On the Enumeration of Groups of Totitives. By Prof. H. W.

LLOYD TANNER. Received and read March 12th, 1896.

This paper explains a method of determining how many groups of given order can be formed with the totitives of any integer n . In the investigation use is made of a function formed from a binomial coefficient by replacing each factor, say r , of the numerator or denominator by $p^r - 1$, so that the binomial coefficient is, in fact, the limiting value of the function as p approaches 1.

There are indications of the existence of a reciprocity theorem [namely, that the number of groups of order r is equal to the number of groups of order $\tau(n)/\nu$], but this theorem is not proved. The attempt to establish the theorem has led to the discovery of some notable properties of the functions—a Vandermonde theorem, for instance—which will be found in the paper.

The functions in question are well known. They were used by Euler as generating functions for the number of partitions, and by Cayley.* Jacobi in a memoir "Ueber einige der Binomialreihe analoge Reihe," 1846 (*Crelle*, xxxii.; *Ges. Werke*, Bd. II., 163–173), starting with a more general function, obtained a number of formulæ which appear to be different from those used in this paper. Gauss in the famous *Summatio serierum quarundam singularium* used these functions, the base being a complex number of modulus 1. They have been used too (in Schellbach's treatise) as a means of forming the theta-functions. The present application is of a different kind. As in Euler's theory, they are used for enumeration; but the number sought is given by the actual value of the function when the base p is a prime factor of rn .

A portion of the following (Arts. 1–17) was communicated to the Society just five years ago as a part of the paper under the title "Some Theorems concerning Groups of Totitives of n ." When revising that paper for the press I found (thanks to the criticism of my colleague Mr. Pinkerton) a flaw in the proof of the reciprocity theorem, and therefore asked permission to withdraw it. Although I am not yet able to give a proof of the theorem, I hope that the

* "Researches on the Partition of Numbers," *Phil. Trans.*, cxlv., C. M. P., Vol. II., p. 243, &c.

method of enumeration and the properties of the functions employed will be acceptable to the Society.

1. The group of all the totitives of n is expressible in one way only (I. 22, 23)* as a product of sub-groups $G_p, G_q, \dots, G_r$, where G_p consists of all the totitives whose orders are powers of p ; $G_q, \dots, G_r$ have the like meaning with respect to $q, \dots, r$; and $p, q, \dots, r$ are all the prime factors of τn .

Similarly any sub-group, G' , of totitives of n is expressible in one way only as a product

$$G'_p, G'_q, \dots, G'_r,$$

where G'_p includes all elements of G' whose orders are powers of p , and so for $G'_q, \dots, G'_r$.

We shall consider two groups, say G', G'' , to be different if either contains an element that is not contained in the other. Thus, if G'_p and G''_p are different groups, the two products

$$G'_p, G'_q, \dots, G'_r \quad \text{and} \quad G''_p, G'_q, \dots, G_r$$

are different. Now suppose that there are P different sub-groups G'_p , which are factors of G_p , counting G_p itself and 1 as sub-groups; and, similarly, Q different groups G'_q which are factors of $G_q, \dots$, and R different groups G'_r factors of G_r . Then it is clear that the number of all the different groups G' (including G and 1) which are factors of G is the product $PQ \dots R$. The problem of enumerating the different groups G' of the totitives of n is thus reduced to the simpler problem of enumerating the different groups G'_p which are factors of G_p , p being any one of the prime factors of τn .

2. The group G_p naturally presents itself as a product of simple independent groups which may be obtained in a canonical form in the following way.

Let
$$n = p^a \cdot q^\beta \dots r^\gamma,$$

where $p, q, \dots, r$ are different primes, and $a, \beta, \dots, \gamma$ are positive integers, but a may be zero. Then the q^β numbers

$$knq^{-\beta} + 1, \quad k = 0, 1, 2, \dots, q^\beta - 1$$

* The reference is to § I., Arts. 21, 22, of a memoir "On Cyclotomic Functions," *Proc. Lond. Math. Soc.*, Vol. xx., pp. 63-83. Similar abbreviations are used in the sequel.

are all prime to $p, \dots, r$, but $1/q$ of them are multiples of q . The rest, $(q-1)q^{s-1}$ in number, make up a group of totitives of n isomorphic with the group of all the totitives of q^s . Hence, if p^r is the highest power of p which is a factor of $q-1$ (so that λ may be zero), this group of totitives of n contains as a factor a simple group of order p^r , and no other elements of G_p . The same process applies to each prime factor of n except p itself. If α , the exponent of p in n , is greater than 1, then there is in general a group of order $p^{\alpha-1}$ consisting of totitives of the form $kpq^s \dots r^v + 1$ ($k=0, 1, 2, \dots, p^{\alpha-1}-1$). There is an exception when $p=2$, in which case the simple group of order $p^{\alpha-1}$ is replaced by the product of two simple groups of orders 2 and $2^{\alpha-1}$, respectively.

3. Using the notation of (I. 33), we shall represent by h_i the number of simple groups of order p^i contained in the canonical form of G_p just obtained, where $i=1, 2, \dots, \mu$ and p^μ is the order of the largest simple group present.

By k_i we denote how many factor groups are of order p^i at least. Thus

$$k_i = h_i + h_{i+1} + \dots + h_\mu.$$

K_i is defined by the equation

$$K_i = k_1 + k_2 + \dots + k_i;$$

so that $K_i = h_1 + 2h_2 + \dots + (i-1)h_{i-1} + i(h_i + h_{i+1} + \dots + h_\mu)$.

It follows that $K_i - K_{i-1} = k_i$;

and, since $K_1 = k_1$, this gives $K_0 = 0$.

4. The numbers h_i, k_i, K_i have been obtained from a special form of the group G_p ; but they have a significance with respect to G_p itself, and are independent of the particular mode in which G_p is represented. For p^{K_i} is the number of elements in G_p of order not greater than p^i (I. 33). This number, and therefore K_i , is evidently independent of the way in which G_p may be factorized. Hence also $k_i = K_i - K_{i-1}$, and $h_i = k_i - k_{i+1}$, are invariants of G_p as well as K_i .

5. It will be convenient, before attacking the general case, to consider the particular case in which G_p is the product of h_1 independent groups of order p . Then G_p contains p^{h_1} elements of which one is of order 1, and p^{h_1} elements of which one is of order 1 and $p^{h_1}-1$ are of order p . Now any group of order p contains $p-1$

elements of order p , and none of these elements can be common to two different groups of order p . Hence the number of different groups of order p which can be formed from the elements of G_p is

$$(p^{h_1}-1)/(p-1).$$

A group of order p^2 must, in this particular case, be the product of two groups of order p —say A, B . Now A may be any one of the $(p^{h_1}-1)/(p-1)$ different groups formed from the elements of G_p ; but A being selected removes $p-1$ of the elements of order p , and leaves only $p^{h_1}-p$ available for the making of B . Thus there are $(p^{h_1}-1)/(p-1)$ different groups B for each group A , and therefore there are $(p^{h_1}-1)(p^{h_1}-p)/(p-1)^2$ different products A, B : if by “different products” we understand products in which either the first factors are different, or the second factors are different, or both different. Now clearly “different products” do not necessarily constitute different groups; in fact, taking a G_p of order p^2 , so that $h_1 = 2$, we find that any product of two simple groups of order p is represented by

$$(p^2-1)(p^2-p)/(p-1)^2$$

different products. Hence the number of different groups of order p^2 that can be formed with elements of G_p is found, on dividing the number of different products A, B by this last number, to be

$$\frac{(p^{h_1}-1)(p^{h_1-1}-1)}{(p^2-1)(p-1)}.$$

This function will be denoted by $\left\{ \begin{smallmatrix} h_1 \\ 2 \end{smallmatrix} \right\}$ in imitation of a well-known notation for binomial coefficients.

Similarly, we shall write

$$\left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} \text{ for } \frac{(p^h-1)(p^{h-1}-1)\dots(p^{h-i+1}-1)}{(p^i-1)(p^{i-1}-1)\dots(p-1)}$$

(h, i being positive integers); from which it follows that

$$\left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} h \\ h-i \end{smallmatrix} \right\} \dots\dots\dots (1),$$

$$\text{and that } \left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} \Big/ \left\{ \begin{smallmatrix} h \\ i-1 \end{smallmatrix} \right\} = \frac{p^{h-i+1}-1}{p^i-1} = \left\{ \begin{smallmatrix} h-i+1 \\ 1 \end{smallmatrix} \right\} \Big/ \left\{ \begin{smallmatrix} i \\ 1 \end{smallmatrix} \right\} \dots (2).$$

6. It can now be shown, by induction from $i-1$ to i , that $\left\{ \begin{smallmatrix} h_1 \\ i \end{smallmatrix} \right\}$ different groups of order p^i can be formed from the elements of G_p .

In fact, we may represent such a group as a product of two groups, A of order p^{i-1} and B of order p . By hypothesis, there are $\left\{ \begin{smallmatrix} h_1 \\ i-1 \end{smallmatrix} \right\}$ different groups A , and each takes up $p^{i-1}-1$ of the elements of order p , leaving p^h-p^{i-1} such elements available for the formation of B . The number of different products thus made is

$$\left\{ \begin{smallmatrix} h_1 \\ i-1 \end{smallmatrix} \right\} \cdot \frac{(p^{h_1-i+1}-1)}{p-1} p^{i-1} = \left\{ \begin{smallmatrix} h_1 \\ i-1 \end{smallmatrix} \right\} \left\{ \begin{smallmatrix} h_1-i+1 \\ 1 \end{smallmatrix} \right\} p^{i-1}$$

But, on putting $h_1 = i$ in this formula, it is seen that one group of order p^i is represented by

$$\left\{ \begin{smallmatrix} i \\ i-1 \end{smallmatrix} \right\} p^{i-1} = \left\{ \begin{smallmatrix} i \\ 1 \end{smallmatrix} \right\} p^{i-1}$$

different products. Hence on division it appears that there are

$$\begin{aligned} \left\{ \begin{smallmatrix} h \\ i-1 \end{smallmatrix} \right\} \left\{ \begin{smallmatrix} h-i+1 \\ 1 \end{smallmatrix} \right\} / \left\{ \begin{smallmatrix} i \\ 1 \end{smallmatrix} \right\} &= \left\{ \begin{smallmatrix} h \\ i-1 \end{smallmatrix} \right\} \left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} / \left\{ \begin{smallmatrix} h \\ i-1 \end{smallmatrix} \right\} \quad [\text{by (2)}] \\ &= \left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} \end{aligned}$$

different groups of order p_i formed from the elements of G_p .

Hence the theorem is true for i if true for $i-1$; and, having been proved for $i-1 = 1, 2$, it is established generally.

7. A consequence of (1), Art. 5, is that, for this particular form of G_p , there are as many different groups of order p^a as there are of order p^{h-a} . The converse is also true—viz., if the groups of order p^a , p^b are equi-numerous, then either $a = b$ or $a + b = h$. For it is clear from (2) of Art. 5 that $\left\{ \begin{smallmatrix} h_1 \\ i \end{smallmatrix} \right\}$ always increases with i when $i+1 < h_1-i$, and decreases as i increases when $h_1-i < i+1$.

General Case. (Arts. 8-15.)

8. In the general case, G_p is a product of k_i simple independent groups—viz., h_i groups of order p_i when $i = 1, 2, \dots, \mu$. A group G'_p , which is a factor of G_p , is a product of k'_i simple independent groups, of which h'_i are of order p^i ($i = 1, 2, \dots, \mu$). It is convenient to extend to accented letters the notation of Art. 3, so that h' , k' , K' have the same meanings in reference to G'_p as h , k , K in reference to G . We proceed to enumerate the number of different groups G'_p for which all the h' are given.

9. G_p contains p^{K_i} elements of order not greater than p^i , and therefore the number of elements of order p^i is

$$p^{K_i} - p^{K_{i-1}} = p^{K_{i-1}} (p^{k_i} - 1).$$

Each of these elements can serve as base of a group of order p^i ; no one of them can be common to two different groups of this order, and every such group contains $p^i - p^{i-1}$ of them. Therefore the number of different monobasic groups of order p^i contained in G_p is

$$p^{K_{i-1}} (p^{k_i} - 1) / p^{i-1} (p - 1) = p^{K_{i-1} - i + 1} \left\{ \begin{matrix} k_i \\ 1 \end{matrix} \right\}$$

10. The investigation might be continued on the lines of Art. 5, but it seems better to use a different process suggested by the form of the last result, which has the advantage of interpreting the two factors.

Let A denote any simple group of order p^i formed from the elements of G_p , having a for its base, and write a for $a^{p^{i-1}}$, so that the group

$$(a, a^p, \dots, a^{p^{i-1}} = 1)$$

is the group of order p that is included in A . This group will be called the penultimate group of A (or of a). It will be observed that a is characterized by being of order p and at the same time a power $a^{p^{i-1}}$. The penultimate group, including all the a 's, is of order p^{k_i} , for it is the penultimate of the product of the k_i groups (order $\geq p^i$). Thus the factor

$$\left\{ \begin{matrix} k_i \\ 1 \end{matrix} \right\}$$

of the result in Art. 9 expresses the number of different penultimate groups in G_p each of which can be the penultimate of a simple group of order p^i . The other factor shows how many different groups of order p^i belong to one and the same penultimate. (Uf. Art. 12.)

11. The number of different penultimate groups in G_p which can be penultimate of G'_p is

$$\prod_i \left\{ \begin{matrix} k_i - k'_i + h'_i \\ h'_i \end{matrix} \right\} = \prod_i \left\{ \begin{matrix} k_i - k'_{i+1} \\ k'_i - k'_{i+1} \end{matrix} \right\}$$

Here h'_i, k'_i are supposed to be known for all values of i ; but G'_p represents any group which is (i.) a factor of G_p , (ii.) has the given constants h'_i, k'_i , but is otherwise unconditioned.

In forming the above expression, we begin with the h'_μ groups of order p^μ in G_p , and then consider in succession the groups of lower order. Now the penultimate of the h'_μ groups of G'_p is necessarily a factor of the penultimate of the h_μ groups (order p_μ) of G_p . Hence (Art. 6) there are

$$\begin{Bmatrix} k_\mu \\ h'_\mu \end{Bmatrix}$$

different penultimates available for the h'_μ groups of G'_p . [This is what the specimen factor of Π becomes when $i = \mu$, since $k'_\mu = h'_\mu$ and $h'_{\mu+1} = 0$. If $h'_\mu = 0$, the value 1 is to be assigned to the symbol.]

Consider now the penultimate of the h'_i groups of G'_p which are of order p^i . It must be a factor of the penultimate of the k_i groups of G_p whose orders are $\geq p^i$. But, of these k_i groups, h'_{i-1} have already been taken up by the p^{i+1} -ordinal groups of G'_p , h'_{i+2} by the groups of order p^{i+2} , and the penultimate of G_p still available for a penultimate of the p^i -ordinal groups of G'_p is a product of

$$k_i - h'_{i+1} - h'_{i+2} - \dots - h'_\mu = k_i - k'_{i+1} = k_i - k'_i + h'_i$$

groups of order p .

From the elements of this product, we can obtain (Art. 6)

$$\begin{Bmatrix} k_i - k'_i + h'_i \\ h'_i \end{Bmatrix} = \begin{Bmatrix} k_i - k'_{i+1} \\ h'_i - k'_{i+1} \end{Bmatrix}$$

different groups of order p^i , each of which is a penultimate of h'_i p^i -ordinal groups.

The product of the numbers just obtained— i being replaced by 1, 2, ..., μ in turn—gives the number of different penultimates of G_p which are penultimates of a G'_p with the given h'_i , k'_i , and this is the statement that was to be proved.

12. To every penultimate group of G_p there correspond

$$\Pi p^{k'_i(K_{i-1} - K'_{i-1})} = p^{\sum h'_i(K_{i-1} - K'_{i-1})}$$

different groups G'_p .

For let a be the base of one of the simple groups in the selected penultimate, and let this simple group be the penultimate of a group of order p^i in G'_p . If a is the base of the last-named group in any one of the groups G'_p , then a is a solution of the congruence

$$a^{p^{i-1}} \equiv a, \text{ mod } n;$$

and ab is a solution if, and only if, b is of order p^{i-1} at most. The number of multipliers b (including unity) is therefore $p^{K_{i-1}}$. The same thing may be done with each of h'_i groups of order p^i , and thus it is seen that, for a given penultimate, we have

$$\prod p^{h'_i K_{i-1}}$$

representations of G'_p which differ from each other in the bases of the several groups. It is obvious, however, that different representations do not mean different groups G'_p ; and, by putting $h_i = h'_i$ (and therefore $K_{i-1} = K'_{i-1}$) for all values of i , we find, from the above formula, that G'_p admits of

$$\prod p^{h'_i K'_{i-1}}$$

different representations. Dividing the former by the latter number, it is found that there are

$$\prod_i p^{h'(K_{i-1} - K'_{i-1})}$$

different groups G'_p the penultimate of which are identical.

13. Combining the results of Arts. 11, 12, we find that the number of different groups G'_p (with given values of h'_i) that can be formed from the elements of a group G_p is

$$p^{\sum_i h'_i (K_{i-1} - K'_{i-1})} \cdot \prod_i \left\{ \frac{h_i - h'_i + h'_i}{h'_i} \right\},$$

where $i = 1, 2, \dots, \mu$. But, since the specimen factor becomes 1 when $h'_i = 0$, it is only needful to consider those values of i for which h'_i does not vanish.

14. To obtain the number of different groups G'_p of given order $p^{\omega'}$, we must form all the sets $h'_1, h'_2, \dots, h'_\mu$ which satisfy the equation

$$\omega' = h'_1 + 2h'_2 + \dots + \mu h'_\mu,$$

subject to the condition that for every value of i

$$h'_i = h'_i + h'_{i+1} + \dots + h'_\mu \leq h_i,*$$

and then calculate the number of groups G'_p for each system. The sum of these numbers is the number of different groups of the proposed order that are contained in G_μ .

* If any set of h' is used in which the condition is violated, the number involves a vanishing factor $\{ \}$ in which the lower symbol is greater than the upper. Accordingly the condition may be ignored if convenient.

15. For the sake of reference, the formulæ are here given for $\omega' = 1, 2, 3, 4$. An example which follows (Art. 17) will sufficiently explain the details of the calculations.

Order of G'_p .	Number of different groups G'_p .	Sets of K .
p' $\left\{ \begin{smallmatrix} k_1 \\ 1 \end{smallmatrix} \right\}$		1
p^2 $\left\{ \begin{smallmatrix} k_1 \\ 2 \end{smallmatrix} \right\} + p^{K_1-1} \left\{ \begin{smallmatrix} k_2 \\ 1 \end{smallmatrix} \right\}$		20; 01
p^3 $\left\{ \begin{smallmatrix} k_1 \\ 3 \end{smallmatrix} \right\} + p^{K_1-2} \left\{ \begin{smallmatrix} k_1-1 \\ 1 \end{smallmatrix} \right\} + p^{K_1-3} \left\{ \begin{smallmatrix} k_2 \\ 1 \end{smallmatrix} \right\}$		300; 110; 001
p^4 $\left\{ \begin{smallmatrix} k_1 \\ 4 \end{smallmatrix} \right\} + p^{K_1-3} \left\{ \begin{smallmatrix} k_1-1 \\ 2 \end{smallmatrix} \right\} \left\{ \begin{smallmatrix} k_2 \\ 1 \end{smallmatrix} \right\} + p^{2K_1-4} \left\{ \begin{smallmatrix} k_2 \\ 2 \end{smallmatrix} \right\}$ $+ p^{K_1-3} \left\{ \begin{smallmatrix} k_1-1 \\ 1 \end{smallmatrix} \right\} \left\{ \begin{smallmatrix} k_2 \\ 1 \end{smallmatrix} \right\} + p^{K_1-3} \left\{ \begin{smallmatrix} k_2 \\ 1 \end{smallmatrix} \right\}$		400; 210; 020 101; 0001.

16. As an example of the mode of working, I take G_p to be the product of four simple groups of orders p^4, p^4, p^3, p , respectively; so that $h_1 = 1, h_2 = 1, h_3 = 0, h_4 = 2$. It will sometimes be useful to symbolize such a group by 4421.

Instances of this group are given by the totitives of

$$n = 5440 = 2^8 \cdot 5 \cdot 17 \quad (\tau n = 2 \cdot 2^4 \times 2^3 \times 2^4),$$

or by the group G_2 for

$$n = 28815 = 3 \cdot 5 \cdot 17 \cdot 113 \quad (\tau n = 2 \times 2^3 \times 2^4 \times 7 \cdot 2^4),$$

or, again, by the group G_3 for

$$n = 5267997 = 3^5 \cdot 7 \cdot 19 \cdot 163 \quad (\tau n = 2 \cdot 3^4 \times 2 \cdot 3 \times 2 \cdot 3^3 \times 2 \cdot 3^4).$$

In each of these instances the other G_p are of a simple character, so that the complete enumeration of the groups of totitives of any proposed order for each of these values of n is effected with ease.

17. It is convenient to arrange the values of h_i, k_i, K in a table, thus—

i	h_i	k_i	K_{i-1}
1	1	4	.
2	1	3	4
3	.	2	7
4	2	2	9

In the same way the number of groups of order p^7 is found as in the following table:—

		p^0	p	p^2	p^3	p^4	p^5	p^6	p^7
43	$p^6 \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	.	.	.	.	.	1	1
421	$p^4 \begin{Bmatrix} 2 \\ 1 \end{Bmatrix} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	.	.	.	1	3	3	1
4111	$p^3 \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	.	.	1	1	.	.	.
331	$p^4 \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	.	.	.	1	1	.	.
322	$p^3 \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	.	.	1	1	.	.	.
3211	$p \begin{Bmatrix} 2 \\ 1 \end{Bmatrix} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	.	1	2	1	.	.	.	.
2221	1	1	.	.	.	.	.	.	.

$$\text{Sum} = 1 + p + 2p^2 + 3p^3 + 4p^4 + 4p^5 + 4p^6 + 2p^7.$$

It will be observed that the number of different groups G_p of order p^4 is equal to the number of groups G_p of order p^7 , these orders being complementary ($p^4 \times p^7 = p^{11}$, the order of G_p).

18. As a second example I take G_p to be a product of two simple groups of orders p^α, p^β , where $\alpha \leq \beta$. The table for G_p is

i	h_i	k_i	K_{i-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	0	2	$2i-2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
α	1	2	$2\alpha-2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	0	2	$\alpha+i-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
β	1	1	$\alpha+\beta-1,$

and it will appear that the number of groups of order p , is

$$\left\{ \begin{smallmatrix} s+1 \\ 1 \end{smallmatrix} \right\} \quad \text{or} \quad \left\{ \begin{smallmatrix} \alpha+1 \\ 1 \end{smallmatrix} \right\} \quad \text{or} \quad \left\{ \begin{smallmatrix} \alpha+\beta-s+1 \\ 1 \end{smallmatrix} \right\},$$

when $s \leq \alpha$ or $\alpha \leq s \leq \beta$ or $\beta \leq s$.

In the boundary cases the two formulæ applicable are equivalent. And here again the complementary theorem is true.

Clearly G'_p is a product of 2 or 1 simple groups, and in the following enumeration I have indicated the orders of these groups in the first column, and the number in the second; the three cases being separately considered.

CASE I. $s \leq \alpha$.

Type of G'_p .	No. of G'_p .	
0, s	$p^{s-1} \left\{ \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\}$	
1, $s-1$	$p^{s-3} \left\{ \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\}$	
$\vdots$		
$t, s-t$	$p^{s-2t-1} \left\{ \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\}$	
$\vdots$		
$s/2, s/2$	1	when s is even
or $(s-1)/2, (s+1)/2$	$\left\{ \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\}$	when s is odd.

For the type $t, s-t$, the auxiliary table gives

$$h'_t = 1, \quad k_t - k'_t = 0, \quad K_{t-1} - K'_{t-1} = 0,$$

and

$$h'_{s-t} = 1, \quad k_{s-t} - k'_{s-t} = 1,$$

$$K_{s-t-1} - K'_{s-t-1} = 2s - 2t - 2 - (s-1) = s - 2t - 1.$$

The sum of the numbers in the second column is

$$p^s + p^{s-1} + \dots + 1 = \left\{ \begin{smallmatrix} s+1 \\ 1 \end{smallmatrix} \right\}.$$

CASE II. $\alpha \leq s \leq \beta$.

Type of G'_p .	No. of G'_p .	
0, s	p^α	
$\vdots$		
$t, s-t$	$p^{\alpha-t}$	where $s-t > \alpha$
$\vdots$		
$s-\alpha, \alpha$	$p^{2\alpha-s-1} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	
$s-\alpha+t, \alpha-t$	$p^{2\alpha-s-2t-1} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	
$\vdots$	$\vdots$	
$s/2, s/2$	1	when s is even
or $(s-1)/2, (s+1)/2$	$\begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	when s is odd.

The total number here is

$$p^\alpha + p^{\alpha-1} + \dots + 1 = \begin{Bmatrix} \alpha+1 \\ 1 \end{Bmatrix}$$

CASE III. $\beta \leq s$.

Type of G'_p .	No. of G'_p .	
$s-\beta, \beta$	$p^{\alpha+\beta-s}$	
$\vdots$		
$s-\beta+t, \beta-t$	$p^{\alpha+\beta-s-t}$	$(\beta-t > \alpha$
$\vdots$		
$s-\alpha, \alpha$	$p^{2\alpha-s-1} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	
$\vdots$		
$s-\alpha+t, \alpha-t$	$p^{2\alpha-s-2t-1} \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$	
$\vdots$		
$s/2, s/2$	1	if s is even
or $(s-1)/2, (s+1)/2$	$\begin{Bmatrix} s \\ 2 \end{Bmatrix}$	if s is odd,

and the number is $\begin{Bmatrix} \alpha+\beta-s+1 \\ 1 \end{Bmatrix}$

This table is formed on the supposition that s is not greater than 2α . If s is greater than 2α , the final group is of the type $\alpha, s-\alpha$ (the

latter the greater number) because G'_p cannot contain two groups of order greater than α , and therefore is only one group G'_p of this type. The total number therefore is the same as before.

19. The examples already given suggest the existence of a theorem that the number of different groups G'_p of a given order p' that can be formed with elements of a group G_p of order p'^{r+s} is the same as the number of different groups G''_p of order p'' that can be formed with elements of G_p . In seeking a direct proof—or the conditions of failure—of this theorem (which still remain to find), some interesting results have come to light which are given in the sequel. It will furnish opportunities of illustrating these incidental theorems if I now explain how they were to be used.

20. A reference to Art. 15 will show that the denumerant of Art. 13 rapidly increases in complication with the order of G'_p . In order to verify the theorem by the use of this formula it would be needful to prove the identity of two expressions, one of which becomes so much the more complicated as the other becomes simpler. Obviously it was desirable to transform the denumerant so that it would assume a simple form when the order of G'_p is nearly equal to that of G_p ; and then compare the denumerants of the complementary groups each in its most manageable shape.

For this we introduce a new set of constants γ, δ, Δ characterizing G'_p , and connected with h', k', K' by the equations

$$h'_i = h_i - \gamma_i, \quad k'_i = k_i - \delta_i, \quad K'_i = K_i - \Delta_i,$$

so that

$$\delta_i = \gamma_i + \gamma_{i+1} + \dots + \gamma_r,$$

$$\Delta_i = \delta_1 + \delta_2 + \dots + \delta_i,$$

recalling the equations of Art. 3. The γ , however, unlike the h' , may be negative. For instance, a simple group of order p^2 ($h_1 = 0, h_2 = 1$) has factor groups of order p ($h'_1 = 1, h'_2 = 0$), so that in this case $\gamma_1 = -1, \gamma_2 = 1$. It follows then that, unlike the k' , the δ_i are not arranged in order of magnitude. For

$$\delta_i - \delta_{i+1} = \gamma_i$$

may be either negative or positive. The δ must all be positive (or zero) because

$$\delta_i = k_i - k'_i,$$

and the latter expression cannot be negative.

21. The original form of the denominator was

$$p^{\sum h'_i (K_{i-1} - K'_{i-1})} \prod \left\{ \begin{matrix} k_i - k'_i + h'_i \\ h'_i \end{matrix} \right\}$$

The second factor becomes, when $k_i - k'_i$, h'_i are replaced,

$$\left\{ \begin{matrix} \delta_i + h_i - \gamma_i \\ h_i - \gamma_i \end{matrix} \right\} = \left\{ \begin{matrix} \delta_i + h_i - \gamma_i \\ \delta_i \end{matrix} \right\} = \left\{ \begin{matrix} h_i + \delta_{i+1} \\ \delta_i \end{matrix} \right\}$$

The exponent of $p = \sum h'_i (K_{i-1} - K'_{i-1}) = \sum (k'_i - k'_{i+1}) (K_{i-1} - K'_{i-1})$

$$= \sum k'_i (K_{i-1} - K'_{i-2}) - k'_i (K'_{i-1} - K'_{i-2})$$

$$= \sum k'_i (k_{i-1} - k'_{i-1})$$

$$= \sum (k_i - \delta_i) \delta_{i-1}.$$

Hence the transformed denominator is

$$p^{\sum \delta_{i-1} k_i - \delta_i \delta_{i-1}} \prod \left\{ \begin{matrix} h_i + \delta_{i+1} \\ \delta_i \end{matrix} \right\}.$$

The number of groups G'_p of given order $p^{\omega'}$ is the sum of the denominators for all G'_p such that

$$\omega' = K_p = k'_1 + k'_2 + \dots + k'_\mu,$$

and every partition of ω' determines one type of G'_p . The number of groups G''_p of complementary order $p^{K_p - \omega'} (= p^{\Delta_p})$ is the sum of the denominators for all G''_p such that

$$\Delta_p = K_p - (K_p - \omega') = \omega',$$

that is to say,

$$\delta_1 + \delta_2 + \dots + \delta_\mu = \omega'.$$

Here the δ are positive integers, but their sequence is not determined, and each *composition* of ω' corresponds to a set of groups of order $p^{\omega'}$.

22. Some examples of the developed formulæ for the numbers of groups of given order nearly equal to the order of G_p follow. (Cf. Art. 15.)

I. For factors of G_p of order p^{-1} we require the compositions of 1,

$$\delta_1 + \delta_2 + \dots + \delta_\mu = 1.$$

These are given by $\delta_i = 1$, and every other $\delta = 0$. The number of

groups for which $\delta_i = 1$ is

$$p^{k_{i+1}} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\}$$

and the total number is $\sum_i p^{k_{i+1}} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\} \quad (i = 1, 2, \dots, \mu).$

II. When the order of G'' is p^{*-2} , the compositions

$$\delta_1 + \dots + \delta_i + \dots + \delta_\mu = 2$$

are of two sets $\delta_i = 2$ and $\delta_i = 1, \delta = 1$,
the other δ being 0.

The first set contributes

$$\sum p^{2p_{i+1}} \left\{ \begin{matrix} h_i \\ 2 \end{matrix} \right\}$$

to the total number.

The second set answers to different numbers according as i, j are or are not consecutive. In the general case when i, j are not consecutive the contribution is

$$\sum_{i,j} p^{k_{i+1} + k_{j+1}} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} \quad (i+1 < j).$$

But, if $\delta_i = 1, \delta_{i+1} = 1$, the number of corresponding groups is

$$\sum p^{k_{i+1} - 1 + k_{i+2}} \left\{ \begin{matrix} h_i + 1 \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\}.$$

III. For the order p^{*-3} , we have the compositions

$$(\delta_i = 3);$$

$$(\delta_i = 2, \delta_j = 1); (\delta_i = 2, \delta_{i+1} = 1); (\delta_i = 1, \delta_{i+1} = 2);$$

$$(\delta_i = 1, \delta_j = 1, \delta_i = 1); (\delta_i = 1, \delta_{i+1} = 1, \delta_j = 1);$$

$$(\delta_i = 1, \delta_{i+1} = 1, \delta_{i+2} = 1);$$

and the number of groups is

$$\begin{aligned} & \sum p^{3k_{i+1}} \left\{ \begin{matrix} h_i \\ 3 \end{matrix} \right\} \\ & + \sum p^{2k_{i+1} + k_{j+1}} \left\{ \begin{matrix} h_i \\ 2 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} \quad (j < i-1 \text{ or } i+1 < j) \end{aligned}$$

$$\begin{aligned}
& + \Sigma p^{2k_{i+1} + k_{i+2} - 2} \left\{ \begin{matrix} h_i + 1 \\ 2 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \\
& + \Sigma p^{k_{i+1} + 2k_{i+2} - 2} \left\{ \begin{matrix} h_i + 2 \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+1} \\ 2 \end{matrix} \right\} \\
& + \Sigma p^{k_{i+1} + k_{j+1} + k_{i+1}} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\} \quad (i+1 < j, j+1 < l) \\
& + \Sigma p^{k_{i+1} + k_{i+2} + k_{j+1} - 1} \left\{ \begin{matrix} h_i + 1 \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} \quad (j < i-1 \text{ or } i+2 < j) \\
& + \Sigma p^{k_{i+1} + k_{i+2} + k_{i+3} - 2} \left\{ \begin{matrix} h_i + 1 \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+1} + 1 \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_{i+2} \\ 1 \end{matrix} \right\}
\end{aligned}$$

23. The first theorem that assists in the identification of the two total denumerants is analogous to the Vandermonde theorem for binomial coefficients and is thus stated.

If r and s be two positive integers less than n (also a positive integer),

$$\left\{ \begin{matrix} n \\ r \end{matrix} \right\} = \left\{ \begin{matrix} n-s \\ r-s \end{matrix} \right\} + \dots + p^{t(r-s+t)} \left\{ \begin{matrix} n-s \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} + \dots + p^r \left\{ \begin{matrix} n-s \\ r \end{matrix} \right\} \dots\dots\dots(s).$$

The last term written corresponds to $t = s$ and implies that $r \leq n-s$, that is, $r+s \leq n$. If $n < r+s$, the actual last term is that for which $t = n-r$, namely,

$$p^{(n-r)(n-s)} \left\{ \begin{matrix} s \\ n-r \end{matrix} \right\},$$

and, if $n = r+s$, the actual last term is that for which $t = s = n-r$, namely, the term p^r . It is, however, indifferent which is written, because the only effect of writing the wrong one is to add so many zero terms.

The theorem can be expressed in other forms, because of the identities such as

$$\left\{ \begin{matrix} s \\ t \end{matrix} \right\} = \left\{ \begin{matrix} s \\ s-t \end{matrix} \right\},$$

by means of which we can make either or both of the lower elements in each term decrease as t increases. The above form seems to be the standard, because in it the index of p is the product of the two lower elements. Besides these changes we may replace r by $n-r$, since this does not alter the value of the left side.

24. When $s = 1$, the theorem becomes

$$\left\{ \begin{matrix} n \\ r \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ r-1 \end{matrix} \right\} + p^r \left\{ \begin{matrix} n-1 \\ r \end{matrix} \right\} \dots\dots\dots(1),$$

and is at once verified by the definition. For

$$\begin{aligned} & \left\{ \begin{matrix} n \\ r \end{matrix} \right\} - \left\{ \begin{matrix} n-1 \\ r-1 \end{matrix} \right\} \\ &= \frac{(p^n-1)(p^{n-1}-1)\dots(p^{n-r+1}-1)}{(p^r-1)(p^{r-1}-1)\dots(p-1)} - \frac{(p^{n-1}-1)\dots(p^{n-r+1}-1)}{(p^{r-1}-1)\dots(p-1)} \\ &= \frac{(p^{n-1}-1)\dots(p^{n-r+1}-1)}{(p^r-1)\dots(p-1)} \{p^n-1-(p^r-1)\} \\ &= \dots\dots\dots (p^{n-r}-1)p^r \\ &= \left\{ \begin{matrix} n-1 \\ r \end{matrix} \right\} p^r. \end{aligned}$$

The proof for any other value of s is effected by induction from $s-1$ to s . Assuming the theorem to be true for $s-1$,

$$\left\{ \begin{matrix} n \\ r \end{matrix} \right\} = \sum p^{t(r-s+1+t)} \left\{ \begin{matrix} s-1 \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s+1 \\ r-s+1+t \end{matrix} \right\} \dots\dots\dots(s-1).$$

But, by (1),

$$\left\{ \begin{matrix} n-s+1 \\ r-s+1+t \end{matrix} \right\} = \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} + p^{r-s+1+t} \left\{ \begin{matrix} n-s \\ r-s+1+t \end{matrix} \right\}.$$

Thus the term of $(s-1)$ written above—say the term t —is separated into two parts

$$\begin{aligned} & p^{t(r-s+1+t)} \left\{ \begin{matrix} s-1 \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} + p^{(t+1)(r-s+1+t)} \left\{ \begin{matrix} s-1 \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-s+1+t \end{matrix} \right\} \\ & \dots\dots\dots(t). \end{aligned}$$

Now, if we combine the first part of the term t with the second part of the term $(t-1)$ similarly analysed, we obtain

$$\begin{aligned} & p^{t(r-s+1+t)} \left\{ \begin{matrix} s-1 \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} + p^{t(r-s+t)} \left\{ \begin{matrix} s-1 \\ t-1 \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} \\ &= p^{t(r-s+t)} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} \left[p^t \left\{ \begin{matrix} s-1 \\ t \end{matrix} \right\} + \left\{ \begin{matrix} s-1 \\ t-1 \end{matrix} \right\} \right] \\ &= p^{t(r-s+t)} \left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\} \left\{ \begin{matrix} s \\ t \end{matrix} \right\} \quad \text{by (1),} \end{aligned}$$

and this is the term t of the expansion (s) . In this way every term of (s) is obtained except the first and the last. But, by putting $t = 0$ in (t) it is verified that the first part of the first term of $(s-1)$ is the first term of (s) ; and, by putting $t = s-1$ in (t) , that the second part of the last term of $(s-1)$ is the last term of (s) . Hence

$$(s) = (s-1) = \dots = (1) = \left\{ \begin{matrix} n \\ r \end{matrix} \right\}$$

25. In the identity (s) replace $\left\{ \begin{matrix} n \\ r \end{matrix} \right\}$ by $\left\{ \begin{matrix} n \\ n-r \end{matrix} \right\}$ and $\left\{ \begin{matrix} n-s \\ r-s+t \end{matrix} \right\}$ by $\left\{ \begin{matrix} n-s \\ n-r-t \end{matrix} \right\}$ for all values of t . Then write r for $n-r$. The identity then becomes

$$\left\{ \begin{matrix} n \\ r \end{matrix} \right\} = \left\{ \begin{matrix} n-s \\ r \end{matrix} \right\} + \dots + p^{t(n-r-s+t)} \left\{ \begin{matrix} s \\ t \end{matrix} \right\} \left\{ \begin{matrix} n-s \\ r-t \end{matrix} \right\} + \dots + p^{s(n-r)} \left\{ \begin{matrix} n-s \\ r-s \end{matrix} \right\}.$$

Further, to introduce a notation more convenient for our immediate purpose, we write x, h for $s, n-s$ respectively. Thus

$$\left\{ \begin{matrix} h+x \\ r \end{matrix} \right\} = \left\{ \begin{matrix} h \\ r \end{matrix} \right\} + \dots + p^{t(h-r+t)} \left\{ \begin{matrix} h \\ r-t \end{matrix} \right\} \left\{ \begin{matrix} x \\ t \end{matrix} \right\} + \dots + p^{x(h+x)} \left\{ \begin{matrix} h \\ r-x \end{matrix} \right\}$$

26. We are now in a position to prove the following theorem:—
Let h_i, k_i have the meanings assigned in Art. 3, so that

$$k_i = h_i + h_{i+1} + \dots + h_\mu \quad (i = 1, 2, \dots, \mu),$$

and

$$k_i = 0, \quad \text{if } i > \mu.$$

Also let a_i be positive integers or zeros, such that

$$a_1 + a_2 + \dots + a_\mu = r.$$

Then I say that

$$\left\{ \begin{matrix} k_1 \\ r \end{matrix} \right\} = \sum p^{a_\mu-1 k_\mu + \dots + a_i k_{i+1} + \dots + a_1 k_2 - A} \left\{ \begin{matrix} h_\mu \\ a_\mu \end{matrix} \right\} \dots \left\{ \begin{matrix} h_i \\ a_i \end{matrix} \right\} \dots \left\{ \begin{matrix} h_1 \\ a_1 \end{matrix} \right\},$$

where the summation includes all the compositions $(a_1, a_2, \dots, a_\mu)$ of r , and $A = \sum a_i a_j$ ($i \neq j$).

By the theorem of Art. 25,

$$\left\{ \begin{matrix} k_1 \\ r \end{matrix} \right\} = \left\{ \begin{matrix} h_\mu + (k_1 - h_\mu) \\ r \end{matrix} \right\} = \sum_t p^{t(h_\mu - r + t)} \left\{ \begin{matrix} h_\mu \\ r-t \end{matrix} \right\} \left\{ \begin{matrix} k_1 - h_\mu \\ t \end{matrix} \right\},$$

the sum including the terms $t = 0, 1, 2, \dots, r$.

In this write a_μ for $r-t$, so that $t=r-a_\mu$, and the equation becomes

$$\left\{ \begin{matrix} k_1 \\ r \end{matrix} \right\} = \Sigma p^{(r-a_\mu)(h_\mu-a_\mu)} \left\{ \begin{matrix} h_\mu \\ a_\mu \end{matrix} \right\} \left\{ \begin{matrix} k_1-h_\mu \\ r-a_\mu \end{matrix} \right\},$$

where a_μ in the several terms on the right is $r, r-1, \dots 1, 0$ respectively.

The last factor of the specimen term can be expanded in the same way, giving

$$\begin{aligned} \left\{ \begin{matrix} k_1-h_\mu \\ r-a_\mu \end{matrix} \right\} &= \left\{ \begin{matrix} h_{\mu-1} + (k_1-h_\mu-h_{\mu-1}) \\ r-a_\mu \end{matrix} \right\} \\ &= \Sigma p^{t(h_{\mu-1}-r+a_\mu+t)} \left\{ \begin{matrix} h_{\mu-1} \\ r-a_\mu-t \end{matrix} \right\} \left\{ \begin{matrix} k_1-h_\mu-h_{\mu-1} \\ t \end{matrix} \right\} \\ &= \Sigma p^{(r-a_\mu-a_{\mu-1})(h_{\mu-1}-a_{\mu-1})} \left\{ \begin{matrix} h_{\mu-1} \\ a_{\mu-1} \end{matrix} \right\} \left\{ \begin{matrix} k_1-h_\mu-h_{\mu-1} \\ r-a_\mu-a_{\mu-1} \end{matrix} \right\}, \end{aligned}$$

where $a_{\mu-1} = r-a_\mu-t$ has in successive terms the values $r-a_\mu, r-a_\mu-1, \dots 1, 0$. Continuing in this way, we obtain ultimately

$$\begin{aligned} \left\{ \begin{matrix} k_1 \\ r \end{matrix} \right\} &= \Sigma p^I \left\{ \begin{matrix} h_\mu \\ a_\mu \end{matrix} \right\} \left\{ \begin{matrix} h_{\mu-1} \\ a_{\mu-1} \end{matrix} \right\} \dots \left\{ \begin{matrix} k_1-h_\mu-h_{\mu-1}-\dots-h_2 \\ r-a_\mu-a_{\mu-1}-\dots-a_2 \end{matrix} \right\} \\ &= \Sigma p^I \left\{ \begin{matrix} h_\mu \\ a_\mu \end{matrix} \right\} \left\{ \begin{matrix} h_{\mu-1} \\ a_{\mu-1} \end{matrix} \right\} \dots \left\{ \begin{matrix} h_1 \\ a_1 \end{matrix} \right\}, \end{aligned}$$

where the summation includes all the compositions $(a_1, a_2, \dots a_\mu)$ of r .

The exponent of p -factor,

$$\begin{aligned} I &= (r-a_\mu)(h_\mu-a_\mu) + \dots + (r-a_\mu-a_{\mu-1}-\dots-a_{i+1})(h_{i+1}-a_{i+1}) + \dots \\ &= (a_{\mu-1}+a_{\mu-2}+\dots+a_1)(h_\mu-a_\mu) + \dots \\ &\quad + (a_i+a_{i-1}+\dots+a_1)(h_{i+1}-a_{i+1}) + \dots \\ &= a_{\mu-1}h_\mu + a_{\mu-2}(h_\mu+h_{\mu-1}) + \dots + a_i(h_\mu+h_{\mu-1}+\dots+h_{i+1}) + \dots \\ &\quad \dots + a_1(h_\mu+\dots+h_2) - \Sigma a_i a_j \quad (j > i) \\ &= a_{\mu-1}k_\mu + a_{\mu-2}k_{\mu-1} + \dots + a_1 k_2 - \Sigma a_i a_j, \end{aligned}$$

and thus the theorem is established.

27. Some particular examples are added in illustration—

$$\begin{Bmatrix} k_1 \\ 1 \end{Bmatrix} = \Sigma p^{k_{i+1}} \begin{Bmatrix} h_i \\ 1 \end{Bmatrix}.$$

Here the compositions of r ($= 1$) are 100 ..., 010 ..., 001 ..., &c.,

$$\begin{Bmatrix} k_1 \\ 2 \end{Bmatrix} = \Sigma p^{2k_{i+1}} \begin{Bmatrix} h_i \\ 2 \end{Bmatrix} + \Sigma p^{k_{i+1} + k_{j+1} - 1} \begin{Bmatrix} h_i \\ 1 \end{Bmatrix} \begin{Bmatrix} h_j \\ 1 \end{Bmatrix}$$

$$\begin{Bmatrix} k_1 \\ 3 \end{Bmatrix} = \Sigma p^{3k_{i+1}} \begin{Bmatrix} h_i \\ 3 \end{Bmatrix} + \Sigma p^{2k_{i+1} + k_{j+1} - 2} \begin{Bmatrix} h_i \\ 2 \end{Bmatrix} \begin{Bmatrix} h_j \\ 1 \end{Bmatrix} \\ + \Sigma p^{k_{i+1} + k_{j+1} + k_{l+1} - 3} \begin{Bmatrix} h_i \\ 1 \end{Bmatrix} \begin{Bmatrix} h_j \\ 1 \end{Bmatrix} \begin{Bmatrix} h_l \\ 1 \end{Bmatrix},$$

and so on.

28. These results enable us to compare the denumerants of Art. 15 with the denumerants of groups of complementary order (Art. 22).

The number of groups of order p contained in G_p is $\begin{Bmatrix} k_1 \\ 1 \end{Bmatrix}$ (Art. 15), the number of groups of order p^{r-1} (Art. 22) is $\Sigma p^{k_{i+1}} \begin{Bmatrix} h_i \\ 1 \end{Bmatrix}$, and these two expressions are equal by the preceding article.

For orders p^3, p^{r-2} the equality to be proved is

$$\begin{Bmatrix} k_1 \\ 2 \end{Bmatrix} + p^{k_{i+1}} \begin{Bmatrix} k_2 \\ 1 \end{Bmatrix} \\ = \Sigma p^{2k_{i+1}} \begin{Bmatrix} h_i \\ 2 \end{Bmatrix} + \Sigma p^{k_{i+1} + k_{j+1}} \begin{Bmatrix} h_i \\ 1 \end{Bmatrix} \begin{Bmatrix} h_j \\ 1 \end{Bmatrix} \\ + \Sigma p^{k_{i+1} + k_{i+2} - 1} \begin{Bmatrix} h_{i+1} \\ 1 \end{Bmatrix} \begin{Bmatrix} h_{i+1} \\ 1 \end{Bmatrix}.$$

Here the left side

$$= \Sigma p^{2k_{i+1}} \begin{Bmatrix} h_i \\ 2 \end{Bmatrix} + \Sigma p^{k_{i+2} + k_{j+1} - 1} \begin{Bmatrix} h_{i+1} \\ 1 \end{Bmatrix} \begin{Bmatrix} h_j \\ 1 \end{Bmatrix} + \Sigma p^{k_1 + k_{i+2} - 1} \begin{Bmatrix} h_{i+1} \\ 1 \end{Bmatrix}$$

Now $p^{k_{i+2} + k_{j+1} - 1} = p^{k_{i+2} + k_{j+1}} (p-1) p^{k_{i+2} + k_{j+1} - 1};$

and therefore the second term

$$\begin{aligned}
 &= \sum p^{k_{i+1}+k_{j+1}} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} - \sum_1^{i-1} p^{k_{i+2}+k_{j+1}-1} (p^{h_j}-1) \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \\
 &= \dots \dots \dots - \sum p^{k_{i+2}-1} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \sum_1^{i-1} (p^{k_j}-p^{k_{j+1}}) \\
 &= \dots \dots \dots - \dots \dots \dots (p^{k_i}-p^{k_i}) \\
 &= \dots \dots \dots - \sum (p^{k_{i+2}+k_1-1} - p^{k_{i+2}+k_{i+1}-1}) \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\},
 \end{aligned}$$

which cancels the third term; and proves the left side

$$= \sum p^{2k_{i+1}} \left\{ \begin{matrix} h_i \\ 2 \end{matrix} \right\} + \sum p^{k_{i+2}+k_{j+1}} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_j \\ 1 \end{matrix} \right\} + \sum p^{k_{i+2}+k_{i+1}-1} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\}$$

The third term of the right side contains a factor

$$\left\{ \begin{matrix} h_i+1 \\ 1 \end{matrix} \right\} = 1 + p \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\},$$

so that the term may be written

$$\sum p^{k_{i+2}+k_{i+1}-1} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} + \sum p^{k_{i+2}+k_{i+1}} \left\{ \begin{matrix} h_{i+1} \\ 1 \end{matrix} \right\} \left\{ \begin{matrix} h_i \\ 1 \end{matrix} \right\},$$

and then the right side becomes identical with the last written value of the left side.

The comparison for orders p^3, p^{n-3} is still more laborious, and it is hopeless to attack the general theorem in this way.

29. The theorem of Art. 23 is useful in the enumeration of the groups which are factors of G_p , a product of h simple independent groups of order p^* . The order of G'_p will be taken to be not greater than p^* , and to avoid accents will be denoted by p^* .

We have in this case $h_i = 0$ for $i = 1, 2, \dots, a-1$, $k_i = h$ and $K_{i-1} = (i-1)h$. Thus the number of groups G'_p of order p^* is

$$\sum p^{\sum h'_i [(i-1)h - K'_{i-1}]} \prod \left\{ \begin{matrix} h - k'_i + h'_i \\ h'_i \end{matrix} \right\},$$

the summation extending to all positive (or zero) values of h' which satisfy the relations

$$h'_1 + h'_2 + \dots + h'_s = h,$$

$$h'_1 + 2h'_2 + \dots + sh'_s = s.$$

The first of these will be replaced by an equation wherein h'_0 denotes a positive integer or 0, namely,

$$h'_0 + h'_1 + h'_2 + \dots + h'_s = h.$$

Then the Π -factor above is

$$= \frac{h!}{h'_s! \dots h'_1! \dots h'_0!},$$

where the symbols $h!$ represent the product

$$(p^h - 1)(p^{h-1} - 1) \dots (p - 1).$$

For the factor exhibited is

$$\frac{(h - k'_i + h'_i)!}{h'_i! (h - k'_i)!} = \frac{(h + k'_i + h'_i)!}{h_i! (h - k'_{i-1} + h'_{i-1})!}$$

The exponent of p

$$\begin{aligned} &= \sum h'_i [(i-1)h - (h'_1 + 2h'_2 + \dots + (i-1)h'_i + \dots + (i-1)h'_s)] \\ &= \sum h'_i [(i-1)h'_0 + (i-2)h'_1 + \dots + h'_{i-2}] \\ &= \sum (i-j-1)h'_i h'_j \quad (j = 0, 1, \dots, i-2; i = 2, 3, \dots, s). \end{aligned}$$

The total number of groups G'_p will be shown to be

$$\left\{ \begin{matrix} s+h-1 \\ s \end{matrix} \right\}$$

This is at once verified for $s = 1, 2$, &c., and the general theorem is established by induction, on the assumption that the theorem is true for all smaller values of s ; and the method is to take together all terms of the sum that have the same value of h_0 .

The type term is

$$= p^{j-1} \sum_{i=j}^{s-1} (i-j-1)h'_i h'_j \frac{h'_0 [h'_2 + 2h'_3 + \dots + (s-1)h'_s]}{p} \left\{ \begin{matrix} h \\ h'_0 \end{matrix} \right\} \frac{(h-h'_0)!}{h'_1! h'_2! \dots h'_s!},$$

where

$$h'_0 + h'_1 + \dots + h'_s = h,$$

and

$$h'_1 + 2h'_2 + sh'_s = s,$$

so that

$$h'_2 + 2h'_3 + \dots + (s-1)h'_s = s - h + h'_0.$$

The term is therefore

$$= p^{h'_0(s-h+h'_0)} \left\{ \begin{matrix} h \\ h'_0 \end{matrix} \right\} \times p^{\sum (i-j-1)h'_i h'_j} \frac{(h-h'_0)!}{h'_1! \dots h'_i! \dots h'_s!}.$$

Here the first factor is constant when h_0 is constant as well as h, s , and the sum of these terms is the product of this factor into the sum of

$$p^{\Sigma(i-j-1)} \frac{h'_i h'_j (h-h'_0)!}{h'_1! \dots h'_s!},$$

where

$$h'_1 + h'_2 + \dots + h'_s = h - h'_0,$$

$$h'_2 + 2h'_3 + \dots + (s-1)h'_s = s - h + h'_0.$$

This summation is similar to the original summation, but the new s is smaller. Assuming the theorem to be true for this smaller s , we have

$$\begin{aligned} \Sigma p^{\Sigma(i-j-1)} \frac{h'_i h'_j (h-h'_0)!}{h'_1! \dots h'_s!} &= \left\{ \frac{s-h+h'_0+(h-h'_0)-1}{s-h+h'_0} \right\} \\ &= \left\{ \frac{s-1}{s-h-h'_0} \right\}, \end{aligned}$$

and the sum of those terms of the denominator which have a given h'_0 is

$$p^{h'_0(s-h+h'_0)} \left\{ \frac{h}{h'_0} \right\} \left\{ \frac{s-1}{s-h+h'_0} \right\}.$$

But the sum of these terms for $h'_0 = h-s, h-s+1, \dots, h-1$ is, by Art. 23,

$$\left\{ \frac{h+s-1}{s} \right\},$$

and thus the proposition is proved.

It will be observed that the order p^* of the simple groups of which G_p is the product does not appear anywhere in the conditions, save as limiting the order p' of G'_p . Hence the theorem will still be true if G_p is the product of h simple groups of orders not less than p^* . (Cf. the example of Art. 18.)

The failure of the formula when $s > \alpha$ is easily explained. When s has this too large value there are

$$\left\{ \frac{s+h-1}{s} \right\}$$

groups G'_p that can be formed from the elements of an extended G_p , whose constituent groups are of sufficiently high order. But some of these G'_p will contain simple groups of higher order than are present in the original G_p . Thus the number given by the formula errs in excess, and it may be noted that the excess is in many cases expressed by a somewhat similar formula.

Thursday, April 23rd, 1896.

Major MACMAHON, R.A., F.R.S., President, in the Chair.

The President read portions of abstracts of papers, viz., "On the Isomorphism of a Group with itself," by Prof. W. Burnside; and "Division of the Lemniscate," by Prof. G. B. Mathews.

Dr. Hobson read a paper "On some General Formulæ for the Potentials of Ellipsoids, Shells, and Discs."

The President made some remarks on "The Compensation for Difference of Capital in Gambling *à outrance*. A contribution to the Theory of the Duration of Play."

Mr. Basset read a paper "On the Stability of a Frictionless Liquid—Theory of Critical Planes." The author and Mr. Love joined in a discussion on the communication.

The following presents to the Library were received:—

"Proceedings of the Royal Society," Vol. LIX., No. 355.

"Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich," Jahrgang 40, Heft 3-4; Zürich, 1895.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xx., St. 3; Leipzig, 1896.

"Queen's College, Galway, Calendar for 1895-6," 8vo; Dublin, 1896.

"Mathematical Questions with their Solutions," edited by W. J. C. Miller, Vol. LXIV., 8vo; London, 1896.

"Journal of the Institute of Actuaries, Index to Vols. XXI.—XXX. (inclusive)"; London, 1896.

"Memoirs and Proceedings of the Manchester Literary and Philosophical Society," Vol. x., No. 1; Manchester, 1896.

Robertson, J. A.—"On a New Method of performing approximately certain Operations in Multiplication and Division" (read before the Institute of Actuaries, 29th April, 1895).

"Berichte über die Verhandlungen der K. Sachs. Gesellschaft der Wissenschaften zu Leipzig," 1895, 5, 6; Leipzig, 1896.

"Bulletin of the American Mathematical Society," 2nd Series, Vol. II., No. 6; New York, 1896.

"Proceedings of the Physical Society," Vol. XIV., Pt. 4; April, 1896.

"Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche," Serie 3, Vol. II., Fasc. 2, 3; Napoli, 1896.

"Bulletin des Sciences Mathématiques," Tome XX.; Paris, Fév., Mars, 1896.

"Tōkyō Mathematical-Physical Society," Maki No. 7, Dai 4; 1896.

VOL. XXVII.—NO. 557.

2 A

"Rendiconti del Circolo Matematico di Palermo," Tomo x., Fasc. 3; May-June, 1895.

"Atti della Reale Accademia dei Lincei—Rendiconti," Vol. v., Fasc. 5, 6; Roma, 1896.

Zeuthen, H. G.—"Om den Historiske Udvikling af Mathematiken som exakt Videnskab indtil Udgangen af det 18^{de} Aarhunderte" (Indbydelsesskrift til Kjøbenhavns Universitets Aarsfest i anledning af Hans Majestat Kongens Fødselsdag den 8^{de} April 1896).

Zeuthen, H. G.—"Die Geometrische Construction als 'Existenzbeweis' in der Antiken Geometrie" (from Band XLVII. of "Math. Annalen," pp. 222-228).

"Sitzungsberichte der K. Preuss. Akademie der Wissenschaften zu Berlin," 1895, 39-63, and Verzeichniss der Eingegangenen Druckschriften, Titel, Inhalt, &c.

"Educational Times," April, 1896.

"Annals of Mathematics," Vol. ix., No. 6; Vol. x., No. 1; Virginia, 1896.

"Annales de la Faculté des Sciences de Marseille," Tome iv., Fasc. 4, Tome v., Fasc. 1, 2, 3; 1894-5.

"Annales de la Faculté des Sciences de Toulouse," Tome ix., Fasc. 4; Paris, 1895.

"Indian Engineering," Vol. xix., Nos. 8-13, February 22nd to March 28th.

On the Isomorphism of a Group with itself. By W. BURNSIDE.

Read April 23rd, 1896. Received May 11th, 1896.

The conception of the isomorphism of a group with itself is not a new one, but it is only recently that it has been developed in any detail. The importance of the conception, both for the general theory of groups and for the actual construction of groups from given factor-groups, is obvious. Indeed the latter problem cannot be undertaken till all possible isomorphisms with themselves of the groups involved are determined. It is to Herr O. Hölder* and Herr G. Frobenius† that the development of the general theory of

* O. Hölder: "Bildung zusammengesetzter Gruppen," *Math. Ann.*, XLVI., pp. 321-422. The subject is also referred to in a paper by the same author in *Math. Ann.*, XLIII.

† G. Frobenius: "Ueber endliche Gruppen," *Berliner Sitzungsberichte*, 1895, pp. 163-194; and "Ueber auflösbare Gruppen II.," *id.*, pp. 1027-1044.