SOME PROPERTIES OF ENUMERATION IN THE THEORY OF MODULAR SYSTEMS

By F. S. MACAULAY.

[Received 3 March, 1926.—Read 11 March, 1926.]

I. *The general polynomial-ideal.*

The object of this note is to discover the limiting relations which must exist between the terms of the series $D_0, D_1, \ldots, D_l, \ldots$ where D_l is the number of linearly independent homogeneous polynomials of degree l (or of degrees less than or equal to l in the case of non-homogeneous polynomials) belonging to some actual modular system, the system being either perfectly general or else general of its kind. A modular system (or in modern nomenclature a *polynomial-ideal*) is defined to be any aggregate of polynomials in n variables such that the sum of any two, and also the product of any one by a constant* or any of the variables $x_1, x_2, \ldots, x_n$, belongs to the ideal or aggregate.

The converse and more important question is that of finding the actual values of $D_0, D_1, D_2, \ldots$ for a given polynomial-ideal, that is, an ideal defined by the stated conditions which its members individually and collectively have to satisfy. But with few exceptions, some of which will be noted later, no general answer can be found to this converse question. In a classical memoir, Hilbert† has shown that *when l is large enough D_l* becomes a polynomial in l; and Ostrowski‡ has employed Hilbert's process

* The domain of the coefficients is supposed to consist of all elements of a corpus, but restricted in general to rational integral functions of any parameters that may be included. A constant means any element of this domain.

† D. Hilbert, "Über die Theorie der algebraischen Formen", *Math. Annalen*, 36 (1890), 473 *ff.* He shows that the number H_l complementary to D_l is expressed, when l is large enough, by a polynomial in l of degree equal to the number of dimensions of the spread of the ideal. This polynomial $\chi(l)$ will be called the Hilbert function.

‡ A. Ostrowski, "Über ein algebraisches Übertragungsprinzip", *Abh. Math. Seminar d. Hamburgischen Universität*, 1 (1922), Hefte 3 and 4, 281 *ff.*

for expressing in a neat form the generating function $D_0+D_1x+D_2x^2+\ldots$, which, if known, gives the value of D_l for *all*, not merely large, values of l.

Polynomial-ideals are of two kinds: (i) H-ideals, or ideals of homogeneous polynomials, and (ii) non-H-ideals, or ideals of non-homogeneous polynomials. Under (i) we shall specially consider a p.p.-ideal*, that is, an ideal of power products or an ideal of which no polynomial is a member unless each of its terms separately is a member. An H-ideal M is a more general kind of ideal than the non-H-ideal $M(x_n=1)$, owing to the fact that the most important point of the H-ideal, viz. the point $(0, 0, \ldots, 0)$, is obliterated† by putting $x_n=1$. If, however, M and $M(x_n=1)$ have the same D series $D_0, D_1, D_2, \ldots$ they are said to be *equivalent*. To every non-H-ideal in n variables there is an equivalent H-ideal in $n+1$ variables (but not *vice versa*) got simply by making all the members of the non-H-ideal homogeneous by the insertion of an additional variable x_0.

Again, the members of an ideal are of two kinds: (i) *principal* and (ii) *derived*. In an H-ideal, if all the members (principal and derived) of degree l are multiplied by $x_1, x_2, \ldots, x_n$ we get all the derived members of degree $l+1$ (which can be reduced to a linearly independent set); and any other set of members of degree $l+1$, linearly independent of one another and of the derived members, may be taken as principal members of degree $l+1$. By Hilbert's theorem (*loc. cit.*) the total number of linearly independent principal members is finite, *i.e.* any polynomial-ideal M defined as above has a *finite basis* $(F_1, F_2, \ldots, F_k)$ in terms of which any member F of M is linearly expressible, viz. $F=A_1F_1+A_2F_2+\ldots+A_kF_k$, where $A_1, A_2, \ldots, A_k$ are polynomials.

The Hilbert number H_l, complementary to D_l, is the number of independent linear relations satisfied by the coefficients of the general member of the ideal of degree l. The linear relations themselves are called the *ideal-equations for degree* l of the ideal.

It is not seldom convenient to express results in terms of $H_0, H_1, H_2, \ldots$ rather than $D_0, D_1, D_2, \ldots$. This can always be done, since D_l+H_l is the number of p.p.'s of degree l in the case of an H-ideal and the number of p.p.'s of degrees $\leqslant l$ in the case of a non-H-ideal. The generating function of the series $D_0+H_0, D_1+H_1, \ldots$ for an H-ideal is $(1-x)^{-n}$, viz.

$$D_l+H_l=\frac{(l+1)(l+2)\ldots(l+n-1)}{1, 2, \ldots, (n-1)}.$$

* The contraction p.p. for power product will be used throughout the paper.

† On this account the theory of H-ideals is completely mutilated if we pay regard only to the ratios of the variables, thus contrasting with the case of homogeneous coordinates in Geometry.

We shall denote* this number D_l+H_l by $(l+1)_{n-1}$, and regard it as a function of l with n a constant. It is to be noticed that $(l)_n$ is zero when $l=0$, and is 1 when $l=1$; also that $(l)_n$ can be expressed as a binomial coefficient $\binom{l+n-1}{n}$, though this notation is clearly inconvenient since it does not dissociate l from n. We have $D_l+H_l=(l+1)_n$ for a non-H-ideal.

The p.p.'s of degree l can be written in a definite order (which we shall call their *ascending* order) according to the rule that $x_1^{p_1}x_2^{p_2}\dots x_n^{p_n}$ comes before $x_1^{q_1}x_2^{q_2}\dots x_n^{q_n}$ if the first of the indices $p_1, p_2, \dots, p_n$ which differs from the corresponding index in $q_1, q_2, \dots, q_n$ is greater than it. Taking $(x_1, x_2, \dots, x_n)^l$ to stand for all p.p.'s of degree l expanded in ascending order, we have

$$(x_1, \dots, x_n)^l = x_1^l,\ x_1^{l-1}(x_2, \dots, x_n),\ \dots,\ x_1^p(x_2, \dots, x_n)^{l-p},\ \dots,\ (x_2, \dots, x_n)^l,$$

of which the part as far as $x_1^p(x_2, \dots, x_n)^{l-p}$ comprises the p.p.'s $x_1^p(x_1, x_2, \dots, x_n)^{l-p}$. The p.p. $x_1^{p_1}x_2^{p_2}\dots x_r^{p_r}x_n^{p_n}$ $(p_r>0)$ is the last p.p. in $x_1^{p_1}\dots x_r^{p_r}(x_{r+1}, \dots, x_n)^{p_n}$ and is followed by the first p.p. in $x_1^{p_1}\dots x_r^{p_r-1}$ $(x_{r+1}, \dots, x_n)^{p_n+1}$, viz. $x_1^{p_1}\dots x_r^{p_r-1}x_{r+1}^{p_n+1}$. Again $(x_0, x_1, \dots, x_n)^l$ or $(1, x_1, \dots, x_n)^l$ is equal to

$$1,\quad (x_1, \dots, x_n),\quad (x_1, \dots, x_n)^2,\quad \dots,\quad (x_1, x_2, \dots, x_n)^l.$$

Corresponding to any given H-ideal M, after subjecting the variables to a general homogeneous linear substitution, we can deduce two corresponding p.p.-ideals P, P', each of which has the same D series $D_0, D_1, D_2, \dots$ as M. The first, P, is the ideal whose members of any degree l consist of the first D_l p.p.'s in $(x_1, x_2, \dots, x_n)^l$. It will be shown immediately that all the p.p.'s of degree $l+1$ which can be *derived* from the first N p.p.'s in $(x_1, x_2. \dots, x_n)^l$ consist of the first $Q(N)$ p.p.'s in $(x_1, x_2, \dots, x_n)^{l+1}$, where $Q(N)$ is a certain function of N. Hence, in order to prove that the aggregate of p.p.'s P as described above constitutes an ideal, it must be shown that the relation $D_{l+1} \geqslant Q(D_l)$ holds for any H-ideal M. The proof is given in § II of the paper, and its truth will be assumed here.

The second p.p.-ideal, P', is obtained thus: write the D_l members of the H-ideal M of degree l so that their terms are in ascending order, and modify them linearly by means of one another so that no two members begin with the same term. The p.p.'s with which they begin are then the

* We prefer $(l+1)_{n-1}$ to $(l)_{n-1}$ because, in the latter case, $(l)_n$ could not be zero unless l took a negative value. Later on we call l in the notation $(l)_{n-1}$ a digit, and we find it convenient to exclude the digit 0.

D_l p.p.'s of P' of degree l. These D_l p.p.'s evidently satisfy the test for an ideal, viz. that the D_{l+1} members include all those that can be *derived* from the D_l members. *This proves the existence of a p.p.-ideal having the same D series $D_0, D_1, D_2, \ldots$ as that of any given H-ideal M.* It was only in order to demonstrate this that we have introduced P' here. The relation $D_{l+1} \geqslant Q(D_l)$, which we wish to prove for any H-ideal, has now only to be proved for any p.p.-ideal. In what follows we shall only consider P, until we come to the proof of $D_{l+1} \geqslant Q(D_l)$ in § II.

The general H-ideal. Let M be any H-ideal, and $D_0, D_1, D_2, \ldots$ its D series. In place of M we take the corresponding p.p.-ideal P having the same D series. Let $x_1^{p_1} x_2^{p_2} \ldots x_r^{p_r} x_n^{p_n}$ be the last of the D_l p.p.'s of P of degree l, where $r \leqslant n-1$ and $p_r \geqslant 1$, and any (or all) of $p_1, p_2, \ldots, p_{r-1}, p_n$ may be zero. Then the D_l p.p.'s of P are

$$x_1^{p_1+1}(x_1, \ldots, x_n)^{l-p_1-1},$$

$$x_1^{p_1} x_2^{p_2+1}(x_2, \ldots, x_n)^{l-p_1-p_2-1}, \ldots, x_1^{p_1} \ldots x_r^{p_r}(x_r, \ldots, x_n)^{l-p_1-\ldots-p_r}$$

where the last set differs from the others in having p_r in place of p_1+1, $p_2+1, \ldots$, in the 1st, 2nd, ..., sets. Also the derived p.p.'s of degree $l+1$, obtained by multiplying the D_l p.p.'s by $(x_1, \ldots, x_n)$, are

$$x_1^{p_1+1}(x_1, \ldots, x_n)^{l-p_1},$$

$$x_1^{p_1} x_2^{p_2+1}(x_2, \ldots, x_n)^{l-p_1-p_2}, \ldots, x_1^{p_1} \ldots x_r^{p_r}(x_r, \ldots, x_n)^{l-p_1 \ldots -p_r+1},$$

which consist of all the p.p.'s of $(x_1, x_2, \ldots, x_n)^{l+1}$ from the first x_1^{l+1} up to $x_1^{p_1} \ldots x_r^{p_r} x_n^{p_n+1}$. Hence, assuming that D_l has neither of its extreme values 0 and $(l+1)_{n-1}$, and putting

$$l-p_1 = l_1, \quad l-p_1-p_2 = l_2, \ldots, l-p_1-\ldots-p_r = l_r-1,$$

we have the result:

If $\quad D_l = (l_1)_{n-1}+(l_2)_{n-2}+\ldots+(l_r)_{n-r}, \quad l \geqslant l_1 \ldots \geqslant l_r \geqslant 1, \quad n > r > 0,$

then $\quad (l+2)_{n-1} \geqslant D_{l+1} \geqslant (l_1+1)_{n-1}+(l_2+1)_{n-2}+\ldots+(l_r+1)_{n-r}.$

The excluded cases, which present no difficulty, are: (i) if $D_l = 0$, then $(l+2)_{n-1} \geqslant D_{l+1} \geqslant 0$; and (ii) if $D_l = (l+1)_{n-1}$, then $D_{l+1} = (l+2)_{n-1}$. It can be easily proved that the above form for D_l is unique, *i.e.* if D_l is known, and $0 < D_l < (l+1)_{n-1}$, the positive integers (or digits) $l_1, l_2, \ldots, l_r$ have unique values.

We denote the number $(a_1)_{n-1}+(a_2)_{n-2}+\ldots+(a_r)_{n-r}$, $a_1 \geqslant a_2 \ldots \geqslant a_r \geqslant 1$, $n > r > 0$, by $(a_1, a_2, \ldots, a_r)_{n-1}$. Also, if $(a_1, a_2, \ldots, a_r)_{n-1} = N$, we denote

$$(a_1+1,\ a_2+1,\ \ldots.\ a_r+1)_{n-1} \text{ by } Q(N), \text{ or } Q_{n-1}(N),$$

and $$(a_1-1,\ a_2-1,\ \ldots,\ a_r-1)_{n-1} \text{ by } Q^{-1}(N), \text{ or } Q_{n-1}^{-1}(N),$$

in which it is to be understood that if a_r-1, $a_{r-1}-1$, ... are zeros *they are not to be written*. Thus $Q(N)$ and $Q^{-1}(N)$ are functions of N; and, if $Q^{-1}(N) = N_1$, N is only equal to $Q(N_1)$ if the digits $a_1, a_2, \ldots, a_r$ of N contain no units; in fact, when $Q^{-1}(N) = N_1$, then N is equal to $Q(N_1)$ increased by the number of units in the digits of N.

What we have proved is that (without exception) there is an H-ideal having $D_0, D_1, D_2, \ldots$ as its D series, provided that

$$(l+2)_{n-1} \geqslant D_{l+1} \geqslant Q(D_l)$$

is true for all values of l, defining $Q(0)$ to be equal to 0; and that there is no such H-ideal unless these relations are satisfied. In the case of the p.p.-ideal P the D_{l+1} p.p.'s consist of the first $Q(D_l)$ p.p.'s in $(x_1, x_2, \ldots, x_n)^{l+1}$, which are *derived* members, followed by the next $D_{l+1}-Q(D_l)$ p.p.'s in the same, which are *principal* members. *P is determinate if we know its D series.* It is to be noticed that the limits of D_{l+1} depend only on the values of l and D_l, and not on the values of $D_0, D_1, \ldots, D_{l-1}$. This might have been foreseen independently.

The general non-H-ideal. The D_l members of a non-H-ideal in n variables consist of D_{l-1} members of degree $\leqslant l-1$, and D_l-D_{l-1} (or ΔD_l) members of actual degree l which are linearly independent, not only in respect to their terms as a whole, but in respect to their terms of highest degree l. If we reject all terms of degree $< l$ in the ΔD_l members ($l = 0, 1, 2, \ldots$) we obtain the members of an H-ideal whose D series is $\Delta D_0, \Delta D_1, \Delta D_2, \ldots$. Conversely, if we take any H-ideal, and merely change the origin, it becomes a non-H-ideal such that the D_l of the H-ideal is equal to the ΔD_l of the non-H-ideal. Hence the conditions for a non-H-ideal are the same as those for an H-ideal if D_l is replaced by ΔD_l; *i.e.* the necessary and sufficient conditions that $D_0, D_1, D_2, \ldots$, may be the D series of some actual non-H-ideal are that the relations

$$(l+2)_{n-1} \geqslant \Delta D_{l+1} \geqslant Q(\Delta D_l)$$

should be true for all values of l. The higher limit of D_{l+1} depends only on the values of l and D_l, and the lower limit, viz. $D_l+Q(D_l-D_{l-1})$, on the values of D_l, D_{l-1}.

The Hilbert function. From the above we can find an expression for the Hilbert function $\chi(l)$ of the general H-ideal, together with the restrictions to which its coefficients must be subject, which neither Hilbert nor Ostrowski finds. $\chi(l)$ is the polynomial in l to which H_l becomes equal when l is large enough. Hilbert expresses it in the form

$$\chi(l) = a\binom{l}{n-r-1}+b\binom{l}{n-r-2}+\ldots+k,$$

in terms of binomial coefficients, while Ostrowski adopts the preferable form

$$\chi(l) = a(l+1)_{n-r-1}+b(l+1)_{n-r-2}+\ldots+k.$$

In both forms a (the *order* of the ideal) has the same positive integral value, and $b, c, \ldots, k$ are integers, positive or negative; r is the *rank* of the ideal, and $n-r-1$ the *dimensions*.*

Since, by Hilbert's theorem, any polynomial-ideal has a finite basis, *i.e.* only a finite number of principal members, it follows that the p.p.-ideal P corresponding to any given H-ideal M has a *last* principal member. Let this be $x_r^{a_r}x_{r+1}^{a_{r+1}}\ldots x_s^{a_s}x_n^{a_n}$, where r, a_r, a_s are all greater than zero, and s is generally equal to $n-1$, but may be less (or the last principal member might possibly be $x_n^{a_n}$). Then the last p.p. of P of degree

$$l \geqslant a_r+\ldots+a_s+a_n \quad \text{is} \quad x_r^{a_r}\ldots x_r^{a_s}x_n^{l-a_r-\ldots-a_s},$$

and we have (from above, where D_l was first calculated),

$$D_l = (l, l, \ldots, \overline{r-1} \text{ times}, l-a_r, l-a_r-a_{r+1}, \ldots, l-a_r-\ldots-a_s+1)_{n-1}$$
$$= (l, l, \ldots, \overline{r-1} \text{ times}, l-a, l-b, \ldots, l-k)_{n-1},\ 1 \leqslant a \leqslant b \ldots \leqslant k.$$

Also $\quad H_l+D_l = (l+1)_{n-1} = (l, l, \ldots, r-1 \text{ times})_{n-1}+(l+1)_{n-r}.$

By subtraction, when l is large enough (viz. $l-k > a_n$),

$$\chi(l) = (l+1)_{n-r}-(l-a, l-b, \ldots, l-k)_{n-r},\ 1 \leqslant a \leqslant b \ldots \leqslant k,\dagger$$

* It is usual to say that an H-ideal of rank r has $n-r-1$, not $n-r$, dimensions, thus excluding the origin $(0, 0, \ldots, 0)$, or treating it as a vertex of projection outside the $(n-1)$-space corresponding to the ratios of the variables.

† With the exception that $\chi(l) = (l+1)_{n-r}-(l-a+1)_{n-r}$ when the last principal member of P is $x_r^{a_r}x_n^{a_n}$. a (or a_r) is the order as before.

which is a polynomial in l of degree $n-r-1$. This seems to be the simplest form in which to leave $\chi(l)$, and shows its restrictions. It can be brought easily to the Ostrowski form, but not easily to the Hilbert form.

The *rank* of a polynomial-ideal is defined as the least number r such that all members of the ideal can be made to vanish by making r of the variables functions of the remaining $n-r$ (regarded as arbitrary parameters). The p.p.-ideal P above has $x_1^\lambda, x_2^\lambda, \ldots, x_r^\lambda$ $(\lambda = a_r+\ldots+a_s+a_n)$ as members, and all its members vanish when $x_1, x_2, \ldots, x_r$ vanish. Hence the rank of P is r, and its spread is $(x_1, x_2, \ldots, x_r)$. There is no ambiguity about the rank of an H-ideal as there is about the dimensions.

II. *Proof of the main theorem.*

Note.—This proof of the theorem which has been assumed earlier is given only to place it on record. It is too long and complicated to provide any but the most tedious reading.

It is required to prove that the relation $D_{l+1} \geqslant Q_{n-1}(D_l)$ holds for any H-ideal in n variables; and, as we have already seen (p. 534), it is sufficient to prove it for any p.p.-ideal. Any given integer $N > 0$ can be expressed uniquely in the form

$$N = (a_1)_{n-1}+(a_2)_{n-2}+\ldots+(a_r)_{n-r} = (a_1, a_2, \ldots, a_r)_{n-1}$$

in the *scale* of $n-1$ with not more than $n-1$ *digits* $a_1 \geqslant a_2 \ldots \geqslant a_r \geqslant 1$.

$$Q_{n-1}(N) = (a_1+1, \ldots, a_r+1)_{n-1}, \quad \text{and} \quad Q_{n-1}^{-1}(N) = (a_1-1, \ldots, a_r-1)_{n-1}$$

if $a_r > 1$, while $Q_{n-1}^{-1}(N) = (a_1-1, \ldots, a_p-1)_{n-1}$ if $a_p > 1$ and $a_{p+1}, \ldots, a_r$ are units (the notation excludes a zero digit). $Q(N)$ and $Q^{-1}(N)$ are both defined as 0 if $N = 0$; also $Q^{-1}(N)$ is defined as 0 if it has no digits, as is the case with $Q_{n-1}^{-1}(N)$ when $N < n$. $Q(N)$, $Q^{-1}(N)$ will be understood to be $Q_{n-1}(N)$, $Q_{n-1}^{-1}(N)$ unless a scale different from $n-1$ is indicated by the context.

If $N = (a_1, a_2, \ldots, a_r)_{n-1}$, we have

$$N+Q^{-1}(N)+Q^{-2}(N)+\ldots = (a_1, a_2, \ldots, a_r)_n,$$

and $N-Q^{-1}(N) = (a_1, a_2, \ldots, a_r)_{n-2}$, though this is not in its proper form if $r = n-1$.

Before proceeding to the proof proper we must prove some properties of $Q(N)$ and $Q^{-1}(N)$, especially such as relate to the increase of $Q(N)$ as N

increases. *The increase in $Q(N)$ is never less than the increase in N, and the increase $Q(N+1)-Q(N)$ in $Q(N)$ due to an increase of* 1 *in N is $n-r(\geqslant 1)$, where r is the number of digits in N.* There are two cases: (i) $r<n-1$, in which case

$$N+1=(a_1,\ a_2,\ \ldots,\ a_r,\ 1)_{n-1} \text{ and } Q(N+1)-Q(N)=(2)_{n-r-1}=n-r;$$

and (ii) $r=n-1$ and the last p digits of N equal, in which case

$$N=(a_1,\ \ldots,\ a_{n-p-1},\ a_{n-p}^{p})_{n-1}.\quad N+1=(a_1,\ \ldots,\ a_{n-p-1},\ a_{n-p}+1)_{n-1},$$

and $$Q(N+1)-Q(N)=(a_{n-p}+2)_p-\{(a_{n-p}+1)^p\}_p=1.$$

LEMMA I.—*The increase $Q(N+I)-Q(N)$ in $Q(N)$ for a given increase I in N has the following properties*: (i) *if $N=0$ it is greater than for any value of $N>0$*; (ii) *if $N+I=(a)_{n-1}$ it is as small as for any less value of N*; (iii) *if $N=(a)_{n-1}$ it is as great as for any greater value of N.*

All this is true in scale 1; for, when $N=0$, $Q_1(N+I)-Q_1(N)=I+1$; and, when $N>0$, $Q_1(N+I)-Q_1(N)=I$. We assume it true for all scales up to $n-2$ and prove it true for scale $n-1$.

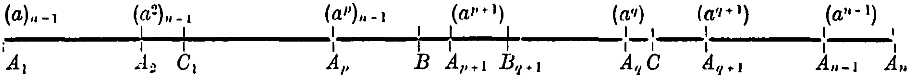
Suppose first that N and $N+I$ are both in the limited range $(a)_{n-1}$ to $(a+1)_{n-1}$. Divide this range into $n-1$ smaller ones of which the p^{th} is $(a^p)_{n-1}$ to $(a^{p+1})_{n-1}$, and the last one $(a^{n-1})_{n-1}$ to $(a^n)_{n-1}$ is a single step, $(a^n)_{n-1}$ being an improper form of $(a+1)_{n-1}$. $Q(N)$ increases along the range $N=(a^p)_{n-1}$ to $(a^{p+1})_{n-1}$ of extent $(a)_{n-p-1}$ in exactly the same way as along the range $N=(a^{p-1},\ a-1)_{n-1}$ to $(a^p)_{n-1}$, that is, a range of the same extent at the end of the previous range $(a^{p-1})_{n-1}$ to $(a^p)_{n-1}$, and therefore also of any preceding range. The reason is that any number N in the range $(a^p)_{n-1}$ to $(a^{p+1})_{n-1}$ short of the end number is $(a^p,\ b,\ \ldots)_{n-1}$, where $b\leqslant a-1$, and to this corresponds the number $(a^{p-1},\ a-1,\ b,\ \ldots)_{n-1}$ in the previous range with the same number of digits, and at the same distance from the end of the range. We express this fact by the symbol $\sim$, meaning "is equivalent as regards increase in $Q(N)$". Thus

$$\begin{aligned}(a^p)_{n-1} \text{ to } (a^{p+1})_{n-1} &\sim (a^{p-1},\ a-1)_{n-1} \text{ to } (a^p)_{n-1}\\ &\sim \{a^{p-2},\ (a-1)^2\}_{n-1} \text{ to } (a^{p-1})_{n-1} \sim \text{etc.}\\ &\sim \{a,\ (a-1)^{p-1}\}_{n-1} \text{ to } (a^2)_{n-1}.\end{aligned}$$

Again $(a^p)_{n-1}$ to $(a^{p+1})_{n-1}$ in scale $n-1\sim 0$ to $(a)_{n-p-1}$ in scale $n-p-1$.

Hence, for an interval $I < (a)_{n-p-1}$ in the range $(a^p)_{n-1}$ to $(a^{p+1})_{n-1}$, $Q(N+I)-Q(N)$ is greater when $N = (a^p)_{n-1}$ than anywhere else, and as small when $N+I = (a^{p+1})_{n-1}$ as anywhere else; since this is true of the range 0 to $(a)_{n-p-1}$ in scale $n-p-1$.

Let the interval I (or BC in the figure) be placed anywhere on the range $(a)_{n-1}$ to $(a+1)_{n-1}$, B (or N) being between A_p, A_{p+1} $\{$or $(a^p)_{n-1}$, $(a^{p+1})_{n-1}\}$, and C (or $N+I$) between A_q, A_{q+1}. When the interval I, or BC, moves up or down the range, let B be at B_{q+1}, ..., B_n when C is at A_{q+1}, ..., A_n; and let C be at C_p, ..., C_1 when B is at A_p, ..., A_1. We have to compare



the values of $Q(N+I)-Q(N)$ for the several I intervals

$$A_1C_1,\ A_2C_2,\ \dots,\ A_pC_p,\ BC,\ B_{q+1}A_{q+1},\ \dots,\ B_nA_n,$$

which values may be denoted by

$$R(A_1C_1)\ \dots,\ R(BC),\ \dots,\ R(B_nA_n).$$

Now $$R(BC)-R(B_{q+1}A_{q+1}) = R(BB_{q+1})-R(CA_{q+1}).$$

But, if B_{q+1} is in A_pA_{p+1}, $R(BB_{q+1})$ is as great as the R of an interval equal to BB_{q+1} ending at A_{p+1}, or at A_{q+1}, *i.e.* $R(BB_{q+1}) \geqslant R(CA_{q+1})$. If, however, B_{q+1} is beyond A_{p+1}, then

$$R(BB_{q+1}) = R(BA_{p+1})+R(A_{p+1}B_{q+1}),$$

and $R(BA_{p+1})$ is equal to the R of an interval equal to BA_{p+1} at the end of CA_{q+1}, and $R(A_{p+1}B_{q+1})$ is greater than the R of an interval equal to $A_{p+1}B_{q+1}$ at the beginning of CA_{q+1}, *i.e.* $R(BB_{q+1}) > R(CA_{q+1})$. In any case $R(BC) \geqslant R(B_{q+1}A_{q+1})$.

Similarly we can prove that

$$R(BC) \geqslant R(B_{q+1}A_{q+1}) \geqslant \dots \geqslant R(B_nA_n);$$

and by the same reasoning we have

$$R(A_1C_1) > R(A_2C_2) > \dots > R(A_pC_p) > R(BC).$$

We can proceed now to the unlimited range 0 to $(a)_{n-1}$, where a is as high as we please. Since

$$(a)_n \text{ to } (a,\ a)_n \text{ in scale } n \sim 0 \text{ to } (a)_{n-1} \text{ in scale } n-1,$$

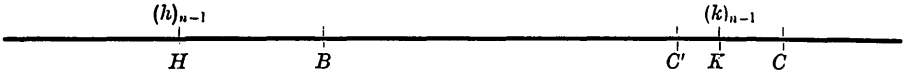
and, for the range in scale n, $Q(N+I)-Q(N)$ is greater when $N=(a)_n$ than anywhere else, and as small when $N+I=(a,\ a)_n$ as anywhere else, so in the range 0 to $(a)_{n-1}$ in scale $n-1$, $Q(N+I)-Q(N)$ is greater when $N=0$ than for any value of $N>0$, and is as small when $N+I=(a)_{n-1}$ as for any less value of N. This proves (i) and (ii).

To prove (iii) we have to repeat some of the reasoning. Let B (or N) be between $(h)_{n-1}$, $(h+1)_{n-1}$, and C (or $N+I$) between $(k)_{n-1}$, $(k+1)_{n-1}$. Take C' so that $HC'=BC=I$. We have to prove first that

$$R(HC')\geqslant R(BC),$$

and this has been proved already when C is in the range $(h)_{n-1}$ to $(h+1)_{n-1}$. So we assume C beyond $(h+1)_{n-1}$, *i.e.* $k\geqslant h+1$. Then

$$R(HC')-R(BC)=R(HB)-R(C'C).$$



If C' is in HK, $R(C'C)=R(C'K)+R(KC)$, and $R(KC)$ is equal to the R of an interval equal to KC beginning at H, since

$$(h)_{n-1}\text{ to }(h+1)_{n-1}\sim(k)_{n-1}\text{ to }(k,\ h+1)_{n-1},$$

and $R(C'K)\leqslant$ the R of the remaining part of the interval HB, by (ii). Hence $R(C'C)\leqslant R(HB)$, *i.e.* $R(HC')\geqslant R(BC)$. If C' is beyond K, $R(HB)$ is equal to the R of an interval equal to HB or $C'C$ beginning at K (by the equivalence above), which is greater than $R(C'C)$; *i.e.* $R(HC')>R(BC)$. In any case $R(HC')\geqslant R(BC)$. Similarly, by taking N at $(h-1)_{n-1}$, $(h-2)_{n-1}$, ..., $(a)_{n-1}$ successively, the value of $Q(N+I)-Q(N)$ is as great when N is at $(a)_{n-1}$ as when N is at B. This proves (iii).

There must clearly be many properties of a similar kind. By (i) we have $Q(I)-Q(0)>Q(N+I)-Q(N)$, or $Q(N_1+N_2)<Q(N_1)+Q(N_2)$ when neither N_1 nor N_2 is zero.

Lemma II.—(i) *If* $N_1<(a+1)_{n-1}$, $N_2\leqslant(a+1)_{n-1}$,

and $$N_1+N_2=(a+1)_{n-1}+R,\quad \textit{where}\ R\geqslant 0,$$

then $$Q(N_1)+Q(N_2)\geqslant Q(a+1)_{n-1}+Q(R).$$

(ii) *If* $N_1 < (a+1)_{n-1}$, $Q^{-1}(N_2) = (a, a_1, \ldots, a_p)_{n-1}$, $N_1 > (a_1, \ldots, a_p)_{n-1}$,

and $N_1+N_2 = (a+1)_{n-1}+R$, *where* $R \geqslant 0$,

then $Q(N_1)+Q(N_2) \geqslant Q(a+1)_{n-1}+Q(R)$.

The theorem is divided into two parts according as $N_2 \leqslant (a+1)_{n-1}$ or $(a+1)_{n-1} \leqslant N_2 \leqslant (a+2)_{n-1}$, because we shall need to use them in this way ; but both might be combined more clearly under one heading, viz.

$$N_1 = (b_1, b_2, \ldots, b_p)_{n-1} < (a+1)_{n-1}, \qquad Q^{-1}(N_2) \leqslant (a, b_1, \ldots, b_p)_{n-1}.$$

The other condition imposed, $N_1+N_2 \geqslant (a+1)_{n-1}$, is not essential. If $N_1+N_2 < (a+1)_{n-1}$ we should take $N_1+N_2 = R$, and obtain

$$Q(N_1)+Q(N_2) \geqslant Q(N_1+N_2),$$

which has just been proved above.

(i) Since $N_2 \leqslant (a+1)_{n-1}$, $(a+1)_{n-1}-N_2 = N_1-R$, where both sides are positive ; also $N_1 < (a+1)_{n-1}$. Hence, by I (ii),

$$Q(a+1)_{n-1}-Q(N_2) \leqslant Q(N_1)-Q(R),$$

or
$$Q(N_1)+Q(N_2) \geqslant Q(a+1)_{n-1}+Q(R).$$

(ii) The property is true for scale 1 (since $N_2 = a+1$ and $N_1 = R$) and can be proved by induction for scale $n-1$. Imagine N_2, or $(a+1, a_1+1, \ldots, a_p+1, 1^q)_{n-1}$, to remain fixed while N_1, R increase together. We have to prove that

$$Q(R)-Q(N_1) \leqslant Q(N_2)-Q(a+1)_{n-1}.$$

When $N_1 = (a_1+1)_{n-1}$, we have

$$R = (a_1+1)_{n-1}+(a_1+1, \ldots, a_p+1, 1^q)_{n-2} = (a_1+1, a_1+1, \ldots, a_p+1, 1^q)_{n-1},$$

$$Q(R)-Q(N_1) = Q_{n-2}(a_1+1, \ldots, a_p+1, 1^q)_{n-2} = Q(N_2)-Q(a+1)_{n-1}.$$

And as $Q(R)-Q(N_1)$ is as great when $N_1 = (a_1+1)_{n-1}$ as for any greater value of N_1 $\{$I (iii)$\}$,

$$Q(R)-Q(N_1) \leqslant Q(N_2)-Q(a+1)_{n-1} \text{ when } N_1 \geqslant (a_1+1)_{n-1}.$$

It remains to prove the same when $N_1 < (a_1+1)_{n-1}$. Put

$$N_1 = (a_1)_{n-1} + N'_1,$$

$$N_2 = (a+1)_{n-1} + N'_2,$$

$$N'_1 + N'_2 = (a_1+1)_{n-2} + R'.$$

Then $\quad N'_1 > (a_2, \ldots, a_p)_{n-2}, \quad Q^{-1}_{n-2}(N'_2) = (a_1, a_2, \ldots, a_p)_{n-2},$

$$N'_1 < (a_1+1)_{n-2}, \quad \text{and} \quad R' \geqslant 0;$$

so that the conditions are satisfied for applying the theorem to N'_1, N'_2, R' in scale $n-2$; *i.e.* we have

$$Q_{n-2}(R') - Q_{n-2}(N'_1) \leqslant Q_{n-2}(N'_2) - Q_{n-2}(a_1+1)_{n-2}.$$

But, by adding the three equations above, we have

$$N_1 + N_2 - (a+1)_{n-1} = (a_1)_{n-1} + (a_1+1)_{n-2} + R',$$

or $\quad R = (a_1+1)_{n-1} + R', \quad$ where $\quad R' < N'_2 < (a_1+2)_{n-2};$

hence $\quad Q(R) = (a_1+2)_{n-1} + Q_{n-2}(R');$

similarly for $Q(N_1)$, $Q(N_2)$. Hence

$$\begin{aligned} Q(R) - Q(N_1) &= (a_1+2)_{n-1} - (a_1+1)_{n-1} + Q_{n-2}(R') - Q_{n-2}(N'_1) \\ &\leqslant (a_1+2)_{n-2} + Q_{n-2}(N'_2) - Q_{n-2}(a_1+1)_{n-2} \\ &\leqslant Q_{n-2}(N'_2) \leqslant Q(N_2) - Q(a+1)_{n-1}. \end{aligned}$$

Q.E.D.

Lemma III.—*If there are s numbers $N_1, N_2, \ldots, N_s$ such that*

$$N_1 < (a+1)_{n-1}, \quad Q^{-1}(N_2) \leqslant N_1, \ \ldots, \ Q^{-1}(N_s) \leqslant N_{s-1},$$

and $\quad N_1 + N_2 + \ldots + N_s = (a+1)_{n-1} + \ldots + (a+t_s-1)_{n-1} + R_s,$

where $\quad 0 \leqslant R_s < (a+t_s)_{n-1},$

then

$$Q(N_1) + Q(N_2) + \ldots + Q(N_s) \geqslant Q(a+1)_{n-1} + \ldots + Q(a+t_s-1)_{n-1} + Q(R_s).$$

This has been proved for two numbers in Lemma II with less restrictive conditions as regards N_1, N_2. We assume the property for p numbers and prove it for $p+1$. Put

$$N_1+N_2+\ldots+N_p=(a+1)_{n-1}+\ldots+(a+t_p-1)_{n-1}+R_p,$$

where $$0\leqslant R_p<(a+t_p)_{n-1}.$$

Now $$N_1<(a+1)_{n-1},\quad Q^{-1}(N_2)\leqslant N_1<(a+1)_{n-1},$$

therefore $$N_2<(a+2)_{n-1},\quad N_3<(a+3)_{n-1},\text{ etc.}$$

Hence $p>t_p-1$, *i.e.* $p\geqslant t_p$. Also $N_p<(a+t_p)_{n-1}$; for if

$$N_p\geqslant(a+t_p)_{n-1},\text{ then } N_p>R_p,\text{ and}$$

$$N_{p-1}\geqslant Q^{-1}(N_p)\geqslant(a+t_p-1)_{n-1},\quad N_{p-2}\geqslant(a+t_p-2)_{n-1},\text{ etc.},$$

which is not consistent with

$$N_p+N_{p-1}+\ldots=R_p+(a+t_p-1)_{n-1}+\ldots,\quad p\geqslant t_p.$$

Now $Q^{-1}(N_{p+1})\leqslant N_p<(a+t_p)_{n-1}$, therefore $N_{p+1}<(a+t_p+1)_{n-1}$.

There is no difficulty in extending the theorem so as to include the number N_{p+1} if $N_{p+1}\leqslant(a+t_p)_{n-1}$ by applying either I (i) or else II (i). So take $N_{p+1}>(a+t_p)_{n-1}$. In this case

$$R_p+N_{p+1}=(a+t_p)_{n-1}+R_{p+1},\quad (a+t_p+1)_{n-1}>N_{p+1}>(a+t_p)_{n-1}.$$

Put $$Q^{-1}(N_{p+1})=(a+t_p-1,\,a_1,\,a_2,\,\ldots)_{n-1}.$$

Then $N_1+N_2+\ldots+N_p\geqslant Q^{-p}(N_{p+1})+Q^{-p+1}(N_{p+1})+\ldots+Q^{-1}(N_{p+1})$,

i.e. $(a+t_p-1)_n-(a)_n+R_p\geqslant(a+t_p-1,\,a_1,\,a_2,\,\ldots)_n$

$$-(a+t_p-p-1,\,a_1-p,\,\ldots)_n,$$

i.e. $$R_p>(a_1,\,a_2,\,\ldots)_{n-1},$$

since $$(a)_n>(a+t_p-p-1,\,a_1-p,\,\ldots)_n,\quad (t_p\leqslant p).$$

Thus all the conditions in II (ii) as regards N_1, N_2, $a+1$, R are satisfied for R_p, N_{p+1}, $a+t_p$, R_{p+1}, and we have

$$Q(R_p)+Q(N_{p+1})\geqslant Q(a+t_p)_{n-1}+Q(R_{p+1}).$$

By adding this to the relation

$$Q(N_1)+Q(N_2)+\ldots+Q(N_p) \geqslant Q(a+1)_{n-1}+\ldots+Q(a+t_p-1)_{n-1}+Q(R_p),$$

Q.E.D.

the property is extended from p to $p+1$ numbers.

We can extend the limit of N_{p+1} to $(a+t_p)_{n-1}$ if this should be higher than the limit given by $Q^{-1}(N_{p+1}) \leqslant N_p$.

We have now to prove that whatever N p.p.'s of degree l in n variables are taken the derived p.p.'s of degree $l+1$ cannot be less in number than $Q_{n-1}(N)$. If $n=2$ the N p.p.'s would have to be chosen successively in order that the number of derived p.p.'s might be as small as possible, and the number would then be $N+1$, which is $Q_1(N)$. We assume the theorem for n variables $x_1, x_2, \ldots, x_n$ and proceed to prove it true for $n+1$ variables $x_0, x_1, x_2, \ldots, x_n$. Let the N p.p.'s consist of N_a p.p.'s $x_0^{l-a}S_a$, N_{a+1} p.p.'s $x_0^{l-a-1}S_{a+1}$, and so on, up to N_b p.p.'s $x_0^{l-b}S_b$, where S_p denotes a collection of N_p p.p.'s of degree p in the n variables $x_1, x_2, \ldots, x_n$ and $N = N_a+N_{a+1}+\ldots+N_b = \Sigma N_p$.

The derived p.p.'s consist of

$$x_0^{l-a+1}S_a,\ x_0^{l-a}S_{a+1},\ \ldots,\ x_0^{l-b+1}S_b, \text{ and } x_0^{l-a}OS_a,\ \ldots,\ x_0^{l-b}OS_b,$$

where OS_p denotes the collection of p.p.'s derived from S_p by multiplying S_p by O or $(x_1, x_2, \ldots, x_n)$. Arranged according to powers of x_0 they are

$$\begin{array}{ccccc} S_a & S_{a+1} & S_{a+2} & \ldots & S_b \\ & OS_a & OS_{a+1} & \ldots & OS_{b-1} & OS_b. \end{array}$$

All these p.p.'s are to be counted, except that those which are repeated in any pair S_{p+1}, OS_p are to be counted only once. The first step in reducing the total number of derived p.p.'s to a minimum is therefore to choose the p.p.'s S_p so that the number of p.p.'s in OS_p may be a minimum, and at the same time may coincide with the p.p.'s in S_{p+1} as far as possible. Both these conditions are fulfilled by choosing the p.p.'s S_p $(p=a, \ldots, b)$ to be the first N_p p.p.'s in $(x_1, x_2, \ldots, x_n)^p$, for then the number of p.p.'s in OS_p is a minimum (assuming the theorem for n variables) and equal to $Q(N_p)$, and the greater of OS_p, S_{p+1} includes the less. Hence, so long as the numbers $N_a, \ldots, N_b$ are fixed the least possible total number of derived p.p.'s is the sum of the higher numbers in the $b-a+2$ pairs

$$\begin{array}{cccccc} N_a & N_{a+1} & N_{a+2} & \ldots & N_b & 0 \\ 0 & Q(N_a) & Q(N_{a+1}) & \ldots & Q(N_{b-1}) & Q(N_b). \end{array}$$

We have now to consider how we may change the numbers $N_a, \ldots, N_b$

(keeping ΣN_p or N unchanged) so that the *total derived number* (or sum of higher numbers in the $b-a+2$ pairs) may not increase at any time; and prove that it can be brought by such a process to $Q_n(N)$. This amounts to proving that the original N p.p.'s have at least $Q_n(N)$ derived p.p.'s of the next higher degree.

If $N_{b-1} < Q^{-1}(N_b)$, increase N_{b-1} up to the old $Q^{-1}(N_b)$, and diminish N_b by a like amount to give the new N_b. This changes the three end pairs; the higher of the first pair N_{b-1}, $Q(N_{b-2})$ is increased *at most* by the increase in N_{b-1}, for $Q(N_{b-2})$ has not been changed; the higher of the next pair has not been increased, for N_b has been decreased and the new $Q(N_{b-1})$ is not greater than the old N_b; and the higher of the last pair has been decreased by *at least* the decrease in N_b. Hence this change does not increase the total derived number. Going downwards from N_{b-1}, let N_p be the next number such that $N_p < Q^{-1}(N_{p+1})$. Increase N_p up to $Q^{-1}(N_{p+1})$ and diminish N_b by a like amount (or N_b to zero, and then N_{b-1} by the remaining amount). This again does not increase the total derived number, and leaves all the relations $N_q \geqslant Q^{-1}(N_{q+1})$, $q > p$, intact. Hence we may assume that $N_p \geqslant Q^{-1}(N_{p+1})$ throughout. This reduces the system of numbers to some sort of ordering.

Take a_1 so that $$(a_1+1)_{n-1} > N_a \geqslant (a_1)_{n-1}.$$

Then, since $$Q^{-1}(N_{a+1}) \leqslant N_a < (a_1+1)_{n-1},$$

we have $N_{a+1} < (a_1+2)_{n-1}$, $N_{a+2} < (a_1+3)_{n-1}$, ... Let N_{a+p} be the first of the numbers N_a, N_{a+1}, ..., such that $N_{a+p} < (a_1+p)_{n-1}$.

Put $N_{a+q} = (a_1+q)_{n-1}+N'_{a+q}$, $q = 0$ to $p-1$, where N'_{a+q} is the number in scale $n-2$ with the same digits as N_{a+q} omitting the first a_1+q. Compare the system of pairs

$$\begin{array}{cccccc} N_a & N_{a+1} & N_{a+2} & \dots & N_b & 0 \\ 0 & Q(N_a) & Q(N_{a+1}) & \dots & Q(N_{b-1}) & Q(N_b) \end{array}$$

with the substituted system

$$\begin{array}{ccccccccc} (a_1)_{n-1} & (a_1+1)_{n-1} & \dots & (a_1+p-1)_{n-1} & N_{a+p} & N_{a+p+1} & \dots & N_b & 0 \\ 0 & (a_1+1)_{n-1} & \dots & (a_1+p-1)_{n-1} & (a_1+p)_{n-1} & Q(N_{a+p}) & \dots & Q(N_{b-1}) & Q(N_b) \end{array}$$

in which $N_{a+p} < (a_1+p)_{n-1}$ by hypothesis. Here we have diminished the whole number N by $N'_a+N'_{a+1}+\dots+N'_{a+p-1}$, or N', and the total derived number by the sum of the higher numbers in the pairs

$$\begin{array}{ccccc} N'_a & N'_{a+1} & \dots & N'_{a+p-1} & 0 \\ 0 & Q_{n-2}(N'_2) & \dots & Q_{n-2}(N'_{a+p-2}) & Q_{n-2}(N'_{a+p-1}), \end{array}$$

that is by a number $\geqslant Q(N')$, assuming the theorem for n variables. This comes by observing that

$$N_{a+q} = (a_1+q)_{n-1}+N'_{a+q}, \quad Q(N_{a+q-1}) = (a_1+q)_{n-1}+Q_{n-2}(N'_{a+q-1}),$$

so that the higher of the pair N_{a+q}, $Q(N_{a+q-1})$ is greater than the higher of the substituted pair $(a_1+q)_{n-1}$, $(a_1+q)_{n-1}$ by the higher of the pair N'_{a+q}, $Q_{n-2}(N'_{a+q-1})$. Note that

$$N' = N_a+\dots+N'_{a+p-1} < (a_1+1)_{n-2}+\dots+(a_1+p)_{n-2} < (a_1+p)_{n-1}.$$

Put

$$N_{a+p}+\dots+N_b = (a_1+p)_{n-1}+(a_1+p+1)_{n-1}+\dots$$
$$+(a_1+t-1)_{n-1}+R_t, \quad 0 \leqslant R_t < (a_1+t)_{n-1},$$

or it is possible to have only R_p on the right with $0 \leqslant R_p < (a_1+p)_{n-1}$.

Then, since

$$N_{a+p} < (a_1+p)_{n-1}, \quad Q^{-1}(N_{a+p+1}) \leqslant N_{a+p}, \quad \dots, \quad Q^{-1}(N_b) \leqslant N_{b-1},$$

we have

$$Q(N_{a+p})+\dots+Q(N_b) \geqslant (a_1+p+1)_{n-1}+\dots+(a_1+t)_{n-1}+Q(R_t),$$

Lemma III, and the total derived number of the substituted system above

$$\{\geqslant (a_1)_{n-1}+\dots+(a_1+p)_{n-1}+Q(N_{a+p})+\dots+Q(N_{b-1})+Q(N_b)\}$$

is equal to or greater than that of the system

$$\begin{array}{cccccc} (a_1)_{n-1} & (a_1+1)_{n-1} & \dots & (a_1+t-1)_{n-1} & R_t & 0 \\ 0 & (a_1+1)_{n-1} & \dots & (a_1+t-1)_{n-1} & (a_1+t)_{n-1} & Q(R_t). \end{array}$$

To this we add at the end the number $N' < (a_1+t)_{n-1}$ which was taken away earlier; and according as $R_t+N' < (a_1+t)_{n-1}$ or $\geqslant (a_1+t)_{n-1}$ we put $R_t+N' = R'$ or $(a_1+t)_{n-1}+R'$, $0 \leqslant R' < (a_1+t)_{n-1}$. In doing this we increase the total derived number by $Q(N')$ at most (II, i), whereas we decreased it in the earlier step by $Q(N')$ at least. Finally if $a_1 > 1$ we add on numbers $(1)_{n-1}$, $(2)_{n-1}$, ..., $(a_1-1)_{n-1}$ at the beginning and subtract their sum from the end, again with no increase to the total derived number. We then have

$$N = (1)_{n-1}+(2)_{n-1}+\dots+(b_1)_{n-1}+R, \quad 0 \leqslant R < (b_1+1)_{n-1},$$

$$= (b_1)_n+(b_2,\ b_3,\ \dots)_{n-1}, \quad \text{where } R = (b_2,\ b_3,\ \dots)_{n-1}, \quad b_2 \leqslant b_1,$$

$$= (b_1,\ b_2,\ b_3,\ \dots)_n\,;$$

and the final total derived number

$$= (1)_{n-1}+(2)_{n-1}+\dots+(b_1+1)_{n-1}+Q(R)$$

$$= (b_1+1)_n+(b_2+1,\ b_3+1,\ \dots)_{n-1} = Q_n(N).$$

Hence the original total derived number $\geqslant Q_n(N)$. Q.E.D.

The final partitioning of N into $(1)_{n-1}$, $(2)_{n-1}$, ..., $(b_1)_{n-1}$, R is such that $N_{p+1} = Q(N_p)$ except for the remainder R. There is a still neater partition such that $N_p = Q^{-1}(N_{p+1})$ throughout, having the same total derived number $Q_n(N)$, but not having a remainder. If $N = (b_1,\ b_2,\ \dots,\ b_r)_n$, the last partial number is $N_{b_1} = (b_1,\ b_2,\ \dots,\ b_r)_{n-1}$, and the others are $Q^{-1}(N_{b_1})$, ..., $Q^{\ b_1+1}(N_{b_1})$. If $r = n$, the last digit b_n in N_{b_1}, though irregular, becomes significant, because it does not disappear till we come to $Q^{-b_n}(N_{b_1})$. The higher of the pair N_{p+1}, $Q(N_p)$ is N_{p+1}; so the total derived number with this partition is

$$\Sigma N_p+Q(N_{b_1}) = (b_1,\ \dots,\ b_r)_n+(b_1+1,\ \dots,\ b_r+1)_{n-1}$$

$$= (b_1+1,\ \dots,\ b_r+1)_n = Q_n(N).$$

III. *Special polynomial-ideals.*

In this section we shall give a few results concerning some special polynomial-ideals* and one or two particular examples.

Ideal of rank n. An H-ideal of rank n in n variables is a point-ideal

* Some references to No. 19 of the "Cambridge Tracts in Mathematics and Mathematical Physics" (*The algebraic theory of modular systems*, Cambridge Univ. Press, 1916) will be made under the reference letter (T).

whose point is the origin (0, 0, ..., 0). A non-H-ideal of rank n is composed of a finite number of point-ideals, which may or may not have the origin as one of its points. The conditions for the H-ideal are simply those already found, viz. $D_{l+1} \geqslant Q(D_l)$ with the addition that $\chi(l) = 0$, or H_l vanishes when $l \geqslant \gamma$ (*i.e.* H_l vanishes when l is sufficiently great, the lowest value of l for which this happens being denoted by γ). The conditions for the non-H-ideal are $\Delta D_{l+1} \geqslant Q(\Delta D_l)$ with $\Delta\chi(l) = 0$, or $\chi(l)$ a constant.

To construct a non-H-ideal of rank n with any assigned D series satisfying the necessary conditions above, take the p.p.-ideal P whose D series is ΔD_0, ΔD_1, ΔD_2, ..., *i.e.* the ideal P whose members of any and every degree l are the first ΔD_l p.p.'s in $(x_1, x_2, \dots, x_n)^l$, and in every member $x_1^{p_1}x_2^{p_2}\dots x_n^{p_n}$ of the basis of P change $x_i^{p_i} (i = 1, 2, \dots, n)$ to $x_i(x_i-1)\dots(x_i-p_i+1)$. This will give the basis of the required non-H-ideal. It will have precisely the same (finite) number of separate points $(q_1, q_2, \dots, q_n)$ as there are p.p.'s $x_1^{q_1}x_2^{q_2}\dots x_n^{q_n}$ which are not members of P. Again, if in P we change $x_1, x_2, \dots, x_n$ to $x_1+a_1, x_2+a_2, \dots, x_n+a_n$ we obtain a non-H-point-ideal having the same assigned D series.

Ideal of the principal class. This term was used by Kronecker, though it seems to have gone out of use and no other term has replaced it. It is not what is called a principal ideal (or ideal of rank 1 with a basis (F) consisting of a single member) but an ideal of rank r with a basis $(F_1, F_2, \dots, F_r)$ consisting of r members only. In an H-ideal $(F_1; F_2, \dots, F_r)$ of rank r the generating function of the H series is

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

where $l_1, l_2, \dots, l_r$ are the degrees of $F_1, F_2, \dots, F_r$. This is proved in (T., § 58) and was known previously.

There is no corresponding formula for a non-H-ideal unless its equivalent H-ideal is also of the principal class. Thus the H-ideal equivalent to $(x_1^2, x_2+x_1x_3)$ is $(x_1^2, x_1x_2, x_2^2, x_0x_2+x_1x_3)$, which is not of the principal class.

Other H-ideals whose generating functions $\Sigma H_l x^l$ can be found (and written down like the formula above) are the ρ-th power $(F_1, F_2, \dots, F_r)^\rho$ of an H-ideal of the principal class, and an H-ideal of rank $k-\rho+1$ whose basis consists of all the determinants of a matrix with k columns and ρ rows such that the differences of the degrees of the elements in any row of the matrix are the same for every row. These ideals are perfect (T., §§ 50, 53, 89); and the generating function of a perfect ideal can always be said to be known, as will be explained immediately.

Unmixed ideals and perfect ideals. An *unmixed* ideal M of rank r is one which includes all polynomials F as members for which a polynomial $\phi(x_{r+1}, \ldots, x_n)$ in $x_{r+1}, \ldots, x_n$ exists such that

$$F\phi(x_{r+1}, \ldots, x_n) = 0(M),$$

the variables $x_1, x_2, \ldots, x_n$ having been subjected to a general homogeneous linear substitution beforehand. In other words an ideal M of rank r is unmixed if (and only if) $F\phi(x_{r+1}, \ldots, x_n) = 0(M)$ always requires $F = 0(M)$. If (after the preliminary substitution) we regard $x_{r+1}, \ldots, x_n$ as parameters and $x_1, x_2, \ldots, x_r$ only as variables, ϕ may be regarded as a constant (footnote p. 531).

Let R, R_p, R_{pq} denote polynomials in $x_{r+1}, \ldots, x_n$ only, and ω_1 $(= 1)$, $\omega_2, \omega_3, \ldots$, p.p.'s in $x_1, x_2, \ldots, x_r$ only. Then it is shown (T., §§ 77–80) that any given unmixed H-ideal M of rank r has a system of members

$$\text{(A)} \qquad R\omega_p + R_{p1}\omega_1 + R_{p2}\omega_2 + \ldots + R_{p\mu}\omega_\mu \quad (p = \mu+1, \mu+2, \ldots, \infty)$$

to which corresponds what is called an r-dimensional inverse system

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

where R and all the R_{pq} are unique, with H.C.F. equal to 1, the number μ, and the p.p.'s $\omega_1, \omega_2, \ldots, \omega_\mu$ are fixed, and ω_p is any p.p. other than $\omega_1, \omega_2, \ldots, \omega_\mu$. The relation $R_1\omega_1 + R_2\omega_2 + \ldots + R_\mu\omega_\mu = 0(M)$ requires $R_1 = R_2 = \ldots = R_\mu = 0$.

The members of (A) and (B) are to include not only those which are written but also any and every linear combination of them with multiples of type R or ϕ, deprived of any factor R_t that will divide out. When (A) and (B) are complete in this sense the number of members of (A) of degree l which are linearly independent as regards all the letters $x_1, x_2, \ldots, x_n$ is D_l; and the like number for (B) will be denoted by G_l. Thus G_l, unlike D_l, is not necessarily zero when l is negative, since the negative powers of $x_1, x_2, \ldots, x_r$ in a member of (B) may overpower the positive powers of $x_{r+1}, \ldots, x_n$. Each member of (B) is a homogeneous infinite power series in $x_1, x_2, \ldots, x_n$; for $R\omega_i^{-1}$, $R_{pi}\omega_p^{-1}$ are of the same degree, since $R\omega_p$, $R_{pi}\omega_i$ in (A) are of the same degree.

The H-ideal M is said to be *perfect* when (and only when) $R = 1$, a property which is not uncommon, the most important examples being those which have been mentioned above. Assuming M perfect, if we put $x_{r+1} = \ldots = x_n = 0$ in (B) we get the system inverse to the point-ideal

$M(x_{r+1} = \ldots = x_n = 0)$, (T., § 80), whose H series we may denote by $1, h_1, h_2, \ldots, h_{\gamma-1}$ ($h_l = 0$ when $l \geqslant \gamma$). There are h_p members actually written in (B) of degree $-p$, which will be brought to degree l by multiplying each of them by any and every p.p. in $x_{r+1}, \ldots, x_n$ of degree $l+p$. In this way we can get all the G_l members of (B) of degree l, and they are all linearly independent in $x_1, x_2, \ldots, x_n$. Hence G_l is the coefficient of x^l in

$$(1+h_1x^{-1}+h_2x^{-2}+\ldots+h_{\gamma-1}x^{-\gamma+1})(1-x)^{-n+r},$$

while H_l is the coefficient of x^l in

$$(1+h_1x+h_2x^2+\ldots+h_{\gamma-1}x^{\gamma-1})(1-x)^{-n+r}.$$

These are then the generating functions of the G and H series for a perfect H-ideal M of rank r, where $1, h_1, h_2, \ldots, h_{\gamma-1}$ is the H series of the point-ideal $M(x_{r+1} = \ldots = x_n = 0)$. In non-perfect ideals the G and H series are to a large extent independent; ideals with the same G series may have very different H series. In perfect ideals they are dependent; and the dependence can be expressed by the relation

$$H_l - \chi(l) = (-1)^{n-r} G_{-l-n+r},$$

as may be shown from the above.

In an H-ideal of the principal class there is a further simplification, viz. the series $1, h_1, h_2, \ldots, h_{\gamma-1}$ reads the same forwards and backwards, so that $G_l = H_{l-\gamma+1}$, where $\gamma-1 = (l_1-1)+(l_2-1)+\ldots+(l_r-1)$, $l_1, l_2, \ldots, l_r$ being the degrees of the members of the basis of the H-ideal. This, of course, may occur for other perfect H-ideals.

Since $1, h_1, \ldots, h_{\gamma-1}$ is the H series of an H-point-ideal the conditions that $D_0, D_1, D_2, \ldots$ may be the D series of some actual perfect H-ideal of rank r in n variables are $\Delta^{n-r}D_{l+1} \geqslant Q(\Delta^{n-r}D_l)$ with $\Delta^{n-r}H_l = 0$ when $l \geqslant \gamma$.

We give finally a very general and fundamental formula connecting *any two H-ideals which are mutually residual with respect to an H-ideal of the principal class.* Such ideals are necessarily unmixed and of the same rank; but they are perfectly general unmixed ideals.

If M is any unmixed H-ideal of rank r, and $\bar{M}$ is the ideal $(F_1, F_2, \ldots, F_r)$, also of rank r, where $F_1, F_2, \ldots, F_r$ are r members of M (of degrees $l_1, l_2, \ldots, l_r$), then M and its residual, M', with respect to $\bar{M}$ are mutually residual with respect to $\bar{M}$; and the following relations hold between the terms of the G and H series of M, M', $\bar{M}$:

$$G_{l-\gamma+1}+H'_l = G'_{l-\gamma+1}+H_l = \bar{G}_{l-\gamma+1} = \bar{H}_l,$$

where $\gamma-1 = (l_1-1)+\ldots+(l_r-1)$. This follows from T., § 86, though it is not stated there. The relations determine the G and H series of M' if the G and H series of M are known; for $\bar{H}_l$ is known, viz. $\bar{H}_l$ is the coefficient of x^l in $(1-x^{l_1})\ldots(1-x^{l_r})(1-x)^{-n}$.

Notes and Examples.

It may have been observed that we have only found the conditions which govern the terms of the D series in the two cases of the general ideal and a perfect ideal and some special cases of the latter. We have not found them for the general unmixed ideal, primary ideal, the ideal with no multiple spread, and prime ideal. Each of these cases is more difficult to solve than the previous one, and I doubt whether the solution can be found for any of them, since there seems to be no law governing the discontinuities which occur. In the rather important case of an H-point-ideal whose inverse system is a principal system, the conditions are that the latter half of its finite H series 1, H_1, ..., $H_{\gamma-1}$ is the first half reversed (T, § 70), while the conditions for the first half are only those of the general H-ideal $D_{l+1} \geqslant Q(D_l)$.

The only method that I know of, which can be called in any sense general, for finding the value of D_l for an ideal whose basis $(F_1, F_2, \ldots, F_k)$ is given is the following:—Find its rank r, which is usually known, and, if not known, is easy to find. If $(F_1, F_2, \ldots, F_k)$ is a non-H-ideal, change it into its equivalent H-ideal. This may be difficult, but it is an essential preliminary for working purposes. Then modify the basis if necessary so that its first r members $(F_1, F_2, \ldots, F_r)$ shall not belong to any ideal of rank $< r$. The rest of the work will be sufficiently clear by taking an example (Ex. i).

Example (i). Find D_l for the H-ideal (F_1, F_2, F_3, F_4) of rank 2:—

$$F_1 = v_1w_2-v_2w_1, \qquad F_2 = u_2v_1w_1-u_1v_1w_2+v_2w_2,$$

$$F_3 = u_2v_1^2-u_1v_1v_2+v_2^2, \quad F_4 = u_2w_1^2-u_1w_1w_2+w_2^2,$$

u_1, v_1, w_1 being linear and u_2, v_2, w_2 quadratic homogeneous polynomials in n variables.

The D_l of (F_1, F_2, F_3, F_4) is the number of linearly independent polynomials of (F_1, F_2) of degree l, that is the D_l of (F_1, F_2), increased by the number of polynomials A_3F_3 of degree l of which no linear combination equals $0(F_1, F_2)$, increased by the number of polynomials A_4F_4 of degree l of which no linear combination equals $0(F_1, F_2, F_3)$. To find the first of these two increases we consider the equation

$$X_3F_3 = 0(F_1, F_2)$$

where X_3F_3 is to be of degree l, and X_3 of degree $l-4$. Now $X_3 = 0(w_1, w_2)$, since $(F_1, F_2) = 0(w_1, w_2)$ and $F_3 \neq 0(w_1, w_2)$. Also both w_1F_3 and $w_2F_3 = 0(F_1, F_2)$. Hence it is not only necessary but *sufficient* that $X_3 = 0(w_1, w_2)$. Hence the number of linearly independent polynomials X_3 of degree $l-4$ is the D_{l-4} of (w_1, w_2); and the number of the A_3 (or A_3F_3 above) is the H_{l-4} of (w_1, w_2), *i.e.* the coefficient of x^{l-4} in $(1-x)(1-x^2)(1-x)^{-n}$, or the coefficient of x^l in $x^4(1-x)(1-x^2)(1-x)^{-n}$. It so happens that the second increase, the number of polynomials A_4, is equally easily found in this example; for $X_4F_4 = 0(F_1, F_2, F_3)$ gives $X_4 = 0(v_1, v_2)$, since $(F_1, F_2, F_3) = 0(v_1, v_2)$; so that the number of the polynomials A_4 equals that of the A_3. We can express the general result symmetrically in the form:—the H_l of $(F_1, F_2, \ldots, F_k)$ of rank r, $F_1, F_2, \ldots, F_k$ being of degrees $l_1, l_2, \ldots, l_k$, is $H_l^{(r)}-H_{l-l_{r+1}}^{(r+1)}-\ldots-H_{l-l_k}^{(k)}$, where $H_l^{(r)}$ is the known H_l of $(F_1, F_2, \ldots, F_r)$, and $H_{l-l_p}^{(p)}$ is the H_{l-l_p} of the ideal (X_p) determined by $X_pF_p = 0(F_1, F_2, \ldots, F_{p-1})$. In the example (F_1, F_2, F_3, F_4), H_l is the coefficient of x^l in

$$\{(1-x^3)(1-x^4)-x^4(1-x)(1-x^2)-x^4(1-x)(1-x^2)\}(1-x)^{-n}.$$

The solution would have been more difficult if the second member F_2 had not been the one actually chosen, but one of the other two F_3, F_4.

Example (ii). Find the basis of the p.p.-ideal P corresponding to the H-ideal (F_1, F_2), where F_1, F_2 are of degrees 2, 4 in 4 variables.

First find the last principal member $x_2^{a_2}x_3^{a_3}x_4^{a_4}$ of P. The Hilbert function (p. 536) is

$$(l+1)_2-(l-a_2,\ l-a_2-a_3+1)_2$$

$$= \text{the coefficient of } x^l \text{ in } (1-x^2)(1-x^4)(1-x)^{-4} = 8l-8,$$

i.e. $a_2 l - \frac{1}{2}a_2(a_2-3)+a_3 = 8l-8$, so that $a_2 = 8$, $a_3 = 12$. The value of a_4 (or a_n) is zero as it generally is. Thus we have to go to degree 20 before obtaining the last member of the basis of P, viz. $x_2^8 x_3^{12}$.

To write down the basis of P we have to provide that the p.p.'s of P of degree l shall be the first D_l p.p.'s of $(x_1, x_2, x_3, x_4)^l$, but we have only to write down the principal members, that is, those members which are not derivable from the D_{l-1} members of P of degree $l-1$. In this way we find that the basis is

$$(x_1^2,\ x_1 x_2^3,\ x_1 x_2^2 x_3^2,\ \ldots,\ x_2^8 x_3^{12}).$$

Thus the last *derived* member of degree 5 is $x_1 x_2^3 x_4$ (the last member of degree 4 multiplied by x_n or x_4); this gives 28 derived members of degree 5, but as there should be 24 members in all, there is one principal member $x_1 x_2^2 x_3^2$, the next after the last derived member $x_1 x_2^3 x_4$. The chief interest of this example is that it shows the extraordinary height to which the basis of P must ascend in general if P is to have the same D series as a given ideal.

Example (iii). As an example of the application of the formula of p. 551 consider the H-ideal determined by a generators of the same system on a quadric surface.

When l is sufficiently high each generator supplies $l+1$ conditions for a polynomial of degree l, independently of the conditions supplied by the other generators, so that $\chi(l) = a(l+1)$. But when l is low enough the conditions become those of containing the quadric surface; *i.e.* H_l is the coefficient of x^l in $(1-x^2)(1-x)^{-4}$, *i.e.* $(l+1)^2$ so long as this $\leqslant a(l+1)$, or so long as $l \leqslant a-1$; and is $a(l+1)$ when $l \geqslant a$. Hence the generating function $1+H_1x+H_2x^2+\ldots$ is

$$1+2^2x+3^2x^2+\ldots+a^2x^{a-1}+a(a+1)x^a+a(a+2)x^{a+1}+\ldots$$

or

$$(1+2x+\ldots+2x^{a-1}-\overline{a-1}x^a)(1-x)^{-2}.$$

The degree of the least polynomial which contains the generators but not the quadric is a, and its residual section with the quadric consists of a generators of the other system. The residual section of a general polynomial F_{a+b} of degree $a+b$ $(b > 0)$ through the a generators will be an irreducible curve C of order $a+2b$.

The inverse system (B) of p. 549 corresponding to the a generators is

$$\text{(B)} \qquad \sum_{p_1, p_2} (a_i x_3+\beta_i x_4)^{p_1}(\gamma_i x_3+\delta_i x_4)^{p_2}(x_1^{p_1} x_2^{p_2})^{-1} \qquad (i = 1, 2, \ldots, a),$$

where $x_1 = \alpha_i x_3 + \beta_i x_4$, $x_2 = \gamma_i x_3 + \delta_i x_4$ are the equations of the i-th generator. These a members of (B) are all of degree zero, and quite independent, because the generators have no points of intersection. Hence $G_l = a(l+1)$ when $l \geqslant 0$, and $G_l = 0$ when $l < 0$, *i.e.* G_l is the coefficient of x^l in $a(1-x)^{-2}$. Applying the formula of p. 551, taking M, M' to be the ideals which correspond to the generators and the curve C, and $\bar{M} = (F_2.\ F_{a+b})$, where F_2 is the quadric, we have

$$H'_l = \bar{H}_l - G_{l-\gamma+1} = \bar{H}_l - G_{l-a-b}$$

$$= \text{coefficient of } x^l \text{ in } (1-x^2)(1-x^{a+b})(1-x)^{-4} - ax^{a+b}(1-x)^{-2}$$

$$= \text{coefficient of } x^l \text{ in } (1+2x+\ldots+2x^{a+b-1} - \overline{a-1}x^{a+b})\,(1-x)^{-2}.$$

Similarly for G'_l. Thus $H'_l = H_l$, and similarly $G'_l = G_l$, when $b = 0$; this is as it should be, since M, M' are exactly alike when $b = 0$.

[*Note added July, 1927, on the Hilbert function of a prime ideal.* There are many reasons for supposing that the Hilbert function $\chi(l)$ of a prime ideal *having no point singularities* (or the "postulation" of the corresponding irreducible non-singular "variety" for hypersurfaces of sufficiently high degree l) is expressible in terms of certain *genera* (so called by analogy with the genus of a curve or surface). I suggest that this formula is the following:

$$\chi(l) = (l+1)_m + p_0(l)_m - p_1(l)_{m-1} + p_2(l)_{m-2} - \ldots + (-1)^m p_m,$$

where m is the number of dimensions of the spread (or variety), and p_i is the *arithmetic* genus of the section of it, of i dimensions, made by $m-i$ general hyperplanes $u_1 = u_2 = \ldots = u_{m-i} = 0$. Thus p_m is the arithmetic genus of the variety itself, and is further defined as follows: Project the variety into $(m+1)$-space, preserving its order unchanged; it will then have a double spread, in general of $m-1$ dimensions, not free from singularities [unless the original variety is already in $(m+1)$-space, in which case it will be already projected and have no double spread.] Let $\psi(l)$ be the polynomial in l to which the D_l of the double spread becomes equal when l is large enough [*i.e.* ψ is the function complementary to the Hilbert function of the double spread for $(m+1)$-space]; then $p_m = \psi(p_0 - m - 1)$, and $p_i = \Delta^{m-i}\psi(p_0 - i - 1)$, $p_0 = a - 1$ (the order of the variety less 1). If the D_l of the double spread is actually equal to $\psi(l)$ when $l \geqslant p_0-m-1$, the variety and all its sections are *regular;* otherwise the variety is *irregular.*

The evidence so far collected for the correctness of the formula is that it is true (i) for a principal ideal (F), the consideration of which first suggested the formula; (ii) for an H-ideal (F_1, F_2) of the principal class; (iii) for the intersection of three quadrics, and that of four quadrics; (iv) when $p_0 = 0$, as is evident, or $p_1 = 0$; (v) when $m = 1$ (Noether), or $m = 2$ (Severi). I was not aware that Severi had proved the last case until Professor H. F. Baker drew my attention to it. It is the only case among the above which includes any irregular varieties. The formula requires further testing for irregular varieties for three or more dimensions.]