# *Groups of Order* $p^3q$. *By* A. E. Western, M.A.

Read February 9th, 1899. Received February 22nd, 1899.

1. I propose to discuss the different types of abstract groups whose orders are $p^3q$, $p$ and $q$ denoting different prime numbers. I must express my thanks to Prof. W. Burnside. F.R.S., for his criticisms on my work, which have enabled me to abbreviate it considerably. Before beginning the consideration of these particular groups it will be well to refer to the previous work of this nature that has been published, and to the general theorems of the theory of groups, of which use will be made.

Throughout this paper the letters $p, q, r, \ldots$ exclusively denote prime numbers, and $\{A, B, \ldots\}$ denotes the group obtained by combining in all possible ways the operations (or groups) $A, B, \ldots$.

There is, as is well known, only one type of group of order $p$, viz., the cyclic group $\{A\}$, where $A^p = 1$ (Burnside, *Theory of Groups*, p. 26).

There are two types of group of order $p^2$:—

(i.) $\{A\}$ where $A^{p^2} = 1$ (and no lesser power of $A$ equal to 1; this proviso will in future be implied, for the sake of brevity).

(ii.) $\{A, B\}$, where $A^p = B^p = 1$, $AB = BA$.

Both of these types are Abelian (*alias* "commutative"). (Burnside, *Theory of Groups*, pp. 63 and 81; Young, "On the Determination of Groups whose Order is the Power of a Prime," *Amer. Jour. of Math.*, Vol. xv., 1893, p. 132, and Cole and Glover, in the same volume, p. 192.)

There are also two possible types of order $pq$:—

(i.) $\{A, B\}$, where $A^p = 1$, $B^q = 1$, $AB = BA$; this may also be written $\{C\}$, where $C^{pq} = 1$.

(ii.) $\{A, B\}$, where $A^p = 1$, $B^q = 1$, and $A^{-1}BA = B^a$, where $a$ is any primitive root of the congruence

$$a^p \equiv 1 \pmod{q}.$$

This type only exists when $q - 1 \equiv 0 \pmod{p}$.

(Burnside, *Theory of Groups*, p. 100, and Cole and Glover, *loc. cit.*, pp. 193, 194.)

Groups of order $p^3$ are dealt with by Burnside, in his *Theory of Groups*, pp. 81, 82, and 87, and by Young, and Cole and Glover, in their papers already referred to. (See also *post*, § 4.)

Groups of order $p^2q$ are given by Burnside, *loc. cit.*, pp. 132–137, and by Cole and Glover, *loc. cit.*

Groups of order $pqr$ are given by Cole and Glover, *loc. cit.*; and, lastly, groups of order $p^4$ are enumerated by Burnside, *Theory of Groups*, pp. 87, 88, and by Young (*loc. cit.*). See also the memoir by Hölder, "Die Gruppen der Ordnungen $p^3$, $pq^2$, $pqr$, $p^4$," *Math. Ann.*, Vol. XLIII.

2. Sylow's theorem forms the basis of attack on all groups whose orders contain more than one prime factor. It is expressed by Burnside (p. 92) as follows:—

"If $p^a$ is the highest power of a prime $p$ which divides the order of a group $G$, the sub-groups of $G$ of order $p^a$ form a single conjugate set, and their number is congruent to unity mod $p$."

An important corollary is that, if $G$ contains more than one sub-group of order $p^a$, the order of $G$ must be divisible by $1+kp$ $(k>0)$. For there are, in the case supposed, $1+kp$ sub-groups of order $p^a$, forming a conjugate set, and the number of sub-groups forming a conjugate set necessarily is a factor of the order of the group.

A second and equally important corollary is that the number of groups of order $p^a$ contained in $G$ can be expressed in the form

$$1+k_1p+k_2p^2+\ldots+k_ap^a,$$

where $k_rp^r$ is the number of groups of order $p^a$ having with a given group $H$ of the set greatest common sub-groups of order $p^{a-r}$ (Burnside, p. 94).

A third, which will also be useful in the sequel, is given by Burnside (p. 94). Using the previous notation, this theorem asserts that, if $h$ is a sub-group common to $H$ and some other sub-group of order $p^a$ such that no sub-group which contains $h$ and is of greater order is common to any two sub-groups of order $p^a$, then there must be some operation of $G$ of order prime to $p$ which is permutable with $h$, and not with $H$.

3. Two other general theorems will be frequently employed later on.

(1) Let $G$ and $H$ be two self-conjugate sub-groups of some third group, having no common operations except identity; then every operation of $G$ is permutable with every operation of $H$ (Burnside, p. 44).

(2) Let $A_1, A_2, \ldots, A_n$ be all the sub-groups (or operations) of a certain type contained in $G$; and let $Q$ be an operation in $G$ of prime order $q$. Transform $A_1$ with respect to $Q$; the result $Q^{-1}A_1Q$ is a sub-group (or operation) of $G$ of the same type as $A_1$, and either it is $A_1$ or it is some other of the set, say $A_2$. In the latter case, transform $A_2$ by $Q$, obtaining $A_3$, say, and so on, till the cycle closes. Then the cycle contains $q$ of the sub-groups (or operations) $A_1, A_2, \ldots$; for, if possible, suppose the cycle closes with $A_x$ $(x<q)$, so that

$$Q^{-x}A_1Q^x = Q^{-1}A_xQ = A_1.$$

Then we get

$$Q^{-xy}A_1Q^{xy} = A_1$$

for all values of $y$.

Now choose $y$ so that $xy \equiv 1 \pmod q$; we thus obtain the result

$$Q^{-1}A_1Q = A_1,$$

which contradicts the hypothesis

$$Q^{-1}A_1Q = A_2.$$

Therefore the sub-groups (or operations) $A_1, A_2, \ldots$ may be divided into $l$ sets of $q$ each, and $m$ each of which is unaltered by transformation with $Q$, *i.e.*, is permutable with $Q$; and then

$$n \doteq m+lq.$$

4. The various groups of order $p^3$ must now be examined, and the facts as to their respective structures proved, which will be needed when I come to consider them as sub-groups of groups of order $p^3q$. In particular it will be useful to know, as to each group of order $p^3$, how it may be made isomorphic to itself (see Burnside, chap. xi.); that is, how to find operations $A_0, B_0, \ldots$ in terms of the generating operations $A, B, \ldots$ such that $A_0, B_0, \ldots$ obey the same number of relations, and these of the same form as $A, B, \ldots$; it is obvious that, if this is so, the group may be regarded as generated by $A_0, B_0, \ldots$, just as much as by $A, B, \ldots$.

I. $\{A\}$, where $A^{p^3} = 1$.

This contains one sub-group of order $p$, $\{A^{p^2}\}$, and one of order $p^2$, $\{A^p\}$. It is generated by $A_0 = A^x$, provided only that $x$ is prime to $p$.

This group contains therefore $p^2(p-1)$ operations of order $p^3$, and so the order of its group of isomorphisms is $p^2(p-1)$. Both its sub-groups are characteristic sub-groups, *i.e.*, such as are unaltered by every isomorphism of the group (Burnside, p. 232).

II. $\{A, B\}$, where $A^{p^2} = 1$, $B^p = 1$, $AB = BA$.

This contains $p+1$ sub-groups of order $p$, $\{A^p\}$, and $\{A^{kp}B\}$ (where $k = 0, 1, \dots, p-1$), and $p$ cyclical sub-groups of order $p^2$ $\{AB^k\}$ (where $k = 0, 1, \dots, p-1$), and one non-cyclical sub-group of order $p^2$ $\{A^p, B\}$.

Let $A_0 = A^xB^y$, $B_0 = A^{zp}B^r$, where $x$ is prime to $p$, and at least one of $z$ and $r$ is prime to $p$; then $A_0^{p^2} = 1$, $B_0^p = 1$, and $A_0B_0 = B_0A_0$.

To secure that $\{A_0, B_0\}$ generate the group, we must also ensure that $B_0$ is independent of $A_0$.

Suppose that $$B_0 = A_0^k;$$
then $$A^{zp}B^r = A^{xk}B^{yk},$$
and so $$xk \equiv zp \pmod{p^2},$$ $$yk \equiv r \pmod{p}.$$

Since $x$ is prime to $p$, $k \equiv 0 \pmod{p}$; that is, $r \equiv 0 \pmod{p}$. Provided therefore that $r \not\equiv 0$, $A_0$ and $B_0$ generate the group, and are evidently the most general expressions for any possible pair of generators. The group of isomorphisms is therefore of order $p^3(p-1)^2$. The characteristic sub-groups are easily seen to be $\{A^p, B\}$ and $\{A^p\}$.

III. $\{A, B, C\}$, where $A^p = B^p = C^p = 1$, $AB = BA$, $AC = CA$, and $BC = CB$.

This contains $p^2+p+1$ sub-groups of order $p$, and the same number of order $p^2$, all of the latter being non-cyclical (Burnside, pp. 59, 60). Every operation of the group is of order $p$ (except 1). $A_0 = A^{a_1}B^{a_2}C^{a_3}$, $B_0 = A^{b_1}B^{b_2}C^{b_3}$, and $C_0 = A^{c_1}B^{c_2}C^{c_3}$ will generate the group, provided that the three congruences given by $A_0^xB_0^yC_0^z = 1$ cannot co-exist; these are

$$a_1x+b_1y+c_1z \equiv 0 \pmod{p},$$
$$a_2x+b_2y+c_2z \equiv 0 \pmod{p},$$
$$a_3x+b_3y+c_3z \equiv 0 \pmod{p}.$$

$a_1a_2 \dots$ must therefore satisfy the condition

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \not\equiv 0 \pmod{p}.$$

The order of the group of isomorphisms is

$$(p^3-1)(p^3-p)(p^3-p^2)$$

(Burnside, pp. 58, 59); that is,

$$p^3(p-1)^3(p+1)(p^2+p+1).$$

This group evidently has no characteristic sub-groups.

These groups I., II., III. exist whatever prime $p$ may represent, either 2 or any greater prime. Since they are Abelian groups, every sub-group is self-conjugate. The remaining groups of order $p^3$ differ in form according as $p$ represents 2 or an odd prime; and they are not Abelian groups.

IV. $\{A, B\}$, where $A^4 = 1$, $B^2 = 1$, $BAB = A^{-1}$.

The operations of this group are

$$1,\ A,\ A^2,\ A^{-1},\ B,\ AB = BA^{-1},\ A^2B = BA^2,\ A^{-1}B = BA.$$

It contains altogether five sub-groups of order 2: of these one is self-conjugate, $\{A^2\}$; two form a conjugate set, $\{B\}$ and $\{A^2B\}$; two form a conjugate set, $\{AB\}$ and $\{A^{-1}B\}$. And it contains three sub-groups of order 4, all being self-conjugate; two are non-cyclical,

$$\{A^2, B\} = (1, A^2, B, A^2B) \quad \text{and} \quad \{A^2, AB\} = (1, A^2, AB, A^{-1}B);$$

and one is cyclical, $\{A\}$.

Obviously the most general expressions for $A_0$ and $B_0$ are $A_0 = A^{\pm 1}$, $B_0 = A^xB$ ($x = 0$, $\pm 1$, or 2); for then $A_0^4 = 1$, $B_0^2 = 1$, and

$$B_0A_0B_0 = A^xBA^{\pm 1}A^xB = A^xA^{\mp 1-x} = A^{\mp 1} = A_0^{-1};$$

and evidently $A_0$ and $B_0$ are independent, except for the above relations.

The order of the group of isomorphisms is therefore 8.

The characteristic sub-groups are $\{A\}$ and $\{A^2\}$.

V. $\{A, B\}$, where $A^4 = 1$, $B^2 = A^2$, $B^{-1}AB = A^{-1}$.

The operations are 1, $A^2$, $A$, $A^{-1}$, $B$, $A^2B$, $AB$, $A^{-1}B$, the latter six being each operations of order 4, and the square of each being $A^2$.

This group contains one sub-group of order 2, $\{A^2\}$, which is self-conjugate; and three sub-groups of order 4 each cyclical and self-conjugate,

$$\{A\},\ \{AB\} = (1, AB, A^2, A^{-1}B), \quad \text{and} \quad \{B\} = (1, B, A^2, A^2B).$$

The group is symmetrical in $A$ and $B$, for from the relations given it follows that $A^{-1}BA = B^{-1}$.

Any independent pair from among the six operations of order 4 may be taken to generate the group, viz.,

$$A_0 = A^{\pm 1},\quad B_0 = A^k B \quad (k = 0,\ \pm 1,\ 2),$$

or

$$B_0 = A^{\pm 1},\quad A_0 = A^k B \quad (k = 0,\ \pm 1,\ 2),$$

or

$$A_0 = A^l B,\quad B_0 = A^m B$$

$$(l = 0 \text{ or } 2,\ m = \pm 1, \text{ or } \textit{vice versa}).$$

And in each case $A_0^4 = 1$, $B_0^2 = A_0^2$, and $B_0^{-1} A_0 B_0 = A_0^{-1}$.

The order of the group of isomorphisms is therefore 24. $\{A^2\}$ is the only characteristic sub-group.

VI. $\{A, B\}$, where $A^{p^2} = 1$, $B^p = 1$, $B^{-1}AB = A^{p+1}$, and $p$ is odd.

This contains one self-conjugate sub-group of order $p$, $\{A^p\}$, and $p$ other sub-groups of order $p$, $\{A^{kp}B\}$, forming a conjugate set; also $p$ cyclical sub-groups of order $p^2$, $\{AB^k\}$, which are self-conjugate, and one non-cyclical self-conjugate sub-group of order $p^2$, $\{A^p, B\}$. In this group

$$(A^a B^b)^x = A^{ax - \frac{1}{2}abpx(x-1)} B^{bx}.$$

Let

$$A_0 = A^a B^b,\quad B_0 = A^{cp} B^d;$$

then $a \not\equiv 0 \pmod p$, or else $A_0$ would be of order $p$, and $d \not\equiv 0$, or else $B_0$ would be a power of $A_0$. Then

$$\begin{aligned} B_0^{-1} A_0 B_0 &= B^{-d} A^{-cp} A^a B^b A^{cp} B^d \\ &= B^{-d} A^a B^d B^b \\ &= A^{a(1+dp)} B^b \end{aligned}$$

and

$$A_0^{1+p} = A^{a(1+p)} B^b.$$

In order that $A_0$ and $B_0$ should take the place of $A$ and $B$ it is necessary that $d = 1$; that is,

$$A_0 = A^a B^b,\quad B_0 = A^{cp} B.$$

And it is easily proved that (if $a$ is prime to $p$) $A_0$ and $B_0$ are not connected by any additional relations.

The order of the group of isomorphisms is therefore $p^3(p-1)$.

The characteristic sub-groups are $\{A^p\}$ and $\{A^p, B\}$.

VII. $\{A, B, C\}$, where $A^p = B^p = C^p = 1$, $AB = BA$, $AC = CA$, and $C^{-1}BC = AB$; whence also $B^{-1}CB = A^{-1}C$; here $p$ must be odd.

From these we derive

$$C^xB^y = A^{-xy}B^yC^x$$

and $$(A^aB^bC^c)^x = A^{ax-\frac{1}{2}bcx(x-1)}B^{bx}C^{cx}.$$

Therefore every operation of the group is of order $p$. $A$ and its powers are the only self-conjugate operations.

This group contains $p^2+p+1$ sub-groups of order $p^2$; of these one is self-conjugate, $\{A\}$; the remainder consist of $p+1$ sets, each set containing $p$ conjugates; the sets are

$$\{A^kB\} \quad (k = 0, 1, \dots, p-1),$$

$$\{A^kC\},\ \{A^kBC\},\ \dots,\ \{A^kB^jC\}, \quad \begin{pmatrix} k = 0, 1, \dots, p-1 \\ j = 0, 1, \dots, p-1 \end{pmatrix}.$$

And it contains $p+1$ non-cyclical self-conjugate sub-groups

$$\{A, B\} \text{ and } \{A, B\,C\} \quad (j = 0, 1, \dots, p-1).$$

The most general transformation of the group into itself that is possible, having regard to $\{A\}$ being the sole self-conjugate sub-group of order $p$, is

$$A_0 = A^x, \quad B_0 = A^{b_1}B^{b_2}C^{b_3}, \quad C_0 = A^{c_1}B^{c_2}C^{c_3}.$$

Then $$A_0B_0 = B_0A_0, \quad A_0C_0 = C_0A_0,$$

and $$C_0^{-1}B_0C_0 = C^{-c_3}B^{-c_2}A^{-c_1}A^{b_1}B^{b_2}C^{b_3}A^{c_1}B^{c_2}C^{c_3}$$
$$= A^{b_1-b_2c_3+b_3c_2}B^{b_2}C^{b_3}$$

and $$A_0B_0 = A^{b_1+x}B^{b_2}C^{b_3};$$

therefore $$x \equiv b_2c_3 - b_3c_2 \pmod{p}.$$

Also the sufficient condition that $C_0$ should not be expressible in terms of $A_0$ and $B_0$ is that $b_2c_3 \not\equiv b_3c_2$, which is, of course, satisfied when the above congruence is satisfied.

To determine the order of the group of isomorphisms, we must find the number of solutions of the congruence

$$x \equiv b_2c_3 - b_3c_2 \pmod{p}$$

such that $x$ is prime to $p$.

There are $2p-1$ pairs of values which $b_2$ and $c_3$ can assume such that

$$b_2c_3 \equiv 0 \pmod{p};$$

with each of these $b_3$ and $c_2$ can each take any of the values $1, 2, \dots, p-1$: thus, if

$$b_2c_3 \equiv 0 \pmod{p},$$

there are $(p-1)^2(2p-1)$ solutions; if

$$b_3c_2 \equiv 0 \pmod p,$$

there are again $(p-1)^2\,(2p-1)$ solutions.

Lastly, if none of $b_2$, $b_3$, $c_2$, $c_3$ are congruent to zero, to each of the $(p-1)^3$ sets of values of $b_2$, $b_3$, and $c_2$ there correspond one value of $c_3$ which makes

$$b_2c_3-b_3c_2 \equiv 0 \pmod p$$

and $p-2$ values which do not; in this case then there are $(p-1)^3\,(p-2)$ solutions.

The order of the group of isomorphisms is therefore

$$p^2\left[2\,(p-1)^2\,(2p-1)+(p-1)^3\,(p-2)\right] = p^3\,(p-1)^2\,(p+1).$$

$\{A\}$ is the only characteristic sub-group.

In future I shall refer to these groups by their numbers in this list.

### 5. *Principles of the Classification of Groups of Order* $p^3q$.

The application of Sylow's theorem to this order shows that there are either 1 or $q$ sub-groups of order $p^3$ in a group of order $p^3q$; iu the latter case,

$$q \equiv 1 \pmod p.$$

Also there are either 1 or $p$, or $p^2$, or $p^3$ sub-groups of order $q$ in such a group; if $p$ such sub-groups, then

$$p \equiv 1 \pmod q;$$

if $p^2$ such sub-groups, then

$$p \equiv 1 \text{ or } -1 \pmod q;$$

if $p^3$ such sub-groups, then

$$p \equiv 1 \text{ or } p^2+p+1 \equiv 0 \pmod q.$$

Thus the groups of order $p^3q$ fall into four principal divisions:—

(1) Those which contain self-conjugate sub-groups of orders $p^3$ and $q$.

(2) Those which contain $q$ sub-groups of order $p^3$, but a self-conjugate sub-group of order $q$.

(3) Those which contain a self-conjugate sub-group of order $p^3$, but more than one sub-group of order $q$.

(4) Those which do not contain self-conjugate sub-groups of order $p^3$ or $q$.

In the remainder of this paper $G$ exclusively denotes a group of order $p^3q$, and $H$ one of its sub-groups of order $p^3$.

6. (1) Evidently the sub-groups of orders $p^3$ and $q$ have no common operation except 1; in this case therefore, applying the theorem of § 3 (1), each operation of order $q$ is permutable with each operation of the sub-group of order $p^3$.

As in § 4, the letters $A$, $B$, and $C$ denote the operations of a group of order $p^3$, while $Q$ denotes an operation of order $q$.

Thus, when $p = 2$, there are five groups of this kind for all values of $q$; viz., the direct products of $\{Q\}$ and the groups I., II., III., IV., and V. of order 8.

And, when $p \neq 2$, there are also five groups for all values of $p$ and $q$; viz., the direct products of $\{Q\}$, and the gr ups I., II., III., VI., and VII. of order $p^3$.

### 7. *Groups containing $q$ Sub-groups of Order $p^3$ and one Sub-group only of Order $q$.*

$$q \equiv 1 \pmod p$$

is a necessary condition for the existence of any group of this kind; evidently then $q$ cannot be 2. It will be convenient to consider separately each of the seven groups of order $p^3$, subdividing each of these cases in accordance with the values of $k_1$ and $k_2$ in the formula (§ 2)

$$q = 1 + k_1 p + k_2 p^2 + k_3 p^3.$$

Let $H$ represent one of the sub-groups of order $p^3$; all of them, of course, being conjugates in the group of order $p^3q$, are of the same type. Then $k_1 p$ is the number of such sub-groups having with $H$ greatest common sub-groups of order $p^2$, $k_2 p^2$ is the number of such sub-groups having with $H$ greatest common sub-groups of order $p$, and $k_3 p^3$ is the number of such sub-groups having no common operations with $H$.

(i.) There may exist a sub-group $h$ of order $p^2$ common to $H$ and some other sub-group of order $p^3$; this must exist if

$$q \not\equiv 1 \pmod{p^2},$$

and it may also exist if $\quad q \equiv 1 \pmod{p^3}$.

Applying the theorem in § 2, we see that $Q$ is permutable with $h$.

(ii.) No such sub-group of order $p^2$ may exist, but there may be a sub-group $h$ of order $p$ common to $H$ and $H'$; then

$$q \equiv 1 \pmod{p^2};$$

this must exist if $\quad q \not\equiv 1 \pmod{p^3}$,

and it may also exist if $\quad q \equiv 1 \pmod{p^3}$.

$Q$ is permutable with $h$ (§ 2).

(iii.) Lastly, the $q$ sub-groups of order $p^3$ may have no common operations between any two of them; in this case

$$q \equiv 1 \pmod{p^3}.$$

The group of isomorphisms of any group of order $q$ is a cyclical group of order $q-1$; now, since $\{Q\}$ is self-conjugate in $G$, every operation of $H$ transforms $\{Q\}$ into itself, and therefore corresponds to an isomorphism of $\{Q\}$. If, then, none of the operations of $H$ are permutable with $Q$, $H$ is simply isomorphic either to the group of isomorphisms of $\{Q\}$ or to a sub-group of the latter; and so in either case $H$ must be cyclical; this only occurs when $H$ is of type I. If some of the operations of $H$ are permutable with $Q$, they form a self-conjugate sub-group (which is called $h$ above), of $H$ (Burnside, p. 42); then each operation of the factor-group $\frac{H}{h}$ corresponds to an isomorphism of $\{Q\}$, and therefore $\frac{H}{h}$ must be cyclical. This condition will reduce the number of different cases to be considered.

Further, since $h$ is a self-conjugate sub-group of $H$, and is permutable with $Q$, it is a self-conjugate sub-group of $G$. Also, by hypothesis $\{Q\}$ is a self-conjugate sub-group of $G$, and evidently $h$ and $\{Q\}$ have no common operations; therefore [§ 3 (1)] every operation of $h$ is permutable with $Q$.

8. I. $A^{p^3} = 1$.

(i.) $h$ must here be $\{A^p\}$, this being the only sub-group of order $p^2$ in $H$. Therefore $Q$ and $A^p$ are permutable operations (§ 7).

And since $\{Q\}$ is self-conjugate, but $Q$ is not permutable with $A$ (a case comprised in § 6),

$$A^{-1}QA = Q^a,$$

where $$a \neq 1.$$

Then $$A^{-p}QA^p = Q^{a^p},$$

and so $$a^p \equiv 1 \pmod{q}.$$

This congruence has primitive roots, since

$$q \equiv 1 \pmod{p}.$$

The same type is obtained whichever root of the congruence is taken; for let

$$b \equiv a^x \pmod{q},$$

$x$ being prime to $p$. Then, if $A_0 = A^x$,

$$A_0^{-1}QA_0 = A^{-x}QA^x = Q^{a^x} = Q^b.$$

Thus we obtain one type,

$$A^{p^3} = 1, \quad Q^q = 1, \quad A^{-1}QA = Q^a,$$

where $a$ is any primitive root of

$$a^p \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p}.$$

(ii.) $h$ must now be $\{A^{p^2}\}$, the only sub-group of order $p$ in $H$. Then $Q$ is permutable with $A^{p^2}$ (§ 7). And so

$$A^{-1}QA = Q^a,$$

where $a$ is a primitive root of

$$a^{p^2} \equiv 1 \pmod{q}.$$

And, as above, there is only one type, whichever primitive root is taken,

$$A^{p^3} = 1, \quad Q^q = 1, \quad A^{-1}QA = Q^a,$$

where $a$ is any primitive root of

$$a^{p^2} \equiv 1 \pmod{q}$$

and where $$q \equiv 1 \pmod{p^3}.$$

(iii.) Here $$A^{-1}QA = Q^a,$$

where $a$ is a primitive root of

$$a^{p^3} \equiv 1 \pmod{q},$$

and, as above, there is only one type,

$$A^{p^3} = 1, \quad Q^q = 1, \quad A^{-1}QA = Q^a,$$

where $a$ is any primitive root of

$$a^{p^3} \equiv 1 \pmod{q},$$

and where

$$q \equiv 1 \pmod{p^3}.$$

9. II. $A^{p^2} = 1$, $B^p = 1$, $AB = BA$.

(i.) This $H$ has two distinct kinds of sub-group of order $p^2$, cyclic and non-cyclic (§ 4, II.).

First, let $h$ be a cyclic sub-group of order $p^2$. We saw in § 4, II., that any operation of $H$ whose order is $p^2$ might be taken as the generator $A$.

Without loss therefore of generality, we may take $h = \{A\}$. Then $AQ = QA$ (§ 7).

Also, since $\{Q\}$ is self-conjugate,

$$B^{-1}QB = Q^a,$$

where $a$ is a primitive root of

$$a^p \equiv 1 \pmod{q}.$$

Since $B^x$ will do, in place of $B$, to generate with $A$ the group $H$, there is only one type,

$$A^{p^2} = 1, \quad B^p = 1, \quad Q^q = 1, \quad AB = BA, \quad AQ = QA, \quad B^{-1}QB = Q^a,$$

where $a$ is any primitive root of

$$a^p \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p}.$$

Secondly, let $h = \{A^p, B\}$, the only non-cyclic sub-group of order $p^2$ in $H$. Then

$$A^pQ = QA^p, \quad BQ = QB \quad (§ 7).$$

Therefore

$$A^{-1}QA = Q^a,$$

where

$$a \neq 1;$$

but, since

$$A^{-p}QA^p = Q,$$

$a$ is a primitive root of

$$a^p \equiv 1 \pmod{q}.$$

As before, there is only one type,

$$A^{p^2} = 1, \quad B^p = 1, \quad Q^q = 1, \quad AB = BA, \quad A^{-1}QA = Q^a, \quad BQ = QB,$$

where $a$ is any primitive root of

$$a^p \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p}.$$

(ii.) Again referring to § 4, II., there are two distinct kinds of sub-group of order $p$ in $H$, $\{A^p\}$, which is generated by the $p$th power of an operation, and $\{A^{kp}B\}$; here $A^{kp}B$ is not the $p$th power of any operation of $H$. No generality is lost by putting $B$ for $A^{kp}B$ in the latter case.

First, $h = \{A^p\}$. This is impossible, for $\frac{H}{h}$ is a non-cyclic group (§ 7).

Secondly, $h = \{B\}$. Then

$$BQ = QB \text{ (§ 7)}, \quad \text{and} \quad A^{-1}QA = Q^a,$$

where $a$ is any primitive root of

$$a^{p^2} \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p^2}.$$

These relations define one type.

10. III. $A^p = B^p = C^p = 1$, $AB = BA$, $AC = CA$, $BC = CB$.

(i.) $h$ is here a non-cyclic sub-group of order $p^2$; suppose it is generated by

$$A_0 = A^{a_1}B^{a_2}C^{a_3}, \quad \text{and} \quad B_0 = A^{b_1}B^{b_2}C^{b_3}.$$

Since $A_0$ and $B_0$ are independent, the congruences

$$\frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \equiv \frac{a_3}{b_3} \pmod{p}$$

cannot both be true.

We can therefore choose $c_1$, $c_2$, $c_3$ so that

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \not\equiv 0 \pmod{p};$$

therefore, writing $C_0 = A^{c_1}B^{c_2}C^{c_3}$,

$A_0$, $B_0$, $C_0$, generate the group $\{A, B, C\}$; and we have

$$h = \{A_0, A_0\} \text{ (§ 4, III.)}.$$

The suffixes may now be dropped. Thus we have the type given by the relations of III.,

$$AQ = QA, \quad BQ = QB, \quad \text{and} \quad C^{-1}QC = Q^a,$$

where $a$ is any primitive root of

$$a^p \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p}.$$

11. IV. $A^4 = 1$, $B^2 = 1$, $BAB = A^{-1}$.

(i.) This group has two different kinds of sub-groups of order 4, the cyclical $\{A\}$ and the non-cyclical $\{A^2, B\}$ and $\{A^2, AB\}$ (§ 4, IV).

Firstly, $h = \{A\}$. Then

$$AQ = QA \text{ (§ 7), and } B^{-1}QB = Q^a,$$

so that
$$a^2 \equiv 1 \pmod{q}.$$

But $a \not\equiv 1$; so $a \equiv -1$; and we have the type

$$A^4 = 1,\quad B^2 = 1,\quad BAB = A^{-1},\quad Q = 1,\quad AQ = QA,\quad BQB = Q^{-1}.$$

Secondly, $h = \{A^2, B\}$ or $\{A^2, AB\}$; since $A$ and $B_0 = AB$ generate $H$, and obey the same relations as $A$ and $B$, it will be sufficient to consider $h = \{A^2, B\}$. Then we get the type

$$A^4 = 1,\quad B^2 = 1,\quad Q^q = 1,\quad BAB = A^{-1},\quad A^{-1}QA = Q^{-1},\quad BQ = QB.$$

(ii.) $H$ has also two different kinds of sub-group of order 2 (§ 4, IV.), $\{A^2\}$ and $\{A^kB\}$ ($k = 0, \pm 1$, or 2). But $h$ cannot be $\{A^2\}$, for $\frac{H}{h}$ would then be non-cyclic. Nor can $h$ be one of the other sub-groups of order 2, for they are not self-conjugate (§ 4, IV.).

12. V. $A^4 = 1$, $B^2 = A^2$, $B^{-1}AB = A^{-1}$.

(i.) Let $h$ be some sub-group of order 4; this group contains three such, $\{A\}$, $\{B\}$, and $\{AB\}$, but without loss of generality we can put

$$A_0 = B \text{ or } AB,$$

and thus get
$$h = \{A\} \text{ (§ 4, V.)}.$$

Then
$$AQ = QA \text{ (§ 7)},$$

and then, since
$$B^{-2}QB^2 = A^{-2}QA^2 = Q,$$

$$B^{-1}QB = Q^{-1}.$$

Thus we get the type

$$A^4 = 1,\quad B^2 = A^2,\quad B^{-1}AB = A^{-1},\quad Q^q = 1,\quad AQ = QA,\quad B^{-1}QB = Q^{-1}.$$

The only sub-group of order 2 is $\{A^2\}$, and this cannot be $h$, for then $\frac{H}{h}$ would be non-cyclic.

13. VI. $A^{p^2}=1$, $B^p=1$, $B^{-1}AB=A^{p+1}$, and $p$ is odd.

(i.) $h$ is either one of the cyclical sub-groups $\{AB^k\}$, or it is the non-cyclical sub-group $\{A^p, B\}$ (§ 4, VI.).

In the first case we can make

$$A_0=AB^k, \quad B_0=B \quad (\S\ 4,\ \text{VI}),$$

and so, dropping suffixes, $h=\{A\}$. Then

$$AQ=QA \ (\S\ 7), \quad \text{and} \quad B^{-1}QB=Q^a,$$

where $$a^p\equiv 1 \pmod q,$$

and $a$ is a primitive root.

We must now find whether any transformation of the group of order $p^3q$ given by these relations for a particular value of $a$ can make the last relation become

$$B_0^{-1}Q_0B_0=Q_0^b,$$

$b$ being some other root of $\quad a^p\equiv 1 \pmod{q}$.

$Q$ and its powers are the only operations of order $q$ in the group; clearly nothing is gained by putting $Q_0=Q^x$. $A^fB^gQ^h$ is of order $p^2$ if $f$ is prime to $p$, but of order $p$ if $f$ is a multiple of $p$.

Let $$A_0=A^fB^gQ^h, \quad B_0=A^{jp}B^xQ^k;$$

then $$A_0^{p^2}=1, \quad B_0^p=1, \quad B_0^{-1}QB_0=B^{-x}QB^x=Q^{a^x},$$

and
$$\begin{aligned} B_0^{-1}A_0B_0 &= Q^{-k}B^{-x}A^{-jp}A^fB^gQ^hA^{jp}B^xQ^k \\ &= Q^{-k}B^{-x}A^fB^gQ^hB^xQ^k \\ &= A^{f(1+xp)}Q^{-k}B^{-x+g}Q^hB^xQ^k \\ &= A^{f(1+xp)}Q^{-k}B^gQ^{ha^x+k} \\ &= A^{f(1+xp)}B^gQ^{ha^x-k(a^g-1)}; \end{aligned}$$

also $$A_0^{1+p}=A^{f(1+p)}B^gQ^h;$$

therefore $$f(1+xp)\equiv f(1+p) \pmod{p^2};$$

*i.e.*, $$x\equiv 1 \pmod{p}.$$

This proves that each primitive root of the congruence

$$a^p\equiv 1 \pmod{q}$$

gives a separate type; there are therefore $p-1$ types, whose generating relations are

$$A^{p^2}=1,\quad B^p=1,\quad Q^q=1,\quad B^{-1}AB=A^{p+1},\quad AQ=QA,\quad B^{-1}QB=Q^a,$$

or $$Q^{a^2},\ \dots,\ Q^{a^{p-1}},$$

where $a$ is a primitive root of

$$a^p\equiv 1 \pmod q, \quad\text{and}\quad q\equiv 1 \pmod p.$$

Secondly, $h=\{A^p, B\}$. Then

$$A^pQ=QA^p,\quad BQ=QB \quad (\S\ 7),$$

and then $$A^{-1}QA=Q^a,$$

where $a$ is any primitive root of

$$a^p\equiv 1 \pmod q.$$

This only gives one type, for we can take $A_0=A^x$, and all the relations are then unaltered, except that $a$ is replaced by $a^x$; its relations are

$$A^{p^2}=1,\quad B^p=1,\quad Q^q=1,\quad B^{-1}AB=A^{p+1},\quad A^{-1}QA=Q^a,\quad BQ=QB,$$

where $a$ is any primitive root of

$$a^p\equiv 1 \pmod q, \quad\text{and}\quad q\equiv 1 \pmod p.$$

(ii.) $\{A^p\}$ is the only self-conjugate sub-group of order $p$ (§ 4, VI.). $h=\{A^p\}$ makes $\frac{H}{h}$ non-cyclic, which is impossible (§ 7), and therefore no type exists in this case.

14. VII. $A^p=B^p=C^p=1,\ AB=BA,\ AC=CA,\ C^{-1}BC=AB$; $p$ is odd.

(i.) $h=\{A, B\}$ or $\{A, C\}$ or $\{A, B^jC\}$ $(j=1, 2, \dots, p-1)$.

If $$h=\{A, C\},$$

we can put $$A_0=A^{-1},\quad B_0=C,\quad C_0=B,$$

and so $$h=\{A_0, B_0\}.$$

If $$h=\{A, B^jC\},$$

we can put $$A_0=A^j,\quad B_0=B^jC,\quad C_0=C,$$

and so $$h=\{A_0, B_0\}.$$

It is sufficient then to consider

$$h = \{A, B\}.$$

Then $$AQ = QA, \quad BQ = QB.$$

Also $$C^{-1}QC = Q^a,$$

where $a$ is a primitive root of $a^p \equiv 1 \pmod{q}$.

And there is only one type, for, if

$$A_0 = A^x, \quad B_0 = B, \quad C_0 = C^x,$$

the condition of § 4, VII., is satisfied, and

$$C_0^{-1}QC_0 = Q^{a^x}.$$

The type is

$$A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA, \quad AQ = QA, \quad BQ = QB,$$
$$C^{-1}BC = AB, \quad C^{-1}QC = Q^a,$$

where $a$ is any primitive root of

$$a^p \equiv 1 \pmod{q}, \quad \text{and} \quad q \equiv 1 \pmod{p}.$$

As before, $h$ cannot be of order $p$, for $\frac{H}{h}$ would then be non-cyclic.

15. The third principal division of the subject—groups containing one self-conjugate sub-group of order $p^3$, but more than one sub-group of order $q$—must now be considered.

$Q$, as before, represents any operation of order $q$ in $G$, and $H$ is the group of order $p^3$ contained in $G$. If the operations of $H$ are all transformed by $Q$, we obtain the same operations in a different order; $Q$ therefore corresponds to an isomorphism of $H$, and $q$, the order of $Q$, must be a divisor of the order of the group of isomorphisms of $H$. Hence, taking the different types of groups of order $p^3$ in order (as in § 4), the following congruences involving $p$ and $q$ must hold:—

I. $p \equiv 1 \pmod{q}$.

II. $p \equiv 1 \pmod{q}$.

III. $p \equiv 1 \pmod{q}$, or $p \equiv -1 \pmod{q}$, or $p^2+p+1 \equiv 0 \pmod{q}$.

IV. No group exists of the required kind.

V. Here $q$ must divide 24; therefore $q = 3$.

VI. $p \equiv 1 \pmod{q}$.

VII. $p \equiv 1 \pmod{q}$ or $p \equiv -1 \pmod{q}$.

For the same reason $Q$ is permutable with the various characteristic sub-groups of $H$, named in § 4.

Each of the above cases may be subdivided, according to the number of sub-groups of order $q$ contained in $G$; this number is either $p$, $p^2$, or $p^3$.

(i.) If $G$ contains $p$ sub-groups of order $q$, $H$ must contain $p^2$ operations (forming a sub-group) each of which is permutable with each sub-group of order $q$; for, if this was not so, the transformation of $\{Q\}$ by each of the operations of $H$ would produce either more or less than $p$ groups of order $q$. Also, in this case

$$p \equiv 1 \pmod{q} \quad (\S\ 5).$$

(ii.) If $G$ contains $p^2$ sub-groups of order $q$, $H$ must (for a similar reason as in the previous case) contain $p$ operations (forming a sub-group) each of which is permutable with each sub-group of order $q$, and

$$p \equiv 1 \quad \text{or} \quad -1 \pmod{q} \quad (\S\ 5).$$

(iii.) Lastly, if $G$ contains $p^3$ sub-groups of order $q$, either

$$p \equiv 1 \pmod{q} \quad \text{or} \quad p^2+p+1 \equiv 0 \pmod{q}.$$

In reference to these congruences it may be noted here that $p$ must be odd when $H$ is either of the types I. and II.; that $p$ must also be odd when $G$ contains $p$ sub-groups of order $q$; that when $q = 2$ the congruences

$$p \equiv 1 \pmod{q} \quad \text{and} \quad p \equiv -1 \pmod{q}$$

are identical; and that when $q = 3$ the congruences

$$p \equiv 1 \pmod{q} \quad \text{and} \quad p^2+p+1 \equiv 0 \pmod{q}$$

are identical, for $\qquad p^2+p+1 \equiv (p-1)^2 \pmod{3}.$

Lastly, let $D$ be one of the operations of $H$ mentioned above which are permutable with $\{Q\}$; then, since

$$D^{-1}\{Q\}D = \{Q\}, \quad D^{-1}QD = Q^k,$$

[and so $\qquad D^{-1}(QDQ^{-1}) = Q^{k-1}.$

Now, $H$ being a self-conjugate sub-group of $G$, $QDQ^{-1}$ is an operation of $H$, and therefore $D^{-1}(QDQ^{-1})$, that is, $Q^{k-1}$ is also an operation

of $H$. Hence
$$Q^{k-1} = 1,$$
and so
$$k = 1.$$
Therefore $D$ and $Q$ are permutable].*

16. I. $A^{p^3} = 1$; $\qquad p \equiv 1 \pmod q$ (§ 15).

(i.) $p$ *Sub-groups of Order* $q$.—The only group of order $p^2$ here is $\{A^p\}$; so (§ 15)
$$QA^p = A^pQ.$$

Also, since $\{A\}$ is self-conjugate in $G$,
$$Q^{-1}AQ = A^a;$$
and therefore
$$a^q \equiv 1 \pmod{p^3}.$$
Also
$$Q^{-1}A^pQ = A^{ap} \quad\text{and}\quad Q^{-1}A^pQ = A^p,$$
so
$$a \equiv 1 \pmod{p^2}.$$
Putting
$$a = 1 + kp^2,$$
we get
$$a^q = (1+kp^2)^q \equiv 1 + kqp^2 \pmod{p^3},$$
that is
$$k \equiv 0 \pmod p,$$
and so
$$a \equiv 1 \pmod{p^3}.$$
This makes $AQ = QA$, contrary to hypothesis.

(ii.) $p^2$ *Sub-groups of Order* $q$.—Here $Q$ is permutable with $A^{p^2}$ (§ 15), just as in the last case this is inconsistent with
$$Q^{-1}AQ = A^a,$$
$a$ being a primitive root of $\qquad a^q \equiv 1 \pmod{p^3}$.

(iii.) $p^3$ *Sub-groups of Order* $q$.—Here
$$Q^{-1}AQ = A^a,$$
where $a$ is a primitive root of $\quad a^q \equiv 1 \pmod{p^3}$.

In order that this should have any primitive roots the necessary and sufficient condition is that
$$p \equiv 1 \pmod q.$$

* Added May 18th, 1899.

By taking $Q_0 = Q^x$, we get $a^x$ in place of $a$; there is, therefore, when $p$ is odd, one type,

$$A^{p^3} = 1, \quad Q^q = 1, \quad Q^{-1}AQ = A^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p^3}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

17. II. $A^{p^2} = B^p = 1$, $AB = BA$,

$$p \equiv 1 \pmod{q} \quad (\S\ 15).$$

(i.) *$p$ Sub-groups of Order $q$.*—The group of order $p^2$ with whose operations $Q$ is permutable (§ 15) is either $\{A^p, B\}$ or $\{AB^k\}$.

First, taking it to be $\{A^p, B\}$, then

$$A^pQ = QA^p, \quad BQ = QB.$$

Then of the $p$ cyclic groups of order $p^2$ in $H$ one at least [§ 3 (2)] is permutable with $Q$; if this is $\{AB^k\}$, we can put

$$A_0 = AB^k,$$

and then $\qquad A_0^p = A^p \quad \text{and} \quad Q^{-1}A_0Q = A_0^a.$

Hence $\qquad a^q \equiv 1 \pmod{p^2}, \quad \text{and} \quad ap \equiv p \pmod{p^2}.$

Therefore $\qquad a \equiv 1 \pmod{p^2},$

and $G$ is Abelian, contrary to hypothesis.

Secondly, let $Q$ be permutable with the operations of $\{AB^k\}$; without loss of generality we may write this $\{A\}$. Then $AQ = QA$. Of the $p$ remaining groups of order $p$ in $H$ besides $\{A^p\}$, since

$$p \equiv 1 \pmod{q},$$

one at least [§ 3 (2)] is permutable with $Q$; without loss of generality, we can take this sub-group to be $\{B\}$, and then

$$Q^{-1}BQ = B^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}.$$

Thus there is one type,

$$A^{p^2} = B^p = Q^q = 1, \quad AB = BA, \quad AQ = QA, \quad Q^{-1}BQ = B^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

(ii.) $p^2$ *Sub-groups of Order* $q$.—The group of order $p$ with whose operations $Q$ is permutable (§ 15) is either $\{A^p\}$ or $\{A^{kp}B\}$ (of which latter $\{B\}$ may be taken as typical). The case of $A^p$ being permutable with $Q$ may be disposed of just as before.

Next, $BQ = QB$. Of the $p$ cyclic sub-groups of order $p^2$ one at least is permutable with $Q$. This may be taken to be $\{A\}$, and then

$$Q^{-1}AQ = A^a,$$

where
$$a^q \equiv 1 \pmod{p^2}.$$

Thus we get one type

$$A^{p^2} = B^p = Q^q = 1,\quad AB = BA,\quad Q^{-1}AQ = A^a,\quad BQ = QB,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p^2}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

(iii.) $p^3$ *Sub-groups of Order* $q$.—As before, at least one of the $p$ cyclic sub-groups of order $p^2$ is permutable with $Q$, and this may be taken as $\{A\}$, and at least one other besides $\{A^p\}$ of the $p+1$ sub-groups of order $p$ is also permutable with $Q$; this may be taken as $\{B\}$.

So
$$Q^{-1}AQ = A^a,$$

where $a$ is a primitive root of $a^q \equiv 1 \pmod{p^2}$,

and
$$Q^{-1}BQ = B^b,$$

where $b$ is a primitive root of $b^q \equiv 1 \pmod{p}$.

How many types do these relations contain? $A^xB^yQ^z$ is of order $q$, but, so far as its effect in transforming any operation of $H$ is concerned, it is equivalent to $Q^z$. Putting $Q_0 = Q^z$, we get $a^z$ in place of $a$, $b^z$ in place of $b$; $a$ may therefore be fixed as any one of the primitive roots of

$$a^q \equiv 1 \pmod{p^2},$$

and there are $q-1$ types corresponding to the $q-1$ values of $b$, which may be taken congruent to

$$a,\ a^2,\ \ldots,\ a^{q-1} \pmod{p}.$$

When
$$b \not\equiv a \pmod{p},$$

that is, for $q-2$ of these types, none other of the cyclic groups of order $p^2$ besides $\{A\}$ and none other of the groups of order $p$ besides $\{A^p\}$ and $\{B\}$ are permutable with $Q$; but, when

$$b \equiv a \pmod{p},$$

all the sub-groups of $H$ are permutable with $Q$. The relations of these $q-1$ types are

$$A^{p^2} = B^p = Q^q = 1, \quad AB = BA, \quad Q^{-1}AQ = A^a, \quad Q^{-1}BQ = B^a,$$

or

$$B^{a^2}, \; \ldots, \; \text{or} \;\; B^{a^{q-1}},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p^2}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

18. III. $A^p = B^p = C^p = 1, \; AB = BA, \; AC = CA, \; BC = CB.$

(i.) *$p$ Sub-groups of Order $q$;* then

$$p \equiv 1 \pmod{q}.$$

—The group of order $p^2$ with whose operations $Q$ is permutable (§15) may, without loss of generality, be taken to be $\{A, B\}$.

Now $H$ contains $p^2+p+1$ sub-groups of order $p$; since

$$AQ = QA, \quad BQ = QB,$$

we know that $Q$ is permutable with $p+1$ of these, viz., $\{A\}$, $\{AB^k\}$. Of the $p^2$ remaining sub-groups of order $p$, since

$$p^2 \equiv 1 \pmod{q},$$

there must be at least one other, independent of $A$ and $B$, which is permutable with $Q$.

Taking it to be $\{C\}$, we get

$$Q^{-1}CQ = C^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

This, combined with the relations of III. and with

$$AQ = QA, \quad BQ = QB,$$

furnishes one type.

19. (ii.) *$p^2$ Sub-groups of Order $q$;* and

$$p \equiv 1 \pmod{q}.$$

—The group of order $p$ with whose operations $Q$ is permutable may be taken to be $\{A\}$; then, if $q > 2$, among the $p^2+p$ other sub-groups of order $p$ there are at least two permutable with $Q$; putting, as we may, $\{B\}$ for one of them, the second may either be $\{A^kB\}$, or else, if independent of $A$ and $B$, may be taken as $\{C\}$. But the first of these alternatives is impossible; for

$$AQ = QA, \quad Q^{-1}BQ = B^a;$$

and therefore $$Q^{-1}A^kBQ = A^kB^a,$$

and this is not a power of $A^kB$; therefore we must have

$$Q^{-1}CQ = C^b.$$

Here $a$ and $b$ are both primitive roots of

$$a^q \equiv 1 \quad (\text{mod } p).$$

We can put $$b \equiv a^x \quad (\text{mod } p),$$

and the question arises, how many different types are there for different values of $x$?

So far as altering $a$ and $b$ is concerned, the most general transformation of $G$ is given by

$$Q_0 = Q^y, \quad B_0 = B \text{ or } C, \quad C_0 = C \text{ or } B.$$

Now $$Q_0 = Q^y, \quad B_0 = B, \quad C_0 = C$$

merely amounts to taking a different root of

$$a^q \equiv 1 \quad (\text{mod } p)$$

for $a$. On the other hand, if

$$Q_0 = Q^y, \quad B_0 = C, \quad C_0 = B,$$

we get $$Q_0A = AQ_0, \quad Q_0^{-1}B_0Q_0 = B_0^{a^{xy}}, \quad Q_0^{-1}C_0Q_0 = C_0^{a^y}.$$

If, then, we choose $y$ so that $xy \equiv 1 \quad (\text{mod } q)$,

we have $$a^{xy} \equiv a \quad (\text{mod } p),$$

and thus we get $Q_0^{-1}B_0Q_0 = B_0^a, \quad Q_0^{-1}C_0Q_0 = C_0^{a^y}$;

the same relations as before with $y$ in the place of $x$.

The number of types is therefore the number of solutions of

$$xy \equiv 1 \quad (\text{mod } q),$$

the order of each pair $(x, y)$ being immaterial.

There are two solutions for which $x \equiv y$, viz.,

$$x \equiv y \equiv 1 \ (\text{mod } q), \quad \text{and} \quad x \equiv y \equiv q-1 \ (\text{mod } q).$$

The remaining $q-3$ residues to the modulus $q$ fall into $\frac{q-3}{2}$ pairs, each pair being a solution of

$$xy \equiv 1 \pmod{q}.$$

Altogether there are $2+\frac{q-3}{2} = \frac{q+1}{2}$ types,

$$A^p = B^p = C^p = Q^q = 1,\ AB = BA,\ AC = CA,\ AQ = QA,\ BC = CB,$$

$$Q^{-1}BQ = B^a,\quad Q^{-1}CQ = C^{a^x},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p},$$

$x$ assumes any of the $\frac{q+1}{2}$ values above mentioned, and

$$p \equiv 1 \pmod{q}.$$

[Each of these types is the direct product of $\{A\}$ and $\{B,\ C,\ Q\}$].*

The case $q=2$ was not included above; besides $\{A\}$, either none or at least two groups of order $p$ are permutable with $Q$; if the latter is the case, we get the one type

$$A^p = B^p = C^p = Q^2 = 1,\ AB = BA,\ AC = CA,\ AQ = QA,$$

$$BC = CB,\ QBQ = B^{-1},\ QCQ = C^{-1}.$$

If, on the other hand, no other group of order $p$ besides $\{A\}$ is permutable with $Q$, $QBQ$ is either $A^xB^y$, or, if independent of $A$ and $B$, may be taken as $C$; first,

$$QBQ = A^xB^y,$$

where $x$ is not zero. Then

$$B = QA^xB^yQ = A^{x+xy}B^{y^2};$$

and therefore $$y \equiv -1 \pmod{p}.$$

But now $$QA^{-x}B^2Q = A^{-x}A^{2x}B^{-2} = (A^{-x}B^2)^{-1};$$

the sub-group $\{A^{-x}B^2\}$ is therefore permutable with $Q$, contrary to hypothesis.

Secondly, let $$QBQ = C,$$

then $$QCQ = B;$$

and therefore $$Q(BC)Q = BC,$$

again contrary to hypothesis.

* Added May 16th, 1899.

20. (iii.) $p^2$ *Sub-groups of Order* $q$;

$$p \equiv -1 \pmod{q},$$

where $q \neq 2$ (§ 15).—The group of order $p$ whose operations are permutable with $\{Q\}$ may be taken to be $\{A\}$; then

$$AQ = QA \quad (\S\ 15).$$

No other group of order $p$ can be permutable with $Q$, for the congruence

$$a^q \equiv 1 \pmod{p}$$

has no primitive roots. Since

$$p^2+p+1 \equiv 1 \pmod{q},$$

at least one of the sub-groups of order $p^2$ is permutable with $Q$. First suppose that this is $\{A, B\}$. Then

$$Q^{-1}BQ = A^aB^b;$$

and therefore $$Q^{-x}BQ^x = A^{a(1+b+\ldots+b^{x-1})}B^{b^x};$$

therefore, when $x = q$,

$$B = A^{a(1+b+\ldots+b^{q-1})}B^{b^q};$$

then $$b^q \equiv 1 \pmod{p},$$

that is, $$b \equiv 1 \pmod{p};$$

and then the index of $A$ is

$$a(1+b+\ldots+b^{q-1}) \equiv qa,$$

an impossible result, since $qa \not\equiv 0 \pmod{p}$.

The sub-group of order $p^2$ permutable with $Q$ cannot then contain $\{A\}$; it may therefore be taken to be $\{B, C\}$. Then we get

$$AQ = QA, \quad Q^{-1}BQ = C, \quad Q^{-1}CQ = B^aC^b.$$

$\{B, C, Q\}$ is a group of order $p^2q$, which is discussed by Burnside in his *Theory of Groups*, p. 136. He shows that the congruence

$$\iota^2 - b\iota - a \equiv 0 \pmod{p}$$

is obtained, and, on the assumption that its two roots are distinct, proves that they are Galoisian imaginaries, each satisfying

$$\iota^q \equiv 1 \pmod{p}.$$

It is easy to verify that $a$ and $b$ cannot have such values that this quadratic congruence has equal roots. We thus get one type, the direct product of $\{A\}$ and $\{B, C, Q\}$, the defining relations of the latter being

$$B^p = C^p = Q^q = 1, \quad BC = CB, \quad Q^{-1}BQ = C, \quad Q^{-1}CQ = B^{-1}C^{\iota^p+\iota},$$

where $\iota$ is any primitive (Galoisian) root of the congruence

$$\iota^q \equiv 1 \pmod{p}, \quad \text{and} \quad p+1 \equiv 0 \pmod{q} \text{ and } q>2.$$

21. (iv.) $p^3$ *Sub-groups of Order* $q$ ; and

$$p \equiv 1 \pmod{q}.$$

—If $q>3$, since $$p^2+p+1 \equiv 3 \pmod{q},$$

at least three groups of order $p$ are permutable with $Q$; let $\{A\}$ and $\{B\}$ be two of these; then

$$Q^{-1}AQ = A^a, \quad Q^{-1}BQ = B;$$

if $a$ is not equal to $b$, the third must be independent of $A$ and $B$, and may be taken as $\{C\}$; if $a$ is equal to $b$, then $\{A\}$ and $\{A^kB\}$ are $p+1$ groups of order $p$ permutable with $Q$, and there must therefore be at least one more, $\{C\}$. We therefore get

$$Q^{-1}AQ = A^a, \quad Q^{-1}BQ = B^{a^x}, \quad Q^{-1}CQ = C^{a^y},$$

where $a$ is a primitive root of

$$a^q \equiv 1 \pmod{p},$$

and $x$ and $y$ may have any of the values $1, 2, \ldots, q-1$. The somewhat difficult matter remains to determine the number of types comprised in these relations.

As in similar cases before, it suffices to consider the results of taking a power of $Q$ for $Q$, and permuting the generators of $H$. In this way we get two distinct equivalences:

First, $$Q_0 = Q^\xi, \quad A_0 = B, \quad B_0 = A, \quad C_0 = C,$$

and $$\xi x \equiv 1 \pmod{q};$$

then $$Q_0^{-1}A_0Q_0 = A_0^a, \quad Q_0^{-1}B_0Q_0 = B_0^{a^\xi}, \quad Q_0^{-1}C_0Q_0 = C_0^{a^{\xi y}}.$$

Second, $$Q_0 = Q^\eta, \quad A_0 = C, \quad B_0 = B, \quad C_0 = A,$$

and $$\eta y \equiv 1 \pmod{q};$$

then $$Q_0^{-1}A_0Q_0 = A_0^a, \quad Q_0^{-1}B_0Q_0 = B_0^{a^{\eta x}}, \quad Q_0^{-1}C_0Q_0 = C_0^{a^\eta}.$$

Thus, for each pair $(x, y)$, we get corresponding pairs $(\xi, \xi y)$ and $(\eta x, \eta)$; and each of these pairs provides the same type of group; on the other hand, any two pairs $(x, y)$ and $(x', y')$ which are not equivalent correspond to different types. Of course the order of $x$ and $y$ in the symbol $(x, y)$ is immaterial.

It will be convenient to replace these numbers $x, y, \xi$, &c., by their indices (mod $q$). Then let

$$x \equiv \gamma^{x_0}, \quad y \equiv \gamma^{y_0}, \quad \xi \equiv \gamma^{-x_0}, \quad \eta \equiv \gamma^{-y_0} \quad (\text{mod } q);$$

we thus get $x_0$ and $y_0$ any two of the complete set of residues to mod $q-1$; viz., $0, 1, 2, \ldots, q-2$. And the trio of equivalent pairs is

$$(x_0, y_0), \quad (-y_0, x_0-y_0), \quad (y_0-x_0, -x_0).$$

Let $$\lambda \equiv -y_0, \quad \mu \equiv x_0, \quad \nu \equiv y_0-x_0 \quad (\text{mod } q-1).$$

Then $$\lambda+\mu+\nu \equiv 0 \qquad (\text{mod } q-1),$$

and the equivalent pairs are

$$(-\lambda, \mu), \quad (-\mu, \nu), \quad (-\nu, \lambda);$$

and we must now enumerate the solutions of this congruence.

Let $a$ be the number of trios $(\lambda, \mu, \nu)$, disregarding order of $\lambda, \mu, \nu$, in which all three numbers are different, $\beta$ the similar number in which two only are equal, and $\gamma$ the similar number in which all three are equal.

If $$q \equiv 1 \quad (\text{mod } 3),$$
$$\gamma = 3,$$

for the solutions of this class are

$$\lambda \equiv \mu \equiv \nu \equiv 0, \text{ or } \equiv \frac{q-1}{3}, \text{ or } \equiv \frac{2(q-1)}{3} \quad (\text{mod } q-1).$$

If $$q \equiv 2 \quad (\text{mod } 3),$$
$$\gamma = 1,$$

viz., $$\lambda \equiv \mu \equiv \nu \equiv 0 \quad (\text{mod } q-1).$$

Next, when two are equal, the congruence is

$$\lambda+2\mu \equiv 0 \quad (\text{mod } q-1).$$

$\mu$ must not be $\equiv 0$, $\frac{q-1}{3}$, or $\frac{2(q-1)}{3}$, for then it would be $\equiv \lambda$.

With these exceptions $\mu$ can have any value, and for each value of $\mu$ the congruence gives one value of $\lambda$. So, when

$$q \equiv 1 \pmod 3),$$
$$\beta = q-4;$$

when

$$q \equiv 2 \pmod 3),$$
$$\beta = q-2.$$

Now the total number of solutions of all kinds of the congruence, considering the order of each trio, is $(q-1)^2$, for $\mu$ and $\nu$ can each have any one of $q-1$ values, and the congruence gives a corresponding value of $\lambda$ to each $\mu$ and $\nu$.

Also, in terms of $\alpha$, $\beta$, and $\gamma$, the total number of solutions considering the order of each trio, is $6\alpha+3\beta+\gamma$. Therefore

$$6\alpha+3\beta+\gamma = (q-1)^2;$$

then, if

$$q \equiv 1 \pmod 3),$$
$$\alpha = \tfrac{1}{6}(q^2-5q+10),$$

but, if

$$q \equiv 2 \pmod 3),$$
$$\alpha = \tfrac{1}{6}(q^2-5q+6).$$

It is necessary to subdivide these $\alpha$ solutions into those ($\alpha_0$ in number) in which one of the trio is 0, and the remainder ($\alpha_1$ in number) in which this is not the case.

Now $\alpha_0$ is the number of solutions of

$$\lambda+\mu \equiv 0 \pmod{q-1},$$

out of the numbers 1, 2, ..., $q-2$, excluding the solution

$$\lambda \equiv \mu \equiv \frac{q-1}{2};$$

so

$$\alpha_0 = \frac{q-3}{2}.$$

Therefore, when

$$q \equiv 1 \pmod 3),$$
$$\alpha_1 = \tfrac{1}{6}(q^2-8q+19),$$

and, when

$$q \equiv 2 \pmod 3),$$
$$\alpha_1 = \tfrac{1}{6}(q^2-8q+15).$$

Each trio $\lambda$, $\mu$, $\nu$ in which all are unequal and different from zero corresponds to one set of equivalent pairs $(-\lambda, \mu)$, $(-\mu, \nu)$, $(-\nu, \lambda)$, and therefore to one type of group; altogether these give $a_1$ types.

Each trio $\lambda$, $\mu \equiv -\lambda$, 0 in which all are unequal corresponds to two distinct sets of equivalent pairs, one being $(-\lambda, -\lambda)$, $(\lambda, 0)$, the other $(\lambda, \lambda)$, $(-\lambda, 0)$, and therefore to two types of group, altogether $2a_0$ types.

Each trio $\lambda$, $\mu$, $\mu$ corresponds to the equivalent pairs $(-\lambda, \mu)$, $(\lambda, -\mu)$, $(-\mu, +\mu)$; the trio $-\lambda$, $-\mu$, $-\mu$ corresponds to the same set; when

$$\mu \equiv \frac{q-1}{2},$$

the trios $(\lambda, \mu, \mu)(-\lambda, -\mu, -\mu)$ form the same solution, but the other trios go in pairs, each pair of trios furnishing one type; thus we get altogether from these trios $\frac{\beta-1}{2}+1$, *i.e.*, $\frac{\beta+1}{2}$, types.

Lastly, when $$q \equiv 1 \pmod 3,$$

there are the two distinct types corresponding to $(0, 0)$, and $\left(\frac{q-1}{3}, -\frac{q-1}{3}\right)$, but, when

$$q \equiv 2 \pmod 3,$$

the single type corresponding to $(0, 0)$.

Adding up these numbers, when

$$q \equiv 1 \pmod 3,$$

the number of types is

$$\frac{q^2-8q+19}{6}+q-3+\frac{q-3}{2}+2=\frac{q^2+q+4}{6};$$

when $$q \equiv 2 \pmod 3,$$

the number is $\frac{q^2-8q+15}{6}+q-3+\frac{q-1}{2}+1=\frac{q^2+q}{6}$.

The relations for these types are

$$A^p = B^p = C^p = Q^q = 1,\quad AB = BA,\quad AC = CA,\quad BC = CB,$$

$$Q^{-1}AQ = A^a,\quad Q^{-1}BQ = B^{a^x},\quad Q^{-1}CQ = C^{a^y},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod p,\quad p \equiv 1 \pmod q,$$

and $x$ and $y$ are chosen as above described.

The cases $q = 2$ and 3 have been hitherto excluded; it is, however, easy to see that, if there are three independent groups of order $p$ permutable with $Q$, all the above work, with the exception of the actual enumeration, applies to these cases.

When $q = 2$, we obtain the single type with the relations

$$Q^{-1}AQ = A^{-1}, \quad Q^{-1}BQ = B^{-1}, \quad Q^{-1}CQ = C^{-1},$$

and, when $q = 3$, the two types

$$Q^{-1}AQ = A^{a}, \quad Q^{-1}BQ = B^{a}, \quad Q^{-1}CQ = C^{a},$$

and $$Q^{-1}AQ = A^{a}, \quad Q^{-1}BQ = B^{a}, \quad Q^{-1}CQ = C^{a^2},$$

where $a$ is any primitive root of

$$a^3 \equiv 1 \pmod{p}, \quad \text{and} \quad p \equiv 1 \pmod{3}.$$

There still remain other possible cases for $q = 2$ or 3, which, however, on examination lead to no fresh types.

$q = 2$.—Suppose that $\{A\}$ is the only group of order $p$ permutable with $Q$; then

$$QAQ = A^{-1}.$$

Either $$QBQ = A^xB^y,$$

or it may be taken to be $C$.

In the first case, $$B = A^{-x+xy}B^{y^2},$$

so $$y = 1,$$

and then $$Q(A^xB^2)Q = A^{-x}A^{2x}B^2 = A^xB^2,$$

which is contrary to hypothesis.

Secondly, $$QBQ = C;$$

then $$QCQ = B,$$

and so $$Q(BC)Q = BC,$$

again contrary to hypothesis.

$q = 3$.—Here, since it is supposed that there are not three groups of order $p$ permutable with $Q$, there are none such; then

$$Q^{-1}AQ = B \text{ (say)}, \quad \text{and} \quad Q^{-1}BQ = A^xB^y \text{ or } C \text{ (say)}.$$

In the first case $$A = Q^{-1}A^xB^yQ = A^{xy}B^{x+y^2},$$

and so $$\left.\begin{aligned} xy &\equiv 1 \\ x &\equiv -y^2 \end{aligned}\right\} \pmod{p}.$$

Either $$x \equiv y \equiv -1, \quad \text{or} \quad x \equiv -a, \quad y \equiv -a^2,$$

$a$ being a primitive root of $$a^3 \equiv 1 \pmod{p},$$

and then either $$Q^{-1}(AB^{-a})\,Q = (AB^{-a})^a,$$

or $$Q^{-1}(AB^{-1})\,Q = (AB^{-1})^a;$$

each of which contradicts the hypothesis.

Lastly, if $$Q^{-1}AQ = B, \quad \text{and} \quad Q^{-1}BQ = C,$$

then $$Q^{-1}CQ = A,$$

and therefore $$Q^{-1}(ABC)\,Q = ABC;$$

this again is impossible.

22. (v.) $p^3$ *Sub-groups of Order* $q$, and
$$p^2+p+1 \equiv 0 \pmod{q};$$

then $q > 3$ (§ 15).—None of the groups of order $p$ can be permutable with $Q$, for, if
$$Q^{-1}AQ = A^a,$$

then $$a^q \equiv 1 \pmod{p};$$

but, $q$ being a divisor of $p^2+p+1$, must be prime to $p-1$, and therefore
$$a \equiv 1 \pmod{p},$$
which is impossible.

The $p^2+p+1$ groups of order $p$ must therefore fall into $\dfrac{p^2+p+1}{q}$ sets, each set being cyclically permuted when its groups are transformed by $Q$.

Then $Q^{-1}AQ$ is not included in $\{A\}$, and may be taken as $B$; and $Q^{-1}BQ$ is either $A^xB^y$ or may be taken as $C$. The former case is, however, impossible; for, if so, $\{A, B, Q\}$ is the group of order $p^2q$ already referred to (§ 20), and a necessary condition for its existence is that
$$p+1 \equiv 0 \pmod{q},$$

which is not true here. We therefore obtain
$$Q^{-1}AQ = B, \quad Q^{-1}BQ = C, \quad Q^{-1}CQ = A^{\alpha}B^{\beta}C^{\gamma}.$$

Let $$Q^{-x}CQ^{x} = A^{\alpha_x}B^{\beta_x}C^{\gamma_x}.$$

Then $\alpha_x$, $\beta_x$, and $\gamma_x$ must be such that for $x = q$, but for no smaller value of $x$, the following congruences are true :—

$$\left.\begin{array}{lll} \alpha_{x-2} \equiv 1, & \alpha_{x-1} \equiv 0, & \alpha_x \equiv 0 \\ \beta_{x-2} \equiv 0, & \beta_{x-1} \equiv 1, & \beta_x \equiv 0 \\ \gamma_{x-2} \equiv 0, & \gamma_{x-1} \equiv 0, & \gamma_x \equiv 1 \end{array}\right\} \pmod{p}.$$

Since $$A^{\alpha_x}B^{\beta_x}C^{\gamma_x} = Q^{-1}A^{\alpha_{x-1}}B^{\beta_{x-1}}C^{\gamma_{x-1}}Q$$
$$= B^{\alpha_{x-1}}C^{\beta_{x-1}}A^{\alpha\gamma_{x-1}}B^{\beta\gamma_{x-1}}C^{\gamma\gamma_{x-1}},$$

$\alpha_x$, $\beta_x$, $\gamma_x$ are determined by the linear difference-congruences

$$\left.\begin{array}{l} \alpha_x \equiv \alpha\gamma_{x-1} \\ \beta_x \equiv \alpha_{x-1}+\beta\gamma_{x-1} \\ \gamma_x \equiv \gamma\gamma_{x-1}+\beta_{x-1} \end{array}\right\} \pmod{p}.$$

Hence $$\gamma_x-\gamma\,\gamma_{x-1}-\beta\,\gamma_{x-2}-\alpha\,\gamma_{x-3} \equiv 0 \pmod{p}.$$

The solution of this difference-congruence depends on the congruence

$$\lambda^3-\gamma\lambda^2-\beta\lambda-\alpha \equiv 0 \pmod{p}.$$

First, suppose that the three roots of this are equal, say $\lambda$. Then the proper form for $\gamma_x$ is

$$\gamma_x \equiv (\delta_1+\delta_2 x+\delta_3 x^2)\,\lambda^x,$$

$\delta_1$, &c., being arbitrary constants.

(Throughout this section, all congruences are to be understood as being to the modulus $p$, unless otherwise expressed.)

In this case $$\gamma \equiv \Sigma\lambda_1 \equiv 3\lambda,$$
$$\beta \equiv -\Sigma\lambda_1\lambda_2 \equiv -3\lambda^2.$$

Now $$\gamma_0 \equiv 1 \quad (\text{for } \alpha_1 \equiv \alpha\gamma_0, \text{ and } \alpha_1 \equiv \alpha),$$
$$\gamma_1 \equiv \gamma \equiv 3\lambda,$$
$$\gamma_2 \equiv \gamma\gamma_1+\beta_1 \equiv \gamma^2+\beta \equiv 6\lambda^2.$$

If $p = 2$, $\lambda \equiv 1$, and we at once obtain $\gamma_3 \equiv 1$; this is impossible.

If $p>2$, $$\delta_1 \equiv 1,$$
$$\delta_2+\delta_2+\delta_3 \equiv 3,$$
$$\delta_1+2\delta_2+4\delta_3 \equiv 6,$$

and so $$\gamma_x = \tfrac{1}{2}(x+1)(x+2)\,\lambda^x.$$

This does not satisfy the conditions

$$\gamma_{q-2} \equiv \tfrac{1}{2}(q-1)\,q\,.\,\lambda^{q-2} \equiv 0,$$

$$\gamma_{q-1} \equiv \tfrac{1}{2}q\,(q+1)\,\lambda^{q-1} \equiv 0,$$

for these congruences are evidently impossible.

Secondly, let two of the three roots of the congruence

$$\lambda^3-\gamma\lambda^2-\beta\lambda-\alpha \equiv 0$$

be congruent; let them be $\lambda_1, \lambda_2, \lambda_2$. Then the proper form for $\gamma_x$ is

$$\gamma_x \equiv \delta_1\lambda_1^x+(\delta_2+\delta_3 x)\,\lambda_2^x.$$

Then
$$\begin{aligned} \delta_1 \;+\delta_2 \qquad\qquad &\equiv 1,\\ \delta_1\lambda_1+\delta_2\lambda_2+\;\delta_3\lambda_2 &\equiv \lambda_1+2\lambda_2,\\ \delta_1\lambda_1^2+\delta_2\lambda_2^2+2\delta_3\lambda_2^2 &\equiv \lambda_1^2+2\lambda_1\lambda_2+3\lambda_2^2, \end{aligned}$$

and so
$$\delta_1 \equiv \frac{\lambda_1^2}{(\lambda_1-\lambda_2)^2},\quad \delta_2 \equiv \frac{\lambda_2^2-2\lambda_1\lambda_2}{(\lambda_1-\lambda_2)^2},$$

and
$$\delta_3 \equiv \frac{-\lambda_2}{\lambda_1-\lambda_2};$$

therefore $\gamma_x \equiv \dfrac{1}{(\lambda_1-\lambda_2)^2}\left\{\lambda_1^{x+2}-(x+2)\,\lambda_1\lambda_2^{x+1}+(x+1)\,\lambda_2^{x+2}\right\}.$

The conditions
$$\gamma_{q-2} \equiv 0,\quad \gamma_{q-1} \equiv 0$$

give
$$\begin{aligned} \lambda_1^q-\lambda_2^q &\equiv q\lambda_2^{q-1}(\lambda_1-\lambda_2),\\ \lambda_1(\lambda_1^q-\lambda_2^q) &\equiv q\lambda_2^q(\lambda_1-\lambda_2). \end{aligned}$$

These lead to
$$\lambda_1^q \equiv \lambda_2^q \equiv 0,$$

which is not possible.

The three roots of $\lambda^3-\gamma\lambda^2-\beta\lambda-\alpha \equiv 0$ are therefore incongruent; let them be $\lambda_1, \lambda_2, \lambda_3$. Then

$$\gamma_x \equiv \delta_1\lambda_1^x+\delta_2\lambda_2^x+\delta_3\lambda_3^x,$$

and so
$$\begin{aligned} \delta_1+\;\;\delta_2+\;\;\delta_3 &\equiv 1,\\ \lambda_1\delta_1+\lambda_2\delta_2+\lambda_3\delta_3 &\equiv \lambda_1+\lambda_2+\lambda_3,\\ \lambda_1^2\delta_1+\lambda_2^2\delta_2+\lambda_3^2\delta_3 &\equiv \lambda_1^2+\lambda_2^2+\lambda_3^2+\lambda_2\lambda_3+\lambda_3\lambda_1+\lambda_1\lambda_2. \end{aligned}$$

Let
$$\Delta \equiv \begin{vmatrix} 1 & 1 & 1\\ \lambda_1 & \lambda_2 & \lambda_3\\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 \end{vmatrix} \equiv (\lambda_1-\lambda_2)(\lambda_2-\lambda_3)(\lambda_3-\lambda_1).$$

Then $\Delta\delta_1 \equiv -(\lambda_2-\lambda_3)\,\lambda_1^2$.

Thus we obtain the results

$$\Delta.\alpha_x \equiv -\alpha\Sigma(\lambda_2-\lambda_3)\,\lambda_1^{x+1} \equiv -\Sigma\lambda_2\lambda_3(\lambda_2-\lambda_3)\,\lambda_1^{x+2},$$

$$\Delta.\beta_x \equiv \quad \Sigma(\lambda_2^2-\lambda_3^2)\,\lambda_1^{x+2},$$

$$\Delta.\gamma_x \equiv - \quad \Sigma(\lambda_2-\lambda_3)\,\lambda_1^{x+2}.$$

Now, in the light of the three relations between $\alpha_x$, $\beta_x$, $\gamma_x$, $\alpha_{x-1}$, $\beta_{x-1}$, $\gamma_{x-1}$, only three of the nine conditions above mentioned are independent; we may take as an independent trio

$$\gamma_{q-2} \equiv 0, \quad \gamma_{q-1} \equiv 0, \quad \gamma_q \equiv 1.$$

From the first two of these

$$(\lambda_2-\lambda_3)\,\lambda_1^q \;+(\lambda_3-\lambda_1)\,\lambda^q \;+(\lambda_1-\lambda_2)\,\lambda_3^q \;\equiv 0,$$

$$(\lambda_2-\lambda_3)\,\lambda_1^{q+1}+(\lambda_3-\lambda_1)\,\lambda_2^{q+1}+(\lambda_1-\lambda_2)\,\lambda_3^{q+1} \equiv 0\,;$$

and therefore

$$(\lambda_3-\lambda_1)\,\lambda_2^q\,(\lambda_1-\lambda_2)+(\lambda_1-\lambda_2)\,\lambda_3^q\,(\lambda_1-\lambda_3) \equiv 0,$$

that is, $\lambda_2^q \equiv \lambda_3^q$.

From the symmetry of these congruences,

$$\lambda_1^q \equiv \lambda_2^q \equiv \lambda_3^q.$$

Thirdly, $-\Sigma\,(\lambda_2-\lambda_3)\,\lambda_1^{q+2} \equiv \Delta$.

But $\Sigma\,(\lambda_2-\lambda_3)\,\lambda_1^{q+2} \equiv \lambda_1^q\Sigma\,(\lambda_2-\lambda_3)\,\lambda_1^2 \equiv -\Delta\lambda_1^q$.

Therefore $\lambda_1^q \equiv \lambda_2^q \equiv \lambda_3^q \equiv 1$,

and $\lambda_1$, $\lambda_2$, $\lambda_3$ are primitive roots of the congruence

$$\lambda^q \equiv 1 \pmod{p}.$$

Since $q$ is not a factor of $p-1$ or $p^2-1$, but is a factor of $p^3-1$, $\lambda_1$, $\lambda_2$, and $\lambda_3$ are Galoisian imaginaries of the third order, and the congruence

$$\lambda^3-\gamma\lambda^2-\beta\lambda-\alpha \equiv 0 \pmod{p}$$

is therefore irreducible.

Let $\lambda$ be any one of the three $\lambda_1$, $\lambda_2$, $\lambda_3$; then $\lambda^p$ and $\lambda^{p^2}$ are the other two; for $\lambda$, $\lambda^p$, $\lambda^{p^2}$ are necessarily incongruent, and

$$\begin{aligned}\lambda^{3p} &\equiv (\gamma\lambda^2+\beta\lambda+\alpha)^p\\ &\equiv \gamma^p\lambda^{2p}+\beta^p\lambda^p+\alpha\\ &\equiv \gamma\lambda^{2p}+\beta\lambda^p+\alpha,\end{aligned}$$

and so $\lambda^p$, and similarly $\lambda^{p^2}$, satisfy the congruence. Then

$$\gamma \equiv \lambda+\lambda^p+\lambda^{p^2},$$

$$\beta \equiv -\lambda^{p+1}-\lambda^{p^2+1}-\lambda^{p^2+p},$$

and $$\alpha \equiv \lambda.\lambda^p.\lambda^{p^2} \equiv 1,$$

since $$p^2+p+1 \equiv 0 \pmod q.$$

Each value of $\lambda$ therefore defines a single group, with the relations

$$Q^{-1}AQ=B,\quad Q^{-1}BQ=C,\quad Q^{-1}CQ=AB^{\beta}C^{\gamma}.$$

I shall now prove that there is the same type, whichever primitive root of

$$\lambda^q \equiv 1 \pmod p$$

is taken. Let $$Q_0=Q^x;$$

then $$B_0=Q_0^{-1}AQ_0=A^{\alpha_{x-2}}B^{\beta_{x-2}}C^{\gamma_{x-2}},$$

$$C_0=Q_0^{-1}B_0Q_0=A^{\alpha_{2x-2}}B^{\beta_{2x-2}}C^{\gamma_{2x-2}},$$

$$Q_0^{-1}C_0Q_0=A^{\alpha_{3x-2}}B^{\beta_{3x-2}}C^{\gamma_{3x-2}},$$

and $$A^{\alpha'}B_0C_0^{\gamma'}=A^{\gamma'\alpha_{2x-2}+\beta'\alpha_{x-2}+\alpha'}B^{\gamma'\beta_{2x-2}+\beta'\beta_{x-2}}C^{\gamma'\gamma_{1x-2}+\beta'\gamma_{x-2}}.$$

Therefore $$Q_0^{-1}C_0Q_0=A^{\alpha'}B_0^{\beta'}C_0^{\gamma'},$$

provided that $\alpha'$, $\beta'$, and $\gamma'$ satisfy the congruences

$$\begin{aligned}\alpha_{3x\cdot2}-\gamma'\alpha_{2x-2}-\beta'\alpha_{x-2}-\alpha' &\equiv 0,\\ \beta_{3x-2}-\gamma'\beta_{2x-2}-\beta'\beta_{x-2} &\equiv 0,\\ \gamma_{3x-2}-\gamma'\gamma_{2x-2}-\beta'\gamma_{x-2} &\equiv 0.\end{aligned}$$

Reverting to the notation $\lambda_1$, $\lambda_2$, and $\lambda_3$ for the roots of the congruence

$$\lambda^3-\gamma\lambda^2-\beta\lambda-\alpha \equiv 0,$$

it is easily seen that these congruences are satisfied by

$$\gamma' \equiv \lambda_1^x+\lambda_2^x+\lambda_3^x,$$

$$\beta' \equiv -\lambda_2^x\lambda_3^x-\lambda_3^x\lambda_1^x-\lambda_1^x\lambda_2^x,$$

$$\alpha' \equiv \lambda_1^x\lambda_2^x\lambda_3^x \equiv 1.$$

For, if $\alpha'$, $\beta'$, and $\gamma'$ have these values, we have

$$\lambda_k^{3x}-\gamma'\lambda_k^{2x}-\beta'\lambda_k^x-\alpha' \equiv 0,$$

identically, for $k = 1, 2, 3$; and then

$$\Delta\,(\alpha_{3x-2}-\gamma'\alpha_{2x-2}-\beta'\alpha_{x-2}-\alpha')$$

$$\equiv -\Sigma\lambda_2\lambda_3\,(\lambda_2-\lambda_3)(\lambda_1^{3x}-\gamma'\lambda_1^{2x}-\beta'\lambda_1^x-\alpha') \equiv 0,$$

$$\Delta\,(\beta_{3x-2}-\gamma'\beta_{2x-2}-\beta'\beta_{x-2}) \equiv \Sigma\,(\lambda_2^2-\lambda_3^2)(\lambda_1^{3x}-\gamma'\lambda_1^{2x}-\beta'\lambda_1^x)$$

$$\equiv \Sigma\,(\lambda_3^2-\lambda_3^2)\,\alpha' \equiv 0,$$

$$\Delta\,(\gamma_{3x-2}-\gamma'\gamma_{2x-2}-\beta'\gamma_{x-2}) \equiv -\Sigma\,(\lambda_2-\lambda_3)(\lambda_1^{3x}-\gamma'\lambda_1^{2x}-\beta'\lambda_1^x)$$

$$\equiv -\Sigma\,(\lambda_2-\lambda_3)\,\alpha' \equiv 0.$$

The effect of making $Q_0 = Q^x$ is therefore to reproduce the original relations, but with $\lambda_1^x$, $\lambda_2^x$, $\lambda_3^x$ in place of $\lambda_1$, $\lambda_2$, $\lambda_3$. Thus the one type exists:

$$A^p = B^p = C^p = Q^q = 1,\quad AB = BA,\quad AC = CA,\quad BC = CB,$$

$$Q^{-1}AQ = B,\quad Q^{-1}BQ = C,\quad Q^{-1}CQ = AB^\beta C^\gamma,$$

where $\beta$ and $\gamma$ have the values above stated, and

$$p^2+p+1 \equiv 0 \pmod{q}.$$

23. V. $A^4 = 1$, $B^2 = A^2$, $B^{-1}AB = A^{-1}$.

Since $q = 3$, there must be four sub-groups of order $q$.

Since $\{A^2\}$ is a characteristic sub-group of $H$ (§ 4, V.), $A^2$ is permutable with $Q$.

$H$ contains three sub-groups of order 4, $\{A\}$, $\{B\}$, and $\{AB\}$. $Q$ is either permutable with each, or else transforms them cyclically.

The former case is impossible, for, if

$$Q^{-1}AQ = A^a,$$

then $$a = 1,$$

and so $A$ and $Q$ would be permutable.

Secondly, $$Q^{-1}AQ = A^kB,$$
which may be taken as $B$ (§ 4, V.). Then
$$Q^{-1}AQ = B;$$
this gives $$Q^{-1}A^2Q = B^2 = A^2,$$
which is right. Also $Q^{-1}BQ = AB$ or $A^{-1}B$.
Either of these is consistent, for each makes
$$Q^{-2}BQ^2 = A,$$
which is true, since $$Q^3 = 1.$$

There is, however, but one type; for, taking the first,
$$Q^{-1}AQ = B, \quad Q^{-1}BQ = AB,$$
let $$Q_0 = Q^2, \quad B_0 = AB, \quad A_0 = A \quad (§ 4, \text{V.});$$
then $Q_0^3 = 1$, $Q_0^{-1}A_0Q_0 = AB = B_0$, and $Q_0^{-1}B_0Q_0 = B = A_0^{-1}B_0$.
This type is
$$A^4 = B^4 = Q^3 = 1, \; B^2 = A^2, \; B^{-1}AB = A^{-1}, \; Q^{-1}AQ = B, \; Q^{-1}BQ = AB.$$

24. VI. $A^{p^2} = B^p = 1$, $B^{-1}AB = A^{p+1}$.—$p$ is odd, and
$$p \equiv 1 \pmod{q}.$$

(i.) *p Sub-groups of Order q.*—The group of order $p^2$ with whose operations $\{Q\}$, and therefore $Q$ (§ 15), is permutable, is either $\{AB^k\}$ or $\{A^p, B\}$.

First, suppose that $Q$ is permutable with $AB^k$. Then we can put
$$A_0 = AB^k, \quad B_0 = B \; (§ 4, \text{VI.}),$$
and so, dropping suffixes, $AQ = QA$.
Then $\{A^p\}$ is a group of order $p$ permutable with $Q$; there remain $p$ others; since
$$p \equiv 1 \pmod{q},$$
at least one of these latter is also permutable with $Q$, say $\{A^{cp}B\}$. Then we can substitnte $B$ for $A^{cp}B$, and thus obtain
$$Q^{-1}BQ = B^a,$$
where $a$ is a primitive root of $a^q \equiv 1 \pmod{p}$.

These relations, however, are not consistent; for
$$B^{-1}AQ = A^{p+1}B^{-1}Q = A^{p+1}QB^{-a},$$

and $$B^{-1}QA = QB^{-a}A = QA^{ap+1}B^{-a} = A^{ap+1}QB^{-a},$$

and so $$a \equiv 1 \pmod{p},$$

which is contrary to hypothesis.

Secondly, let the group of order $p^2$ whose operations are permutable with $\{Q\}$ be $\{A^p, B\}$. Then (§ 15)

$$A^pQ = QA^p, \quad BQ = QB.$$

Of the $p$ cyclic groups of order $p^2$ at least one is permutable with $Q$, since $$p \equiv 1 \pmod{q}.$$

It may be taken to be $\{A\}$, without interfering with the result

$$A^pQ = QA^p,$$

above obtained, for $$(AB^k)^p = A^p \quad (\S\, 4, \text{VI.}).$$

Then $$Q^{-1}AQ = A^a,$$

where $a$ is a primitive root of $a^q \equiv 1 \pmod{p^2}$.

But $$Q^{-1}A^pQ = A^{ap},$$

and so $$a \equiv 1 \pmod{p},$$

which is inconsistent with $a$ being a primitive root of

$$a^q \equiv 1 \pmod{p^2}.$$

(ii.) $p^2$ *Sub-groups of Order* $q$.—Here $Q$ is permutable with the operations of some group of order $p$. This cannot be $\{A^p\}$, for the same reason that $Q$ in the last case could not be permutable with the operations of $\{A^p, B\}$.

This group of order $p$ may therefore be taken to be $\{B\}$. So

$$BQ = QB.$$

One of the $p$ cyclic groups of order $p^2$ is permutable with $Q$; we may take it to be $\{A\}$. Then

$$Q^{-1}AQ = A^a,$$

and $a$ is a primitive root of $a^q \equiv 1 \pmod{p^2}$.

By taking $Q_0 = Q^x$ in place of $Q$, we get any other root of this congruence in place of $a$; hence the single type

$$A^{p^2} = B^p = Q^q = 1, \quad B^{-1}AB = A^{p+1}, \quad BQ = QB, \quad Q^{-1}AQ = A^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p^2}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

(iii.) $p^3$ *Sub-groups of Order* $q$.—Of the $p$ cyclic groups of order $p^2$, one, say $\{A\}$, is permutable with $Q$. Then

$$Q^{-1}AQ = A^a.$$

Besides $\{A^p\}$, at least one other group of order $p$, say $\{B\}$, is permutable with $Q$. Then

$$Q^{-1}BQ = B^b.$$

These relations, however, are mutually inconsistent, unless $b = 1$; for

$$B^{-1}AB = A^{p+1},$$

and so $$Q^{-1}B^{-1}ABQ = Q^{-1}A^{p+1}Q = A^{a(p+1)}.$$

But $$BQ = QB^b, \quad Q^{-1}B^{-1} = B^{-b}Q^{-1};$$

therefore $$A^{a(p+1)} = B^{-b}Q^{-1}AQB^b = B^{-b}A^aB^b = A^{a(bp+1)},$$

and so $$b \equiv 1 \pmod{p}.$$

This makes $$BQ = QB,$$

which is contrary to hypothesis.

25. VII. $A^p = B^p = C^p = 1$, $AB = BA$, $AC = CA$, $C^{-1}BC = AB$ $(p > 2)$.

$Q$ is permutable with $\{A\}$, the characteristic sub-group of this group.

(i.) $p$ *Sub-groups of Order* $q$; then

$$p \equiv 1 \pmod{q}.$$

—The operations of some group of order $p^2$ are permutable with $Q$ (§ 15); it may be assumed to be $\{A, B\}$. Then

$$AQ = QA, \quad BQ = QB,$$

and $Q$ is thus permutable with $p+1$ groups of order $p$, viz., $\{B\}$ and $\{AB^k\}$ $(k = 0, 1, \ldots, p-1)$; there remain $p^2$ other such groups; now

$$p^2 \equiv 1 \pmod{q},$$

so at least one of the latter is permutable with $Q$. Suppose it is $\{A^kB^mC\}$; then we can put

$$A_0 = A, \quad B_0 = B, \quad C_0 = A^kB^mC,$$

and, dropping suffixes,

$$AQ = QA, \quad BQ = QB, \quad \text{and} \quad Q^{-1}CQ = C^a,$$

where $a$ is a primitive root of $a^q \equiv 1 \pmod{p}$.

These relations are, however, inconsistent with

$$C^{-1}BC = AB.$$

For, since $$BQ = QB,$$
$C^{-1}BC$ is permutable with $C^{-1}QC$. Now

$$C^{-1}QC = QC^{-a+1};$$

therefore $ABQC^{-a+1} = QC^{-a+1}AB = AQA^{a-1}BC^{-a+1} = A^aBQC^{-a+1}$;

therefore $$a \equiv 1 \pmod{p},$$
which makes $Q$ permutable with $C$, contrary to hypothesis.

26. (ii.) *$p^3$ Sub-groups of Order $q$*; and

$$p \equiv 1 \pmod{q}.$$

—The operations of some one group of order $p$ are permutable with $Q$ (§ 15).

This case falls into two principal sections according as (1) this group is $\{A\}$, or (2) some other sub-group of $H$, say $\{B\}$.

(1) $AQ = QA$.

Besides $\{A\}$, there are $p^2+p$ other groups of order $p$ in $H$; now

$$p^2+p \equiv 2 \pmod{q}.$$

Except therefore in the case $q = 2$, in which it may be that no other group of order $p$ is permutable with $Q$ (which supposition will be considered later), there are at least two such besides $\{A\}$ permutable with $Q$, and, of course, this may be the case when $q = 2$. Taking, as we may, $\{B\}$ to be one of these, the other cannot be $\{A^kB\}$, for

$$Q^{-} A^kBQ = A^kB^a,$$

where $$a \neq 1;$$
and $A^kB^a$ is not a power of $\{A^kB\}$.

The third group of order $p$ permutable with $Q$ may therefore be taken as $\{C\}$. Thus we get

$$Q^{-1}BQ = B^a, \quad Q^{-1}CQ = C^b,$$

where $a$ and $b$ are primitive roots of

$$a^q \equiv 1 \pmod{p};$$

$a$ and $b$, however, are not independent, for

$$C^{-1}BC = AB.$$

Transforming this relation with $Q$, we obtain

$$Q^{-1}C^{-1}BCQ = Q^{-1}ABQ = AB^{a}.$$

Now $$CQ = QC^{b}, \quad Q^{-1}C^{-1} = C^{-b}Q^{-1};$$

and therefore

$$AB^{a} = Q^{-1}C^{-1}BCQ = C^{-b}Q^{-1}BQC^{b} = C^{-b}B^{a}C^{b} = A^{ab}B^{a} \quad (\S\, 4, \text{VII.}).$$

To render the relations consistent it is necessary that

$$ab \equiv 1 \pmod{p},$$

that is, $$b \equiv a^{q-1} \pmod{p}.$$

It will appear on examination that the other relations may be transformed and combined in every possible manner without any inconsistency emerging, provided that the condition

$$b \equiv a^{q-1} \pmod{p}$$

is satisfied.

The relations furnish one type only, for the transformation $Q_0 = Q^x$ changes $a$ into $a^x$:

$$A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA, \quad AQ = QA,$$

$$C^{-1}BC = AB, \quad Q^{-1}BQ = B^{a}, \quad Q^{-1}CQ = C^{a^{q-1}},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

When $q = 2$, there remains the supposed case of the $p^2+p$ groups of order $p$ being all non-permutable with $Q$. Either

$$QBQ = A^xB^y,$$

or it may be taken to be $C$.

First, $$QBQ = A^xB^y;$$

then, since $Q^2 = 1$, $$B = A^{x+xy}B^{y^2},$$

so $$y \equiv -1 \pmod{p}.$$

and then $$Q(A^{-x}B^2)Q = A^{-x}A^{2x}B^{-2} = (A^{-x}B^2)^{-1},$$

which is contrary to hypothesis.

Secondly, $$QBQ = C;$$

then $$QCQ = B,$$

and so $$QBC^{-1}Q = CB^{-1} = (BC^{-1})^{-1},$$

again contrary to hypothesis.

(2) Having disposed of the case $AQ = QA$, we must now consider the second case, $BQ = QB$.

As before, there are at least two other groups of order $p$ besides $\{B\}$ permutable with $Q$; the only conceivable exception being when $q = 2$; this, however, may easily be proved impossible, as in the previous case. And one of these we know is $\{A\}$. Then

$$Q^{-1}AQ = A^a, \quad QB = BQ.$$

The other group of order $p$ permutable with $Q$ may without loss of generality be taken to be $\{C\}$, and so

$$Q^{-1}CQ = C^b;$$

here $$a^q \equiv b^q \equiv 1 \pmod{p}.$$

Now, since $C^{-1}BC = AB$, $Q^{-1}C^{-1}BCQ = Q^{-1}ABQ = A^aB$.

Now $$CQ = QC^b,$$

and so $$A^aB = C^{-b}Q^{-1}BQC^b = C^{-b}BC^b = A^bB;$$

and therefore $$b \equiv a \pmod{p}.$$

The other relations give rise to no fresh conditions and no inconsistencies. We therefore get the one type

$$A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA, \quad C^{-1}BC = AB,$$
$$Q^{-1}AQ = A^a, \quad QB = BQ, \quad Q^{-1}CQ = C^a,$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}, \quad \text{and} \quad p \equiv 1 \pmod{q}.$$

27. (iii.) $p^3$ *Sub-groups of Order* $q$; and

$$p \equiv -1 \pmod{q};$$

here $q > 2$.—Since $Q$ is permutable with $\{A\}$, and the congruence

$$a^q \equiv 1 \pmod{p}$$

has no real primitive roots, $Q$ must be permutable with $A$. For the same reason, no other group of order $p$ besides $\{A\}$ can be permutable with $Q$. Then

$$Q^{-1}BQ = A^\alpha B^\beta, \text{ or else } A^\alpha B^\beta C^\gamma.$$

If $$Q^{-1}BQ = A^\alpha B^\beta,$$

then $$Q^{-q}BQ^q = A^{\alpha(1+\beta+\ldots+\beta^{q-1})}B^{\beta^q},$$

so $$\beta^q \equiv 1 \pmod{p},$$

that is $$\beta = 1;$$

and so $$B = A^{aq}B,$$

which is impossible. Therefore

$$Q^{-1}BQ = A^{a}B^{\beta}C^{\gamma}.$$

Let $$A_0 = A^{\gamma}, \quad B_0 = B, \quad C_0 = A^{a}B^{\beta}C^{\gamma} \quad (\S\, 4, \text{VII.}).$$

Then $$A_0Q = QA_0, \quad Q^{-1}B_0Q = C_0.$$

Dropping suffixes, we get

$$AQ = QA, \quad Q^{-1}BQ = C, \quad Q^{-1}CQ = A^{a}B^{\beta}C^{\gamma}.$$

Let $$Q^{-x}CQ^{x} = A^{a_x}B^{\beta_x}C^{\gamma_x}.$$

Then

$$\begin{aligned} A^{a_x}B^{\beta_x}C^{\gamma_x} &= Q^{-1}A^{a_{x-1}}B^{\beta_{x-1}}C^{\gamma_{x-1}}Q \\ &= A^{a_{x-1}}C^{\beta_{x-1}}\left(A^{a}B^{\beta}C^{\gamma}\right)^{\gamma_{x-1}} \\ &= A^{a_{x-1}+a\gamma_{x-1}-\frac{1}{2}\beta\gamma\gamma_{x-1}(\gamma_{x-1}-1)-\beta\beta_{x-1}\gamma_{x-1}}B^{\beta\gamma_{x-1}}C^{\beta_{x-1}+\gamma\gamma_{x-1}}; \end{aligned}$$

and therefore

$$\left.\begin{aligned} a_x - a_{x-1} &\equiv a\gamma_{x-1} - \beta\gamma\frac{\gamma_{x-1}(\gamma_{x-1}-1)}{2} - \beta\beta_{x-1}\gamma_{x-1} \\ \beta_x &\equiv \beta\gamma_{x-1} \\ \gamma_x &\equiv \gamma\gamma_{x-1} + \beta_{x-1} \end{aligned}\right\} \pmod{p}.$$

Then $$\gamma_x - \gamma\gamma_{x-1} - \beta\gamma_{x-2} \equiv 0.$$

If the roots of the congruence

$$\lambda^2 - \gamma\lambda - \beta \equiv 0 \pmod{p}$$

are equal, each being $\lambda$, then

$$\gamma \equiv 2\lambda, \quad \beta \equiv -\lambda^2,$$

and so $$\gamma_x \equiv (1+x)\lambda^x.$$

But $$\gamma_{q-1} \equiv 0,$$

and so $$q\lambda^{q-1} \equiv 0 \pmod{p},$$

which is impossible. Therefore the roots must be unequal, $\lambda_1$ and $\lambda_2$ say, and then

$$\gamma_x \equiv \frac{\lambda_1^{x+1} - \lambda_2^{x+1}}{\lambda_1 - \lambda_2}, \quad \beta_x \equiv \beta\frac{\lambda_1^{x} - \lambda_2^{x}}{\lambda_1 - \lambda} \pmod{p}.$$

Now $$\gamma_{q-1} \equiv 0, \quad \gamma_q \equiv 1;$$

therefore $$\lambda_1^q \equiv \lambda_2^q \equiv 1 \pmod{p}.$$

Also $$\lambda_2 \equiv \lambda_1^p;$$

therefore $$\lambda_1 \lambda_2 \equiv \lambda_1^{p+1} \equiv (\lambda^q)^{(p+1)/q} \equiv 1;$$

and so $$\beta \equiv -1.$$

Then $$2(\lambda_1-\lambda_2)^2(a_x-a_{x-1})$$

$$\equiv (2a-\gamma)(\lambda_1^2-1)\lambda_1^{x-1}+(2a-\gamma)(\lambda_2^2-1)\lambda_2^{x-1}+\lambda_1^{2x+1}-\lambda_1^{2x-1}+\lambda_2^{2x+1}-\lambda^{2x-1},$$

and so

$$2(\lambda_1-\lambda_2)^2 a_{x-1} \equiv (2a-\gamma)(\lambda_1^x+\lambda_2^x+\lambda_1^{x-1}+\lambda_2^{x-1}-\gamma-2)+\lambda_1^{2x-1}+\lambda_2^{2x-1}-\gamma.$$

These values of $a_x$, $\beta_x$, and $\gamma_x$ satisfy the conditions

$$a_{q-1} \equiv a_q \equiv 0, \quad \beta_{q-1} \equiv 1, \quad \beta_q \equiv 0, \quad \gamma_{q-1} \equiv 0, \quad \gamma_q \equiv 1.$$

Thus we obtain the relations

$$AQ = QA, \quad Q^{-1}BQ = C, \quad Q^{-1}CQ = A^a B^{-1} C^\gamma,$$

where $$\gamma \equiv \lambda+\lambda^p,$$

and $\lambda$ is any primitive root of $\lambda^q \equiv 1 \pmod{p}$.

These are self-consistent, and the only question remaining is, How many types are included therein?

Let $$A_0 = A^m, \quad B_0 = A^l B^m C^n, \quad C_0 = A^r C$$

(which express an isomorphism of $H$, § 4, VII.), and

$$Q_0 = Q^k.$$

Then $$Q_0^{-1} B_0 Q_0$$

$$= Q^{-k} A^l B^m C^n Q^k = A \ (A^{a_{k-1}} B^{-\gamma_{k-2}} C^{\gamma_{k-1}})^m (A^{a_k} B^{-\gamma_{k-1}} C^{\gamma_k})^n$$

$$\doteq A^{l+ma_{k-1}+na_k+\frac{1}{2}m(m-1)\gamma_{k-2}\gamma_{k-1}+\frac{1}{2}n(n-1)\gamma_{k-1}\gamma_k+mn\gamma_{k-1}^2}$$

$$\times B^{-m\gamma_{k-2}-n\gamma_{k-1}} C^{m\gamma_{k-1}+n\gamma_k},$$

and this is to be $$C_0 = A^r C.$$

Then $$r \equiv l+f(m, n), \tag{1}$$

the right side being the index of $A$ in $Q_0^{-1} B_0 Q_0$. Also

$$m\gamma_{k-2}+n\gamma_{k-1} \equiv 0, \quad m\gamma_{k-1}+n\gamma_k \equiv 1.$$

These last give $$m \equiv \gamma_{k-1}, \quad n \equiv -\gamma_{k-2},$$

since we have $$\gamma_{k-1}^2-\gamma_k\gamma_{k-2}\equiv 1,$$
identically. Also $$Q_0^{-1}C_0Q_0 = Q^{-k}A^rCQ^k$$
$$= A^{r+a_k}B^{-\gamma_{k-1}}C^{\gamma_k},$$

and this is equal to $B_0^{-1}C_0^{\delta}$, which is the same as
$$C^{-n}B^{-m}A^{-l+r\delta}C^{\delta} = A^{-l+r\delta-mn}B^{-m}C^{-n+\delta},$$
provided that $$\delta\equiv\gamma_k-\gamma_{k-2}, \qquad (2)$$
and $$-l+r\delta-mn\equiv r+a_k. \qquad (3)$$

Congruences (1) and (3) can always be satisfied by proper values for $l$ and $r$. Also
$$\delta\equiv\gamma_k-\gamma_{k-2}\equiv\lambda_1^k+\lambda_2^k,$$
and this shows that the same type is obtained whatever value of $\lambda$ is taken among the primitive roots of
$$\lambda^q\equiv 1 \pmod p.$$

Thus there is only one type of group of this kind whose generating relations may be taken to be
$$A^p = B^p = C^p = Q^q = 1,\quad AB = BA,\quad AC = CA,\quad C^{-1}BC = AB,$$
$$AQ = QA,\quad Q^{-1}BQ = C,\quad Q^{-1}CQ = B^{-1}C^{\gamma},$$
where $$\gamma\equiv\lambda+\lambda^p,$$
and $\lambda$ is any primitive root of $\lambda^q\equiv 1 \pmod p$.

28. (iv.) $p^3$ *Sub-groups of Order* $q$; then
$$p\equiv 1 \pmod q.$$

—If $q>2$, at least two of the $p^2+p$ sub-groups of order $p$, besides $\{A\}$, are permutable with $Q$, and this may also be the case when $q=2$. The possible exceptions to this when $q=2$ will be treated later.

We have $$Q^{-1}AQ = A^a;$$
let $\{B\}$ be another group of order $p$ permutable with $Q$; then
$$Q^{-1}BQ = B^b.$$

If $a$ is not equal to $b$, $Q$ cannot be permutable with $\{A^xB\}$, and so the third group of order $p$ may be taken to be $\{C\}$. And if $a=b$, then we have $p+1$ such groups, viz., $\{A\}$, $\{A^xB\}$ permutable with $Q$;

there remain $p^3$, one at least of which is also permutable with $Q$; here again it may be taken to be $\{C\}$. So

$$Q^{-1}AQ = A^a, \quad Q^{-1}BQ = B^{a^x}, \quad Q^{-1}CQ = C^{a^y},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p}.$$

Evidently the alteration of $a$ to $a^\lambda$, $x$ and $y$ remaining constant, does not make a fresh type. Since

$$C^{-1}BC = AB,$$

$$Q^{-1}C^{-1}BCQ = Q^{-1}ABQ = A^aB^{a^x}.$$

But $$CQ = QC^{a^y}.$$

So $$A^aB^{a^x} = C^{-a^y}Q^{-1}BQC^{a^y} = C^{-a^y}B^{a^x}C^{a^y} = A^{a^{x+y}}B^{a^x}.$$

Therefore $$a^{x+y} \equiv a \pmod{p},$$

that is, $$x+y \equiv 1 \pmod{q}.$$

If this condition is satisfied, all the relations are consistent.

It remains to find how many types are included in these relations for different values of $x$ and $y$.

For this purpose, let $B_0 = A^\lambda B^\mu C^\nu$;

we must take for $Q_0$ the most general form of operation of order $q$. Since $G$ contains $p^3$ sub-groups of order $q$, every operation of the form $A^fB^gC^hQ^k$ is of order $q$. Since $a$ may be considered fixed, we may put $k = 1$, and, since $A$ is permutable with $B$ and $C$, we can omit the $A^f$; thus we have

$$Q_0 = B^gC^hQ.$$

Then, writing $$b \equiv a^x, \quad c \equiv a^y,$$

we obtain $$Q_0^{-1}B_0Q_0 = A^{a\lambda + ah\mu - ag\nu}B^{b\mu}C^{c\nu}.$$

Also $$B_0^{b_0} = A^{\lambda b_0 - \frac{1}{2}\mu\nu b_0(b_0-1)}B^{b_0\mu}C^{b_0\nu}.$$

Since $\mu$ and $\nu$ are not both $\equiv 0$, $b_0 \equiv b$ or $c \pmod{p}$.

So the only change that can be made to $b$ and $c$ is to interchange them; thus $x$, $y$ and $y$, $x$ give the same type. The number of types is therefore the number of solutions (order being disregarded), of the congruence

$$x+y \equiv 1 \pmod{q}.$$

Neither $x$ nor $y$ can be 0 or 1, for this would make $Q$ permutable with $B$ or $C$. When $q = 2$, this congruence has no solutions of the proper kind; when $q > 2$, there is one solution

$$x \equiv y \equiv \frac{q+1}{2}$$

for which $x \equiv y$,

and $\frac{q-3}{2}$ solutions for which $x \not\equiv y$.

Thus we obtain altogether $\frac{q-1}{2}$ types:

$$A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA, \quad C^{-1}BC = AB,$$

$$Q^{-1}AQ = A^a, \quad Q^{-1}BQ = B^{a^x}, \quad Q^{-1}CQ = C^{a^{q+1-x}},$$

where $a$ is any primitive root of

$$a^q \equiv 1 \pmod{p},$$

$q$ is greater than 2, $\quad p \equiv 1 \pmod{q}$,

and $x$ takes any of the values $2, 3, \ldots, \frac{q+1}{2}$.

*The case* $q = 2$.—Here either one only or at least three groups of order $p$ are permutable with $Q$; the case of three permutable with $Q$ has been already discussed, and shown to be impossible for $q = 2$.

Suppose now that only one group of order $p$ is permutable with $Q$; it must be $\{A\}$, and so

$$QAQ = A^{-1};$$

and then $QBQ$ cannot belong to $\{A, B\}$ (as in § 26), and so may be taken to be $C$; then

$$QBQ = C, \quad QCQ = B,$$

and so $\quad QA^{\frac{1}{2}(p-1)}BCQ = A^{\frac{1}{2}(p-1)}BC,$

which is contrary to hypothesis.

29. We now reach the fourth and last of the principal divisions of the subject (see § 5)—the groups of order $p^3q$ which do not contain self-conjugate sub-groups of orders $p^3$ or $q$.

Since there must now be $q$ groups of order $p^3$,

$$q \equiv 1 \pmod{p},$$

and therefore $\quad p < q$.

There cannot therefore be $p$ groups of order $q$, for this requires that

$$p \equiv 1 \pmod{q}.$$

Nor can there be $p^3$ groups of order $q$, for then $p^3(q-1)$ operations of the group are of order $q$, leaving only $p^3$ other operations; in this case there can only be one group of order $p^3$. If there are any groups of the kind now sought for, they must therefore contain $p^2$ groups of order $q$, with the condition

$$p+1 \equiv 0 \pmod{q}.$$

The only values of $p$ and $q$ satisfying this and the previous condition

$$q \equiv 1 \pmod{p}$$

are

$$p = 2, \quad q = 3.$$

Accordingly, if there are any such groups, they are of order 24. In Burnside's *Theory of Groups* (pp. 101–104), the groups of this order are discussed, and it is unnecessary for me to reproduce this discussion here; it will suffice to give the generating relations of the sole group which has no self-conjugate sub-groups of order 8 or 3,

$$A^4 = B^2 = Q^3 = 1, \quad BAB = A^{-1}, \quad Q^{-1}A^2Q = B, \quad Q^{-1}BQ = A^2B,$$
$$A^{-1}QA = Q^2A^2B.$$

*Summary.*

30. It will be best to keep distinct the cases $p =$ and $>2$.

First, *Groups of Order* $8q$.

Number of Types.

(1) $A^8 = Q^q = 1,\ AQ = QA$ ...................................... 1

This is the cyclic group of order $8q$.

(2) $A^4 = B^2 = Q^q = 1,\ AB = BA,\ AQ = QA,\ BQ = QB$... 1

(3) $A^2 = B^2 = C^2 = C^q = 1,\quad AB = BA,\quad AC = CA,$
$BC = CB,\ AQ = QA,\ BQ = QB,\ CQ = QC$ ........ 1

These first three groups are Abelian.

(4) $A^4 = B^2 = Q^q = 1,\ BAB = A^{-1},\ AQ = QA,\ BQ = QB.$ 1

(5) $A^4 = B^4 = Q^q = 1,\ B^2 = A^2,\ B^{-1}AB = A^{-1},\ AQ = QA,$
$BQ = QB$ ................................................ 1

(6) $A^8 = Q^q = 1,\ A^{-1}QA = Q^{-1}$ ................................ 1

(7) $A^4 = B^2 = Q^q = 1,\ AB = BA,\ AQ = QA,\ BQB = Q^{-1}.$ 1

Number of Types.

(8) $A^4 = B^2 = Q^q = 1,\ AB = BA,\ A^{-1}QA = Q^{-1},\ BQ = QB.$ 1

(9) $A^2 = B^2 = C^2 = Q^q = 1,\quad AB = BA,\quad AC = CA,$
$BC = CB,\ AQ = QA,\ BQ = QB,\ CQC = Q^{-1}$...... 1

(10) $A^4 = B^2 = Q^q = 1,\ BAB = A^{-1},\ AQ = QA,\ BQB = Q^{-1}.$ 1

(11) $A^4 = B^2 = Q^q = 1,\quad BAB = A^{-1},\quad A^{-1}QA = Q^{-1},$
$BQ = QB$ ............................................ 1

(12) $A^4 = B^4 = Q^q = 1,\ B^2 = A^2,\ B^{-1}AB = A^{-1},\ AQ = QA,$
$B^{-1}QB = Q^{-1}$ ............................................ 1

The above twelve groups exist for all values of $q$ ($q$ being supposed a prime number greater than 2).

In addition, when $q \equiv 1 \pmod 4$, there are :—

(13) $A^8 = Q^q = 1,\ A^{-1}QA = Q^a$, where $a$ is any primitive root of $a^4 \equiv 1 \pmod q$ .................................... 1

(14) $A^4 = B^2 = Q^q = 1,\ AB = BA,\ A^{-1}QA = Q^a,\ BQ = QB$, where $a$ has the same meaning as in the previous group ............................................ 1

Thus, if $q \equiv 1 \pmod 4$, there are fourteen types.

Lastly, if $q \equiv 1 \pmod 8$, in addition to these, there is :—

(15) $A^8 = Q^q = 1,\ A^{-1}QA = Q^a$, where $a$ is any primitive root of $a^8 \equiv 1 \pmod q$ .................................... 1

There are, therefore, twelve, fourteen, or fifteen groups of order $8q$ containing a self-conjugate sub-group of order $q$, according as $q-1$ is a multiple of 2 only, 4 only, or 8.

In addition, for certain values of $q$, there are groups not containing a self-conjugate sub-group of order $q$ (i.) when $q = 3$ :—

(16) The Galoisian $\iota$ in this case satisfies $\iota^3 \equiv 1 \pmod 2$. Therefore $\iota^2 + \iota + 1 \equiv 0 \pmod 2$ ; and so
$A^2 = B^2 = C^2 = Q^3 = 1,\quad AB = BA,\quad AC = CA,$
$BC = CB,\ AQ = QA,\ Q^{-1}BQ = C,\ Q^{-1}CQ = BC$... 1

(17) $A^4 = B^4 = Q^3 = 1,\ B^2 = A^2,\ B^{-1}AB = A^{-1},\ Q^{-1}AQ = B,$
$Q^{-1}BQ = AB$ ............................................ 1

Number
of Types.

(18) $A^4 = B^2 = Q^3 = 1, \quad BAB = A^{-1}, \quad Q^{-1}A^2Q = B,$
$Q^{-1}BQ = A^2B, \quad A^{-1}QA = Q^2A^2B$ ........................ 1

And (ii.) when $q = 7$ :—

(19) The values of $\beta$ and $\gamma$ are

$$\beta \equiv -\lambda^3-\lambda^5-\lambda^6, \quad \gamma \equiv \lambda+\lambda^2+\lambda^4,$$

where $\lambda^7 \equiv 1 \pmod 2$. So $\gamma+\beta \equiv 1 \pmod 2$, and we can take $\beta = 1$, $\gamma = 0$; the type is
$A^2 = B^2 = C^2 = Q^7 = 1, \quad AB = BA, \quad AC = CA,$
$BC = CB, \; Q^{-1}AQ = B, \; Q^{-1}BQ = C, \; Q^{-1}CQ = AB$... 1

There are, therefore, altogether fifteen groups of order 24, being the twelve types which exist for all values of $q$ and the three special types just mentioned. And there are thirteen groups of order 56.

My results for the order 24 are confirmed by Burnside's list (pp. 101–104), in which are given the generating relations of the fifteen groups. And the results just given as to groups of order $8q$ are confirmed, so far as the number of types is concerned, by Dr. Miller, in his paper, "The Operation Groups of Order $8p$, $p$ being any Prime Number," *Philosophical Magazine*, Vol. XLII., pp. 195–200.

31. *Groups of Order $p^3q$, where $p$ is odd.*

First, those containing self-conjugate sub-groups of orders $p^3$ and $q$.

Number
of Types.

(1) $A^{p^3} = 1, \; Q^q = 1, \; AQ = QA$ ................................ 1

(2) $A^{p^2} = B^p = Q^q = 1, \; AB = BA, \; AQ = QA, \; BQ = QB$ ... 1

(3) $A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA,$
$BC = CB, \; AQ = QA, \; BQ = QB, \; CQ = QC$ ......... 1

(4) $A^{p^2} = B^p = Q^q = 1, \quad B^{-1}AB = A^{p+1}, \quad AQ = QA,$
$BQ = QB$ ................................................ 1

(5) $A^p = B^p = C^p = Q^q = 1, \quad AB = BA, \quad AC = CA,$
$C^{-1}BC = AB, \; AQ = QA, \; BQ = QB, \; CQ = QC$ ... 1

Secondly, those containing a self-conjugate sub-group of order $q$, but not one of order $p^3$.

Number of Types.

If $q \equiv 1 \pmod{p}$, there are the following:—

(6) $A^{p^3} = Q^q = 1$, $A^{-1}QA = Q^a$, where $a$ (here and in the next five groups) is any primitive root of $a^p \equiv 1 \pmod{q}$ .......... 1

(7) $A^{p^2} = B^p = Q^q = 1$, $AB = BA$, $AQ = QA$, $B^{-1}QB = Q^a$ .......... 1

(8) $A^{p^2} = B^p = Q^q = 1$, $AB = BA$, $A^{-1}QA = Q^a$, $BQ = QB$ .......... 1

(9) $A^p = B^p = C^p = Q^q = 1$, $AB = BA$, $AC = CA$, $BC = CB$, $AQ = QA$, $BQ = QB$, $C^{-1}QC = Q^a$ ... 1

(10) $A^{p^2} = B^p = Q^q = 1$, $B^{-1}AB = A^{p+1}$, $AQ = QA$, $B^{-1}QB = Q^b$, where $b = a$, or $a^2$, ..., or $a^{p-1}$ .......... $p-1$

(11) $A^p = B^p = C^p = Q^q = 1$, $AB = BA$, $AC = CA$, $AQ = QA$, $BQ = QB$, $C^{-1}BC = AB$, $C^{-1}QC = Q^a$ .......... 1

And if $q \equiv 1 \pmod{p^2}$, there are, in addition to the above:—

(12) $A^{p^3} = Q^q = 1$, $A^{-1}QA = Q^a$, where $a$ (here and in the next group) is any primitive root of $a^{p^2} \equiv 1 \pmod{q}$ .......... 1

(13) $A^{p^2} = B^p = Q^q = 1$, $AB = BA$, $A^{-1}QA = Q^a$, $BQ = QB$ .......... 1

And if $q \equiv 1 \pmod{p^3}$, there is, in addition:—

(14) $A^{p^3} = Q^q = 1$, $A^{-1}QA = Q^a$, where $a$ is any primitive root of $a^{p^3} \equiv 1 \pmod{q}$ .......... 1

Therefore the number of groups of order $p^3q$ containing a self-conjugate sub-group of order $q$ is 5 when $q \not\equiv 1 \pmod{p}$, $p+9$ when $q \equiv 1 \pmod{p}$, $p+11$ when $q \equiv 1 \pmod{p^2}$, and $p+12$ when $q \equiv 1 \pmod{p^3}$.

Thirdly, those containing a self-conjugate sub-group of order $p^3$, but not one of order $q$.

When $p \equiv 1 \pmod{q}$, there are the following types:—

[$a$ denotes a primitive root of $a^q \equiv 1 \pmod{p}$, $a_2$ of $a^q \equiv 1 \pmod{p^2}$, and $a_3$ of $a^q \equiv 1 \pmod{p^3}$.]

Number of Types.

(15) $A^{p^3} = Q^q = 1,\ Q^{-1}AQ = A^{\alpha_3}$ ........................ 1

(16) $A^{p^2} = B^p = Q^q = 1,\quad AB = BA,\quad AQ = QA,$
$Q^{-1}BQ = B^{\alpha}$ ........................................ 1

(17) $A^{p^2} = B^p = Q^q = 1,\quad AB = BA,\quad Q^{-1}AQ = A^{\alpha_2},$
$BQ = QB$.............................................. 1

(18) $A^{p^2} = B^p = Q^q = 1,\quad AB = BA,\quad Q^{-1}AQ = A^{\alpha_2},$
$Q^{-1}BQ = B^{\alpha_2}$, or $B^{\alpha_2^2}$, ..., or $B^{\alpha_2^{q-1}}$ ................ $q-1$

(19) $A^p = B^p = C^p = Q^q = 1,\quad AB = BA,\quad AC = CA,$
$BC = CB,\ AQ = QA,\ BQ = QB,\ Q^{-1}CQ = C^{\alpha}$... 1

(20) $q = 2.\quad A^p = B^p = C^p = Q^2 = 1,\quad AB = BA,$
$AC = CA,\ BC = CB,\ AQ = QA,\ QBQ = B^{-1},$
$QCQ = C^{-1}$ ............................................ 1

$q > 2.\quad A^p = B^p = C^p = Q^q = 1,\quad AB = BA,$
$AC = CA,\ BC = CB,\ AQ = QA,\ Q^{-1}BQ = B^{\alpha},$
$Q^{-1}CQ = C^{\alpha^{\lambda}}$, where $\lambda$ represents one of
$\frac{q+1}{2}$ values (as shown in § 19)...................... $\frac{q+1}{2}$

(21) $q \equiv 0$ *or* $-1$ (*mod* 3). $A^p = B^p = C^p = Q^q = 1,$
$AB = BA,\ AC = CA,\ BC = CB,\ Q^{-1}AQ = A^{\alpha},$
$Q^{-1}BQ = B^{\alpha^x},\ Q^{-1}CQ = C^{\alpha^y}$, where $x$ and $y$
have the values shown in § 21 ...................... $\frac{q^2+q}{6}$

$q \equiv 1$ (*mod* 3).—The same relations as in the
last case ............................................ $\frac{q^2+q+4}{6}$

(22) $A^{p^2} = B^p = Q^q = 1,\quad B^{-1}AB = A^{p+1},\quad BQ = QB,$
$Q^{-1}AQ = A^{\alpha_2}$ ........................................ 1

(23) $A^p = B^p = C^p = Q^q = 1,\ AB = BA,\quad AC = CA,$
$AQ = QA,\quad C^{-1}BC = AB,\quad Q^{-1}BQ = B^{\alpha},$
$Q^{-1}CQ = C^{\alpha^{q-1}}$ ........................................ 1

(24) $A^p = B^p = C^p = Q^q = 1,\quad AB = BA,\quad AC = CA,$
$C^{-1}BC = AB,\quad Q^{-1}AQ = A^{\alpha},\quad QB = BQ,$
$Q^{-1}CQ = C^{\alpha}$ ........................................ 1

Number of Types.

(25) $q > 2$. $A^p = B^p = C^p = Q^q = 1$, $AB = BA$,
$AC = CA$, $C^{-1}BC = AB$, $Q^{-1}AQ = A^a$,
$Q^{-1}BQ = B^{a^x}$, $Q^{-1}CQ = C^{a^{q+1-x}}$, where $x = 2$,
or 3, ..., or $\frac{q+1}{2}$........................................ $\frac{q-1}{2}$

When $p \equiv -1 \pmod q$, and $q > 2$, there are :—

(26) $A^p = B^p = C^p = Q^q = 1$, $AB = BA$, $AC = CA$,
$BC = CB$, $AQ = QA$, $Q^{-1}BQ = C$,
$Q^{-1}CQ = B^{-1}C^{\iota^p+\iota}$, where $\iota$ is any primitive
Galoisian root of $\iota^q \equiv 1 \pmod p$.................... 1

(27) $A^p = B^p = C^p = Q^q = 1$, $AB = BA$, $AC = CA$,
$C^{-1}BC = AB$, $AQ = QA$, $Q^{-1}BQ = C$,
$Q^{-1}CQ = B^{-1}C^{\iota^p+\iota}$ ($\iota$ being the same as in the
previous type) ....................................... 1

And, lastly, when $p^2+p+1 \equiv 0 \pmod q$, and $q > 3$, there is the one type :—

(28) $A^p = B^p = C^p = Q^q = 1$, $AB = BA$, $AC = CA$,
$BC = CB$, $Q^{-1}AQ = B$, $Q^{-1}BQ = C$,
$Q^{-1}CQ = AB^{-\lambda^{-1}-\lambda^{-p}-\lambda^{-p^2}}C^{\lambda+\lambda^p+\lambda^{p^2}}$, where $\lambda$ is
a Galois imaginary of the third order, which is
a primitive root of $\lambda^q \equiv 1 \pmod p$ ................. 1

32. Some interesting facts as to the numbers of types of groups of order $p^3q$ can be derived from the foregoing summary.

The most noticeable fact is that (if certain conditions as to the relations between $p$ and $q$ are satisfied) the number of groups of order $p^3q$ increases indefinitely as $p$ or $q$ increases. This is not the case with groups of orders $p$, $p^2$, $pq$, $p^3$, or $p^4$; but it is the case with those of order $p^2q$ (see Burnside, *Theory of Groups*, p. 136), where, when

$$p \equiv 1 \pmod q,$$

the number of types is of the form $aq+b$, $a$ and $b$ being constants.

When
$$p \equiv 1 \pmod q,$$

the number of groups of order $p^3q$ having a self-conjugate sub-group of order $p^3$, but not one of order $q$,

(i.) if $q = 2$, is 10.

(ii.) If $q>2$, and $=3$, or $\equiv -1$ (mod 3), the number is $\frac{1}{6}(q^2+13q+36)$, that is $\frac{(q+4)(q+9)}{6}$.

(iii.) If $q>2$, and $\equiv 1$ (mod 3), the number is $\frac{1}{6}(q^2+13q+40)$, that is $\frac{(q+5)(q+8)}{6}$.

When $$p \equiv -1 \pmod{q}, \quad \text{and} \quad q>2,$$
the number of groups of this sort is 2; and when
$$p^2+p+1 \equiv 0 \pmod{q}, \quad \text{and} \quad q>3,$$
the number is 1.

Consequently the total number of groups of order $2p^3$ is 15. This enumeration is confirmed by Dr. Miller's paper in the *Quar. Jour. of Math.*, December, 1898 (see pp. 259-263). It is curious that there should be this same number 15 of groups of order $p^4$, when $p$ is odd (Burnside, *Theory of Groups*, p. 87), and also of order $8q$, where
$$q \equiv 1 \pmod{8}$$
(*ante*, § 30).

Also the total number of groups of order $3p^3$ (where $p$ is odd and $>3$) is 19, when
$$p \equiv 1 \pmod{3},$$
but 6 only when $$p \equiv -1 \pmod{3}.$$

The total number of groups of order $5p^3$ ($p \neq 2$ or 5) is 26, when
$$p \equiv 1 \pmod{5},$$
6 when $$p \equiv -1 \pmod{5},$$
and 5 when $$p \equiv \pm 2 \pmod{5}.$$

And the total number of groups of order $7p^3$ ($p \neq 2$ or 7) is 12, when
$$p = 3,$$
35 when $$p \equiv 1 \pmod{7},$$
6 when $$p \equiv 2,\ 4, \text{ or } 6 \pmod{7},$$
and 5 when ($p>3$)
$$p \equiv 3 \text{ or } 5 \pmod{7}.$$

Finally, I give a table showing the number of types of group for all orders of the form $p^3q$ less than 400.

| Order. | Factors of Order. | Number of Types. |
|---|---|---|
| 24 | $2^3 . 3$ | 15 |
| 40 | $2^3 . 5$ | 14 |
| 54 | $3^3 . 2$ | 15 |
| 56 | $2^3 . 7$ | 13 |
| 88 | $2^3 . 11$ | 12 |
| 104 | $2^3 . 13$ | 14 |
| 135 | $3^3 . 5$ | 5 |
| 136 | $2^3 . 17$ | 15 |
| 152 | $2^3 . 19$ | 12 |
| 184 | $2^3 . 23$ | 12 |
| 189 | $3^3 . 7$ | 12 |
| 232 | $2^3 . 29$ | 14 |
| 248 | $2^3 . 31$ | 12 |
| 250 | $5^3 . 2$ | 15 |
| 296 | $2^3 . 37$ | 14 |
| 297 | $3^3 . 11$ | 5 |
| 328 | $2^3 . 41$ | 15 |
| 344 | $2^3 . 43$ | 12 |
| 351 | $3^3 . 13$ | 13 |
| 375 | $5^3 . 3$ | 7 |
| 376 | $2^3 . 47$ | 12 |

## *On the Complete System of Multilinear Differential Covariants of a single Pfaffian Expression, and of a set of Pfaffian Expressions.* By J. Brill, M.A.

Received January 31st, 1899. Read February 9th, 1899. Received in revised form April 5th, 1899.

1. An account of the bilinear covariant of a Pfaffian expression is to be found in Forsyth's *Theory of Differential Equations*, Part I., ch. xi. This covariant involves the first set of Pfaffians belonging to the given expression, and is derived from the said expression by