III. GENERAL PROPERTIES OF MODULES

23. Several arithmetical terms are used in connection with modules suggesting an analogy between the properties of polynomials and the properties of natural numbers. Two modules have a G.C.M., an L.C.M., a product, and a residual (integral quotient); but no sum or difference. Also a prime module answers to a prime number and a primary module to a power of a prime number. Such terms must not be used for making deductions by analogy.

Definitions. Any member F of a module M is said to *contain* M. Also the module (F) contains M. It is immaterial in this statement as in many others whether we regard F as a polynomial or a module. The term *contains* is used as an extension and generalisation of the phrase *is divisible by*.

More generally a module M is said to *contain* another M' if every member of M contains M'; and this will be the case if every member of the basis of M contains M'. Thus $(F_1, F_2, \ldots, F_k)$ contains $(F_1, F_2, \ldots, F_{k+1})$, and a module becomes less by adding new members to it.

If M contains M' and M' contains M we say that M, M' are the same module, or $M = M'$.

If M contains M' the spread of M contains the spread of M', but the converse is not true in general.

If in a given finite or infinite set of modules there is one which is contained in every other one, that one is called the *least* module of the set; or if there is one which contains every other one, that one is called the *greatest* module of the set. Two modules cannot be compared as to greater or less unless one contains the other.

There is a module which is contained in all modules, the *unit module* (1). Also (0) may be conceived of as a module which contains all modules; but it seldom comes into consideration and will not be mentioned again. These two modules are called non-proper modules, and all others are *proper* modules. In general by a module a proper module is to be understood.

The G.C.M. of k given modules $M_1, M_2, \ldots, M_k$ is the greatest of all modules M contained in M_1 and $M_2 \ldots$ and M_k, and is denoted by $(M_1, M_2, \ldots, M_k)$. In order that M may be contained in each of $M_1, M_2, \ldots, M_k$, or that each of $M_1, M_2, \ldots, M_k$ may contain M, it is necessary and sufficient that all the members of the bases of M_1, M_2, ..., M_k should contain M; hence the module whose basis consists of all these members contains all the modules M, and is at the same time one of the modules M. It is therefore the greatest of all the modules M and the G.C.M. of M_1, M_2, ..., M_k. The notation $(M_1, M_2, \ldots, M_k)$ agrees with the notation $(F_1, F_2, \ldots, F_k)$, since the latter is the G.C.M. of $F_1, F_2, \ldots, F_k$ regarded as modules.

The L.C.M. of M_1, M_2, ..., M_k is the least of all modules M containing M_1 and M_2 ... and M_k, and is denoted by $[M_1, M_2, \ldots, M_k]$. Its members consist of all polynomials which contain M_1 and M_2 ... and M_k; for the basis of any module M containing M_1 and M_2 ... and M_k must consist of a certain number of such polynomials, and the whole aggregate of such polynomials constitutes a module M which is the least of all the modules M.

The *product* of $M_1, M_2, \ldots, M_k$ is the module whose basis consists of all products $F_1F_2 \ldots F_k$, where F_i is any member of the basis of M_i $(i = 1, 2, \ldots, k)$. The product is denoted by $M_1M_2 \ldots M_k$, and is evidently a definite module independent of what bases may be chosen for M_1, M_2, ..., M_k. The product $M_1M_2 \ldots M_k$ contains the L.C.M. $[M_1, M_2, \ldots, M_k]$.

The product of γ modules each of which is the same module M is denoted by M^γ and is called a power of M. If P is the point $(a_1, a_2, \ldots, a_n)$ the module $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ is denoted by P. If O is the origin the module O is $(x_1, x_2, \ldots, x_n)$, and O^γ is a module having for basis all power products of $x_1, x_2, \ldots, x_n$ of degree γ. A polynomial F, or module M, which contains P^γ is said to have a γ-point at P.

The *residual* (L, p. 49) of a given module M' with respect to another M is the least module whose product with M' contains M and is denoted by M/M'. Its members consist of every polynomial whose product with each member separately of the basis of M' is a member of M; for the basis of any module whose product with M' contains M must consist of a certain number of such polynomials, and the whole aggregate of such polynomials constitutes the least such module.

In the case of the natural numbers the residual of m' with respect to m is the least number whose product with m' contains m, and is the quotient of m by the G.C.M. of m and m'. It is the same to some extent with modules, viz. $M/M' = M/(M, M')$; for if $M/M' = M''$ then M'' is the least module such that $M'M''$ contains M, and is therefore the least module such that $(M, M')M''$ contains M, i.e. $M'' = M/(M, M')$.

Nevertheless $M/(M, M')$ is not called the quotient of M by (M, M') because it is not true in general that the product of (M, M') and $M/(M, M')$ is M.

If M, M', M'' are three modules such that $M'M''$ contains M it is clear that M' contains M/M'' and M'' contains M/M'. Since MM' contains M, M contains M/M'. The module M/M' is a module contained in M having a special relation to M independently of what M' may be (§ 26 (i)).

There is a least module which can be substituted for M' without changing M/M', viz. $M/(M/M')$, § 26 (ii). This module is contained in (M, M'), for (M, M') can be substituted for M' without changing M/M', but is in general different from (M, M').

24. Comment on the definitions. The non-proper unit module (1) has no spread. Conversely a module which has no spread is the module (1), since the complete resolvent is 1 and is a member of the module. The unit module is of importance from the fact that it often comes at the end of a series of modules derived by some process from a given module.

$(M_1, M_2, \ldots, M_k)$ and $[M_1, M_2, \ldots, M_k]$ obey the associative law $[M_1, M_2, M_3] = [[M_1, M_2], M_3] = [M_1, [M_2, M_3]]$, and the commutative law $(M_1, M_2) = (M_2, M_1)$. Also $(M_1, M_2, \ldots, M_k)$ obeys the distributive law $M(M_1, M_2) = (MM_1, MM_2)$; but $[M_1, M_2, \ldots, M_k]$ does not.

Example. As an example of the last statement we have

$$(x_1, x_2)[(x_1^2, x_2^2), (x_1 x_2)] = (x_1, x_2)(x_1^2 x_2, x_1 x_2^2) = (x_1 x_2)(x_1, x_2)^2,$$

while $$[(x_1, x_2)(x_1^2, x_2^2), (x_1, x_2)(x_1 x_2)] = (x_1 x_2)(x_1, x_2).$$

Given the bases of $M_1, M_2, \ldots, M_k, M, M'$ we know at once a basis for $(M_1, M_2, \ldots, M_k)$ and for $M_1 M_2 \ldots M_k$; but it may be extremely difficult to find a basis for $[M_1, M_2, \ldots, M_k]$ or for M/M'. Hilbert (H, pp. 492–4, 517) has given a process for finding a basis of $[M_1, M_2, \ldots, M_k]$; and the same process can be applied for finding a basis for M/M'. This process is chiefly of theoretical value in so far as it has any value.

We can have (i) $MM' = MM''$, or $M/M' = M/M''$, without $M' = M''$; (ii) $M/M' = M''$ without $M/M'' = M'$; (iii) $M/M' = M''$ and $M/M'' = M'$ without $M = M'M''$; and (iv) $M = M'M''$ without $M/M' = M''$ or $M/M'' = M'$.

Examples. (i) $$(x_1, x_2)(x_1, x_2)^2 = (x_1, x_2)(x_1^2, x_2^2),$$
$$(x_1, x_2)^3/(x_1, x_2)^2 = (x_1, x_2)^3/(x_1^2, x_2^2);$$

(ii) $(x_1, x_2)^3/(x_1^2, x_2^2) = (x_1, x_2)$, while $(x_1, x_2)^3/(x_1, x_2) = (x_1, x_2)^2$;

(iii) $(x_1^2, x_2^2)/(x_1, x_2) = (x_1, x_2)^2$ and $(x_1^2, x_2^2)/(x_1, x_2)^2 = (x_1, x_2)$,
while
$$(x_1^2, x_2^2) \neq (x_1, x_2)(x_1, x_2)^2;$$

(iv)
$$(x_1, x_2)^6 = (x_1^3, x_1^2 x_2, x_2^3)(x_1^3, x_1 x_2^2, x_2^3),$$
while $(x_1, x_2)^6/(x_1^3, x_1^2 x_2, x_2^3)$ and $(x_1, x_2)^6/(x_1^3, x_1 x_2^2, x_2^3)$ are both equal to $(x_1, x_2)^3$.

25. *The product of the* G.C.M. *and* L.C.M. *of two modules contains the product of the modules.*

Let $M = (F_1, F_2, \ldots, F_k)$ and $M' = (F_1', F_2', \ldots, F'_{k'})$ be the two modules and let F_L be any member of the basis of their L.C.M. Then, since $F_L = 0 \bmod M$, $F_i' F_L = 0 \bmod MM'$; and since $F_L = 0 \bmod M'$, $F_i F_L = 0 \bmod MM'$; i.e. the product of any member of the basis of (M, M') with any member of the basis of $[M, M']$ contains MM', or $(M, M')[M, M']$ contains MM'.

When M, M' have no point in common $(M, M') = (1)$ and consequently $[M, M']$ contains MM', i.e. $[M, M'] = MM'$. This case is proved by König (K, p. 356); although it is to be noticed that (M, M') cannot be (1) in the case of modules of homogeneous polynomials. Thus the L.C.M. of any finite number of simple modules (§ 33) is the same as their product (Mo).

26. *The modules M/M' and $M/(M/M')$ are mutually residual with respect to M, i.e. each is the residual of the other with respect to M.*

Let $M/M' = M''$ and $M/(M/M') = M'''$; then we have $M''' = M/M''$, and we have to prove that $M'' = M/M'''$. Let $M/M''' = M^{iv}$. Now $M'M''$ contains M; therefore M' contains M/M'' or M'''. Also $M''M'''$ contains M; therefore M'' contains M/M''' or M^{iv}. Again, since M' contains M''' (proved) and $M'''M^{iv}$ contains M, $M'M^{iv}$ contains M, i.e. M^{iv} contains M/M' or M''. But M'' contains M^{iv} (proved). Hence $M'' = M^{iv} = M/M'''$.

Two results follow from this:

(i) *M/M' is a module contained in M of a particular type;* for M/M' and its residual with respect to M are mutually residual with respect to M, and this is not true in general of any module contained in M and the residual module (Ex. ii, § 24).

(ii) *The least module which can be substituted for M' without changing M/M' is $M/(M/M')$.* Let M^{iv} be any module such that $M/M^{iv} = M/M'$; then the product of M^{iv} and M/M' contains M, and M^{iv} contains $M/(M/M')$. Also $M/(M/M')$ is one of the modules M^{iv};

for if $M/(M/M') = M'''$ then $M/M''' = M/M'$, by the theorem. Hence $M/(M/M')$ is the least of the modules M^{iv} which can be substituted for M' without changing M/M'.

27. *If M', M'' are mutually residual with respect to any module they are mutually residual with respect to $M'M''$.*

Suppose M', M'' are mutually residual with respect to M. Then $M'M''$ contains M; and if $M'M''/M' = M'''$, $M'M'''$ contains $M'M''$ which contains M; hence M''' contains M/M' or M''. Also M'' contains $M'M''/M'$ or M'''. Hence $M'' = M''' = M'M''/M'$. Similarly $M' = M'M''/M''$ (cf. statement iv, § 24).

Any module M with respect to which M', M'' are mutually residual contains $[M', M'']$ and is contained in $M'M''$.

28. *If $M, M_1, M_2, \ldots, M_k$ are any modules, then*

$$M/(M_1, M_2, \ldots, M_k) = [M/M_1, M/M_2, \ldots, M/M_k],$$

and

$$[M_1, M_2, \ldots, M_k]/M = [M_1/M, M_2/M, \ldots, M_k/M].$$

For $M/(M_1, M_2, \ldots, M_k)$ contains M/M_i and therefore contains $[M/M_1, M/M_2, \ldots, M/M_k]$. Also $M_i[M/M_1, \ldots, M/M_k]$ contains $M_i \times M/M_i$ which contains M; hence $(M_1, \ldots, M_k)[M/M_1, \ldots, M/M_k]$ contains M, and $[M/M_1, \ldots, M/M_k]$ contains $M/(M_1, \ldots, M_k)$. This proves the first part.

Again $[M_1, \ldots, M_k]/M$ contains M_i/M and therefore contains $[M_1/M, \ldots, M_k/M]$. Also $M[M_1/M, \ldots, M_k/M]$ contains M_i and therefore contains $[M_1, \ldots, M_k]$; hence $[M_1/M, \ldots, M_k/M]$ contains $[M_1, \ldots, M_k]/M$. This proves the second part.

29. Prime and Primary Modules. *Definitions.* A *prime module* is defined by the property that no product of two modules contains it without one of them containing it.

A *primary module* is defined by the property that no product of two modules contains it without one of them containing it or both containing its spread. Hence if one does not contain the spread the other contains the module.

Primary modules will be understood to include prime modules.

Lasker introduced and defined the term primary (L, p. 51), though not in the same words as given here. The conception of a primary module is a fundamental one in the theory of modular systems.

Any irreducible spread determines a prime module, viz. the module whose members consist of all polynomials containing the spread. That this module is prime follows from the fact that no product of two polynomials can contain the spread without one of them containing it (§ 22) and the module; and the same is true if for polynomials we write modules.

If $M=(F_1, F_2, \ldots, F_k)$ is the prime module of rank r determined by an irreducible spread of dimensions $n-r$, and if the origin be moved to a general point of the spread, the constant terms of $F_1, F_2, \ldots, F_k$ will vanish, and the linear terms will be equivalent to r independent linear polynomials, i.e. the sub-determinants of order $> r$ of the matrix

$$\begin{vmatrix} \dfrac{\partial F_1}{\partial x_1}, & \dfrac{\partial F_1}{\partial x_2}, & \cdots & \dfrac{\partial F_1}{\partial x_n} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{\partial F_k}{\partial x_1}, & \dfrac{\partial F_k}{\partial x_2}, & \cdots & \dfrac{\partial F_k}{\partial x_n} \end{vmatrix}$$

will vanish, while those of order r will not vanish, at the origin. This will be equally true for any general point of the spread without moving the origin to it. Any point of the spread for which the sub-determinants of order r of this matrix vanish is called a *singular point* of the spread, and the aggregate of such points the *singular spread* contained in the given spread. The singular spread (if any exists) is therefore the spread determined by $F_1, F_2, \ldots, F_k$ and the sub-determinants of order r of the above matrix.

If $M=(F_1, F_2, \ldots, F_k)$ is the L.C.M. of the prime modules determined by any finite number of irreducible spreads of the same dimensions $n-r$, the same definition holds concerning singularities of the whole spread. In this case the singular spread consists of the intersections of all pairs of the irreducible spreads, together with all the singular spreads contained in the irreducible spreads considered individually.

30. *The spread of any prime or primary module is irreducible.* For if not the complete u-resolvent has at least two factors corresponding to two different irreducible spreads of the module neither of which contains the other, and is the product of two polynomials neither of which contains the whole spread of the module, i.e. the module is neither prime nor primary.

31. *There is only one prime module with a given (irreducible) spread, viz. the module whose members consist of all polynomials containing the spread.*

Let $M=(F_1, F_2, \ldots, F_k)$ be any prime module of rank r. It will be sufficient to prove that every polynomial which contains the spread of M contains the module M. The first complete partial u-resolvent of M other than 1 will be a power $R_u{}^m$ of an irreducible polynomial R_u in $x, x_{r+1}, \ldots, x_n$. Also the complete u-resolvent is a member of $(f_1, f_2, \ldots, f_k)$, § 18, which is prime; and every factor except $R_u{}^m$ is of too high rank to contain the spread of $(f_1, f_2, \ldots, f_k)$. Hence $R_u{}^m$, and therefore R_u itself, is a member of $(f_1, f_2, \ldots, f_k)$. Hence $(R_u)_{x=u_1x_1+\ldots+u_nx_n}$ is a member of M, and also the whole coefficient of any power product of $u_1, u_2, \ldots, u_n$ in $(R_u)_{x=u_1x_1+\ldots+u_nx_n}$. We have proved (§ 21) that

$$(R_u)_{x=u_1x_1+\ldots+u_nx_n} = \ldots + u_r^{d-1}(u_1\psi_1 + \ldots + u_{r-1}\psi_{r-1}) + u_r^d\phi,$$

where $\psi_1 = x_1\phi' - \phi_1, \ldots, \psi_{r-1} = x_{r-1}\phi' - \phi_{r-1}$. Hence $\psi_1, \ldots, \psi_{r-1}, \phi$ are all members of M.

Let F be any polynomial which contains the spread of M. In F put $x_1 = \phi_1/\phi', x_2 = \phi_2/\phi', \ldots, x_{r-1} = \phi_{r-1}/\phi'$; then F becomes a rational function of $x_r, x_{r+1}, \ldots, x_n$ of which the denominator is ϕ'^l, where l is the degree of F. This rational function vanishes for all points of the spread at which ϕ' does not vanish, and its numerator is therefore divisible by ϕ. We have then

$$F\left(\frac{\phi_1}{\phi'}, \frac{\phi_2}{\phi'}, \ldots, \frac{\phi_{r-1}}{\phi'}, x_{r+1}, \ldots, x_n\right) = \frac{X\phi}{\phi'^l},$$

where X is a whole function of $x_r, x_{r+1}, \ldots, x_n$; i.e.

$$F\left(x_1 - \frac{\psi_1}{\phi'}, x_2 - \frac{\psi_2}{\phi'}, \ldots, x_{r-1} - \frac{\psi_{r-1}}{\phi'}, x_{r+1}, \ldots, x_n\right) = \frac{X\phi}{\phi'^l},$$

or $\qquad \phi'^l F(x_1, x_2, \ldots, x_n) = 0 \bmod (\psi_1, \ldots, \psi_{r-1}, \phi) = 0 \bmod M.$

Hence $F = 0 \bmod M$, which proves the theorem.

It follows that a module which is the L.C.M. of a finite number of prime modules, whether of the same rank or not, is uniquely determined by its spread, and any polynomial containing the spread contains the module.

32. *If M is a primary module and M_1 the prime module determined by its spread some finite power of M_1 contains M.*

This theorem, in conjunction with Lasker's theorem (§ 39), is equivalent to the Hilbert-Netto theorem (§ 46). The proofs of the theorem by Lasker and König are both wrong. Lasker first assumes the theorem (L, p. 51) and then proves it (L, p. 56); and König makes an absurdly false assumption concerning divisibility (K, p. 399).

By the same reasoning as in the last theorem it follows that $R_u{}^m$ (but not R_u) is a member of $(f_1, f_2, \ldots, f_k)$, and

$$(R_u{}^m)_{x=u_1x_1+\ldots+u_nx_n} = \{\ldots + u_r{}^{d-1}(u_1\psi_1 + \ldots + u_{r-1}\psi_{r-1}) + u_r{}^d\phi\}^m = 0 \bmod M.$$

Picking out the coefficients of $u_r{}^{dm}$ and $u_r{}^{dm-m}u_1{}^m$, we have

$$\phi^m = 0 \bmod M, \quad \text{and} \quad \psi_1{}^m = X\phi \bmod M; \quad \therefore \quad \psi_1{}^{m^2} = 0 \bmod M;$$

and similarly $\psi_2{}^{m^2} = \ldots = \psi_{r-1}^{m^2} = 0 \bmod M$. Also if F is any member of M_1, then, by the last theorem,

$$\phi'^l F = 0 \bmod (\psi_1, \ldots, \psi_{r-1}, \phi).$$

Hence the product of any rm^2 polynomials F and ϕ'^{lrm^2} is a member of $(\psi_1{}^{m^2}, \psi_2 \ , \ldots \psi_{r-1}^{m^2}, \phi^{m^2})$ and of M, i.e. $M_1{}^{rm^2}$ contains M.

33. *Definitions.* If M is a primary module and M_1 the corresponding prime module the least number γ such that $M_1{}^\gamma$ contains M is called the *characteristic number* of M.

A *simple* module is a module containing one point only (Mo). For example, $O^\gamma = (x_1, x_2, \ldots, x_n)^\gamma$ is a simple module with characteristic number γ.

A module of homogeneous polynomials will be called an *H-module.* A simple H-module has the origin for its spread; but a simple module having the origin for spread is not in general an H-module.

A simple module is primary. For if M is a simple module, and M', M'' any two modules whose product contains M, of which M' does not contain the spread of M, then (M, M') contains no point and is the module (1); but $(M, M')\,M''$ contains M, i.e. M'' contains M; hence M is primary.

34. *There is no higher limit to the number of members that may be required to constitute a basis of a prime module.* This is not in conflict with Kronecker's statement, proved by König (K, p. 234), that there always exist $n+1$ polynomials containing a given algebraic spread which have no point in common outside the spread.

Example. Consider $\frac{1}{2}l(l-1)$ straight lines through the origin O in 3-dimensional space, not lying on any cone of order $l-2$. Draw a cone of order l and a surface (not a cone) of order l through the $\frac{1}{2}l(l-1)$ lines so as to intersect again in an irreducible curve of order $\frac{1}{2}l(l+1)$ with $\frac{1}{2}l(l-1)$ tangents at O. Then no basis of the prime module determined by this curve can have less than l members, where l is a number which can be chosen as high as we please.

This can be proved by considering residuation on the cone. The original $\frac{1}{2}l(l-1)$ generators have a residual on the cone of $\frac{1}{2}l(l-1)$ generators, which again have a residual of $\frac{1}{2}l(l-1)$ generators, of which $l-1$ can be chosen at will. This last set of generators is residual to the irreducible curve and together they make the whole intersection of the cone with a surface of order l having an $(l-1)$-point at O. Hence there are l surfaces of order l containing the irreducible curve which have an $(l-1)$-point at O and in which the terms of degree $l-1$ are linearly independent, while there is no surface containing the curve with less than an $(l-1)$-point at O. The prime module determined by the curve must therefore have at least l members in its basis. The module has in fact a basis of $l+1$ members, the $l+1$ linearly independent surfaces of order l containing it (including the cone); and these can be reduced to l members.

In the case $n=2$ the curve is an ordinary space cubic determining a prime module

$$(f_1, f_2, f_3) = (vw' - v'w,\ wu' - w'u,\ uv' - u'v),$$

where u, v, w, u', v', w' are linear. The basis of three members can be reduced to two $f_1 - af_2$, $f_1 - bf_3$ provided constants a, b, λ, λ' and linear functions α, β can be chosen so that

$$f_1 = \alpha(f_1 - af_2) + \beta(f_1 - bf_3),$$

or

$$(1 - \alpha - \beta) f_1 + a\alpha f_2 + b\beta f_3 = 0,$$

or

$$1 - \alpha - \beta = \lambda u + \lambda' u', \quad a\alpha = \lambda v + \lambda' v', \quad b\beta = \lambda w + \lambda' w';$$

and this can be done.

35. *The* L.C.M. *of any number of primary modules with the same spread is a primary module with the same spread.*

Let $M_1, M_2, \ldots, M_k$ be primary modules with the same spread, and let M be their L.C.M. Then M has the same irreducible spread, since the product, which contains the L.C.M., has the same spread. Also if the product $M'M''$ contains M, and M' does not contain the spread, then M'' contains M_1 and $M_2 \ldots$ and M_k, i.e. M'' contains M. Hence M is primary. The G.C.M. is not primary in general.

36. *If M is primary and M' is any module not containing M then M/M' is primary and has the same spread as M.*

Let $M/M' = M''$. Then since $M'M''$ contains M, and M' does not contain M, M'' contains the spread of M. Also M contains M''; hence M'' has the same spread as M. Also if M_1M_2 contains M'' then

$M'M_1M_2$ contains $M'M''$ which contains M; and if M_1 does not contain the spread of M (that is of M'') $M'M_2$ contains M, and M_2 contains M/M' or M''; i.e. M'' is primary.

37. Hilbert's Theorem (H, p. 474). *If $F_1, F_2, F_3, \ldots$ is an infinite series of homogeneous polynomials there exists a finite number k such that $F_h = 0$ mod $(F_1, F_2, \ldots, F_k)$ when $h > k$.*

The following proof is substantially König's (K, p. 362). It must be clearly understood that $F_1, F_2, F_3, \ldots$ *are given in a definite order.* In the case of a single variable the series $F_1, F_2, F_3, \ldots$ consists of powers of the variable, and if F_k is the least power then $F_h = 0$ mod F_k when $h > k$. Hence the theorem is true in this case. We shall assume it for $n-1$ variables and prove it for n variables.

The series $F_1', F_2', F_3', \ldots$ is called a modified form of the series $F_1, F_2, F_3, \ldots$ if $F_1' = F_1$ and $F_i' = F_i$ mod $(F_1, F_2, \ldots, F_{i-1})$ for $i > 1$. Thus the modules $(F_1, F_2, \ldots, F_i)$ and $(F_1', F_2', \ldots, F_i')$ are the same. The theorem will be proved if we show that the series $F_1', F_2', \ldots$ can be so chosen that all its terms after a certain finite number become zero. We assume that F_1 is regular in x_n, and we choose the modified series so that each of its terms F_i' after the first is of as low degree as possible in x_n, and therefore of lower degree in x_n than F_1'. The terms of the series $F_1', F_2', \ldots$ of degree zero in x_n will be polynomials in $x_1, x_2, \ldots, x_{n-1}$ and these can be modified so that all after a certain finite number become zero, since the theorem is assumed true for $n-1$ variables. Let $F'_{l_1}, F'_{l_2}, F'_{l_3}, \ldots$ be all the terms of $F_1', F_2', F_3', \ldots$, taken in order, which are of one and the same degree $l > 0$ in x_n; and let $f'_{l_1}, f'_{l_2}, \ldots$ be the whole coefficients of x_n^l in them. Then $f'_{l_1}, f'_{l_2}, f'_{l_3}, \ldots$ are polynomials in $n-1$ variables; and we cannot have $f'_{l_i} = 0$ mod $(f'_{l_1}, f'_{l_2}, \ldots, f'_{l_{i-1}})$ for any value of i; for if $f'_{l_i} = A_1 f'_{l_1} + A_2 f'_{l_2} + \ldots + A_{i-1} f'_{l_{i-1}}$, then $F'_{l_i} - A_1 F'_{l_1} - \ldots - A_{i-1} F'_{l_{i-1}}$ is of less degree than l in x_n, which cannot be. Hence the number of the polynomials $f'_{l_1}, f'_{l_2}, \ldots$, or the number of terms $F'_{l_1}, F'_{l_2}, \ldots$ in the series $F_1', F_2', \ldots$, is finite. And the number of values of l is also finite, the greatest value of l being the value it has in F_1'. Hence the theorem is proved.

The theorem can be extended at once to an infinite series $F_1, F_2, \ldots$ of non-homogeneous polynomials since they can all be made homogeneous by introducing a variable x_0 of homogeneity.

The following is an immediate consequence of the theorem:

Any module of polynomials has a basis consisting of a finite number of members.

To prove this it is only necessary to show that a complete linearly independent set of members of any module can be arranged in a definite order in an infinite series. If l is the lowest degree of any member we can first take any complete linearly independent set of members of degree l, then any complete set of members of degree $l+1$ whose terms of degree $l+1$ are linearly independent, then a similar set of members of degree $l+2$, and so on. In this way a complete linearly independent set of members is obtained in a definite order. It does not matter in what order the members of a set are taken, nor is it necessary to know how to find the members of a set. It is sufficient to know that there is a definite finite number of members belonging to each set.

38. The *H*-module equivalent to a given module. Consider a complete linearly independent set of members of a given module M, not an H-module, arranged in a series in the order described above; and make all the members homogeneous by introducing a new variable x_0. We then have a series of homogeneous polynomials belonging to an H-module M_0, whose basis consists of a finite number of members of the series. The module M_0 is called *the H-module equivalent to M*, and a basis of M obtained from any basis of M_0 by putting $x_0=1$ is called an *H-basis* of M. The distinctive property of an H-basis $(F_1, F_2, \ldots, F_k)$ of M is that any member F of M can be put in the form $A_1F_1+A_2F_2+\ldots+A_kF_k$ where A_iF_i $(i=1, 2, \ldots, k)$ *is not of greater degree than* F. *Every module has an H-basis*, which may necessarily consist of more members than would suffice for a basis in general.

The following relations exist between M and its equivalent H-module M_0: (i) to any member F of M corresponds a member F_0 of M_0 of the same degree as F, and an infinity of members $x_0^pF_0$ of higher degree; (ii) to any member F_0 of M_0 corresponds one and only one member of M, viz. $(F_0)_{x_0=1}$; (iii) there is a one-one correspondence between the members of M_0 of degree l and the members of M of degree $\leqslant l$.

If $x_0F_0=0 \bmod M_0$, then $(F_0)_{x_0=1}=0 \bmod M$, and $F_0=0 \bmod M_0$ by (i), i.e. there is no member x_0F_0 of M_0 such that F_0 is not a member of M_0, and $M_0/(x_0)=M_0$. Conversely *an H-module M in n variables* $x_1, x_2, \ldots, x_n$ *is equivalent to the module* $M_{x_n=1}$ *if* $M/(x_n)=M$, *and not otherwise.*

In any basis $(F_1, F_2, \ldots, F_k)$ of an H-module in which no member is irrelevant, i.e. no $F_i = 0 \bmod (F_1, \ldots, F_{i-1}, F_{i+1}, \ldots, F_k)$, the number of members of each degree is fixed; as can be easily seen by arranging $F_1, F_2, \ldots, F_k$ in order of degree. *Hence in any H-basis of a module in which no member is irrelevant the number of members of each degree is fixed.* On account of this and the other properties of an H-basis mentioned above an H-basis gives a simpler and clearer representation of a module than a basis which is not an H-basis.

Example. Find an H-basis of the module $(x_1^2, x_2 + x_1x_3)$.

Take the H-module $(x_1^2, x_2x_0 + x_1x_3)$ and solve the equation

$$x_0 X_0 = 0 \bmod (x_1^2, x_2x_0 + x_1x_3),$$

or

$$x_0 X_0 = x_1^2 X_1 + (x_2x_0 + x_1x_3) X_2.$$

Putting $x_0 = 0$ we have

$$(x_1^2 X_1 + x_1x_3 X_2)_{x_0=0} = 0,$$

i.e.

$$X_1 = x_3 X, \quad X_2 = -x_1 X, \quad \text{when } x_0 = 0,$$

i.e.

$$X_1 = x_3 X + x_0 Y_1, \quad X_2 = -x_1 X + x_0 Y_2.$$

Hence

$$x_0 X_0 = x_1^2 (x_3 X + x_0 Y_1) + (x_2x_0 + x_1x_3)(-x_1 X + x_0 Y_2)$$
$$= x_0 (x_1^2 Y_1 - x_1x_2 X + \overline{x_2x_0 + x_1x_3} Y_2),$$

i.e.

$$X_0 = 0 \bmod (x_1^2, x_1x_2, x_2x_0 + x_1x_3).$$

Again, if we solve the equation

$$x_0 Y_0 = 0 \bmod (x_1^2, x_1x_2, x_2x_0 + x_1x_3),$$

we find

$$Y_0 = 0 \bmod (x_1^2, x_1x_2, x_2^2, x_2x_0 + x_1x_3);$$

and if we solve

$$x_0 Z_0 = 0 \bmod (x_1^2, x_1x_2, x_2^2, x_2x_0 + x_1x_3),$$

we find

$$Z_0 = 0 \bmod (x_1^2, x_1x_2, x_2^2, x_2x_0 + x_1x_3).$$

Hence $(x_1^2, x_1x_2, x_2^2, x_2x_0 + x_1x_3)$ is the H-module equivalent to $(x_1^2, x_2 + x_1x_3)$, and $(x_1^2, x_1x_2, x_2^2, x_2 + x_1x_3)$ is an H-basis of $(x_1^2, x_2 + x_1x_3)$.

The extra members x_1x_2, x_2^2 might of course have been found more quickly by multiplying $x_2 + x_1x_3$ first by x_1 and then by x_2. The method given is a general one.

39. Lasker's Theorem (L, p. 51). *Any given module M is the* L.C.M. *of a finite number of primary modules.*

Let M be of rank r. Express its first complete partial u-resolvent $D_u^{(r-1)}$ in irreducible factors, viz.

$$D_u^{(r-1)} = R_1^{m_1} R_2^{m_2} \ldots R_j^{m_j};$$

and let $C_1, C_2, \ldots, C_j$ denote the irreducible spreads, of dimensions $n-r$, corresponding to $R_1, R_2, \ldots, R_j$ respectively.

Consider the whole aggregate M_i of polynomials F for each of which there exists a polynomial F', not containing C_i, such that $FF'=0 \bmod M$. We shall prove first that M_i is a primary module whose spread is C_i $(i=1, 2, \ldots, j)$.

Let F_1, F_2 be any two members of M_i. Then since $F_1F_1'=0 \bmod M$, and $F_2F_2'=0 \bmod M$, where neither F_1' nor F_2' contains C_i, we have $(A_1F_1+A_2F_2)F_1'F_2'=0 \bmod M$, where $F_1'F_2'$ does not contain C_i. Hence $A_1F_1+A_2F_2$ belongs to the aggregate M_i, i.e. M_i is a module.

Again, since $FF'=0 \bmod M$, F contains C_i, and M_i contains C_i. Now, if F_u is the complete u-resolvent of M,

$$(F_u)_{x=u_1x_1+\ldots+u_nx_n}=0 \bmod M,$$

while $(R_i^{m_i})_{x=u_1x_1+\ldots+u_nx_n}$ is the only factor of $(F_u)_{x=u_1x_1+\ldots+u_nx_n}$ which contains C_i. Hence $(R_i^{m_i})_{x=u_1x_1+\ldots+u_nx_n}=0 \bmod M_i$. But the polynomial $(R_i)_{x=u_1x_1+\ldots+u_nx_n}$ does not vanish identically (i.e. irrespective of $u_1, u_2, \ldots, u_n$) for any point outside C_i (§ 21); hence M_i contains no point outside C_i, i.e. C_i is the spread of M_i.

Lastly M_i is primary; for if $F''F'''=0 \bmod M_i$, then

$$F'F''F'''=0 \bmod M,$$

where F' does not contain C_i; hence, if F'' does not contain C_i, $F'F''$ does not, and $F'''=0 \bmod M_i$. Hence also if $M''M'''$ contains M_i, and M'' does not contain C_i, M''' contains M_i. Thus M_i is a primary module whose spread is C_i. Also M contains M_i, for every member of M is a member of M_i.

The module M/M_i does not contain C_i; for if $M_i=(F_1, F_2, \ldots, F_k)$ and $F_1', F_2', \ldots, F_k'$ are polynomials not containing C_i such that

$$F_lF_l'=0 \bmod M \quad (l=1, 2, \ldots, k),$$

then $$F_lF_1'F_2'\ldots F_k'=0 \bmod M \quad (l=1, 2, \ldots, k).$$

Hence $F_1'F_2'\ldots F_k'$ is a member of M/M_i not containing C_i; and therefore M/M_i cannot contain C_i.

Since M/M_i does not contain C_i, $(M/M_1, M/M_2, \ldots, M/M_j)$ does not contain any of the spreads $C_1, C_2, \ldots, C_j$. We can now prove that if ϕ is any single member of $(M/M_1, M/M_2, \ldots, M/M_j)$ which does not contain any of the spreads $C_1, C_2, \ldots, C_j$, then

$$M=[M_1, M_2, \ldots, M_j, (M, \phi)].$$

Since M contains $[M_1, M_2, \ldots, M_j, (M, \phi)]$ it has only to be proved that the latter contains M, or that

$$F=0 \bmod [M_1, M_2, \ldots, M_j, (M, \phi)] \text{ requires } F=0 \bmod M.$$

We have $\quad F=0 \bmod (M, \phi)=f\phi \bmod M=f\phi \bmod M_i;$

but $F=0 \bmod M_i$; therefore $f\phi=0 \bmod M_i$, and, since ϕ does not contain C_i,

$$f=0 \bmod M_i=0 \bmod [M_1, M_2, \ldots, M_j].$$

Hence $f\phi=0 \bmod [M_1, M_2, \ldots, M_j](M/M_1, \ldots, M/M_j)=0 \bmod M$ (§ 28), and $F=f\phi \bmod M=0 \bmod M$. Hence $M=[M_1, M_2, \ldots, M_j, (M, \phi)]$.

Now the spread of (M, ϕ) is of dimensions $< n-r$, since ϕ does not contain any spread of M of dimensions $n-r$. Hence the same process can be applied to (M, ϕ) as to M; and we finally arrive at a module $(M, \phi, \phi', \ldots)$ with no spread, which is the module (1). Hence $M=[Q_1, Q_2, \ldots, Q_k]$ where $Q_1, Q_2, \ldots, Q_k$ are all primary modules of ranks $\leqslant r$.

40. Comment on Lasker's Theorem. The above is in all essentials the remarkable proof given by Lasker of this fundamental theorem. He considers H-modules only and makes use of homogeneous coordinates, in consequence of which his enunciation of the theorem is not quite as simple as the one above.

Any module among $Q_1, Q_2, \ldots, Q_k$ which is contained in the L.C.M. of all the rest is *irrelevant* and may be omitted. It will be understood in writing $M=[Q_1, Q_2, \ldots, Q_k]$ that all irrelevant modules have been omitted. Those that remain will be called the *relevant primary modules* into which M resolves, and their spreads will be called the *relevant spreads* of M. A relevant spread which is not contained in another of higher dimensions is called an *isolated spread* and the corresponding module an *isolated primary module* of M. The other relevant spreads and modules are called *imbedded* spreads and modules of M. All the relevant spreads of M whether isolated or imbedded are unique. Also the isolated primary modules are unique, but the imbedded primary modules are to some extent indeterminate.

A process by which $Q_1, Q_2, \ldots, Q_k$ can be theoretically obtained, without bringing in any irrelevant modules, is described in (M). The isolated spreads are found from the irreducible factors of the complete u-resolvent after rejecting all factors which give imbedded spreads. To these correspond unique primary modules of M which can be found. Let $M^{(0)}$ be their L.C.M. The isolated spreads of $M/M^{(0)}$ are the relevant spreads of M imbedded to the first degree. To these correspond indeterminate imbedded primary modules of M which are chosen as simply as possible. Although not uniquely determinate the L.C.M. of each one and $M^{(0)}$ is unique, and the L.C.M. of them all and $M^{(0)}$ is a unique module $M^{(1)}$. The isolated spreads of $M/M^{(1)}$ are the relevant spreads of M imbedded to the second degree; and the L.C.M. of the corresponding (indeterminate) primary modules and $M^{(1)}$ is a unique module $M^{(2)}$. The process is continued until a module $M^{(l)}$ is obtained such that $M/M^{(l)}=(1)$, when there will be no more relevant primary modules to find.

41. An *unmixed module* is usually understood to be one whose *isolated* irreducible spreads are all of the same dimensions; but it is clear from the above that this cannot be regarded as a satisfactory view. It should be defined as follows:

Definition. An *unmixed module* is one whose relevant spreads, both isolated and imbedded, are all of the same dimensions; and a *mixed module* is one having at least two relevant spreads of different dimensions.

An unmixed module cannot have any relevant imbedded spreads.

A primary module is an unmixed module whose spread is irreducible. This cannot be taken as a definition because the meaning of *unmixed* depends on the meaning of *primary*.

Condition that a module may be unmixed. In order that a module M of rank r may be unmixed it is necessary and sufficient that it should have no relevant spread of rank $>r$. This condition may be expressed by saying that $\phi F=0 \bmod M$ requires $F=0 \bmod M$ where ϕ is any polynomial involving $x_{r+1}, \dots, x_n$ only. For if M contains a relevant primary module of rank $>r$ a ϕ can be chosen which contains it, and an F which does not contain it but contains all the other relevant primary modules of M, so that $\phi F=0 \bmod M$ does not require $F=0 \bmod M$; while if M contains no relevant primary module of rank $>r$ there is no ϕ containing a relevant spread of M and $\phi F=0 \bmod M$ requires $F=0 \bmod M/(\phi)=0 \bmod M$ (§ 42).

A primary module Q has a certain *multiplicity* (§ 68). To a given primary module $Q^{(\mu)}$ of multiplicity μ corresponds a series of primary modules $Q^{(1)}, Q^{(2)}, \dots, Q^{(\mu)}$ of multiplicities $1, 2, \dots, \mu$ all having the same spread as $Q^{(\mu)}$ and such that $Q^{(p)}$ contains $Q^{(p-1)}$ and is contained in $Q^{(p+1)}$. $Q^{(1)}$ is the prime module determined by the spread of $Q^{(\mu)}$ and is unique; but the intermediate modules $Q^{(2)}, Q^{(3)}, \dots, Q^{(\mu-1)}$ are to a great extent indeterminate (M, p. 89). Thus $Q^{(1)}, Q^{(2)}, \dots, Q^{(\mu)}$ may be regarded as successive stages in constructing $Q^{(\mu)}$. *Two primary modules with the same spread and the same multiplicity such that one contains the other must be the same module.*

42. Deductions from Lasker's Theorem. *A module of rank n resolves into simple (primary) modules of which it is the product* (§ 25).

If M' does not contain any relevant spread of M then $M/M' = M$. Let $M/M' = M''$. Then since $M'M''$ contains M, and M' does not contain any relevant spread of M, M'' contains all the relevant primary modules into which M resolves, i.e. $M'' = M$.

It follows that if $M/M' \neq M$, M' must contain a relevant spread of M. *Thus if a polynomial F exists such that $(x_1 - a_1)F, (x_2 - a_2)F, \ldots, (x_n - a_n)F$ are all members of M, while F is not, M contains a relevant simple module whose spread is the point $P(a_1, a_2, \ldots, a_n)$; for $M/P \neq M$.*

Example. The module $M = (x_1^3, x_2^3, \overline{x_1^2 + x_2^2}\, x_4 + x_1 x_2 x_3)$ has a relevant simple module at the origin; for $x_i x_1^2 x_2^2$ is a member of $M\,(i = 1, 2, 3, 4)$, but $x_1^2 x_2^2$ is not. The simplest corresponding imbedded primary module, not contained in the L.C.M. of all the other relevant primary modules of M, is (x_1^3, x_2^3, x_3, x_4); cf. Ex. iii, § 17. This example shows that *it is possible for a mixed module M to contain a relevant primary module of higher rank than the number of members in a basis of M.* For the rank of (x_1^3, x_2^3, x_3, x_4) is 4.

If M is an H-module not having a relevant simple module at the origin the variables can be subjected to such a linear homogeneous substitution that x_n will not contain any relevant spread of M, and we shall then have $M/(x_n) = M$, and M will be equivalent to $M_{x_n=1}$ (§ 38). *Thus the only condition (remaining permanent under a linear substitution) that an H-module M may be equivalent to the module $M_{x_n=1}$ is that M should not contain a relevant simple module.*

A simple H-module M is not equivalent to $M_{x_n=1}$; in fact $M_{x_n=1}$ is in this case the module (1).

If M' contains any relevant spread of M then $M/M' \neq M$. Let $M = [Q_1, Q_2, \ldots, Q_k]$, and let M' contain the spread of Q_i. Then some power M'^{γ} of M' contains Q_i (§ 32), and $Q_i/M'^{\gamma} = (1)$. Hence the spread of Q_i is not a relevant spread of

$$M/M'^{\gamma} = [Q_1/M'^{\gamma}, Q_2/M'^{\gamma}, \ldots, Q_k/M'^{\gamma}], \text{ § 28};$$

and consequently $M/M'^{\gamma} \neq M$. Hence also $M/M' \neq M$; for if $M/M' = M$ then $M/M'^{\gamma} = M$.

It follows that if $M/M' = M$ then M' does not contain any relevant spread of M. If M_0 is the H-module equivalent to M we know that $M_0/(x_0) = M_0$ (§ 38); hence x_0 does not contain any relevant spread of M_0, i.e. *no module has a relevant spread at infinity.*

If M, M' are any two modules such that M resolves into isolated primary modules only, viz. $Q_1, Q_2, \ldots, Q_k$, and (M, M') into primary modules $Q_1', Q_2', \ldots, Q_l'$, of which $Q_1', Q_2', \ldots, Q_k'$ have the same spreads as $Q_1, Q_2, \ldots, Q_k$ respectively, then

$$M/M' = [Q_1/Q_1', Q_2/Q_2', \ldots, Q_k/Q_k'].$$

The spread of (M, M') is contained in the spread of M; and it is to be understood that if (M, M') does not contain the spread of Q_i, then $Q_i' = (1)$. The spreads of $Q'_{k+1}, \ldots, Q_l'$ are contained in those of $Q_1, Q_2, \ldots, Q_k$, but do not contain any of the latter. Now we have

$$M/M' = M/(M, M') = [Q_1, Q_2, \ldots, Q_k]/[Q_1', Q_2', \ldots, Q_l'].$$

Hence the theorem follows, by the second part of § 28, provided

$$Q_i/[Q_1', Q_2', \ldots, Q_l'] = Q_i/Q_i'.$$

This is true; for Q_i/Q_i' contains $Q_i/[Q_1', Q_2', \ldots, Q_l']$, since $[Q_1', Q_2', \ldots, Q_l']$ contains Q_i', and, for a similar reason, $Q_i/[Q_1', Q_2', \ldots, Q_l']$ contains $Q_i/Q_1'Q_2'\ldots Q_l'$ or Q_i/Q_i'.

43. *If a module M of rank r is regarded as a module $M^{(s)}$ in s variables $x_1, x_2, \ldots, x_s$, while $x_{s+1}, \ldots, x_n$ are regarded as parameters; and if $F^{(s)}$ is a whole member of $M^{(s)}$, that is, a whole function of the parameters as well as of the variables, then $F^{(s)}$, regarded as a polynomial in $x_1, x_2, \ldots, x_n$, contains all the relevant primary modules of M of rank $\leqslant s$; and conversely, any polynomial which contains all these primary modules is a member of $M^{(s)}$. The most important case is that in which $s = r$.*

In other words, to treat a module M as a module in s variables has the sole effect of eliminating all the primary modules of M of rank $> s$; and when $s < r$ it reduces M to the module (1).

Let $M = (F_1, F_2, \ldots, F_k)$; then $F^{(s)} = A_1F_1 + A_2F_2 + \ldots + A_kF_k$, where $A_1, A_2, \ldots, A_k$ are whole functions of $x_1, x_2, \ldots, x_s$ and rational functions of $x_{s+1}, \ldots, x_n$, with a common denominator $D^{(s)}$. Hence $D^{(s)}F^{(s)} = 0 \bmod M$, and $F^{(s)}$ contains all the primary modules of M of rank $\leqslant s$, since $D^{(s)}$ does not contain any of their spreads.

Conversely, if $F^{(s)}$ contains all the primary modules of M of rank $\leqslant s$, and $D^{(s)}$, a whole function of $x_{s+1}, \ldots, x_n$ only, contains all the primary modules of M of rank $> s$, then $D^{(s)}F^{(s)} = 0 \bmod M$, and $F^{(s)} = 0 \bmod M^{(s)}$, since $D^{(s)}$ in respect to $M^{(s)}$ does not involve the variables.

The module $M^{(r)}$ resolves into simple modules, any primary module of M of rank r and order d contributing d simple modules to $M^{(r)}$. By finding these simple modules we are able to find the primary modules of M of rank r; and this completely resolves M if M is unmixed.

44. *If M is a module of rank $r < n$ and no-one of the modules M, $(M, x_n - a_n)$, $(M, x_{n-1} - a_{n-1}, x_n - a_n)$, ... $(M, x_{r+2} - a_{r+2}, ..., x_n - a_n)$ contains a relevant simple module ($a_{r+2}, ..., a_n$ having non-special values) then M is unmixed. In the contrary case M is mixed.*

This theorem will be used later for proving that certain modules are unmixed. We shall prove first that if M is mixed and does not contain a relevant simple module then $(M, x_n - a_n)$ is mixed. Let M' be the prime module determined by a relevant spread of M of rank $> r$ and $< n$, since M is mixed and has no relevant spread of rank n. To prove that $(M, x_n - a_n)$ is mixed it is sufficient to show that $(M', x_n - a_n)$ contains a relevant spread of $(M, x_n - a_n)$.

Suppose this is not the case; then (§ 42)

$$(M, x_n - a_n)/(M', x_n - a_n) = (M, x_n - a_n),$$

i.e.
$$(M, x_n - a_n)/M' = (M, x_n - a_n),$$

and therefore M/M' contains $(M, x_n - a_n)$. Let F be any member of M/M' and $(F_1, F_2, ..., F_k)$ a basis of M; then

$$F = A_1F_1 + ... + A_kF_k \bmod (x_n - a_n),$$

i.e.
$$F_{x_n=a_n} = (A_1F_1 + ... + A_kF_k)_{x_n=a_n}.$$

Here we may regard a_n as a parameter replacing x_n. Hence F is a member of M regarded as a module in $n-1$ variables, and therefore contains all the primary modules of M of rank $\leqslant n-1$ (§ 43); i.e. $F = 0 \bmod M$. Hence M/M' contains M, which is not true. It follows that $(M, x_n - a_n)$ is mixed in general, i.e. if a_n has a non-special value. By the same reasoning, if $(M, x_n - a_n)$ does not contain a relevant simple module, $(M, x_{n-1} - a_{n-1}, x_n - a_n)$ is mixed, and so on. Finally if $(M, x_{r+2} - a_{r+2}, ..., x_n - a_n)$ is mixed it must contain a relevant simple module since it is of rank $n-1$. Hence if M is mixed one of the above modules contains a relevant simple module. It follows that if no-one of the modules contains a relevant simple module, then M is unmixed.

Conversely if one of the above modules contains a relevant simple module (or more generally if one is mixed) then M is mixed. Suppose for instance that $(M, x_n - a_n)$ is mixed. Then since $(M, x_n - a_n)$ is of rank $r+1$ it has a relevant spread of rank $\geqslant r+2$. Hence there is a whole function ϕ of $x_{r+1}, \cdots, x_{n-1}$ only containing this spread, and a polynomial F in $x_1, x_2, \ldots, x_n$ such that

$$\phi F = 0 \bmod (M, x_n - a_n), \text{ while } F \neq 0 \bmod (M, x_n - a_n).$$

Let $(F_1, F_2, \ldots, F_k)$ be a basis of M. Then

$$\phi F = A_1 F_1 + \ldots + A_k F_k \bmod (x_n - a_n),$$

where we may assume that F, ϕ, $A_1, \ldots, A_k$ are whole functions of a_n as well as of $x_1, x_2, \ldots x_n$. Putting $x_n = a_n$,

$$(\phi F)_{x_n = a_n} = (A_1 F_1 + \ldots + A_k F_k)_{x_n = a_n}.$$

In this we can replace a_n by x_n, and we then have

$$(\phi F)_{a_n = x_n} = 0 \bmod M.$$

But $\phi_{a_n = x_n}$ is a whole function of $x_{r+1}, \ldots, x_n$ only, and $F_{a_n = x_n} \neq 0 \bmod M$, since $F \neq 0 \bmod (M, x_n - a_n)$. Hence M is mixed. This completes the proof of the theorem.

If M is unmixed all the modules are unmixed; nevertheless *if* $a_{r+2}, \ldots, a_n$ *have special values, some of the modules may be mixed notwithstanding that M is unmixed.*

Example. The module

$$M = (u_0 u_4 - u_1 u_3,\ u_1^3 - u_0^2 u_3,\ u_3^3 - u_1 u_4^2,\ u_1^2 u_4 - u_0 u_3^2)$$

is prime and of rank 2 $\left(\text{its spread being given by } \dfrac{u_0}{\lambda^0} = \dfrac{u_1}{\lambda^1} = \dfrac{u_3}{\lambda^3} = \dfrac{u_4}{\lambda^4}\right)$ while the module $(M, c_4 u_0 + c_3 u_1 + c_1 u_3 + c_0 u_4)$ is of rank 3 and mixed. For the latter has $u_0 F$, $u_1 F$, $u_3 F$, $u_4 F$ as members, where

$$F = c_4 u_1^2 + c_3 u_0 u_3 + c_1 u_1 u_4 + c_0 u_3^2 \neq 0 \bmod (M, c_4 u_0 + c_3 u_1 + c_1 u_3 + c_0 u_4).$$

Hence if u_0, u_1, u_3, u_4 are linear functions of x_1, x_2, x_3, x_4 and (a_1, a_2, a_3, a_4) their common point, the module $(M, x_4 - a_4)$ is mixed notwithstanding that M is unmixed (cf. § 89, end).

45. *If M contains a relevant simple module at the point $(a_1, a_2, \ldots, a_n)$ then $(M, x_n - a_n)$ contains a relevant simple module at the same point.*

Let $u, u', u'', \ldots$ be linear functions of $x_1, x_2, \ldots, x_n$ containing the point $(a_1, a_2, \ldots, a_n)$ and no other relevant spread of M. Suppose that $(M, x_n - a_n)$ does not contain a relevant simple module at $(a_1, a_2, \ldots, a_n)$; then it may be assumed that (M, u), (M, u'), (M, u''),... do not either. Let F be a polynomial such that $uF = 0 \bmod M$ and $F \neq 0 \bmod M$.

Then $\qquad uF = 0 \bmod (M, u'),$

therefore $\qquad F = 0 \bmod (M, u') = u'F' \bmod M,$

therefore $\qquad uu'F' = 0 \bmod M = 0 \bmod (M, u''),$

therefore $\qquad F' = 0 \bmod (M, u'') = u''F'' \bmod M,$

and $\qquad F = u'u''F'' \bmod M.$

Similarly $\qquad F = u'u'' \ldots u^{(l)} F^{(l)} \bmod M.$

Now l can be chosen so great that $u'u''...u^{(l)}$ contains the relevant simple module of M at $(a_1, a_2, ..., a_n)$; and since F contains all the other relevant primary modules of M we have $F=0 \bmod M$, which is not true. Hence $(M, x_n - a_n)$ does contain a relevant simple module at the point $(a_1, a_2, ..., a_n)$.

46. The Hilbert-Netto Theorem (H_1, Ne). *If M' is any module containing the spread of a given module M some finite power of M' contains M.*

For M' contains all the relevant spreads of M and some finite power of M' contains all the relevant primary modules of M (§ 32) and therefore contains M.

The theorem is proved in (Ne) for the case of two variables and in (H_1) for the general case.

47. *Definition.* A module of rank r having a basis consisting of r members only is called a *module of the principal class* (Kr, p. 80). Hence a module $(F_1, F_2, ..., F_r)$ of rank r is of the principal class.

It is possible for the resultant of a module of the principal class to vanish identically. An example is given at the end of § 12.

The H-module equivalent to a given module of the principal class is not necessarily of the principal class, e.g. the H-module equivalent to $(x_1^2, x_2 + x_1 x_3)$ has four members in its basis $(x_1^2, x_1 x_2, x_2^2, x_2 x_0 + x_1 x_3)$, § 38.

A proper module is of rank $\leqslant n$ and $\geqslant 1$.

A proper module with a basis consisting of r members is of rank $\leqslant r$ (cf. ex. § 42); for the module contains some point P in the finite region and a spread of dimensions $n-r$ at least through any such point. Nevertheless a module with a basis of two or more members may be the non-proper module (1); e.g. $(F, 1+F)=(1)$.

The unit module is sometimes said to be of rank $n+1$; but it is better to say that it is without rank, and that no module is of rank $> n$. In the absolute theory a module can be of rank $n+1$.

If $(F_1, F_2, ..., F_r)$ is of rank r it does not necessarily follow that $(F_2, F_3, ..., F_r)$ is of rank $r-1$. Thus $(f, f_1 + ff_1, f_2 + ff_2)$ is the same as (f, f_1, f_2), and can be of rank 3, while $(f_1 + ff_1, f_2 + ff_2)$ contains $(1+f)$ and is of rank 1. If however the series $F_1, F_2, ..., F_r$ is suitably modified beforehand (§ 37) then $(F_{s+1}, ..., F_r)$ will be of rank $r-s$ if $(F_1, F_2, ..., F_r)$ is of rank r. It will be sufficient to prove that $(F_2 + a_2 F_1, F_3 + a_3 F_1, ..., F_r + a_r F_1)$ is of rank $r-1$ when $a_2, a_3, ..., a_r$

are (at first) undetermined constants. If it is of rank $s < r-1$ then the module $(\phi_1, \phi_2, \ldots, \phi_s)$ is of rank s, where

$$\begin{aligned}\phi_i &= \lambda_{i2}(F_2 + a_2F_1) + \lambda_{i3}(F_3 + a_3F_1) + \ldots + \lambda_{ir}(F_r + a_rF_1)\\ &= \lambda_{i1}F_1 + \lambda_{i2}F_2 + \ldots + \lambda_{ir}F_r\end{aligned}$$

$$(\lambda_{i1} = \lambda_{i2}a_2 + \lambda_{i3}a_3 + \ldots + \lambda_{ir}a_r, \quad i = 1, 2, \ldots, s),$$

and the λ_{ij} are all arbitrary constants. We may regard the s relations $\lambda_{i1} = \lambda_{i2}a_2 + \ldots + \lambda_{ir}a_r$ as determining the s constants $a_2, a_3, \ldots, a_{s+1}$, leaving at least a_r $(s+1 \leqslant r-1)$ quite arbitrary, whatever the values of the λ_{ij} are. Now some spread of $(\phi_1, \phi_2, \ldots, \phi_s)$ of rank s is a spread of $(F_2 + a_2F_1, \ldots, F_r + a_rF_1)$ and is contained in $F_r + a_rF_1$, and therefore in F_1 (since a_r is independent of the λ_{ij}), and in each of $F_2, F_3, \ldots, F_r$. This would make $(F_1, F_2, \ldots, F_r)$ of rank s, which is not the case.

Unmixed Modules

48. A useful test as to whether a given module is mixed or unmixed is proved in § 44.

Theorem. *A module of the principal class is unmixed.* Lasker proves this for H-modules (L, p. 58). The following is a general proof.

It is clear that any module of rank n is unmixed, since it resolves into primary modules which are all of rank n. Also a module of the principal class of rank 1 is unmixed. Hence the theorem is true for two variables, since in this case the module can only be of rank 1 or 2. We shall assume the theorem true for $n-1$ variables and prove it for n variables. We also assume that the members of the basis have been modified if necessary so that, when $(F_1, F_2, \ldots, F_r)$ is of rank r, $(F_2, F_3, \ldots, F_r)$ is of rank $r-1$ (§ 47).

We prove first that a module $M = (F_1, F_2, \ldots, F_r)$ of rank $r < n$ cannot contain any relevant simple module by showing that $(x_n - c_n)F = 0 \bmod M$ requires $F = 0 \bmod M$ no matter what value, special or otherwise, c_n may have.

Let $$(x_n - c_n)F = X_1F_1 + X_2F_2 + \ldots + X_rF_r;$$
then $$(X_1F_1 + X_2F_2 + \ldots + X_rF_r)_{x_n=c_n} = 0,$$
and $$(X_1F_1)_{x_n=c_n} = 0 \bmod (F_2, F_3, \ldots, F_r)_{x_n=c_n}.$$
But $(F_2, F_3, \ldots, F_r)_{x_n=c_n}$ is a module of rank $r-1$ in $n-1$ variables, so that (by the assumption) all its relevant spreads are of rank $r-1$, and $(F_1)_{x_n=c_n}$ does not contain any of them. Hence

$$(X_1)_{x_n=c_n} = 0 \bmod (F_2, F_3, \ldots, F_r)_{x_n=c_n},$$
i.e. $$X_1 = X_{12}F_2 + X_{13}F_3 + \ldots + X_{1r}F_r + (x_n - c_n)Y_1.$$

Substituting this value for X_1 in the equation

$$(X_1F_1+X_2F_2+\ldots+X_rF_r)_{x_n=c_n}=0,$$

we have $\{(X_2+X_{12}F_1)F_2+\ldots+(X_r+X_{1r}F_1)F_r\}_{x_n=c_n}=0.$

Hence, by the same reasoning as before,

$$X_2+X_{12}F_1=X_{23}F_3+\ldots+X_{2r}F_r+(x_n-c_n)Y_2,$$
$$X_3+X_{13}F_1+X_{23}F_2=X_{34}F_4+\ldots+X_{3r}F_r+(x_n-c_n)Y_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_r+X_{1r}F_1+X_{2r}F_2+\ldots+X_{r-1,r}F_{r-1}=(x_n-c_n)Y_r.$$

Multiplying these equations by $F_1, F_2, \ldots, F_r$ and adding we have

$$X_1F_1+X_2F_2+\ldots+X_rF_r=(x_n-c_n)(Y_1F_1+Y_2F_2+\ldots+Y_rF_r),$$

all the terms $\Sigma X_{ij}F_iF_j\,(i<j)$ cancelling from both sides. It follows that

$$F=Y_1F_1+Y_2F_2+\ldots+Y_rF_r=0 \bmod M,$$

and that $(F_1, F_2, \ldots, F_r)$ does not contain any relevant simple module.

Now if $(F_1, F_2, \ldots, F_r)$ were mixed then for some value of $s \geqslant r+2$ the module $(F_1, \ldots, F_r, x_s-a_s, \ldots, x_n-a_n)$ would contain a relevant simple module (§ 44); but it does not, because it is of the principal class. Hence $(F_1, F_2, \ldots, F_r)$ is unmixed.

49. Deductions from the theorem. *A basis $(F_1, F_2, \ldots, F_r)$ of a module M of the principal class of rank r is an H-basis of M or not, and an H-basis of $M^{(r)}$ or not, according as the H-module determined by the terms of highest degree in $F_1, F_2, \ldots, F_r$ is of rank r or not.*

Let M_0 be the H-module in $x_1, x_2, \ldots, x_n, x_0$ corresponding to the basis $(F_1, F_2, \ldots, F_r)$, so that $(M_0)_{x_0=0}$ is the H-module mentioned in the enunciation. Let $(M_0)_{x_0=0}$ be of rank r. Then it follows by the same reasoning as in the theorem that $x_0F_0=0 \bmod M_0$ requires $F_0=0 \bmod M_0$. Hence M_0 is equivalent to M (§ 38), i.e. $(F_1, F_2, \ldots, F_r)$ is an H-basis of M. It is also an H-basis of $M^{(r)}$. This follows in the same way by considering the H-module $M_0^{(r)}$ in $x_1, x_2, \ldots, x_r, x_0$ corresponding to $(F_1, F_2, \ldots, F_r)$ regarded as a basis of $M^{(r)}$. The module $(M_0^{(r)})_{x_0=0}$ is a simple H-module not involving $x_{r+1}, \ldots, x_n$.

If on the contrary $(M_0)_{x_0=0}$ is not of rank r it is of rank $<r$, and x_0 contains a relevant spread of M_0 of rank $\leqslant r$, so that $M_0/(x_0) \neq M_0$ and M_0 is not equivalent to M (§ 38). Hence $(F_1, F_2, \ldots, F_r)$ is not an H-basis of M or of $M^{(r)}$.

If $(F_1, F_2, \ldots, F_k)$ is an H-basis of a module of rank r the H-module determined by the terms of highest degree in $F_1, F_2, \ldots, F_k$ is of rank r.

But the converse is not true in general when $k>r$; i.e. if the module determined by the terms of highest degree in $F_1, F_2, \ldots, F_k$ is of the same rank r as the module $(F_1, F_2, \ldots, F_k)$ the basis $(F_1, F_2, \ldots, F_k)$ is not in general an H-basis when $k>r$.

50. *Any power of a module of the principal class is unmixed.*

Let the module be $M=(F_1, F_2, \ldots, F_r)$ of rank r. The spread of M^γ is the same as the spread of M. Hence it will be sufficient to show that $AF=0 \bmod M^\gamma$ requires $F=0 \bmod M^\gamma$ provided A does not contain any relevant spread of M. When $\gamma=2$ we have

$$AF=0 \bmod M^2\text{; hence } F=0 \bmod M=A_1F_1+\ldots+A_rF_r,$$

and $A(A_1F_1+\ldots+A_rF_r)=0 \bmod M^2=F_1F^{(1)} \bmod (F_2, \ldots, F_r)^2$,

where
$$F^{(1)}=0 \bmod M.$$

Hence
$$(AA_1-F^{(1)})F_1=0 \bmod (F_2, \ldots, F_r),$$
$$AA_1-F^{(1)}=0 \bmod (F_2, \ldots, F_r),$$
$$AA_1=0 \bmod M, \text{ and } A_1=0 \bmod M.$$

Similarly $A_i=0 \bmod M$, and $F=A_1F_1+\ldots+A_rF_r=0 \bmod M^2$.

Next suppose $\gamma=3$. Then since

$$AF=0 \bmod M^3,$$
$$F=0 \bmod M^2=F_1F^{(1)}+\phi^{(2)},$$

where $F^{(1)}=A_1F_1+\ldots+A_rF_r$, and $\phi^{(2)}=0 \bmod (F_2, \ldots, F_r)^2$.

Now $A(F_1F^{(1)}+\phi^{(2)})=0 \bmod M^3=F_1F^{(2)} \bmod (F_2, \ldots, F_r)^3$,

where
$$F^{(2)}=0 \bmod M^2;$$

hence
$$(AF^{(1)}-F^{(2)})F_1=0 \bmod (F_2, \ldots, F_r)^2,$$
$$AF^{(1)}-F^{(2)}=0 \bmod (F_2, \ldots, F_r)^2,$$
$$F^{(1)}=0 \bmod M^2.$$

Thus every coefficient A_i in $F^{(1)}\,(=A_1F_1+\ldots+A_rF_r)$ is a member of M (as proved when $\gamma=2$), i.e. every coefficient of the terms of $F=F_1F^{(1)}+\phi^{(2)}$ furnished by $F_1F^{(1)}$ is a member of M; and the same must therefore be true of the terms of F furnished by $\phi^{(2)}$. Hence

$$F=0 \bmod M^3.$$

Similarly, if $AF=0 \bmod M^\gamma$, and the theorem is assumed true for $M^{\gamma-1}$ we have $F=0 \bmod M^{\gamma-1}=F_1F^{(\gamma-2)}+\phi^{(\gamma-1)}$, and can prove that every coefficient in $F^{(\gamma-2)}$ and $\phi^{(\gamma-1)}$ is a member of M. Hence

$$F=0 \bmod M^\gamma.$$

51. *If M is a module of the principal class which resolves into prime modules the module whose members consist of all polynomials having a γ-point at every point of M is the module M^γ.*

The theorem is true when $\gamma = 1$. We shall prove it for M^γ assuming it for $M^{\gamma-1}$. Let $M = (F_1, F_2, \ldots, F_r)$ be of rank r and let $F^{(\gamma)}$ be any polynomial with a γ-point at every point of M.

Then
$$F^{(\gamma)} = 0 \bmod M^{\gamma-1},$$

i.e. $F^{(\gamma)} = \Sigma A_{p_1, p_2, \ldots, p_r} F_1^{p_1} F_2^{p_2} \ldots F_r^{p_r}$, where $p_1 + p_2 + \ldots + p_r = \gamma - 1$. Take $\xi_1, \xi_2, \ldots, \xi_n$ for the variables instead of $x_1, x_2, \ldots, x_n$, and move the origin to any point $(x_1, x_2, \ldots, x_n)$ of M. Then F_1 becomes

$$F_1(\xi_1 + x_1, \ldots, \xi_n + x_n) = \xi_1 \frac{\partial F_1}{\partial x_1} + \ldots + \xi_n \frac{\partial F_1}{\partial x_n} + \tfrac{1}{2}\xi_1^2 \frac{\partial^2 F_1}{\partial x_1^2} + \ldots,$$

and the terms of lowest degree in $F^{(\gamma)}$ are

$$\Sigma A_{p_1, p_2, \ldots, p_r} \left(\xi_1 \frac{\partial F_1}{\partial x_1} + \ldots + \xi_n \frac{\partial F_1}{\partial x_n}\right)^{p_1} \ldots \left(\xi_1 \frac{\partial F_r}{\partial x_1} + \ldots + \xi_n \frac{\partial F_r}{\partial x_n}\right)^{p_r},$$

where $A_{p_1, p_2, \ldots, p_r}$ have their original values as functions of $x_1, x_2, \ldots, x_n$. This last expression is of degree $\gamma - 1$ in $\xi_1, \xi_2, \ldots, \xi_n$ and must vanish identically, since $F^{(\gamma)}$ has a γ-point at every point of M. Now the r quantities $\xi_1 \frac{\partial F_i}{\partial x_1} + \ldots + \xi_n \frac{\partial F_i}{\partial x_n}$ $(i = 1, 2, \ldots, r)$ are either capable of taking any r values ($\xi_1, \ldots, \xi_n$ being undetermined quantities and $x_1, \ldots, x_n$ fixed quantities) or they are not. If they are, every $A_{p_1, p_2, \ldots, p_r}$ vanishes. If they are not, every determinant of the matrix

$$\left|\begin{array}{cccc} \frac{\partial F_1}{\partial x_1} & \frac{\partial F_1}{\partial x_2} & \ldots & \frac{\partial F_1}{\partial x_n} \\ \multicolumn{4}{c}{\ldots\ldots\ldots\ldots\ldots\ldots} \\ \frac{\partial F_r}{\partial x_1} & \frac{\partial F_r}{\partial x_2} & \ldots & \frac{\partial F_r}{\partial x_n} \end{array}\right|$$

vanishes, i.e. $(x_1, x_2, \ldots, x_n)$ is a singular point of M (§ 29). Hence every $A_{p_1, p_2, \ldots, p_r}$ vanishes for every non-singular point of M and is therefore a member of M (§ 22). Hence $F^{(\gamma)} = 0 \bmod M^\gamma$, which proves the theorem.

52. *Definition.* The module whose basis consists of all the determinants of the matrix

$$\left|\begin{array}{cccc} u_1, & u_2, & \ldots, & u_k \\ v_1, & v_2, & \ldots, & v_k \\ \multicolumn{4}{c}{\ldots\ldots\ldots\ldots\ldots\ldots} \end{array}\right|,$$

where the elements $u, v, w, \ldots$ are polynomials, will be denoted by

$$\begin{pmatrix} u_1, & u_2, & \ldots, & u_k \\ v_1, & v_2, & \ldots, & v_k \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

This is only an extension of the notation $(F_1, F_2, \ldots, F_k)$ for a module M.

If M_1 is a prime module of rank r, and $F_1, F_2, \ldots, F_r$ any r members of M_1 such that $M = (F_1, F_2, \ldots, F_r)$ resolves into M_1 and a second prime module M_1' of rank r, then it may happen that M_1' must have a certain fixed spread in common with M_1 irrespective of the choice of $F_1, F_2, \ldots, F_r$. Such a spread (if any exists) must be a singular spread of M_1; but it does not necessarily follow from M_1 having a singular spread that M_1' must contain the spread; it depends on the nature of the singularity. *If M_1' does not cut M_1 in a fixed spread then M_1^γ is unmixed, and is the module whose members consist of all polynomials having a γ-point at every point of M_1. In the contrary case some power M_1^γ of M_1 will be mixed and will have the fixed spread in which M_1' cuts it as a relevant imbedded spread, while polynomials $F^{(\gamma)}$ having a γ-point at every point of M_1, but not members of M_1^γ, will exist.*

Example i. The square of the prime module M_1 determined by an irreducible curve in space of three dimensions having a triple* point, the tangents at which do not lie in one plane, is mixed; and there is consequently a surface having a 2-point at every point of the curve which is not a member of M_1^2.

Thus if

$$M_1 = \begin{pmatrix} x_1, & x_2, & x_3 \\ x_2, & x_3, & x_1^2 \end{pmatrix} = (x_1x_3 - x_2^2,\ x_2x_3 - x_1^3,\ x_3^2 - x_1^2x_2),$$

the surface $(x_2x_3 - x_1^3)^2 - (x_2^2 - x_1x_3)(x_3^2 - x_1^2x_2)$, after removal of the factor x_1, will have a 2-point at every point of M_1, but is not a member of M_1^2; for the surface has only a 3-point at the origin, whereas every member of M_1^2 has a 4-point.

Example ii. If $M_1 = \begin{pmatrix} u_1, & u_2, & u_3, & u_4 \\ v_1, & v_2, & v_3, & v_4 \\ w_1, & w_2, & w_3, & w_4 \end{pmatrix} = (F_1, F_2, F_3, F_4),$

* A triple point is not a 3-point. The general member of M_1 has only a 2-point at the triple point of the curve.

It is evident that the module whose members consist of all polynomials having a γ-point at every point of a given irreducible spread is primary and unmixed.

where each u, v, w is a homogeneous linear function of x_1, x_2, x_3, x_4, M_1 being a prime module of rank 2, we have

$$u_1F_1 + u_2F_2 + u_3F_3 + u_4F_4 = 0,$$

and two other similar identities. From these we can find the continued ratio $x_1 : x_2 : x_3 : x_4$ as the ratio of four members of M_1^3 by expressing each u, v, w in full. The common factor of these four members is a polynomial of degree 8 having a 3-point at every point of M_1, but not a member of M_1^3. In this example M_1^3 is mixed while M_1^2 is unmixed.

53. Theorem. *The module with a basis of r rows and k columns*

$$M = \begin{pmatrix} u_1, & u_2, & \dots, & u_k \\ v_1, & v_2, & \dots, & v_k \\ w_1, & w_2, & \dots, & w_k \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

is of rank $\leqslant k-r+1$ $(0 < k-r+1 \leqslant n)$, and if of rank $k-r+1$ is unmixed.

Also if $D_{p_1, p_2, \dots, p_r}$ denotes the determinant formed by the p_1^{th}, p_2^{th}, ..., p_r^{th} columns of the basis, the general solution of the equation

$$\Sigma D_{p_1, p_2, \dots, p_r} X_{p_1, p_2, \dots, p_r} = 0 \quad (p_1, p_2, \dots, p_r = 1, 2, \dots, k)$$

is
$$X_{p_1, p_2, \dots, p_r} = \sum_{p=1}^{p=k} U_{p_1, \dots, p_r, p}\, u_p + \sum_{p=1}^{p=k} V_{p_1, p_2, \dots, p_r, p}\, v_p + \dots,$$

where $U_{p_1, \dots, p_r, p}$, $V_{p_1, \dots, p_r, p}$, ... are arbitrary polynomials subject with the unknowns $X_{p_1, p_2, \dots, p_r}$ to the same law of signs as the determinants $D_{p_1, p_2, \dots, p_r}$, viz. each $X_{p_1, p_2, \dots, p_r}$, $U_{p_1, p_2, \dots, p_r, p}$, ... changes in sign (but not in magnitude) for each interchange of any pair of suffixes p_1, ..., p_r, p.

These two theorems will be proved together by a double process of induction. Assuming both theorems for $r-1$ rows and $k-1$ columns, and also for r rows and $k-1$ columns, we prove both theorems for r rows and k columns. Both theorems have been proved for $r=1$ in § 48.

It is understood that M is a proper module, i.e. the determinants of its basis all vanish for some point whose coordinates are finite, but do not all vanish identically. After proving that M is of rank $\leqslant k-r+1$ we assume that if M is of rank $k-r+1$ the module

$$\begin{pmatrix} u_2 + a_2u_1, & u_3 + a_3u_1, & \dots, & u_k + a_ku_1 \\ v_2 + a_2v_1, & v_3 + a_3v_1, & \dots, & v_k + a_kv_1 \\ \dots & \dots & \dots & \dots \end{pmatrix},$$

where a_2, a_3, ..., a_k are suitably chosen constants or polynomials, is of rank $k-r$. This can be proved in a similar way to the corresponding property in § 47. We shall also suppose the matrix to have been so modified beforehand that if the first $s \leqslant k-r$ columns are removed the rank diminishes by s. It can be shown that the second part of the theorem is true before modification if it is true after. The same is true of the first part of the theorem, since the modification of the basis does not alter the module.

The general proof will be sufficiently indicated if we suppose M to have 3 rows and 5 columns. Then

$$M = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 \\ v_1 & v_2 & v_3 & v_4 & v_5 \\ w_1 & w_2 & w_3 & w_4 & w_5 \end{pmatrix}$$

and we assume both parts of the theorem for the module

$$M_1 = \begin{pmatrix} u_2 & u_3 & u_4 & u_5 \\ v_2 & v_3 & v_4 & v_5 \\ w_2 & w_3 & w_4 & w_5 \end{pmatrix}$$

and also for $$M_1' = \begin{pmatrix} u_2 & u_3 & u_4 & u_5 \\ v_2 & v_3 & v_4 & v_5 \end{pmatrix}.$$

If A, B, C are the determinants of the matrix formed by the last two columns of the basis of M, we have

$$Au_i + Bv_i + Cw_i = D_{i45} \quad (i = 1, 2, 3, 4, 5).$$

Giving to i the values p_1, p_2, p_3 and solving for C (or D_{45}) we have

$$D_{45} D_{p_1 p_2 p_3} = D_{p_2 p_3} D_{p_1 45} + D_{p_3 p_1} D_{p_2 45} + D_{p_1 p_2} D_{p_3 45},$$

where $D_{p_1 p_2}$ denotes the determinant $\begin{vmatrix} u_{p_1} & u_{p_2} \\ v_{p_1} & v_{p_2} \end{vmatrix}$. This shows that every determinant $D_{p_1 p_2 p_3}$ when multiplied by D_{45} is of the form $X_1 D_{145} + X_2 D_{245} + X_3 D_{345}$. Hence if there is a point of the module M for which D_{45} does not vanish the module must have a spread of rank $\leqslant 3$ (or $k-r+1$) through that point. If however D_{45} contains the whole of the spread of M we move the origin to a point of the spread and modify the last row of the basis by the other rows so as to make the constant terms in the elements of the last row all zero. After doing this we change u_4, u_5, v_4, v_5 in the first two rows only to $u_4 + a$, $u_5 + b$, $v_4 + c$, $v_5 + d$, where a, b, c, d are constants. We thus get a new module containing the origin such that the new D_{45} does not contain the origin. This new module has a spread of rank $\leqslant 3$ through the origin; and since this is true for general values of a, b, c, d, it is still true when we put $a = b = c = d = 0$; for no diminution in the dimensions of the spread through the origin, i.e. no increase in the rank, could be produced by giving special values to a, b, c, d. Hence M is of rank $\leqslant 3$; and we have to prove that M is unmixed if its rank is 3.

Consider the equation $\Sigma D_{p_1p_2p_3}X_{p_1p_2p_3}=0$ in which we suppose $p_1<p_2<p_3$, so that each term occurs once and once only. Multiplying by D_{45} we have

$$\Sigma\,(D_{p_2p_3}D_{p_145}+D_{p_3p_1}D_{p_245}+D_{p_1p_2}D_{p_345})\,X_{p_1p_2p_3}=0.$$

In this the terms containing D_{145} are obtained by putting $p_1=1$ and giving p_2, p_3 the values (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5), viz. $D_{145}(D_{23}X_{123}+D_{24}X_{124}+D_{25}X_{125}+D_{34}X_{134}+D_{35}X_{135}+D_{45}X_{145})$, and this is a member of (D_{245}, D_{345}) and therefore of M_1. But M_1 is unmixed and of rank 2, and D_{145} does not contain any of its relevant spreads; for if, after modification of the last two columns of M_1 by the first two, D_{145} contains a relevant spread of M_1 then every $D_{1p_2p_3}$ contains the same spread, and consequently M contains the spread and is of rank 2, which is contrary to the data. Hence

$$\begin{aligned}\Sigma D_{p_2p_3}X_{1p_2p_3}&=0 \bmod M_1\\ &=D_{234}W'_{234}+D_{235}W'_{235}+D_{245}W'_{245}+D_{345}W'_{345}\\ &=(D_{34}w_2+D_{42}w_3+D_{23}w_4)\,W'_{234}+\dots\\ &=D_{23}(w_4W'_{234}+w_5W'_{235})+\dots\\ &=\Sigma D_{p_2p_3}(W'_{p_2p_32}w_2+W'_{p_2p_33}w_3+W'_{p_2p_34}w_4+W'_{p_2p_35}w_5);\end{aligned}$$

or
$$\Sigma D_{p_2p_3}X_{p_2p_3}=0 \quad (p_2<p_3=2,\,3,\,4,\,5),$$
where
$$X_{p_2p_3}=X_{1p_2p_3}-\sum_p W'_{p_2p_3p}\,w_p \quad (p=2,\,3,\,4,\,5).$$

The equation $\Sigma D_{p_2p_3}X_{p_2p_3}=0$ stands in the same relation to M_1' as $\Sigma D_{p_1p_2p_3}X_{p_1p_2p_3}=0$ to M, and the general solution is

$$X_{p_2p_3}=\sum_p U'_{p_2p_3p}\,u_p+\sum_p V'_{p_2p_3p}\,v_p \quad (p=2,\,3,\,4,\,5)$$

which gives

$$X_{1p_2p_3}=\sum_p U'_{p_2p_3p}\,u_p+\sum_p V'_{p_2p_3p}\,v_p+\sum_p W'_{p_2p_3p}\,w_p \quad (p=2,\,3,\,4,\,5).$$

Substituting these values for $X_{1p_2p_3}$ in the equation

$$\Sigma D_{p_1p_2p_3}X_{p_1p_2p_3}=0$$

it becomes, after simplifying,

$$D_{234}(X_{234}+U'_{234}u_1+V'_{234}v_1+W'_{234}w_1)+\dots=0,$$

an equation in reference to M_1 of which the solution is

$$X_{234}=-U'_{234}u_1-V'_{234}v_1-W'_{234}w_1+\sum_p U_{234p}\,u_p+\dots+\dots \quad (p=2,\,3,\,4,\,5)$$

and similar expressions for X_{235}, X_{245}, X_{345}. If in these and the expressions found for $X_{1p_2p_3}$ we put

$$-U'_{p_2p_3p}=U_{p_2p_3p1}, \quad -V'_{p_2p_3p}=V_{p_2p_3p1}, \quad -W'_{p_2p_3p}=W_{p_2p_3p1},$$

we have, for all values of $p_1, p_2, p_3 = 1, 2, 3, 4, 5$,

$$X_{p_1p_2p_3} = \sum_p U_{p_1p_2p_3p}\, u_p + \sum_p V_{p_1p_2p_3p}\, v_p + \sum_p W_{p_1p_2p_3p}\, w_p \quad (p = 1, 2, 3, 4, 5),$$

which proves the second part of the theorem for M.

To prove the first part, that M is unmixed, it has to be shown that neither M nor $(M, x_s - a_s, \ldots, x_n - a_n)$ can contain a relevant simple module, where s is any number $\geqslant k - r + 3$ (§ 44). Let

$$(x_1 - c_1) F = 0 \bmod (M, x_s - a_s, \ldots, x_n - a_n)$$

$$= \sum D_{p_1, p_2, \ldots, p_r} X_{p_1, p_2, \ldots, p_r} \bmod (x_s - a_s, \ldots, x_n - a_n).$$

Then $\qquad (\sum D_{p_1, p_2, \ldots, p_r} X_{p_1, p_2, \ldots, p_r})_{x_1 - c_1 = x_s - a_s = \ldots = x_n - a_n = 0} = 0.$

In putting $x_1 - c_1 = x_s - a_s = \ldots = x_n - a_n = 0$ in M the number of variables is diminished but the rank remains equal to $k - r + 1$. Hence

$$(X_{p_1, p_2, \ldots, p_r})_{x_1 - c_1 = \ldots = 0} = (\sum_p U_{p_1, \ldots, p_r, p}\, u_p + \ldots)_{x_1 - c_1 = \ldots = 0};$$

therefore

$$X_{p_1, p_2, \ldots, p_r}$$
$$= \sum_p U_{p_1, \ldots, p_r, p}\, u_p + \ldots + (x_1 - c_1) Y_{p_1, p_2, \ldots, p_r} \bmod (x_s - a_s, \ldots, x_n - a_n),$$

and

$$(x_1 - c_1) F = (x_1 - c_1) \sum D_{p_1, p_2, \ldots, p_r} Y_{p_1, p_2, \ldots, p_r} \bmod (x_s - a_s, \ldots, x_n - a_n).$$

Hence, since $(x_s - a_s, \ldots, x_n - a_n)$ is a module of the principal class, and $x_1 - c_1$ does not contain its spread,

$$F - \sum D_{p_1, p_2, \ldots, p_r} Y_{p_1, p_2, \ldots, p_r} = 0 \bmod (x_s - a_s, \ldots, x_n - a_n),$$

and $\qquad F = 0 \bmod (M, x_s - a_s, \ldots, x_n - a_n).$

Hence $(M, x_s - a_s, \ldots, x_n - a_n)$ cannot contain any relevant simple module, which proves the theorem.

Solution of Homogeneous Linear Equations

54. *Homogeneous linear equations with constants for coefficients.* In a system of r independent equations with constant coefficients for k unknowns $X_1, X_2, \ldots, X_k$ there are r' independent solutions, where $r+r'=k$, and the general solution is expressible in terms of the r' solutions. The array of the coefficients of the r equations and the array of the r' solutions together form a square array

$$\left|\begin{array}{c} a_{11} \quad a_{12} \ldots a_{1k} \\ \ldots\ldots\ldots\ldots \\ a_{r1} \quad a_{r2} \ldots a_{rk} \\ \hline b_{11} \quad b_{12} \ldots b_{1k} \\ \ldots\ldots\ldots\ldots \\ b_{r'1} \quad b_{r'2} \ldots b_{r'k} \end{array}\right|$$

and the general solution is $X_i = \mu_1 b_{1i} + \mu_2 b_{2i} + \ldots + \mu_{r'} b_{r'i}$ $(i=1, 2, \ldots, k)$, where $\mu_1, \mu_2, \ldots, \mu_{r'}$ are arbitrary quantities.

The two arrays are called conjugate arrays; but we shall find it more convenient to call them *inverse* arrays. Their principal properties are :—(i) the sum of the products of the elements in any row of one array with the elements in any row of the other array is zero; (ii) the determinants of one array are proportional to the complementary determinants of the other array with a rule as regards sign; (iii) the determinant of the combined arrays is not zero if the elements are real. We shall not have occasion to use either (ii) or (iii) explicitly.

Homogeneous linear equations with polynomials as coefficients (H, p. 483). Let there be r independent equations, viz.

$$u_1 X_1 + u_2 X_2 + \ldots + u_k X_k = 0,$$

$$v_1 X_1 + v_2 X_2 + \ldots + v_k X_k = 0, \text{ etc.}$$

Then there is an array of solutions

$$\left|\begin{array}{c} f_{11}, f_{12}, \ldots, f_{1k} \\ f_{21}, f_{22}, \ldots, f_{2k} \\ \ldots\ldots\ldots\ldots \\ f_{l1}, f_{l2}, \ldots, f_{lk} \end{array}\right|$$

whose elements are polynomials, such that the general solution is

$$X_i = A_1 f_{1i} + A_2 f_{2i} + \dots + A_l f_{li} \quad (i = 1, 2, \dots, k)$$

where $A_1, A_2, \dots, A_k$ are arbitrary polynomials. The rows of this array are not independent.

The general case of r equations can be reduced to that of solving a single equation. Consider first the single equation

$$F_1 X_1 + F_2 X_2 + \dots + F_k X_k = 0.$$

The conditions imposed by this equation on X_1 are merely that it must be a member of the module $(F_2, F_3, \dots, F_k)/(F_1)$. Let $(f_{11}, f_{21}, \dots, f_{l'1})$ be a basis of this module. Then the general solution for X_1 is

$$X_1 = A_1 f_{11} + A_2 f_{21} + \dots + A_{l'} f_{l'1}.$$

To each separate solution $X_1 = f_{j1}$ there corresponds a solution $f_{j2}, f_{j3}, \dots, f_{jk}$ for $X_2, X_3, \dots, X_k$, giving a row $f_{j1}, f_{j2}, \dots, f_{jk}$ of the array of solutions. The remaining solutions are those for which $X_1 = 0$, when the equation reduces to

$$X_2 F_2 + \dots + X_k F_k = 0.$$

To each solution for $X_2 = f_{j'2}$ $(j' = l' + 1, l' + 2, \dots, l'')$ there corresponds a row $0, f_{j'2}, f_{j'3}, \dots, f_{j'k}$ of the array of solutions in which the first element is zero. Similarly there are rows in which the first two elements are zero, and so on. The method may give more rows altogether than are necessary. Any row of the array which can be modified by the other rows so as to become a row of zeros should be omitted.

In the case of r equations we eliminate $X_1, X_2, \dots, X_{r-1}$, obtaining $D_{1,2,\dots,r} X_r + D_{1,2,\dots,r-1,r+1} X_{r+1} + \dots + D_{1,2,\dots,r-1,k} X_k = 0$, and find the complete solution of this equation by the method just described. To each solution there is a unique set of values for $X_1, X_2, \dots, X_{r-1}$ which are in general polynomials. In an exceptional case the unknowns $X_1, X_2, \dots, X_k$ may be subjected to a linear substitution beforehand.

The principal case. The principal case is that in which the module

$$\begin{pmatrix} u_1 & u_2 & \cdots & u_k \\ v_1 & v_2 & \cdots & v_k \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

is of rank $k - r + 1$. In this case it is seen from the equation in $X_r, X_{r+1}, \dots, X_k$ above that X_k is a member of the module

$$\begin{pmatrix} u_1 & u_2 & \cdots & u_{k-1} \\ v_1 & v_2 & \cdots & v_{k-1} \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

by § 53, and similarly for each unknown. The complete array of solutions is therefore obtained by putting any $k-r-1$ of the unknowns equal to zero and solving for the ratios of the remaining $r+1$ unknowns. The $\dfrac{\lfloor k}{\lfloor r+1 \, \lfloor k-r-1}$ solutions found in this way are of the type

$$X_{p_1} = D_{p_2,\ldots,p_{r+1}},\ X_{p_2} = -D_{p_1,p_3,\ldots,p_{r+1}},\ \ldots\ X_{p_{r+1}} = (-1)^r D_{p_1,p_2,\ldots,p_r},$$
$$X_{p_{r+2}} = \ldots = X_{p_k} = 0,$$

where $p_1, p_2, \ldots, p_k$ is any permutation of $1, 2, \ldots, k$.

Noether's Theorem

55. Noether's "fundamental theorem in algebraic functions" (N) furnishes a remarkably direct method of testing whether a given polynomial is a member of a given module or not; but it only attains complete success in its application to a module of rank n. A variation of the method, depending on the same principle, can be applied successfully to any module known to be primary, when the equations to its spread in the form of § 21 have been found (M, p. 88).

Noether proved that if f, ϕ were any two given polynomials in two variables x_1, x_2, without common factor, then the independent linear equations satisfied identically by the coefficients of the power products of x_1, x_2, in $A'f + B'\phi$, where A', B' are ordinary power series with undetermined coefficients, were finite and determinate; and that any polynomial F whose coefficients satisfied all these identical equations, when the origin was taken successively at each point of (f, ϕ), was a member of (f, ϕ). Thus the conditions which F has to satisfy in order to be a member of (f, ϕ) can be collected locally, so to speak, by going to each point of (f, ϕ) to find them. On going to a point not in (f, ϕ) we get no conditions, for at such a point every polynomial is of the form $A'f + B'\phi$. That the conditions are necessary is evident; for if $F = 0 \bmod (f, \phi)$ then F is of the form $A'f + B'\phi$ wherever the origin is taken.

König (K, p. 385) proved the theorem for the case of a module $(f_1, f_2, \ldots, f_n)$ of rank n in n variables; and Lasker generalized the theorem in the Lasker-Noether theorem given below.

That the theorem is true for any module of rank n (not merely for a module of the principal class of rank n, the case proved by König) follows from the Hilbert-Netto and Lasker theorems. For, by Lasker's theorem, the module is the L.C.M. of a finite number of simple modules $Q_1, Q_2, \ldots, Q_l$; and if γ is the characteristic number of $Q_i = (f_1, f_2, \ldots, f_h)$ and the origin is taken at the point of Q_i, we have

$$F = P_1 f_1 + P_2 f_2 + \ldots + P_h f_h \text{ (where } P_1, P_2, \ldots, P_h \text{ are power series)}$$
$$= X_1 f_1 + X_2 f_2 + \ldots + X_h f_h \bmod O^\gamma = 0 \bmod Q_i.$$

Thus F contains $[Q_1, Q_2, \ldots, Q_l]$.

56. The Lasker-Noether Theorem (L, p. 95). *If*

$$M = (F_1, F_2, \ldots, F_k) \text{ and } F = P_1 F_1 + P_2 F_2 + \ldots + P_k F_k,$$

where $P_1, P_2, \ldots, P_k$ are ordinary power series, there exists a polynomial ϕ not containing the origin such that $F\phi = 0 \bmod M$.

Let $Q_1, Q_2, \ldots, Q_l$ be the relevant primary modules into which M resolves, and let $Q_1, Q_2, \ldots, Q_{l'}$ be those which contain the origin, and $Q_{l'+1}, \ldots, Q_l$ those which do not. Then, assuming the theorem to be true, it follows that

$$F = 0 \bmod [Q_1, Q_2, \ldots, Q_{l'}],$$

since ϕ cannot contain the spread of any of the modules $Q_1, Q_2, \ldots, Q_{l'}$. Conversely if $F = 0 \bmod [Q_1, Q_2, \ldots, Q_{l'}]$ and $\phi = 0 \bmod [Q_{l'+1}, \ldots, Q_l]$, where ϕ does not contain the origin, then $F\phi = 0 \bmod M$. Hence the aggregate of all polynomials F which are of the form

$$P_1 F_1 + P_2 F_2 + \ldots + P_k F_k$$

constitutes the module $[Q_1, Q_2, \ldots, Q_{l'}]$.

Definition. A module which resolves into primary modules all of which contain the origin, such as the module $[Q_1, Q_2, \ldots, Q_{l'}]$ above, will be called a *Noetherian module.*

Thus a Noetherian module, like an H-module, ceases to be such in general when the origin is changed. Moreover an H-module is a particular kind of Noetherian module; for all the primary modules into which an H-module resolves are H-modules and contain the origin.

In order that a polynomial F may be a member of a Noetherian module $(F_1, F_2, \ldots, F_h)$ it is sufficient that F should be of the form $P_1 F_1 + P_2 F_2 + \ldots + P_h F_h$.

Proof of the theorem. It is evident that the theorem is true for a module of rank n or dimensions 0 (§ 55). We shall prove the theorem for a module of dimensions $n - r$ assuming it true for a module of dimensions $n-r-1$. It will be sufficient to prove the theorem for a primary module Q which contains the origin; for it is clear that it will then be true in general.

Let $Q=(f_1, f_2, \ldots, f_h)$, and $f=P_1 f_1+P_2 f_2+\ldots+P_h f_h$,

where $P_1, P_2, \ldots, P_h$ are power series. Let $Q_O=(f_1', f_2', \ldots, f'_{h'})$ be the module whose members consist of all polynomials of the form of f, and Q_P the like module obtained by moving the origin to P (and then back to O). Choose a point P so near to O as to come within the range of convergency of all the power series $P_1, P_2, \ldots, P_h$ for each member f_i' of the basis of Q_O when expressed in the form of f. Then we have $f_i'=0 \bmod Q_P$, i.e. Q_O contains Q_P. But it does not follow that Q_P contains Q_O however near P may be to O; for O might be a special point of the spread of Q. We assume for the present that O is not a special point of the spread; and we choose P to be another point of the spread so near to O that Q_P contains Q_O. Then $Q_O=Q_P$.

Let u be a fixed arbitrarily chosen linear homogeneous polynomial, and f' any member of Q_O. Then

$$f'=0 \bmod Q_O=0 \bmod (Q, u)_O.$$

But (Q, u) is of $n-r-1$ dimensions; hence, assuming the general theorem as regards (Q, u), there exists a polynomial ϕ not containing O such that

$$f'\phi=0 \bmod (Q, u)=pu \bmod Q,$$

where p is a polynomial. Hence, since $f_1', f_2', \ldots, f'_{h'}$ are members of Q_O,

$$f_i'\phi_i=p_i u \bmod Q \quad (i=1, 2, \ldots, h');$$

hence $$p_i u=0 \bmod Q_O=0 \bmod Q_P;$$

but u does not contain P, and $\dfrac{1}{u}$ can be expanded as a power series when P is taken as origin; hence

$$p_i=0 \bmod Q_P=0 \bmod Q_O$$
$$=p_{i1}f_1'+p_{i2}f_2'+\ldots+p_{ih'}f'_{h'}.$$

Hence

$$f_i'\phi_i=(p_{i1}f_1'+p_{i2}f_2'+\ldots+p_{ih'}f'_{h'})\,u \bmod Q \quad (i=1, 2, \ldots, h').$$

Solving these h' equations for $f_1', f_2', \ldots, f'_{h'}$ we have

$$Df_i'=0 \bmod Q,$$

where

$$D = \begin{vmatrix} p_{11}u - \phi_1 & p_{12}u & \dots & p_{1h'}u \\ p_{21}u & p_{22}u - \phi_2 & \dots & p_{2h'}u \\ \dots & \dots & \dots & \dots \\ p_{h'1}u & p_{h'2}u & \dots & p_{h'h'}u - \phi_{h'} \end{vmatrix} = (-1)^{h'} \phi_1 \phi_2 \dots \phi_{h'} \bmod u.$$

Now u contains the origin, but $\phi_1, \phi_2, \dots, \phi_{h'}$ and consequently D do not; i.e. D does not contain the spread of Q. Hence $f_i' = 0 \bmod Q$. Hence Q_O contains Q, i.e., $Q_O = Q$.

This has been proved for a non-special point O of Q. If O is a special point, choose P a non-special point of Q so near to O that Q_O contains Q_P. Then since $Q_P = Q$ we have again $Q_O = Q$.

The above proof only differs from the proof given by Lasker in the part relating to $Q_O = Q_P$. In this part Lasker's proof seems to be faulty.