M of rank n, and M′ any module contained in M, and M″ the residual module M/M′, then M′, M″ are mutually residual with respect to M, and

$$H'_{l'}-H''_{l''}=H'_{l'+l''}-H_{l''}=H_{l'}-H''_{l'+l''},$$

where $l'+l''+n+1$ is the sum of the degrees of $F_1, F_2, \ldots, F_n$, and H_l, H'_l, H''_l are the numbers of modular equations of M, M′, M″ for degree l.

This gives the values of H''_l for all values of l in terms of the values of H'_l for all values of l; for H_l is known by § 58.

The theorem is a generalization of the Brill-Noether reciprocity theorem (BN, p. 280, § 5, "Der Riemann-Roch'sche Satz"). It expresses the reciprocal relations between the numbers of the conditions which must be satisfied by members of M' and M'' in order that the product $M'M''$ may contain M.

A somewhat more general theorem is the following:

If $(F_1, F_2, \ldots, F_k)$ is an H-basis of a module M of rank n such that the H-module determined by the terms of highest degree in $F_1, F_2, \ldots, F_k$ is a principal system with characteristic number γ, and if M′ is any module contained in M, and M″ the residual module M/M′, then M′, M″ are mutually residual with respect to M, and

$$H'_{l'}-H''_{l''}=H'_{l'+l''}-H_{l''}=H_{l'}-H''_{l'+l''}, \textit{ where } l'+l''=\gamma-2.$$

We shall prove this more general theorem which includes the other. We must prove first that the simple modules of M are all principal systems*. Let M_0, M_0', M_0'' be the H-modules in $x_1, x_2, \ldots, x_n, x_0$ equivalent to M, M', M''. Then $(M_0)_{x_0=0}$ is a principal system; and

* The converse that if M is a module of rank n whose simple modules are all principal systems $(M_0)_{x_0=0}$ is a principal system is not true. For example, if M is the module in 2 variables determined by 3 points in a plane, then $(M_0)_{x_0=0}$ has the modular equations $x_1^{-1}=x_2^{-1}=1=0$, and is not a principal system.

the multiplicities μ, μ', μ'' of $(M_0)_{x_0=0}$, $(M_0')_{x_0=0}$, $(M_0'')_{x_0=0}$ are the sums of the multiplicities of the simple modules of M, M', M'' (§ 75). Let Q' be the module determined by the α points forming the spread of M, and Q'' the residual module M/Q'. Also let Q_0', Q_0'' be the H-modules equivalent to Q', Q''. Then, since $Q'Q''$ contains M, $Q_0'Q_0''$ contains M_0, and $(Q_0'Q_0'')_{x_0=0}$ contains $(M_0)_{x_0=0}$, which is a principal system. Hence also $(Q_0'')_{x_0=0}$ contains $(M_0)_{x_0=0}/(Q_0')_{x_0=0}$ whose multiplicity is $\mu-\alpha$; i.e. the sum of the multiplicities of the simple modules of $Q''\geqslant\mu-\alpha$. This is only possible when the simple modules of M are all principal systems; for if $[E_1, \ldots, E_h]$ is the simple module of M at the point P (say), the corresponding simple modules of Q', Q'' are P and $[E_1, E_2, \ldots, E_h]/P$, and the multiplicity of the latter is h less than that of $[E_1, E_2, \ldots, E_h]$; so that $\mu-\Sigma h\geqslant\mu-\alpha$, $\Sigma h\leqslant\alpha=\alpha$, and $h=1$. It follows that M' and M'' are mutually residual with respect to M.

It also follows that $\mu=\mu'+\mu''$, and that $(M_0')_{x_0=0}$ and $(M_0'')_{x_0=0}$ are mutually residual with respect to $(M_0)_{x_0=0}$. Hence $\mu'_{l'+1}+\mu''_{l''}=\mu_{l'+1}=\mu_{l''}$ (§ 74). Also $H'_{l'}=1+\mu_1'+\mu_2'+\ldots+\mu'_{l'}$ (§ 75). Hence

$$
\begin{aligned}
&(H'_{l'+l''}-H'_{l'})+H''_{l''}\\
&\qquad=(\mu'_{l'+1}+\mu'_{l'+2}+\ldots+\mu'_{l'+l''})+(1+\mu_1''+\mu_2''+\ldots+\mu''_{l''})\\
&\qquad=1+(\mu'_{l'+l''}+\mu_1'')+(\mu'_{l'+l''-1}+\mu_2'')+\ldots+(\mu'_{l'+1}+\mu''_{l''})\\
&\qquad=1+\mu_1+\mu_2+\ldots+\mu_{l''}=H_{l''};
\end{aligned}
$$

i.e.
$$H'_{l'}-H''_{l''}=H'_{l'+l''}-H_{l''}=H_{l'}-H''_{l'+l''}.$$

Modular Equations of Unmixed Modules

77. We have hitherto specially considered modules of rank n, that is, modules which resolve into simple modules. The H-module of rank n is of a special type, since it is itself a simple module, and its equations are homogeneous. The general case of a module of rank n is therefore that of a module which is not an H-module. When however we consider a module of rank $<n$ it is of some advantage to replace it by its equivalent H-module, which is of the same rank but of greater dimensions by 1. We shall not avoid by this means the consideration of modules which are not H-modules, but the results obtained will be expressed more conveniently. We shall therefore assume that the given module M whose modular equations and properties are to be discussed is an H-module in n variables $x_1, x_2, \ldots, x_n$.

By treating any H-module M of rank r (whether mixed or unmixed) as a module $M^{(r)}$ in r variables $x_1, x_2, \ldots, x_r$ it will resolve into simple modules and have only a finite number of modular equations, viz. a number μ equal to the sum of the multiplicities of its simple modules. The unknowns in the modular equations will be represented by negative power products of $x_1, x_2, \ldots, x_r$ while the coefficients will be whole functions of the parameters $x_{r+1}, \ldots, x_n$. The module determined by these modular equations will be unmixed, viz. the L.C.M. of all the primary modules of M of rank r (§ 43); and will be the module M itself if M is unmixed. We proceed to discuss these equations and shall call them the *r-dimensional modular equations* of M (or the modular equations of $M^{(r)}$) since they are obtained by regarding the module M as a module $M^{(r)}$ in space of r dimensions. $M^{(r)}$ is not an H-module.

The dialytic array of $M^{(r)}$. We choose any basis $(F_1, F_2, \ldots, F_k)$ of M as the basis of $M^{(r)}$. This is not in general an H-basis of $M^{(r)}$. The module $M_{x_{r+1}=\ldots=x_n=0}$ determined by the highest terms of the members of the basis of $M^{(r)}$ is of rank r (assuming that $x_1, x_2, \ldots, x_n$ have been subjected to a linear homogeneous substitution beforehand) and is therefore a simple H-module whose characteristic number will be denoted by γ.

Construct a dialytic array for $M^{(r)}$ whose elements are whole functions of $x_{r+1}, \ldots, x_n$ in which each row represents an elementary member $\omega_i F_j$ of $M^{(r)}$, where ω_i is a power product of $x_1, x_2, \ldots, x_r$ (cf. § 59). The first set of rows will represent the members of the basis which are of lowest degree l, the next set a complete set of elementary members of degree $l+1$ which are linearly independent of one another and of the complete rows in the first set, the next set a complete set of elementary members of degree $l+2$ linearly independent of one another and of the complete rows in the first two sets, and so on.

In comparing this with the scheme of § 59 there is the obvious difference that the elements of the array are whole functions of $x_{r+1}, \ldots, x_n$ instead of pure constants; and there is the more important difference that *the compartments l, $l+1$, ... do not necessarily consist of independent rows*, because the array is not constructed from an H-basis of $M^{(r)}$. It is only the complete rows of the array that are independent. *The elements in the compartments are all pure constants independent of $x_{r+1}, \ldots, x_n$.* The diagram of § 59 serves perfectly well to illustrate the dialytic array although its properties are now different.

In each compartment we choose a set of independent rows such that all the remaining rows of the compartment are dependent on them, and we name them *regular* rows and *extra* rows respectively, and apply the same terms to the complete rows of which they form part. In the compartment γ the regular rows will form a square array, and the same will be true of the compartments $\gamma+1$, $\gamma+2$, ... Eventually a compartment $\delta \geqslant \gamma$ will be reached such that the number of rows in the whole array for degree δ is exactly μ less than the whole number of columns, where μ is the number of modular equations of $M^{(r)}$ as mentioned above. After this all succeeding compartments $\delta+1$, $\delta+2$, ... will consist of square arrays only without any extra rows.

We can now modify any extra row of the array by regular rows so as to make all its elements which project beyond the columns of degree $\gamma-1$ vanish, and this leaves its elements in the columns up to degree $\gamma-1$ whole functions of $x_{r+1}, \ldots, x_n$ of the same degrees as they were before. If this is done with all the extra rows projecting beyond the columns of degree $\gamma-1$ the array may be said to be brought to its *regular form* in which the whole number of rows of the array for degree $\gamma-1$ is μ less than the whole number of columns, and all the compartments γ, $\gamma+1$, ... are made square. The extra rows, modified so as to end at the columns of degree $\gamma-1$, represent members of $M^{(r)}$ of degree $\gamma-1$ which are not elementary members $\omega_i F_j$.

We may further modify the *regular form* of the complete array for degree $\gamma-1$ so as to reduce the number of rows in each compartment $\gamma-1$, $\gamma-2$, ... successively to independent rows. The elements of some of the rows of the array for degree $\gamma-1$ may thus become fractional in $x_{r+1}, \ldots, x_n$, and the whole number of compartments will in general be increased, so that the last (or first) compartment will be numbered $l' < l$. Supposing this to be done we can choose a *simple* complete set of remainders for $M^{(r)}$ consisting of all power products of $x_1, x_2, \ldots, x_r$ of degree $< l'$ and as many power products of each degree $l'' \geqslant l'$ as the number of columns of the compartment l'' exceeds the number of rows of the same. We denote these power products in ascending degree by $\omega_1, \omega_2, \ldots, \omega_\mu$ (so that $\omega_1 = 1$) and all remaining power products to infinity in ascending degree by $\omega_{\mu+1}, \omega_{\mu+2}, \ldots$. The two series $\omega_1, \omega_2, \ldots, \omega_\mu$ and $\omega_{\mu+1}, \omega_{\mu+2}, \ldots$ overlap in respect to the degrees of their terms.

The basis of M used for constructing the dialytic array of $M^{(r)}$ must be one in which each member is of the same degree in $x_1, x_2, \ldots, x_r$ as in $x_1, x_2, \ldots, x_n$. We shall say that M is a *perfect* module if the array of $M^{(r)}$ as originally constructed has no extra rows, i.e. if the basis $(F_1, F_2, \ldots, F_k)$ is an H-basis of $M^{(r)}$.

78. Solution of the dialytic equations of $M^{(r)}$. We return to what has been called above the regular form of the dialytic array of $M^{(r)}$. Each row represents a member of $M^{(r)}$ and supplies a congruence equation mod $M^{(r)}$. Solving these equations, regarding $\omega_{\mu+1}, \omega_{\mu+2}, \ldots$ as the unknowns, we have

$$D\omega_p + D_{p1}\omega_1 + D_{p2}\omega_2 + \ldots + D_{p\mu}\omega_\mu = 0 \bmod M^{(r)} \quad (p = \mu+1, \mu+2, \ldots).$$

There are two slightly different cases according as the degree of $\omega_p < \gamma$ or $\geqslant \gamma$. If ω_p is of degree $< \gamma$ we use the regular form of the array for degree $\gamma - 1$ for solving for ω_p. D is then the determinant of this array formed from the columns corresponding to $\omega_{\mu+1}, \omega_{\mu+2}, \ldots$, and D_{pi} the determinant formed from the columns corresponding to $\omega_{\mu+1}, \ldots, \omega_{p-1}, \omega_i, \omega_{p+1}, \ldots$. If ω_p is of degree $\geqslant \gamma$ we must use the array up to the degree of ω_p in order to solve for ω_p. D is the same as in the former case except for a factor independent of $x_{r+1}, \ldots, x_n$ (since the compartments $\gamma, \gamma+1, \ldots$ are square and all their elements are pure constants) by which the equation can be divided. Also D_{pi} is a sum of products of determinants of the regular form of the array for degree $\gamma - 1$ with determinants from the remaining rows of the larger array, so that the H.C.F. of the determinants of the array for degree $\gamma - 1$ can be divided out, and we obtain in both cases

$$\text{(A)} \qquad R\omega_p + R_{p1}\omega_1 + \ldots + R_{p\mu}\omega_\mu = 0 \bmod M^{(r)} \quad (p = \mu+1, \mu+2, \ldots).$$

This equation is homogeneous in $x_1, x_2, \ldots, x_n$, and each R_{pi} is homogeneous in $x_{r+1}, \ldots, x_n$. Also, owing to the fact that the remainders $\omega_1, \omega_2, \ldots, \omega_\mu$ are a *simple* set, each ω_p is congruent mod $M^{(r)}$ to a linear combination of those power products $\omega_1, \omega_2, \ldots, \omega_\mu$ which are of equal or less degree than ω_p. *Hence R_{pi} vanishes if the degree of ω_i exceeds the degree of ω_p. Also $R = 1$ if M is perfect* (cf. § 81).

79. The modular equations of $M^{(r)}$. If the coefficient of $\omega_p = x_1^{p_1} x_2^{p_2} \ldots x_r^{p_r}$ in the general member of $M^{(r)}$ of any degree is represented by $\omega_{-p} = (x_1^{p_1} x_2^{p_2} \ldots x_r^{p_r})^{-1}$ we have

$$\omega_{-1}\omega_1 + \omega_{-2}\omega_2 + \ldots + \omega_{-p}\omega_p + \ldots = 0 \bmod M^{(r)},$$

and, by (A),

$$R(\omega_{-1}\omega_1 + \ldots + \omega_{-\mu}\omega_\mu) = \sum_{p=\mu+1}^{\infty} \omega_{-p}(R_{p1}\omega_1 + R_{p2}\omega_2 + \ldots + R_{p\mu}\omega_\mu) \bmod M^{(r)}.$$

Here coefficients of $\omega_1, \omega_2, \ldots, \omega_\mu$ on both sides are equal, i.e.

$$\text{(B)} \qquad R\omega_{-i} = \sum_{p=\mu+1}^{\infty} R_{pi}\omega_{-p} \quad (i = 1, 2, \ldots, \mu).$$

This is the complete system of modular equations of $M^{(r)}$, *or* r*-dimensional modular equations of* M, *and the system includes all its own derivates.* R *and all the* R_{pi} *are definite whole functions of* $x_{r+1}, \ldots, x_n$. If any other complete system were given and solved for $\omega_{-1}, \omega_{-2}, \ldots, \omega_{-\mu}$ in terms of $\omega_{-\mu-1}, \omega_{-\mu-2}, \ldots$ the result would be the unique system (B).

Since in (A) $R\omega_p$ and $R_{pi}\omega_i$ are of the same degree in $x_1, x_2, \ldots, x_n$, so in (B), $R\omega_{-i}$ and $R_{pi}\omega_{-p}$ are of the same degree, i.e. all terms in one equation (B) are of the same degree in $x_1, x_2, \ldots, x_n$. Also since (§ 78) R_{pi} vanishes if the degree of ω_i exceeds the degree of ω_p *there is no* ω_{-p} *on the right-hand side of* (B) *of less absolute degree than* ω_{-i}; but every ω_{-p} of the same degree as ω_{-i} and not among $\omega_{-1}, \omega_{-2}, \ldots, \omega_{-\mu}$ will appear on the right-hand side of (B).

(B) is the complete system of r-dimensional equations of the L. C. M. of all the primary modules of M of rank r; and will decompose into separate distinct systems corresponding to the separate primary modules of rank r if M has more than one irreducible spread of rank r.

The n*-dimensional equations.* We can obtain the whole system of n-dimensional equations of M corresponding to the system (B) as follows: ω_{-p} or $(x_1^{p_1}x_2^{p_2}\ldots x_r^{p_r})^{-1}$ represents the whole coefficient of $x_1^{p_1}x_2^{p_2}\ldots x_r^{p_r}$ in the general member of $M^{(r)}$, i.e. it stands for

$$\Sigma\,(x_1^{p_1}\ldots x_n^{p_n})^{-1}\,x_{r+1}^{p_{r+1}}\ldots x_n^{p_n},$$

the summation extending to all values of $p_{r+1}, \ldots, p_n$ only. If this be substituted for each $(x_1^{p_1}\ldots x_r^{p_r})^{-1}$ in each of the equations (B) the whole coefficients of the power products of $x_{r+1}, \ldots, x_n$ will represent the n-dimensional equations. *This will be the whole system of* n*-dimensional equations of* M *if* M *is unmixed, as we shall assume hereafter is the case.*

The whole system of modular equations of a mixed module may be regarded as consisting of the separate systems corresponding to the primary modules into which it resolves.

80. *The system of homogeneous equations*

$$\text{(C)} \qquad R\omega_{-i} = \Sigma R_{pi}\omega_{-p} \quad (i = 1, 2, \ldots, \mu)$$

obtained from the system (B) *by retaining only those terms on the right hand in which* R_{pi} *and* ω_{-p} *are of the same degrees as* R *and* ω_{-i}

respectively is the complete system of equations of the simple H-module determined by the highest terms in $x_1, x_2, \ldots, x_r$ *of the members of an H-basis of* $M^{(r)}$.

This can be seen by considering the diagram of § 59 assuming that it had been constructed from an H-basis of $M^{(r)}$. The compartments $l, l+1, l+2, \ldots$ in the two arrays in § 59 are the dialytic and inverse arrays of the simple H-module determined by the highest terms of the members of the H-basis; and the modular equations of this simple H-module are represented by the compartments $0, 1, \ldots, l, l+1, \ldots$ of the inverse array. The system (C) is that which is represented by the compartments of the inverse array.

81. *If* $R=1$ *the module* M *(assumed unmixed) is perfect.* Since M is unmixed every whole member of $M^{(r)}$ is a member of M (§ 43). Also, since $R=1$, there is an inverse array of $M^{(r)}$ each of whose compartments consists of independent rows in which all the elements are pure constants. Hence there is a corresponding dialytic array having the same property. From this it follows that M is perfect (§ 77).

82. The r-dimensional and n-dimensional equations of M.

If the system (B) is a principal system, i.e. if all its equations are derivates of a single one of them, each simple module of $M^{(r)}$ is a principal system; for if F is a polynomial containing all the simple modules of $M^{(r)}$ except one, then $M^{(r)}/(F)$ is the last one, and is a principal system (§ 62). The converse is also true (see § 72). Also the unmixed module M in n variables is a principal system, as we proceed to prove.

Let the r-dimensional equation of which all the equations of the system (B) are derivates be

$$\sum^{\infty} R_{p_1, p_2, \ldots, p_r} (x_1^{p_1} x_2^{p_2} \ldots x_r^{p_r})^{-1} = 0,$$

where $R_{p_1, p_2, \ldots, p_r}$ is a homogeneous polynomial in $x_{r+1}, \ldots, x_n$ of degree $p_1 + p_2 + \ldots + p_r + \delta$. The integer δ may be negative, but the more unfavourable case for the proof is that in which it is positive. Let $c_{p_1, p_2, \ldots, p_n}$ be the coefficient of $x_{r+1}^{p_{r+1}} \ldots x_n^{p_n}$ in $R_{p_1, p_2, \ldots, p_r}$, so that $p_{r+1} + \ldots + p_n = p_1 + \ldots + p_r + \delta$. To convert the equation into an n-dimensional equation we put

$$(x_1^{p_1} x_2^{p_2} \ldots x_r^{p_r})^{-1} = \sum_q^{\infty} x_{r+1}^{q_{r+1}} \ldots x_n^{q_n} (x_1^{p_1} \ldots x_r^{p_r} x_{r+1}^{q_{r+1}} \ldots x_n^{q_n})^{-1}$$

as in § 79, and we have

$$\sum_p c_{p_1,\dots,p_n} x_{r+1}^{p_{r+1}} \dots x_n^{p_n} \sum_q x_{r+1}^{q_{r+1}} \dots x_n^{q_n} (x_1^{p_1} \dots x_r^{p_r} x_{r+1}^{q_{r+1}} \dots x_n^{q_n})^{-1} = 0, \quad \dots(1)$$

or, equating the whole coefficient of $x_{r+1}^{l_{r+1}} \dots x_n^{l_n}$ to zero,

$$\sum_p c_{p_1,p_2,\dots,p_n} (x_1^{p_1} \dots x_r^{p_r} x_{r+1}^{l_{r+1}-p_{r+1}} \dots x_n^{l_n-p_n})^{-1} = 0, \quad \dots\dots\dots(2)$$

which is homogeneous and of absolute degree $l_{r+1} + \dots + l_n - \delta$. Similarly the general n-dimensional equation obtained from the coefficient of $x_{r+1}^{m_{r+1}} \dots x_n^{m_n}$ in the $x_1^{t_1} \dots x_r^{t_r}$-derivate of (1) is

$$\sum_p c_{p_1,p_2,\dots,p_n} (x_1^{p_1-t_1} \dots x_r^{p_r-t_r} x_{r+1}^{m_{r+1}-p_{r+1}} \dots x_n^{m_n-p_n})^{-1} = 0, \quad \dots\dots(3)$$

where $t_1, \dots, t_r, m_{r+1}, \dots, m_n$ are any n fixed positive integers (including zeros) such that $t_1 + \dots + t_r \leqslant$ a fixed limit τ (since there are only a finite number of linearly independent derivates of the original r-dimensional equation) and $(x_1^{p_1-t_1} \dots x_r^{p_r-t_r} x_{r+1}^{m_{r+1}-p_{r+1}} \dots x_n^{m_n-p_n})^{-1}$ is zero if any one of the indices $p_1 - t_1, \dots, p_r - t_r, m_{r+1} - p_{r+1}, \dots, m_n - p_n$ is negative.

Consider all the n-dimensional modular equations of degree l, that is, all the equations of the system (3) of absolute degree l. The absolute degree of (3) is

$$m_{r+1} + \dots + m_n - \delta - t_1 - \dots - t_r = l.$$

Hence each of $m_{r+1}, \dots, m_n$ is equal to or less than $l + \delta + \tau$; and every equation (3) of absolute degree l is a derivate of the single equation (2) if $l_{r+1}, \dots, l_n$ are all chosen as high as $l + \delta + \tau$. Hence there is a single equation of which all the modular equations of M of degree l are derivates, and any equation (2) in which $l_{r+1}, \dots, l_n$ are not numerically specified will serve for the single equation.

It follows that *the inverse system of any module M has a finite basis* $[E_1, E_2, \dots, E_h]$; for M resolves into a finite number of primary modules of the same or of different ranks, and each primary module of rank r has a finite number of r-dimensional equations, and a smaller number of r-dimensional equations of which all the others are derivates, and an equal or still smaller number of n-dimensional equations of which all the others are derivates.

83. If (B) is a principal system it does not follow that (C) is a principal system (footnote § 76). *If however* (C) *is a principal system*

(B) *is a principal system.* For the basis equation of the system (C) must be the homogeneous equation

$$R\,\omega_{-\mu} = \Sigma R_{p\mu}\,\omega_{-p},$$

and all the other equations of (C) must be of less absolute degree. Now the system (B) is unique and any equation obtained from it

$$R_1\,\omega_{-1} + R_2\omega_{-2} + \ldots + R_p\,\omega_{-p} + \ldots = 0$$

must be the result of multiplying the equations of (B) by $R_\mu, R_{\mu-1}, \ldots, R_1$ and adding and dividing out R. Hence the equation

$$R\,\omega_{-i} = \overset{\infty}{\Sigma} R_{pi}\,\omega_{-p}$$

is exactly the same derivate of $R\,\omega_{-\mu} = \overset{\infty}{\Sigma} R_{p\mu}\,\omega_{-p}$ as the corresponding homogeneous equation $R\omega_{-i} = \Sigma R_{pi}\,\omega_{-p}$ is of $R\,\omega_{-\mu} = \Sigma R_{p\mu}\,\omega_{-p}$.

If (C) is a principal system the formulae of § 76 apply to any two modules M', M'' mutually residual with respect to M when regarded as modules in r variables. If (B) is a principal system, but not (C), the formula $\mu = \mu' + \mu''$ applies, where μ, μ', μ'' are the numbers of equations in the systems (B), (B'), (B'') for M, M', M''. This follows from § 73 by summing for all the simple modules of $M^{(r)}$.

84. Modular equations of an H-module of the principal class.

In the case of an H-module $(F_1, F_2, \ldots, F_r)$ of rank r (C) is a principal system (§ 71); and $R = 1$, since $(F_1, F_2, \ldots, F_r)$ is an H-basis of $M^{(r)}$ (§ 49). Also, if $F_1, F_2, \ldots, F_r$ are of degrees $l_1, l_2, \ldots, l_r$, a complete set of remainders for $M^{(r)}$ consists of the $l_1 l_2 \ldots l_r$ factors of $x_1^{l_1-1}x_2^{l_2-1}\ldots x_r^{l_r-1}$, since this is a complete set of remainders for $(x_1^{l_1}, x_2^{l_2}, \ldots, x_r^{l_r})$, cf. § 58. Hence the system (B) for M consists of the single equation

$$(x_1^{l_1-1}\ldots x_r^{l_r-1})^{-1} = \overset{\infty}{\Sigma} R_{p_1, p_2, \ldots, p_r}(x_1^{p_1}x_2^{p_2}\ldots x_r^{p_r})^{-1} \quad \ldots\ldots\ldots(4)$$

and its derivates, where $p_1 + \ldots + p_r \geqslant l_1 + \ldots + l_r - r$, and consequently $p_i \geqslant l_i$ for one value at least of i. The corresponding n-dimensional equation is (§ 82)

$$\sum_q x_{r+1}^{q_{r+1}}\ldots x_n^{q_n}(x_1^{l_1-1}\ldots x_r^{l_r-1}x_{r+1}^{q_{r+1}}\ldots x_n^{q_n})^{-1}$$
$$= \sum_p c_{p_1, \ldots, p_n} x_{r+1}^{p_{r+1}}\ldots x_n^{p_n}\sum_q x_{r+1}^{q_{r+1}}\ldots x_n^{q_n}(x_1^{p_1}\ldots x_r^{p_r}x_{r+1}^{q_{r+1}}\ldots x_n^{q_n})^{-1},$$

or, by equating coefficients of $x_{r+1}^{l_{r+1}-1}\ldots x_n^{l_n-1}$ on both sides,

$$(x_1^{l_1-1}x_2^{l_2-1}\ldots x_n^{l_n-1})^{-1} = \sum_p c_{p_1, p_2, \ldots, p_n}(x_1^{p_1}\ldots x_r^{p_r}x_{r+1}^{l_{r+1}-1-p_{r+1}}\ldots x_n^{l_n-1-p_n})^{-1}.$$

When $F_1, F_2, \ldots, F_r$ are general with letters for coefficients, the $c_{p_1, p_2, \ldots, p_n}$ are rational functions of the coefficients and on multiplying up by their common denominator K we can write the equation

$$K(x_1^{l_1-1} x_2^{l_2-1} \ldots x_n^{l_n-1})^{-1} = \sum_p K_{p_1, p_2, \ldots, p_n} (x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}, \quad \ldots(5)$$

where $p_1 + p_2 + \ldots + p_n = l_1 + l_2 + \ldots + l_n - n$, and at least one $p_i \geqslant l_i$ $(i = 1, 2, \ldots, r)$ and every $p_j < l_j$ $(j = r+1, \ldots, n)$. This is the n-dimensional modular equation of $(F_1, F_2, \ldots, F_r)$ of which all others are derivates, $l_{r+1}, \ldots, l_n$ being unspecified numerically. More explicitly it is the unique modular equation of the simple module $(F_1, F_2, \ldots, F_r, x_{r+1}^{l_{r+1}}, \ldots, x_n^{l_n})$; for it is a relation satisfied by the coefficients of the general member of $(F_1, F_2, \ldots, F_r)$ of degree $l_1 + l_2 + \ldots + l_n - n$ in which $p_j < l_j$ $(j = r+1, \ldots, n)$, i.e. it is the unique relation (§ 58) satisfied by the coefficients of the general member of

$$(F_1, \ldots, F_r, x_{r+1}^{l_{r+1}}, \ldots, x_n^{l_n})$$

of degree $l_1 + \ldots + l_n - n$. The coefficients $K_{p_1, p_2, \ldots, p_n}$ are whole functions of the coefficients of $F_1, F_2, \ldots, F_r$ of a similar kind to the resultant of $(F_1, \ldots, F_r, x_{r+1}^{l_{r+1}}, \ldots, x_n^{l_n})$ and of degree 1 less than this resultant in the coefficients of each of $F_1, F_2, \ldots, F_r$, viz. of degree $L_i - 1$ in the coefficients of F_i where $L_i l_i = l_1 l_2 \ldots l_n = L$. The vanishing of $K_{p_1, p_2, \ldots, p_n}$ is the condition that

$$x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n} = 0 \bmod (F_1, F_2, \ldots, F_r, x_{r+1}^{l_{r+1}}, \ldots, x_n^{l_n})$$

(§ 61, since the $x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$-derivate of (5) then vanishes), whereas the non-vanishing of the resultant is the condition that every power product of degree $l_1 + \ldots + l_n - n + 1$ is a member of the module. It is probable that some of the quantities $K_{p_1, p_2, \ldots, p_n}$ factorise but that they have not all a common factor. The resultant of

$$(F_1, F_2, \ldots, F_r, x_{r+1}^{l_{r+1}}, \ldots, x_n^{l_n})$$

is $R_{r+1}^{l_{r+1} \ldots l_n}$ (§ 8).

85. Whole basis of the system inverse to $M^{(r)}$. The simplest *whole* basis $[E_1, E_2, \ldots, E_h]$ of the r-dimensional system inverse to an unmixed H-module M of rank r, or the simplest expression for the system of equations (B), satisfies the following conditions: (i) each E_i $(i = 1, 2, \ldots, h)$ is a *whole* member of the inverse system, i.e. its coefficients are whole functions of the parameters $x_{r+1}, \ldots, x_n$;

(ii) all the members $E_1, E_2, \ldots, E_h$ are relevant; (iii) any whole member of the system $[E_1, E_2, \ldots, E_h]$ is of the form

$$X_1 \,.\, E_1 + X_2 \,.\, E_2 + \ldots + X_h \,.\, E_h,$$

where $X_1, X_2, \ldots, X_h$ are whole functions of $x_{r+1}, \ldots, x_n$ as well as of $x_1, x_2, \ldots, x_r$; (iv) $E_1, E_2, \ldots, E_h$ have as high absolute under-degrees in $x_1, x_2, \ldots, x_r$ as possible. A whole basis, as distinguished from a simplest whole basis, is defined by (i) and (iii).

A basis $(F_1, F_2, \ldots, F_k)$ of M furnishes a whole basis of $M^{(r)}$, and any whole basis of $M^{(r)}$ satisfying the condition corresponding to (iii) above is a basis of M. A simplest whole basis* of $M^{(r)}$ is one in which the degrees of $F_1, F_2, \ldots, F_k$ in $x_1, x_2, \ldots, x_r$ are as low as possible.

If $(F_1, F_2, \ldots, F_r)$ is any module of rank r containing M such that $(F_1, F_2, \ldots, F_r)_{x_{r+1}=\ldots=x_n=0}$ is of rank r, and $M = (F_1, F_2, \ldots, F_{k'})$, and the degrees of $F_{r+1}, \ldots, F_{k'}$ in $x_1, x_2, \ldots, x_r$ are as low as possible, the basis $(F_1, F_2, \ldots, F_{k'})$ will be called *a whole basis of $M^{(r)}$ in reference to $(F_1, F_2, \ldots, F_r)$*. All of $F_{r+1}, \ldots, F_{k'}$ are to be relevant, but some or all of $F_1, F_2, \ldots, F_r$ may be irrelevant for a basis of M.

86. Properties of H-modules mutually residual with respect to an H-module of the principal class.

Let $F_1, F_2, \ldots, F_r$, of degrees $l_1, l_2, \ldots, l_r$, be any r members of the unmixed H-module M of rank r such that

$$(F_1, F_2, \ldots, F_r)_{x_{r+1}=\ldots=x_n=0}$$

is of rank r; and let M' be the residual module $(F_1, F_2, \ldots, F_r)/M$. Also let $(F_1, \ldots, F_r, F'_{r+1}, \ldots, F'_{r+h})$ be a whole basis of $M'^{(r)}$ in reference to $(F_1, F_2, \ldots, F_r) = [E]$. Since F'_{r+i} is of as low degree in $x_1, x_2, \ldots, x_r$ as possible the terms of F'_{r+i} of highest degree in $x_1, x_2, \ldots, x_r$ do not form a member of the module

$$(F_1, F_2, \ldots, F_r)_{x_{r+1}=\ldots=x_n=0},$$

and are therefore of degree $l'_{r+i} \leqslant l_1 + l_2 + \ldots + l_r - r$ in $x_1, x_2, \ldots, x_r$. Also, since E begins with terms which represent the modular equation

* A simplest whole basis of $M^{(r)}$ is a whole basis which approaches most nearly to an H-basis; but is not necessarily an H-basis. For example,

$$(x_1{}^4,\ x_1{}^3x_2,\ x_1x_2{}^3,\ x_2{}^4,\ x_1{}^3x_3{}^2 + x_1{}^2x_2{}^2x_4,\ x_2{}^3x_4{}^2 + x_1{}^2x_2{}^2x_3)$$

is the basis of a module M of rank 2, and a simplest whole basis of $M^{(2)}$, but not an H-basis of $M^{(2)}$; since $x_1{}^3x_3{}^3 - x_2{}^3x_4{}^3$ is needed for an H-basis of $M^{(2)}$, but is irrelevant for a basis of M or whole basis of $M^{(2)}$.

of $(F_1, F_2, \ldots, F_r)_{x_{r+1}=\ldots=x_n=0}$ of degree $l_1+l_2+\ldots+l_r-r$, $F'_{r+i}\,.\,E$ will begin with terms of absolute degree $l_1+\ldots+l_r-r-l'_{r+i}$ in $x_1, x_2, \ldots, x_r$ which do not vanish identically.

Now M, M' are mutually residual with respect to $(F_1, \ldots, F_r)$ or $[E]$. Hence

$$M=[E]/M'=[E]/(F_1, \ldots, F_r, F'_{r+1}, \ldots, F'_{r+h})$$
$$=[F'_{r+1}\,.\,E, F'_{r+2}\,.\,E, \ldots, F'_{r+h}\,.\,E].$$

This basis of the r-dimensional system inverse to M is a simplest whole basis $[E_1, E_2, \ldots, E_h]$ as defined in § 85. All its members are relevant, for if (say)

$$F'_{r+h}\,.\,E=(X_1F'_{r+1}+\ldots+X_{h-1}F'_{r+h-1})\,.\,E,$$

then

$$F'_{r+h}-X_1F'_{r+1}-\ldots-X_{h-1}F'_{r+h-1}=0 \bmod (F_1, F_2, \ldots, F_r),$$

which is not the case. Also any r-dimensional modular equation of M is a derivate of $E=0$, and if a whole equation, is $F'.\,E=0$, where F' is a whole function of $x_1, x_2, \ldots, x_n$, since $[E]$ is a whole basis; and if F is any member of M, $FF'.\,E$ vanishes identically, i.e.

$$FF'=0 \bmod (F_1, F_2, \ldots, F_r)$$

and

$$F'=0 \bmod M'=X_1F'_{r+1}+\ldots+X_hF'_{r+h} \bmod (F_1, F_2, \ldots, F_r),$$

and
$$F'.\,E=X_1\,.\,E_1+X_2\,.\,E_2+\ldots+X_h\,.\,E_h.$$

Finally the absolute underdegrees of $E_1, E_2, \ldots, E_h$ are as high as possible since the degrees of $F'_{r+1}, \ldots, F'_{r+h}$ in $x_1, x_2, \ldots, x_r$ are as low as possible. The coefficients of the terms in E_i and F'_{r+i} which involve the parameters $x_{r+1}, \ldots, x_n$ to the least degree involve them to the same degree, so that $E_1, E_2, \ldots, E_h$ and $F'_{r+1}, F'_{r+2}, \ldots, F'_{r+h}$ are of the same degree of complexity in this respect.

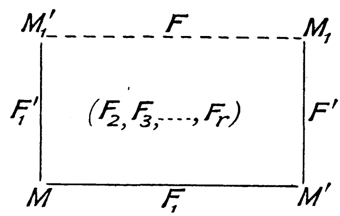
It follows from the above that if M' is the residual of a given unmixed H-module M of rank r with respect to any H-module $(F_1, F_2, \ldots, F_r)$ of rank r containing M, and if

$$M'=(F_1, F_2, \ldots, F_r, F'_{r+1}, \ldots, F'_{r+h}),$$

where $F'_{r+1}, \ldots, F'_{r+h}$ are all relevant, then h is a fixed number independent of the choice of $F_1, F_2, \ldots, F_r$, viz. the number of members in a simplest whole basis $[E_1, E_2, \ldots, E_h]$ of the system inverse to $M^{(r)}$. Also if the degrees of $F'_{r+1}, \ldots, F'_{r+h}$ in respect to $x_1, x_2, \ldots, x_r$ are made as low as possible the degree of F'_{r+i} in respect to $x_1, x_2, \ldots, x_r$

is $l-\alpha_i$ and in respect to $x_1, x_2, \ldots, x_n$ is $l-\alpha_i+\beta_i$, where l is the sum of the degrees of $F_1, F_2, \ldots, F_r$ diminished by r, α_i is the absolute degree of the terms with which E_i begins, and β_i is the degree of the coefficients of these terms in $x_{r+1}, \ldots, x_n$.

87. The Theorem of Residuation. As in the last article let M be any unmixed H-module of rank r, and $(F_1, F_2, \ldots, F_r)$ any module of rank r containing M, and M' the residual module $(F_1, F_2, \ldots, F_r)/M$, so that M, M' are mutually residual with respect to $(F_1, F_2, \ldots, F_r)$. In geometrical terminology M, M' are residuals on $(F_2, F_3, \ldots, F_r)$ determined by the section F_1. Replace F_1 by another member F_1' of M, which we will suppose to be of the same degree as F_1, giving another section of $(F_2, F_3, \ldots, F_r)$ through M, and let $M_1'=(F_1', F_2, \ldots, F_r)/M$ be the residual section or module. Also let F' be a section through M', F' being of the same degree as F_1, and $M_1=(F', F_2, \ldots, F_r)/M'$ the residual section or module. Then M', M_1' are coresidual on $(F_2, F_3, \ldots, F_r)$ having a common residual M; and M_1 is any other residual of M'. *The theorem of residuation says that every residual M_1 of M' on $(F_2, F_3, \ldots, F_r)$ is also a residual of M_1', i.e. to every section F' through M' there corresponds a section F through M_1' having the same residual section on $(F_2, F_3, \ldots, F_r)$.* This theorem is a generalization of Sylvester's theory of residuation (Salmon's *Higher Plane Curves*, Chap. v) and the *Restsatz* of Brill and Noether* (BN, p. 271). Besides this relation of M' to M_1' there are properties connecting them both with M which are proved in the last article, viz. the number of members over and above $F_1, F_2, \ldots, F_r$ (or $F_1', F_2, \ldots, F_r$) required for a basis of M' (or M_1') is equal to the number of members required for a whole basis of the system inverse to $M^{(r)}$; and the number of members required for a whole basis of the system inverse to $M'^{(r)}$ (or $M_1'^{(r)}$) is equal to the number of members over and above $F_1, F_2, \ldots, F_r$ (or $F_1', F_2, \ldots, F_r$) required for a basis of M.



* It would be more correct to say that the *Restsatz* can be deduced from the theorem proved here; but not such extensions of it as have been made to surfaces etc., because these bring in mixed modules. The module M may be composed of *any* primary modules of rank r; and corresponding to each one which is not of the principal Noetherian class M' must contain a residual primary module with the same spread.

The polynomials F_1, F_1', F' and the modules M, M', M_1, M_1' having been defined as above it is required to prove that there exists a polynomial F such that M_1, M_1' are mutually residual with respect to $(F, F_2, \ldots, F_r)$. Let μ, μ', μ_1, μ_1' be the numbers of r-dimensional modular equations of M, M', M_1, M_1'; then

$$\mu + \mu' = \mu + \mu_1' = \mu' + \mu_1 = l_1 l_2 \ldots l_r$$

and therefore each equals $\mu_1 + \mu_1'$. Let ϕ, ϕ', ϕ_1, ϕ_1' be general members of M, M', M_1, M_1' with coefficients involving linear parameters. Then

$$F'F_1' = 0 \bmod MM' = 0 \bmod (F_1, F_2, \ldots, F_r) = FF_1 \bmod (F_2, \ldots, F_r), \quad \ldots\ldots(1)$$

where F is a polynomial of the same degree as F_1, F_1', F'. Also

$$F_1\phi_1' = 0 \bmod MM_1' = X_1'F_1' \bmod (F_2, \ldots, F_r), \quad \ldots\ldots(2)$$

and $$\phi\phi_1' = 0 \bmod MM_1' = XF_1' \bmod (F_2, \ldots, F_r);$$

hence by cross multiplying and dividing out $\phi_1'F_1'$,

$$X_1'\phi = XF_1 \bmod (F_2, \ldots, F_r) = 0 \bmod (F_1, F_2, \ldots, F_r),$$

$$\therefore\ X_1' = 0 \bmod (F_1, F_2, \ldots, F_r)/M = 0 \bmod M'.$$

Similarly $$F_1\phi_1 = 0 \bmod M'M_1 = X'F' \bmod (F_2, \ldots, F_r), \quad \ldots\ldots(3)$$

where $X' = 0 \bmod M$;

$$\therefore\ X'X_1' = 0 \bmod MM' = X_1F_1 \bmod (F_2, \ldots, F_r). \quad \ldots\ldots(4)$$

Multiplying (1), (2), (3), (4), and dividing out $F'F_1'F_1^2X'X_1'$,

$$\phi_1\phi_1' = X_1F \bmod (F_2, \ldots, F_r) = 0 \bmod (F, F_2, \ldots, F_r).$$

Hence M_1M_1' contains $(F, F_2, \ldots, F_r)$; and since M_1, M_1' have only μ_1, μ_1' r-dimensional modular equations, while $(F, F_2, \ldots, F_r)$ has $\mu_1 + \mu_1'$ and is a principal system, it follows that $M_1^{(r)}$, $M_1'^{(r)}$, and consequently M_1, M_1', are mutually residual with respect to $(F, F_2, \ldots, F_r)$.

The theorem has been proved on the supposition that the modules are H-modules and the degrees of F_1, F_1', F' are equal; but it is true without any of these restrictions. In the case of modules which are not H-modules the region at infinity must be regarded as non-existent and the usual conception of residual and coresidual must be slightly extended. Thus if through a point P on a plane cubic curve two lines are drawn parallel to two asymptotes cutting the curve again in Q, R, then P is residual to Q and R, and Q, R are coresidual. If through Q a line is drawn cutting the curve again in two points these two are residual to R, i.e. a curve (viz. a conic) can be drawn through them and R which does not meet the curve again except at infinity.

As an illustration of the general theorem we may suppose M to be any unmixed module of rank 2 in space of three dimensions. Then F_1, F_2 are any two surfaces containing M whose whole intersection consists of a finite number of irreducible spreads (excluding infinity); and to each spread or curve corresponds a primary principal system of (F_1, F_2). M contains a certain part of some of these principal systems and no part of others; M' has to contain the whole of the latter and the residual part of each of the former. These conditions determine M', and similarly for M_1 and M_1'.

88. Perfect Modules. *Definition.* If a module M of rank r in n variables and the corresponding module $M^{(r)}$ in r variables have a common H-basis of which each member is of the *same degree in the r variables as in the n variables* then M is called a *perfect module.*

Any module of rank n is perfect, by definition.

An unmixed H-module of rank $n-1$ *is perfect*; for its basis is an H-basis of $M^{(n-1)}$.

An H-module of the principal class is perfect (§ 49).

A module of the principal class which is not an H-module is not necessarily perfect. For example, the module $(x_1^2, x_2+x_1x_3)$ whose H-basis is $(x_1^2, x_1x_2, x_2^2, x_2+x_1x_3)$, § 38, is not perfect since $x_2+x_1x_3$ is of less degree in x_1, x_2 than in x_1, x_2, x_3.

A prime module is not necessarily perfect. For example, the prime module of rank 2 whose spread is given by $u=\lambda u_1=\lambda^3 u_3=\lambda^4 u_4$, where u, u_1, u_3, u_4 are linear, has an H-basis

$$(uu_4-u_1u_3,\ u_1^3-u^2u_3,\ u_1^2u_4-uu_3^2,\ u_1u_4^2-u_3^3)=(f, f_1, f_2, f_3)$$

and no other member than $uu_4-u_1u_3$ of degree 2. But it has a second member $\lambda_1 f_1+\lambda_2 f_2+\lambda_3 f_3+(\lambda_4 x_1+\lambda_5 x_2)f$ which can be made of degree 2 in x_1, x_2; hence it is not perfect.

89. *An H-module M of rank r is perfect or not according as the multiplicity of the simple module* $M_{x_{r+1}=\ldots=x_n=0}$ *is equal to or greater than the number of modular equations of* $M^{(r)}$ *or of* $M^{(r)}{}_{x_{r+2}=\ldots=x_n=0}$. The difference between the two numbers when M is unmixed is the total number of *extra* rows of the dialytic array of $M^{(r)}$ when carried as far as degree δ (§ 77), and when M is mixed is still greater. The property affords the simplest test for deciding whether a given module is perfect or not; for the two numbers can generally be found. For example, the prime module M in § 88 is of rank 2 and order 4, while the multiplicity of $M_{x_3=\ldots=x_n=0}$ is 5, so that M is not perfect. The property may also be stated in the form that *an H-module M of rank r is perfect or not according as* $M^{(r)}{}_{x_{r+2}=\ldots=x_n=0}$ *is perfect (i.e. unmixed) or not.*

90. *A perfect module is unmixed.* If M is perfect the module $M^{(r)}$ has an H-basis of which each member has its highest terms independent of the parameters $x_{r+1}, \ldots, x_n$. Hence the dialytic array of $M^{(r)}$ constructed from an H-basis has pure constants for the elements in all its compartments; and a non-vanishing determinant D can be selected from the array for any degree t which is a pure constant. Let ϕF be a member of M, where ϕ is a whole function of the parameters only. Then F is a member of $M^{(r)}$ and if we insert a row in the array representing F it will be dependent on the rest, i.e.

$$F = \lambda_1 F_1 + \lambda_2 F_2 + \ldots + \lambda_\rho F_\rho,$$

where $F_1, F_2, \ldots, F_\rho$ are the members of $M^{(r)}$ represented by the rows of the array, and $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ are rational functions of $x_{r+1}, \ldots, x_n$. Equating coefficients on the two sides of power products of $x_1, x_2, \ldots, x_r$ corresponding to the columns of the determinant D mentioned above, and solving for $\lambda_1, \lambda_2, \ldots, \lambda_\rho$, we see that $\lambda_i D$ and consequently λ_i is a whole function of $x_{r+1}, \ldots, x_n$. Hence F is a member of M, since $F_1, F_2, \ldots, F_\rho$ are all members of M; and $\phi F = 0 \bmod M$ requires $F = 0 \bmod M$. Hence M is unmixed.

If M is a perfect module of rank r and M′ a module in $x_{r+1}, \ldots, x_n$ *(independent of* $x_1, x_2, \ldots, x_r$*) the* L.C.M. *of M, M′ is the same as their product MM′.* For if the F above is a member of the L.C.M. of M, M' the elements in the row representing F are all members of M', and the λ_i are linear functions of them and therefore also members of M'. Hence

$$F = \Sigma \lambda_i F_i = 0 \bmod MM', \quad \text{i.e.} \quad [M, M'] = MM',$$

since $\lambda_i = 0 \bmod M'$ and $F_i = 0 \bmod M$.

91. *The number* H_l *of modular equations of degree l of a perfect H-module M of rank r is the coefficient of* x^l *in*

$$(1 + \mu_1 x + \mu_2 x^2 + \ldots + \mu_{\gamma-1} x^{\gamma-1})(1-x)^{r-n},$$

where γ *is the characteristic number, and* μ_m *the number of modular equations of degree m, of the simple module* $M_{x_{r+1}=\ldots=x_n=0}$.

For the general member of M of degree l is (§ 90)

$$\lambda_1 F_1 + \lambda_2 F_2 + \ldots + \lambda_\rho F_\rho,$$

where $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ are whole functions of $x_{r+1}, \ldots, x_n$, and cannot vanish identically unless $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ all vanish identically. Hence the number of linearly independent members of M of degree l is the total number of terms in $\lambda_1, \lambda_2, \ldots, \lambda_\rho$. Now the number of the polynomials $F_1, F_2, \ldots, F_\rho$ which are of degree m is μ_m less than the number of power products of $x_1, x_2, \ldots, x_r$ of degree m, and the number of terms in each corresponding λ (of degree $l-m$) is the coefficient of x^l in $x^m(1-x)^{r-n}$. Hence the number of linearly independent members of M of degree l is less than the number of power products of $x_1, x_2, \ldots, x_n$ of degree l by the coefficient of x^l in

$$(1+\mu_1 x+\mu_2 x^2+\ldots+\mu_l x^l)(1-x)^{r-n};$$

and this coefficient is the value of H_l. § 75 is a particular case.

92. *If M is a perfect H-module of rank r such that the simple module $M_{x_{r+1}=\ldots=x_n=0}$ is a principal system, and M' a perfect H-module of rank r contained in M, the module M/M' is perfect.*

The μ and μ' r-dimensional modular equations of M and M' begin with the μ and μ' modular equations of $M_{x_{r+1}=\ldots=x_n=0}$ and $M'_{x_{r+1}=\ldots=x_n=0}$. Also the $\mu-\mu'$ r-dimensional modular equations of M/M' are the F'-derivates of the modular equations of M, where F' is any member of M', and begin with the $F'_{x_{r+1}=\ldots=x_n=0}$-derivates of the modular equations of $M_{x_{r+1}=\ldots=x_n=0}$, that is, with the modular equations of $M_{x_{r+1}=\ldots=x_n=0}/M'_{x_{r+1}=\ldots=x_n=0}$. These are $\mu-\mu'$ in number, since $M_{x_{r+1}=\ldots=x_n=0}$ is a principal system containing $M'_{x_{r+1}=\ldots=x_n=0}$. Hence M/M' is perfect (§ 81).

93. We may sum up some of the relations between different kinds of modules.

A module of the principal class is unmixed and a principal system, and in the case of an H-module is perfect.

Any power of a module of the principal class is unmixed, and in the case of an H-module is perfect (§ 89, end), but is not a principal system; e.g. $(x_1, x_2)^2$ is not a principal system.

A module of rank $k-r+1$ whose basis is a matrix with r rows and k columns is unmixed, and in the case of an H-module is perfect (§ 89, end), but is not a principal system; e.g. the module $\begin{pmatrix} 0 & x_1 & x_2 \\ x_1 & x_2 & 0 \end{pmatrix}$ is not a principal system.

A primary module of the principal Noetherian class is a principal system, but not perfect.