

The Project Gutenberg EBook of Groups of Order  $p^m$  Which Contain Cyclic Subgroups of Order  $p^{(m-3)}$ , by Lewis Irving Neikirk

Copyright laws are changing all over the world. Be sure to check the copyright laws for your country before downloading or redistributing this or any other Project Gutenberg eBook.

This header should be the first thing seen when viewing this Project Gutenberg file. Please do not remove it. Do not change or edit the header without written permission.

Please read the "legal small print," and other information about the eBook and Project Gutenberg at the bottom of this file. Included is important information about your specific rights and restrictions in how the file may be used. You can also find out about how to make a donation to Project Gutenberg, and how to get involved.

**\*\*Welcome To The World of Free Plain Vanilla Electronic Texts\*\***

**\*\*eBooks Readable By Both Humans and By Computers, Since 1971\*\***

**\*\*\*\*\*These eBooks Were Prepared By Thousands of Volunteers!\*\*\*\*\***

Title: Groups of Order  $p^m$  Which Contain Cyclic Subgroups of Order  $p^{(m-3)}$

Author: Lewis Irving Neikirk

Release Date: February, 2006 [EBook #9930]  
[Yes, we are more than one year ahead of schedule]  
[This file was first posted on November 1, 2003]

Edition: 10

Language: English

Character set encoding: TeX

**\*\*\* START OF THE PROJECT GUTENBERG EBOOK GROUPS OF ORDER  $P^M$  \*\*\***

Produced by Cornell University, Joshua Hutchinson, Lee Chew-Hung, John Hagerson, and the Online Distributed Proofreading Team.

GROUPS OF ORDER  $p^m$  WHICH CONTAIN  
CYCLIC SUBGROUPS OF ORDER  $p^{m-3}$

BY

LEWIS IRVING NEIKIRK

SOMETIME HARRISON RESEARCH FELLOW IN MATHEMATICS

1905

## INTRODUCTORY NOTE.

This monograph was begun in 1902-3. Class I, Class II, Part I, and the self-conjugate groups of Class III, which contain all the groups with independent generators, formed the thesis which I presented to the Faculty of Philosophy of the University of Pennsylvania in June, 1903, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

The entire paper was rewritten and the other groups added while the author was Research Fellow in Mathematics at the University.

I wish to express here my appreciation of the opportunity for scientific research afforded by the Fellowships on the George Leib Harrison Foundation at the University of Pennsylvania.

I also wish to express my gratitude to Professor George H. Hallett for his kind assistance and advice in the preparation of this paper, and especially to express my indebtedness to Professor Edwin S. Crawley for his support and encouragement, without which this paper would have been impossible.

LEWIS I. NEIKIRK.

UNIVERSITY OF PENNSYLVANIA, *May, 1905.*

GROUPS OF ORDER  $p^m$ , WHICH CONTAIN CYCLIC  
SUBGROUPS OF ORDER  $p^{(m-3)1}$

BY

LEWIS IRVING NEIKIRK

*Introduction.*

The groups of order  $p^m$ , which contain self-conjugate cyclic subgroups of orders  $p^{m-1}$ , and  $p^{m-2}$  respectively, have been determined by BURNSIDE,<sup>2</sup> and the number of groups of order  $p^m$ , which contain cyclic non-self-conjugate subgroups of order  $p^{m-2}$  has been given by MILLER.<sup>3</sup>

Although in the present state of the theory, the actual tabulation of all groups of order  $p^m$  is impracticable, it is of importance to carry the tabulation as far as may be possible. In this paper *all groups of order  $p^m$  ( $p$  being an odd prime) which contain cyclic subgroups of order  $p^{m-3}$  and none of higher order* are determined. The method of treatment used is entirely abstract in character and, in virtue of its nature, it is possible in each case to give explicitly the generational equations of these groups. They are divided into three classes, and it will be shown that these classes correspond to the three partitions:  $(m-3, 3)$ ,  $(m-3, 2, 1)$  and  $(m-3, 1, 1, 1)$ , of  $m$ .

We denote by  $G$  an abstract group  $G$  of order  $p^m$  containing operators of order  $p^{m-3}$  and no operator of order greater than  $p^{m-3}$ . Let  $P$  denote one of these operators of  $G$  of order  $p^{m-3}$ . The  $p^3$  power of every operator in  $G$  is contained in the cyclic subgroup  $\{P\}$ , otherwise  $G$  would be of order greater than  $p^m$ . The complete division into classes is effected by the following assumptions:

- I. There is in  $G$  at least one operator  $Q_1$ , such that  $Q_1^{p^2}$  is not contained in  $\{P\}$ .
- II. The  $p^2$  power of every operator in  $G$  is contained in  $\{P\}$ , and there is at least one operator  $Q_1$ , such that  $Q_1^p$  is not contained in  $\{P\}$ .
- III. The  $p$ th power of every operator in  $G$  is contained in  $\{P\}$ .

---

<sup>1</sup>Presented to the American Mathematical Society April 25, 1903.

<sup>2</sup>*Theory of Groups of a Finite Order*, pp. 75-81.

<sup>3</sup>Transactions, vol. 2 (1901), p. 259, and vol. 3 (1902), p. 383.

The number of groups for Class I, Class II, and Class III, together with the total number, are given in the table below:

	I	II <sub>1</sub>	II <sub>2</sub>	II <sub>3</sub>	II	III	Total
$p > 3$ $m > 8$	9	$20 + p$	$6 + 2p$	$6 + 2p$	$32 + 5p$	23	$64 + 5p$
$p > 3$ $m = 8$	8	$20 + p$	$6 + 2p$	$6 + 2p$	$32 + 5p$	23	$63 + 5p$
$p > 3$ $m = 7$	6	$20 + p$	$6 + 2p$	$6 + 2p$	$32 + 5p$	23	$61 + 5p$
$p = 3$ $m > 8$	9	23	12	12	47	16	72
$p = 3$ $m = 8$	8	23	12	12	47	16	71
$p = 3$ $m = 7$	6	23	12	12	47	16	69

### Class I.

1. *General notations and relations.*—The group  $G$  is generated by the two operators  $P$  and  $Q_1$ . For brevity we set<sup>4</sup>

$$Q_1^a P^b Q_1^c P^d \dots = [a, b, c, d, \dots].$$

Then the operators of  $G$  are given each uniquely in the form

$$[y, x] \begin{pmatrix} y = 0, 1, 2, \dots, p^3 - 1 \\ x = 0, 1, 2, \dots, p^{m-3} - 1 \end{pmatrix}.$$

We have the relation

$$(1) \quad Q_1^{p^3} = P^{hp^3}.$$

There is in  $G$ , a subgroup  $H_1$  of order  $p^{m-2}$ , which contains  $\{P\}$  self-conjugately.<sup>5</sup> The subgroup  $H_1$  is generated by  $P$  and some operator  $Q_1^y P^x$  of  $G$ ; it then contains  $Q_1^y$  and is therefore generated by  $P$  and  $Q_1^{p^2}$ ; it is also self-conjugate in  $H_2 = \{Q_1^p, P\}$  of order  $p^{m-1}$ , and  $H_2$  is self-conjugate in  $G$ .

From these considerations we have the equations<sup>6</sup>

$$(2) \quad Q_1^{-p^2} P Q_1^{p^2} = P^{1+kp^{m-4}},$$

$$(3) \quad Q_1^{-p} P Q_1^p = Q_1^{\beta p^2} P^{\alpha_1},$$

$$(4) \quad Q_1^{-1} P Q_1 = Q_1^{bp} P^{\alpha_1}.$$

<sup>4</sup>With J. W. YOUNG, *On a certain group of isomorphisms*, American Journal of Mathematics, vol. 25 (1903), p. 206.

<sup>5</sup>BURNSIDE: *Theory of Groups*, Art. 54, p. 64.

<sup>6</sup>*Ibid.*, Art. 56, p. 66.

2. *Determination of  $H_1$ . Derivation of a formula for  $[yp^2, x]^s$ .*—From (2), by repeated multiplication we obtain

$$[-p^2, x, p^2] = [0, x(1 + kp^{m-4})];$$

and by a continued use of this equation we have

$$[-yp^2, x, yp^2] = [0, x(1 + kp^{m-4})y] = [0, x(1 + kyp^{m-4})] \quad (m > 4)$$

and from this last equation,

$$(5) \quad [yp^2, x]^s = [syp^2, x\{s + k\binom{s}{2}yp^{m-4}\}].$$

3. *Determination of  $H_2$ . Derivation of a formula for  $[yp, x]^s$ .*—It follows from (3) and (5) that

$$[-p^2, 1, p^2] = \left[ \beta \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^2, \alpha_1^p \left\{ 1 + \frac{\beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^{m-4} \right\} \right] \quad (m > 4).$$

Hence, by (2),

$$\begin{aligned} \beta \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^2 &\equiv 0 \pmod{p^3}, \\ \alpha_1^p \left\{ 1 + \frac{\beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^{m-4} \right\} + \beta \frac{\alpha_1^p - 1}{\alpha_1 - 1} hp^2 &\equiv 1 + kp^{m-4} \pmod{p^{m-3}}. \end{aligned}$$

From these congruences, we have for  $m > 6$

$$\alpha_1^p \equiv 1 \pmod{p^3}, \quad \alpha_1 \equiv 1 \pmod{p^2},$$

and obtain, by setting

$$\alpha_1 = 1 + \alpha_2 p^2,$$

the congruence

$$\frac{(1 + \alpha_2 p^2)^p - 1}{\alpha_2 p^3} (\alpha_2 + h\beta) p^3 \equiv kp^{m-4} \pmod{p^{m-3}};$$

and so

$$(\alpha_2 + h\beta) p^3 \equiv 0 \pmod{p^{m-4}},$$

since

$$\frac{(1 + \alpha_2 p^2)^p - 1}{\alpha_2 p^3} \equiv 1 \pmod{p^2}.$$

From the last congruences

$$(6) \quad (\alpha_2 + h\beta)p^3 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

Equation (3) is now replaced by

$$(7) \quad Q_1^{-p} P Q_1^{-p} = Q_1^{\beta p^2} P^{1+\alpha_2 p^2}.$$

From (7), (5), and (6)

$$[-yp, x, yp] = [\beta xyp^2, x\{1 + \alpha_2 yp^2\} + \beta k \binom{x}{2} yp^{m-4}].$$

A continued use of this equation gives

$$(8) \quad [yp, x]^s = [syp + \beta \binom{s}{2} xyp^2, \\ xs + \binom{s}{2} \{\alpha_2 xyp^2 + \beta k \binom{x}{2} yp^{m-4}\} + \beta k \binom{s}{3} x^2 yp^{m-4}].$$

4. *Determination of G.*—From (4) and (8),

$$[-p, 1, p] = [Np, a_1^p + Mp^2].$$

From the above equation and (7),

$$a_1^p \equiv 1 \pmod{p^2}, \quad a_1 \equiv 1 \pmod{p}.$$

Set  $a_1 = 1 + a_2p$  and equation (4) becomes

$$(9) \quad Q_1^{-1} P Q_1 = Q_1^{bp} P^{1+a_2p}.$$

From (9), (8) and (6)

$$[-p^2, 1, p^2] = \left[ \frac{(1 + a_2p)^{p^2} - 1}{a_2p} bp, (1 + a_2p)^{p^2} \right],$$

and from (1) and (2)

$$\frac{(1 + a_2p)^{p^2} - 1}{a_2p} bp \equiv 0 \pmod{p^3}, \\ (1 + a_2p)^{p^2} + bh \frac{(1 + a_2p)^{p^2} - 1}{a_2p} p \equiv 1 + kp^{m-4} \pmod{p^{m-3}}.$$

By a reduction similar to that used before,

$$(10) \quad (a_2 + bh)p^3 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

The groups in this class are completely defined by (9), (1) and (10).

These defining relations may be presented in simpler form by a suitable choice of the second generator  $Q_1$ . From (9), (6), (8) and (10)

$$[1, x]^{p^3} = [p^3, xp^3] = [0, (x+h)p^3] \quad (m > 6),$$

and, if  $x$  be so chosen that

$$x + h \equiv 0 \pmod{p^{m-6}},$$

$Q_1 P^x$  is an operator of order  $p^3$  whose  $p^2$  power is not contained in  $\{P\}$ . Let  $Q_1 P^x = Q$ . The group  $G$  is generated by  $Q$  and  $P$ , where

$$Q^{p^3} = 1, \quad P^{p^{m-3}} = 1.$$

Placing  $h = 0$  in (6) and (10) we find

$$\alpha_2 p^3 \equiv a_2 p^3 \equiv k p^{m-4} \pmod{p^{m-3}}.$$

Let  $\alpha_2 = \alpha p^{m-7}$ , and  $a_2 = a p^{m-7}$ . Equations (7) and (9) are now replaced by

$$(11) \quad \begin{aligned} Q^{-p} P Q^p &= Q^{\beta p^2} P^{1+\alpha p^{m-5}}, \\ Q^{-1} P Q &= Q^{bp} P^{1+ap^{m-6}}. \end{aligned}$$

As a direct result of the foregoing relations, the groups in this class correspond to the partition  $(m-3, 3)$ . From (11) we find<sup>7</sup>

$$[-y, 1, y] = [byp, 1 + ayp^{m-6}] \quad (m > 8).$$

It is important to notice that by placing  $y = p$  and  $p^2$  in the preceding equation we find that<sup>8</sup>

$$b \equiv \beta \pmod{p}, \quad a \equiv \alpha \equiv k \pmod{p^3} \quad (m > 7).$$

A combination of the last equation with (8) yields<sup>9</sup>

$$(12) \quad \begin{aligned} [-y, x, y] &= [bxyp + b^2 \binom{x}{2} yp^2, \\ &x(1 + ayp^{m-6}) + ab \binom{x}{2} yp^{m-5} + ab^2 \binom{x}{3} yp^{m-4}] \quad (m > 8). \end{aligned}$$

<sup>7</sup>For  $m = 8$  it is necessary to add  $a^2 \binom{y}{2} p^4$  to the exponent of  $P$  and for  $m = 7$  the terms  $a(a + \frac{abp}{2}) \binom{y}{2} p^2 + a^3 \binom{y}{3} p^3$  to the exponent of  $P$ , and the term  $ab \binom{y}{2} p^2$  to the exponent of  $Q$ . The extra term  $27ab^2 k \binom{y}{3}$  is to be added to the exponent of  $P$  for  $m = 7$  and  $p = 3$ .

<sup>8</sup>For  $m = 7$ ,  $ap^2 - \frac{a^2 p^3}{2} \equiv ap^2 \pmod{p^4}$ ,  $ap^3 \equiv kp^3 \pmod{p^4}$ . For  $m = 7$  and  $p = 3$  the first of the above congruences has the extra terms  $27(a^3 + ab\beta k)$  on the left side.

<sup>9</sup>For  $m = 8$  it is necessary to add the term  $a \binom{y}{2} xp^4$  to the exponent of  $P$ , and for  $m = 7$  the terms  $x\{a(a + \frac{abp}{2}) \binom{y}{2} p^2 + a^3 \binom{y}{3} p^3\}$  to the exponent of  $P$ , with the extra term  $27ab^2 k \binom{y}{3} x$  for  $p = 3$ , and the term  $ab \binom{y}{2} xp^2$  to the exponent of  $Q$ .



From (12) we get<sup>10</sup>

$$(13) \quad [y, x]^s = [ys + by\{(x + b\binom{x}{2}p)\binom{s}{2} + x\binom{s}{3}p\}p, \\ xs + ay\{(x + b\binom{x}{2}p + b^2\binom{x}{3}p^2)\binom{s}{2} \\ + (bx^2p + 2b^2x\binom{x}{2}p^2)\binom{s}{3} + bx^2\binom{s}{4}p^2\}p^{m-6}] \quad (m > 8).$$

5. *Transformation of the Groups.*—The general group  $G$  of Class I is specified, in accordance with the relations (2) (11) by two integers  $a, b$  which (see (11)) are to be taken mod  $p^3$ , mod  $p^2$ , respectively. Accordingly setting

$$a = a_1p^\lambda, \quad b = b_1p^\mu,$$

where

$$dv[a_1, p] = 1, \quad dv[b_1, p] = 1 \quad (\lambda = 0, 1, 2, 3; \mu = 0, 1, 2),$$

we have for the group  $G = G(a, b) = G(a, b)(P, Q)$  the generational determination:

$$G(a, b) : \begin{cases} Q^{-1} P Q = Q^{b_1p^{\mu+1}} P^{1+a_1p^{m+\lambda-6}} \\ Q^{p^3} = 1, \quad P^{p^{m-3}} = 1. \end{cases}$$

Not all of these groups however are distinct. Suppose that

$$G(a, b)(P, Q) \sim G(a', b')(P', Q'),$$

by the correspondence

$$C = \begin{bmatrix} Q, & P \\ Q'_1, & P'_1 \end{bmatrix},$$

where

$$Q'_1 = Q'^y P'^x p^{m-6}, \quad \text{and} \quad P'_1 = Q'^y P'^x,$$

<sup>10</sup>For  $m = 8$  it is necessary to add the term  $\frac{1}{2}axy\binom{s}{2}[\frac{1}{3}y(2s-1) - 1]p^4$  to the exponent of  $P$ , and for  $m = 7$  the terms

$$x\left\{\frac{a}{2}\left(a + \frac{ab}{2}p\right)\left(\frac{2s-1}{3}y - 1\right)\binom{s}{2}yp^2 + \frac{a^3}{3!}\left(\binom{s}{2}y^2 - (2s-1)y + 2\right)yp^3 \right. \\ \left. + \frac{a^2bxy^2}{2}\binom{s}{3}\frac{3s-1}{2}p^3 + \frac{a^2b}{2}\left(\frac{s(s-1)^2(s-4)}{4!}y - \binom{s}{3}\right)yp^3\right\}$$

with the extra terms

$$27abxy\left\{\frac{bk}{3!}\left[\binom{s}{2}y^2 - (2s-1)y + 2\right]\binom{s}{3} + x(b^2k + a^2)(2y^2 + 1)\binom{s}{3}\right\},$$

for  $p = 3$ , to the exponent of  $P$ , and the terms  $\frac{ab}{2}\{2s - \frac{1}{3}y - 1\}\binom{s}{2}xyp^2$  to the exponent of  $Q$ .

with  $y'$  and  $x$  prime to  $p$ .

Since

$$Q^{-1} P Q = Q^{bp} P^{1+ap^{m-6}},$$

then

$$Q_1'^{-1} P_1' Q_1' = Q_1'^{bp} P_1'^{1+ap^{m-6}},$$

or in terms of  $Q'$ , and  $P'$

$$\begin{aligned} [y + b'xy'p + b'^2 \binom{x}{2} y'p^2, x(1 + a'y'p^{m-6}) + a'b' \binom{x}{2} y'p^{m-5} \\ + a'b'^2 \binom{x}{3} y'p^{m-4}] = [y + by'p, x + (ax + bx'p)p^{m-6}] \quad (m > 8) \end{aligned}$$

and

$$(14) \quad by' \equiv b'xy' + b'^2 \binom{x}{2} y'p \pmod{p^2},$$

$$(15) \quad ax + bx'p \equiv a'y'x + a'b' \binom{x}{2} y'p + a'b'^2 \binom{x}{3} y'p^2 \pmod{p^3}.$$

The necessary and sufficient condition for the simple isomorphism of these two groups  $G(a, b)$  and  $G(a', b')$  is, that the above congruences shall be consistent and admit of solution for  $x, y, x'$  and  $y'$ . The congruences may be written

$$\begin{aligned} b_1 p^\mu &\equiv b'_1 x p^{\mu'} + b_1'^2 \binom{x}{2} p^{2\mu'+1} \pmod{p^2}, \\ a_1 x p^\lambda + b_1 x' p^{\mu+1} &\equiv \\ y' \{ a'_1 x p^{\lambda'} + a'_1 b'_1 \binom{x}{2} p^{\lambda'+\mu'+1} + a'_1 b_1'^2 \binom{x}{3} p^{\lambda'+2\mu'+2} \} &\pmod{p^3}. \end{aligned}$$

Since  $dv[x, p] = 1$  the first congruence gives  $\mu = \mu'$  and  $x$  may always be so chosen that  $b_1 = 1$ .

We may choose  $y'$  in the second congruence so that  $\lambda = \lambda'$  and  $a_1 = 1$  except for the cases  $\lambda' \geq \mu + 1 = \mu' + 1$  when we will so choose  $x'$  that  $\lambda = 3$ .

The type groups of Class I for  $m > 8$ <sup>11</sup> are then given by

$$(I) \quad G(p^\lambda, p^\mu) : Q^{-1} P Q = Q^{p^{1+\mu}} P^{1+p^{m-6+\lambda}}, \quad Q^{p^3} = 1, \quad P^{p^{m-3}} = 1 \\ \left( \begin{array}{l} \mu = 0, 1, 2; \lambda = 0, 1, 2; \lambda \geq \mu; \\ \mu = 0, 1, 2; \lambda = 3 \end{array} \right).$$

Of the above groups  $G(p^\lambda, p^\mu)$  the groups for  $\mu = 2$  have the cyclic subgroup  $\{P\}$  self-conjugate, while the group  $G(p^3, p^2)$  is the abelian group of type  $(m-3, 3)$ .

---

<sup>11</sup>For  $m = 8$  the additional term  $ayp$  appears on the left side of the congruence (14) and  $G(1, p^2)$  and  $G(1, p)$  become simply isomorphic. The extra terms appearing in congruence (15) do not effect the result. For  $m = 7$  the additional term  $ay$  appears on the left side of (14) and  $G(1, 1)$ ,  $G(1, p)$ , and  $G(l, p^2)$  become simply isomorphic, also  $G(p, p)$  and  $G(p, p^2)$ .

## Class II.

### 1. General relations.

There is in  $G$  an operator  $Q_1$  such that  $Q_1^{p^2}$  is contained in  $\{P\}$  while  $Q_1^p$  is not.

$$(1) \quad Q_1^{p^2} = P^{hp^2}.$$

The operators  $Q_1$  and  $P$  either generate a subgroup  $H_2$  of order  $p^{m-1}$ , or the entire group  $G$ .

### Section 1.

#### 2. Groups with independent generators.

Consider the first possibility in the above paragraph. There is in  $H_2$ , a subgroup  $H_1$  of order  $p^{m-2}$ , which contains  $\{P\}$  self-conjugately.<sup>12</sup>  $H_1$  is generated by  $Q_1^p$  and  $P$ .  $H_2$  contains  $H_1$  self-conjugately and is itself self-conjugate in  $G$ .

From these considerations<sup>13</sup>

$$(2) \quad Q_1^{-p} P Q_1^p = P^{1+kp^{m-4}},$$

$$(3) \quad Q_1^{-1} P Q = Q_1^{\beta p} P^{\alpha_1}.$$

#### 3. Determination of $H_1$ and $H_2$ .

From (2) we obtain

$$(4) \quad [yp, x]^s = [syp, x\{s + k\binom{s}{2}yp^{m-4}\}] \quad (m > 4),$$

and from (3) and (4)

$$[-p, 1, p] = \left[ \frac{\alpha_1^p - 1}{\alpha_1 - 1} \beta p, \alpha_1^p \left\{ 1 + \frac{\beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^{m-4} \right\} \right].$$

A comparison of the above equation with (2) shows that

$$\begin{aligned} \frac{\alpha_1^p - 1}{\alpha_1 - 1} \beta p &\equiv 0 \pmod{p^2}, \\ \alpha_1^p \left\{ 1 + \frac{\beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^{m-4} \right\} + \frac{\alpha_1^p - 1}{\alpha_1 - 1} \beta h p &\equiv 1 + kp^{m-4} \pmod{p^{m-3}}, \end{aligned}$$

and in turn

$$\alpha_1^p \equiv 1 \pmod{p^2}, \quad \alpha_1 \equiv 1 \pmod{p} \quad (m > 5).$$

Placing  $\alpha_1 = 1 + \alpha_2 p$  in the second congruence, we obtain as in Class I

$$(5) \quad (\alpha_2 + \beta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}} \quad (m > 5).$$

<sup>12</sup>BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

<sup>13</sup>*Ibid.*, Art. 56, p. 66.

Equation (3) now becomes

$$(6) \quad Q_1^{-1} P Q_1 = Q^\beta P^{1+\alpha_2 p}.$$

The generational equations of  $H_2$  will be simplified by using an operator of order  $p^2$  in place of  $Q_1$ .

From (5), (6) and (4)

$$[y, x]^s = [sy + U_s p, sx + W_s p]$$

in which

$$\begin{aligned} U_s &= \beta \binom{s}{2} xy, \\ W_s &= \alpha_2 \binom{s}{2} xy + \left\{ \beta k \left[ \binom{s}{2} \binom{x}{2} + \binom{s}{3} x^2 y \right] \right. \\ &\quad \left. + \frac{1}{2} \alpha k \left[ \frac{1}{3!} s(s-1)(2s-1)y^2 - \binom{s}{2} y \right] x \right\} p^{m-5}. \end{aligned}$$

Placing  $s = p^2$  and  $y = 1$  in the above

$$[Q_1 P^x]^{p^2} = Q_1^{p^2} P^{xp^2} = P^{(x+h)p^2}.$$

If  $x$  be so chosen that

$$(x+h) \equiv 0 \pmod{p^{m-5}} \quad (m > 5)$$

$Q_1 P^x$  will be the required  $Q$  of order  $p^2$ .

Placing  $h = 0$  in congruence (5) we find

$$\alpha_2 p^2 \equiv k p^{m-4} \pmod{p^{m-3}}.$$

Let  $\alpha_2 = \alpha p^{m-6}$ .  $H_2$  is then generated by

$$Q^{p^2} = 1, \quad P^{p^{m-3}} = 1.$$

$$(7) \quad Q^{-1} P Q = Q^{\beta p} P^{1+\alpha p^{m-5}}.$$

Two of the preceding formulæ now become

$$(8) \quad [-y, x, y] = [\beta xyp, x(1 + \alpha yp^{m-5}) + \beta k \binom{x}{2} yp^{m-4}],$$

$$(9) \quad [y, x]^s = [sy + U_s p, xs + W_s p^{m-5}],$$

where

$$U_s = \beta \binom{s}{2} xy$$

and<sup>14</sup>

$$W_s = \alpha \binom{s}{2} xy + \beta k \left\{ \binom{s}{2} \binom{x}{2} + \binom{s}{3} x^2 \right\} yp \quad (m > 6).$$

---

<sup>14</sup>For  $m = 6$  it is necessary to add the terms  $\frac{\alpha k}{2} \left\{ \frac{s(s-1)(2s-1)}{3!} y^2 - \binom{s}{2} y \right\} p$  to  $W_s$ .

4. *Determination of G.*

Let  $R_1$  be an operation of  $G$  not in  $H_2$ .  $R_1^p$  is in  $H_2$ . Let

$$(10) \quad R_1^p = Q^{\lambda p} P^{\mu p}.$$

Denoting  $R_1^a Q^b P^c R_1^d Q^e P^f \dots$  by the symbol  $[a, b, c, d, e, f, \dots]$ , all the operations of  $G$  are contained in the set  $[z, y, x]$ ;  $z = 0, 1, 2, \dots, p-1$ ;  $y = 0, 1, 2, \dots, p^2-1$ ;  $x = 0, 1, 2, \dots, p^{m-3}-1$ .

The subgroup  $H_2$  is self-conjugate in  $G$ . From this<sup>15</sup>

$$(11) \quad R_1^{-1} P R_1 = Q^{b_1} P^{a_1},$$

$$(12) \quad R_1^{-1} Q R_1 = Q^{d_1} P^{c_1 p^{m-5}}.$$

In order to ascertain the forms of the constants in (11) and (12) we obtain from (12), (11), and (9)

$$[-p, 1, 0, p] = [0, d_1^p + Mp, Np^{m-5}].$$

By (10) and (8)

$$R_1^p Q R_1^p = P^{-\mu p} Q P^{\mu p} = Q P^{-a\mu p^{m-4}}.$$

From these equations we obtain

$$d_1^p \equiv 1 \pmod{p} \quad \text{and} \quad d_1 \equiv 1 \pmod{p}.$$

Let  $d_1 = 1 + dp$ . Equation (12) is replaced by

$$(13) \quad R_1^{-1} Q R_1 = Q^{1+dp} P^{e_1 p^{m-5}}.$$

From (11), (13) and (9)

$$[-p, 0, 1, p] = \left[ \frac{a_1^p - 1}{a_1 - 1} b_1 + Kp, a_1^p + b_1 L p^{m-5} \right]$$

in which

$$K = a_1 b_1 \beta \sum_1^{p-1} \binom{a_1^y}{2}.$$

By (10) and (8)

$$R_1^{-p} P R_1^p = Q^{-\lambda p} P Q^{\lambda p} = P^{1+a\lambda p^{m-4}},$$

---

<sup>15</sup>BURNSIDE, *Theory of Groups*, Art. 24, p. 27.

and from the last two equations

$$a_1^p \equiv 1 \pmod{p^{m-5}}$$

and

$$a_1 \equiv 1 \pmod{p^{m-6}} \quad (m > 6); \quad a_1 \equiv 1 \pmod{p} \quad (m = 6).$$

$$\text{Placing } a_1 = 1 + a_2 p^{m-6} \quad (m > 6); \quad a_1 = 1 + a_2 p \quad (m = 6).$$

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

and<sup>16</sup>

$$\frac{a_1^p - 1}{a_1 - 1} b_1 \equiv b_1 p \equiv 0 \pmod{p^2}, \quad b_1 \equiv 0 \pmod{p}.$$

Let  $b_1 = bp$  and we find

$$a_1^p \equiv 1 \pmod{p^{m-4}}, \quad a_1 \equiv 1 \pmod{p^{m-5}}.$$

Let  $a_1 = 1 + a_3 p^{m-5}$  and equation (11) is replaced by

$$(14) \quad R_1^{-1} P R_1 = Q^{bp} P^{1+a_3 p^{m-5}}.$$

The preceding relations will be simplified by taking for  $R_1$  an operator of order  $p$ . This will be effected by two transformations.

From (14), (9) and (13)<sup>17</sup>

$$[1, y]^p = \left[ p, yp, \frac{-c_1 y}{2} p^{m-4} \right] = \left[ 0, (\lambda + y)p, \mu p - \frac{c_1 y}{2} p^{m-4} \right],$$

and if  $y$  be so chosen that

$$\lambda + y \equiv 0 \pmod{p},$$

$R_2 = R_1 Q^y$  is an operator such that  $R_2^p$  is in  $\{P\}$ .

Let

$$R_2^p = P^{lp}.$$

Using  $R_2$  in the place of  $R_1$ , from (15), (9) and (14)

$$[1, 0, x]^p = \left[ p, 0, xp + \frac{ax}{2} p^{m-4} \right] = \left[ 0, 0, (x+l)p + \frac{ax}{2} p^{m-4} \right],$$

<sup>16</sup> $K$  has an extra term for  $m = 6$  and  $p = 3$ , which reduces to  $3b_1 c_1$ . This does not affect the reasoning except for  $c_1 = 2$ . In this case change  $P^2$  to  $P$  and  $c_1$  becomes 1.

<sup>17</sup>The extra terms appearing in the exponent of  $P$  for  $m = 6$  do not alter the result.

and if  $x$  be so chosen that

$$x + l + \frac{ax}{2}p^{m-5} \equiv 0 \pmod{p^{m-4}},$$

then  $R = R_2P^x$  is the required operator of order  $p$ .

$R^p = 1$  is permutable with both  $Q$  and  $P$ . Preceding equations now assume the final forms

$$(15) \quad Q^{-1} P Q = Q^{\beta p} P^{1+ap^{m-5}},$$

$$(16) \quad R^{-1} P R = Q^{bp} P^{1+ap^{m-4}},$$

$$(17) \quad R^{-1} Q R = Q^{1+dp} P^{cp^{m-4}},$$

with  $R^p = 1$ ,  $Q^{p^2} = 1$ ,  $P^{p^{m-3}} = 1$ .

The following derived equations are necessary<sup>18</sup>

$$(18) \quad [0, -y, x, 0, y] = [0, \beta xyp, x(1 + \alpha yp^{m-5}) + \alpha \beta \binom{x}{2} yp^{m-4}],$$

$$(19) \quad [-y, 0, x, -y] = [0, b xyp, x(1 + ayp^{m-4}) + ab \binom{x}{2} yp^{m-4}],$$

$$(20) \quad [-y, x, 0, y] = [0, x(1 + dyp), c xyp^{m-4}].$$

From a consideration of (18), (19) and (20) we arrive at the expression for a power of a general operator of  $G$ .

$$(21) \quad [z, y, x]^s = [sz, sy + U_s p, sx + V_s p^{m-5}],$$

where<sup>19</sup>

$$U_s = \binom{s}{2} \{bxz + \beta xy + d yz\},$$

$$V_s = \binom{s}{2} \left\{ \alpha xy + [axz + \alpha \beta \binom{x}{2} y + cyz + ab \binom{x}{2} z] p \right\}$$

$$+ \alpha \binom{s}{3} \{bxz + \beta xy + d yz\} xp.$$

5. *Transformation of the groups.* All groups of this section are given by equations (15), (16), and (17) with  $a, b, \beta, c, d = 0, 1, 2, \dots, p-1$ , and  $\alpha = 0, 1, 2, \dots, p^2-1$ , independently. Not all these groups, however, are distinct. Suppose that  $G$  and  $G'$  of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R'_1, & Q'_1, & P'_1 \end{bmatrix},$$

in which

$$R'_1 = R'^{z''} Q'^{y''} P'^{x''} p^{m-4},$$

$$Q'_1 = R'^{z'} Q'^{y'} P'^{x'} p^{m-5},$$

$$P'_1 = R'^z Q'^y P'^x,$$

<sup>18</sup>For  $m = 6$  the term  $a^2 \binom{x}{2} xp^2$  must be added to the exponent of  $P$  in (18).

<sup>19</sup>When  $m = 6$  the following terms are to be added to  $V_s$ :  $\frac{a^2 x}{2} \left\{ \frac{s(s-1)(2s-1)}{3!} y^2 - \binom{s}{2} y \right\} p$ .

where  $x$ ,  $y'$  and  $z''$  are prime to  $p$ .

The operators  $R'_1$ ,  $Q'_1$ , and  $P'_1$  must be independent since  $R$ ,  $Q$ , and  $P$  are, and that this is true is easily verified. The lowest power of  $Q'_1$  in  $\{P'_1\}$  is  $Q_1'^{p^2} = 1$  and the lowest power of  $R'_1$  in  $\{Q'_1, P'_1\}$  is  $R_1'^p = 1$ . Let  $Q_1'^{s'} = P_1'^{sp^{m-5}}$ .

This in terms of  $R'$ ,  $Q'$ , and  $P'$  is

$$\left[ s'z', y' \left\{ s' + d' \binom{s'}{2} z'p \right\}, s'x'p^{m-5} + c' \binom{s'}{2} y'z'p^{m-4} \right] = [0, 0, sxp^{m-5}].$$

From this equation  $s'$  is determined by

$$\begin{aligned} s'z' &\equiv 0 \pmod{p} \\ y' \left\{ s' + d' \binom{s'}{2} z'p \right\} &\equiv 0 \pmod{p^2}, \end{aligned}$$

which give

$$s'y' \equiv 0 \pmod{p^2}.$$

Since  $y'$  is prime to  $p$

$$s' \equiv 0 \pmod{p^2}$$

and the lowest power of  $Q'_1$  contained in  $\{P'_1\}$  is  $Q_1'^{p^2} = 1$ .

Denoting by  $R_1'^{s''}$  the lowest power of  $R'_1$  contained in  $\{Q'_1, P'_1\}$ .

$$R_1'^{s''} = Q_1'^{s'p} P_1'^{sp^{m-4}}.$$

This becomes in terms of  $R'$ ,  $Q'$ , and  $P'$

$$[s''z'', s''y''p, s''x''p^{m-4}] = [0, s'y'p, \{s'x' + sx\}p^{m-4}].$$

$s''$  is now determined by

$$s''z'' \equiv 0 \pmod{p}$$

and since  $z''$  is prime to  $p$

$$s'' \equiv 0 \pmod{p}.$$

The lowest power of  $R'_1$  contained in  $\{Q'_1, P'_1\}$  is therefore  $R_1'^p = 1$ .

Since  $R$ ,  $Q$ , and  $P$  satisfy equations (15), (16), and (17)  $R'_1$ ,  $Q'_1$ , and  $P'_1$  also satisfy them. Substituting in these equations the values of  $R'_1$ ,  $Q'_1$ , and  $P'_1$  and reducing we have in terms of  $R'$ ,  $Q'$ , and  $P'$

$$(22) \quad [z, y + \theta_1p, x + \phi_1p^{m-5}] = [z, y + \beta y'p, x(1 + \alpha p^{m-5}) + \beta x p^{m-4}],$$

$$(23) \quad [z, y + \theta_2p, x + \phi_2p^{m-4}] = [z, y + \beta y'p, x(1 + \alpha p^{m-4}) + \beta x' p^{m-4}],$$

$$(24) \quad [z', y' + \theta_3p, (x' + \phi_3p)p^{m-5}] = [z', y'(1 + dp), x(1 + dp)p^{m-5} + cxp^{m-4}],$$



in which

$$\begin{aligned}
\theta_1 &= d'(yz' - y'z) + x(b'z' + \beta'y'), \\
\theta_2 &= d'yz'' + b'xz'', \\
\theta_3 &= d'y'z'', \\
\phi_1 &= \alpha'xy' + \{\alpha'(\beta'y' + b'z')\binom{x}{2} + a'xz + c'(yz' - y'z)\}p, \\
\phi_2 &= \alpha'xy'' + a'xz'' + \alpha'b'\binom{x}{2}z'' + c'yz'', \\
\phi_3 &= c'yz''.
\end{aligned}$$

A comparison of the members of the above equations give six congruences between the primed and unprimed constants and the nine indeterminates.

$$\begin{aligned}
\text{(I)} & \quad \theta_1 \equiv \beta y' \pmod{p}, \\
\text{(II)} & \quad \phi_1 \equiv \alpha x + \beta x' p \pmod{p^2}, \\
\text{(III)} & \quad \theta_2 \equiv b y' \pmod{p}, \\
\text{(IV)} & \quad \phi_2 \equiv a x + b x' \pmod{p}, \\
\text{(V)} & \quad \theta_3 \equiv d y' \pmod{p}, \\
\text{(VI)} & \quad \phi_3 \equiv c x + d x' \pmod{p}.
\end{aligned}$$

The necessary and sufficient condition for the simple isomorphism of the two groups  $G$  and  $G'$  is, that the above congruences shall be consistent and admit of solution for the nine indeterminates, with the condition that  $x$ ,  $y'$  and  $z''$  be prime to  $p$ .

For convenience in the discussion of these congruences, the groups are divided into six sets, and each set is subdivided into 16 cases.

The group  $G'$  is taken from the simplest case, and we associate with this case all cases, which contain a group  $G$ , simply isomorphic with  $G'$ . Then a single group  $G$ , in the selected case, simply isomorphic with  $G'$ , is chosen as a type.

$G'$  is then taken from the simplest of the remaining cases and we proceed as above until all the cases are exhausted.

Let  $\kappa = \kappa_1 p^{\kappa_2}$ , and  $dv_1[\kappa_1, p] = 1$  ( $\kappa = a, b, \alpha, \beta, c$ , and  $d$ ).

The six sets are given in the table below.

I.

	$\alpha_2$	$d_2$		$\alpha_2$	$d_2$
$A$	0	0	$D$	2	0
$B$	0	1	$E$	1	1
$C$	1	0	$F$	2	1

The subdivision into cases and the results are given in Table II.

II.

	$a_2$	$b_2$	$\beta_2$	$c_2$	$A$	$B$	$C$	$D$	$E$	$F$
1	1	1	1	1						
2	0	1	1	1	$A_1$	$B_1$		$C_2$		$E_2$
3	1	0	1	1	$A_1$		$C_1$	$D_1$		
4	1	1	0	1	$A_1$		$C_1$	$D_1$		$E_4$
5	1	1	1	0	$A_1$		$C_1$	$D_1$		$E_5$
6	0	0	1	1	$A_1$	$B_3$	$C_2$	$C_2$	$E_3$	$F_3$
7	0	1	0	1	$A_1$	$B_4$	$C_2$	$C_2$		$E_7$
8	0	1	1	0	$A_1$	$B_5$	$C_2$	$C_2$	$E_5$	$E_5$
9	1	0	0	1	$A_1$	$B_3$	$C_1$	$D_1$	$E_3$	$F_3$
10	1	0	1	0	$A_1$		$C_2$	$C_2$		$E_{10}$
11	1	1	0	0	$A_1$		*	$C_1$		$E_{11}$
12	0	0	0	1	$A_1$	$B_3$	$C_2$	$C_2$	*	$E_3$
13	0	0	1	0	$A_1$	$B_{10}$	*	*	$E_{10}$	$E_{10}$
14	0	1	0	0	$A_1$	$B_{11}$	$C_2$	$C_2$	$E_{11}$	$E_{11}$
15	1	0	0	0	$A_1$	$B_{10}$	$C_2$	$C_2$	$E_{10}$	$E_{10}$
16	0	0	0	0	$A_1$	$B_{10}$	*	*	$E_{10}$	$E_{10}$

The groups marked (\*) divide into two or three parts.

Let  $ad - bc = \theta_1 p^{\theta_2}$ ,  $\alpha_1 d - \beta c = \phi_1 p^{\phi_2}$  and  $\alpha_1 b - a\beta = \chi_1 p^{\chi_2}$  with  $\theta_1, \phi_1$ , and  $\chi_1$  prime to  $p$ .

III.

*	$\theta_2$	$\phi_2$	$\chi_2$		*	$\theta_2$	$\phi_2$	$\chi_2$	
$C_{11}$		1		$D_1$	$D_{13}$	1			$D_1$
$C_{11}$		0		$C_1$	$D_{13}$	0			$C_2$
$C_{13}$	1			$C_1$	$D_{16}$	1			$C_1$
$C_{13}$	0			$C_2$	$D_{16}$	0			$C_2$
$C_{16}$	1	1		$D_1$	$E_{12}$			1	$F_3$
$C_{16}$	1	0		$C_1$	$E_{12}$			0	$E_3$
$C_{16}$	0			$C_2$					

6. *Types.*

The type groups are given by equations (15), (16) and (17) with the values of the constants given in Table IV.

IV.

	$a$	$b$	$\alpha$	$\beta$	$c$	$d$		$a$	$b$	$\alpha$	$\beta$	$c$	$d$
$A_1$	0	0	1	0	0	1	$E_1$	0	0	$p$	0	0	0
$B_1$	0	0	1	0	0	0	$E_2$	1	0	$p$	0	0	0
$B_3$	0	1	1	0	0	0	$E_3$	0	1	$p$	0	0	0
$B_4$	0	0	1	1	0	0	$E_4$	0	0	$p$	1	0	0
$B_5$	0	0	1	0	1	0	$E_5$	0	0	$p$	0	1	0
$B_{10}$	0	1	1	0	$\kappa$	0	$E_7$	1	0	$p$	1	0	0
$B_{11}$	0	0	1	1	1	0	$E_{10}$	0	1	$p$	0	$\kappa$	0
$C_1$	0	0	$p$	0	0	1	$E_{11}$	0	0	$p$	1	1	0
$C_2$	$\omega$	0	$p$	0	0	1	$F_1$	0	0	0	0	0	0
$D_1$	0	0	0	0	0	1	$F_3$	0	1	0	0	0	0

$\kappa = 1$ , and a non-residue  $(\text{mod } p)$ ,  
 $\omega = 1, 2, \dots, p-1$ .

The congruences for three of these cases are completely analyzed as illustrations of the methods used.

$B_{10}$ .

The congruences for this case have the special forms.

- (I)  $b'xz' \equiv \beta y' \pmod{p}$ ,
- (II)  $\alpha'y' \equiv \alpha \pmod{p}$ ,
- (III)  $b'xz'' \equiv by' \pmod{p}$ ,
- (IV)  $\alpha'xy'' + \alpha'b'\binom{x}{2}z'' + c'yz'' \equiv ax + bx' \pmod{p}$ ,
- (V)  $d \equiv 0 \pmod{p}$ ,
- (VI)  $c'y'z'' \equiv cx \pmod{p}$ .

Since  $z'$  is unrestricted (I) gives  $\beta \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

From (II) since  $y' \not\equiv 0, \alpha \not\equiv 0 \pmod{p}$ .

From (III) since  $x, y', z'' \not\equiv 0, b \not\equiv 0 \pmod{p}$ .

In (IV)  $b \not\equiv 0$  and  $x'$  is contained in this congruence alone, and, therefore,  $a$  may be taken  $\equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

(V) gives  $d \equiv 0 \pmod{p}$  and (VI),  $c \not\equiv 0 \pmod{p}$ .

Elimination of  $y'$  between (III) and (VI) gives

$$b'c'z''^2 \equiv bc \pmod{p}$$

so that  $bc$  is a quadratic residue or non-residue (mod  $p$ ) according as  $b'c'$  is a residue or non-residue.

The types are given by placing  $a = 0$ ,  $b = 1$ ,  $\alpha = 1$ ,  $\beta = 0$ ,  $c = \kappa$ , and  $d = 0$  where  $\kappa$  has the two values, 1 and a representative non-residue of  $p$ .

$C_2$ .

The congruences for this case are

$$\begin{aligned}
\text{(I)} \quad & d'(yz' - y'z) \equiv \beta y' \pmod{p}, \\
\text{(II)} \quad & \alpha_1' xy' + a'xz' \equiv \alpha_1 x + \beta x' \pmod{p}, \\
\text{(III)} \quad & d'yz'' \equiv by' \pmod{p}, \\
\text{(IV)} \quad & a'xz'' \equiv ax + bx' \pmod{p}, \\
\text{(V)} \quad & d'z'' \equiv d \pmod{p}, \\
\text{(VI)} \quad & cx + dx' \equiv 0 \pmod{p}.
\end{aligned}$$

Since  $z$  appears in (I) alone,  $\beta$  can be either  $\equiv 0$  or  $\not\equiv 0 \pmod{p}$ . (II) is linear in  $z'$  and, therefore,  $\alpha \equiv 0$  or  $\not\equiv 0 \pmod{p}$ , (III) is linear in  $y$  and, therefore,  $b \equiv 0$  or  $\not\equiv 0$ .

Elimination of  $x'$  and  $z''$  between (IV), (V), and (VI) gives

$$a'd^2 \equiv d'(ad - bc) \pmod{p}.$$

Since  $z''$  is prime to  $p$ , (V) gives  $d \not\equiv 0 \pmod{p}$ , so that  $ad - bc \not\equiv 0 \pmod{p}$ . We may place  $b = 0$ ,  $\alpha = p$ ,  $\beta = 0$ ,  $c = 0$ ,  $d = 1$ , then  $a$  will take the values  $1, 2, 3, \dots, p-1$  giving  $p-1$  types.

$D_1$ .

The congruences for this case are

$$\begin{aligned}
\text{(I)} \quad & d'(yz' - y'z) \equiv \beta y' \pmod{p}, \\
\text{(II)} \quad & \alpha_1 x + \beta x' \equiv 0 \pmod{p}, \\
\text{(III)} \quad & d'yz'' \equiv by' \pmod{p}, \\
\text{(IV)} \quad & ax + bx' \equiv 0 \pmod{p}, \\
\text{(V)} \quad & d'z'' \equiv d \pmod{p}, \\
\text{(VI)} \quad & cx + dx' \equiv 0 \pmod{p}.
\end{aligned}$$

$z$  is contained in (I) alone, and therefore  $\beta \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

(III) is linear in  $y$ , and  $b \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

(V) gives  $d \not\equiv 0 \pmod{p}$ .

Elimination of  $x'$  between (II) and (VI) gives  $\alpha_1 d - \beta c \equiv 0 \pmod{p}$ , and between (IV) and (VI) gives  $ad - bc \equiv 0 \pmod{p}$ . The type group is derived by placing  $a = 0$ ,  $b = 0$ ,  $\alpha = 0$ ,  $\beta = 0$ ,  $c = 0$  and  $d = 1$ .

## Section 2.

1. *Groups with dependent generators.* In this section,  $G$  is generated by  $Q_1$  and  $P$  where

$$(1) \quad Q_1^{p^2} = P^{hp^2}.$$

There is in  $G$ , a subgroup  $H_1$ , of order  $p^{m-2}$ , which contains  $\{P\}$  self-conjugately.<sup>20</sup>  $H_1$  either contains, or does not contain  $Q_1^p$ . We will consider the second possibility in the present section, reserving the first for the next section.

2. *Determination of  $H_1$ .*  $H_1$  is generated by  $P$  and some other operator  $R_1$  of  $G$ .  $R_1^p$  is contained in  $\{P\}$ . Let

$$(2) \quad R_1^p = P^{lp}.$$

Since  $\{P\}$  is self-conjugate in  $H_1$ ,<sup>21</sup>

$$(3) \quad R_1^{-1} P R_1 = P^{1+kp^{m-4}}$$

Denoting  $R_1^a P^b R_1^c P^d \dots$  by the symbol  $[a, b, c, d, \dots]$  we derive from (3)

$$(4) \quad [-y, x, y] = [0, x(1 + kyp^{m-4})] \quad (m > 4),$$

and

$$(5) \quad [y, x]^s = \left[ sy, x \left\{ s + k \binom{s}{2} yp^{m-4} \right\} \right]$$

Placing  $s = p$  and  $y = 1$  in (5) we have, from (2)

$$[R_1 P^x]^p = R_1^p P^{xp} = P^{(l+x)p}.$$

Choosing  $x$  so that

$$x + l \equiv 0 \pmod{p^{m-4}},$$

$R = R_1 P^x$  is an operator of order  $p$ , which will be used in the place of  $R_1$ , and  $H = \{R, P\}$  with  $R^p = 1$ .

3. *Determination of  $H_2$ .* We will now use the symbol  $[a, b, c, d, e, f, \dots]$  to denote  $Q_1^a R^b P^c Q_1^d R^e P^f \dots$ .

$H_1$  and  $Q_1$  generate  $G$  and all the operations of  $G$  are given by  $[x, y, z]$  ( $z = 0, 1, 2, \dots, p^2 - 1$ ;  $y = 0, 1, 2, \dots, p - 1$ ;  $x = 0, 1, 2, \dots, p^{m-3} - 1$ ), since these are  $p^m$  in number and are all distinct. There is in  $G$  a subgroup  $H_2$  of order  $p^{m-1}$  which contains  $H_1$  self-conjugately.  $H_2$  is generated by  $H_1$  and

<sup>20</sup>BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

<sup>21</sup>BURNSIDE, *Theory of Groups*, Art. 56, p. 66.

some operator  $[z, y, x]$  of  $G$ .  $Q_1^z$  is then in  $H_2$  and  $H_2$  is the subgroup  $\{Q_1^p, H_1\}$ . Hence,

$$(6) \quad Q_1^{-p} P Q_1^p = R^\beta P^{\alpha_1},$$

$$(7) \quad Q_1^{-p} P Q_1^p = R^{b_1} P^{ap^{m-4}}.$$

To determine  $\alpha_1$  and  $\beta$  we find from (6), (5) and (7)

$$[-p^2, 0, 1, p^2] = \left[ 0, \frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1} \beta, \alpha_1^p \left\{ 1 + \frac{\beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} p^{m-4} \right\} \right. \\ \left. + a\beta \left\{ p \frac{\alpha_1^{p-1}}{\alpha_1 - b_1} - \frac{\alpha_1^p - b_1^p}{(\alpha_1 - b_1)^2} \right\} p^{m-4} \right].$$

By (1)

$$Q_1^{-p^2} P Q_1^{p^2} = P,$$

and, therefore,

$$\frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1} \beta \equiv 0 \pmod{p}, \\ \alpha_1^p \equiv 1 \pmod{p^{m-4}}, \quad \text{and} \quad \alpha_1 \equiv 1 \pmod{p^{m-5}} \quad (m > 5).$$

Let  $\alpha_1 = 1 + \alpha_2 p^{m-5}$  and equation (6) is replaced by

$$(8) \quad Q_1^{-p} P Q_1^p = R^\beta P^{1+\alpha_2 p^{m-5}}.$$

To find  $a$  and  $b_1$  we obtain from (7), (8) and (5)

$$[-p^2, 1, 0, p^2] = \left[ 0, b_1^p, a \frac{b_1^p - 1}{b_1 - 1} p^{m-4} \right].$$

By (1) and (4)

$$Q_1^{-p^2} R Q_1^{p^2} = P^{-lp^2} R P^{lp^2} = R,$$

and, hence,

$$b_1^p \equiv 1 \pmod{p}, \quad a \frac{b_1^p - 1}{b_1 - 1} \equiv 0 \pmod{p},$$

therefore  $b_1 = 1$ .

Substituting  $b_1 = 1$  and  $\alpha_1 = 1 + \alpha_2 p^{m-5}$  in the congruence determining  $\alpha_1$  we obtain  $(1 + \alpha_2 p^{m-5})^p \equiv 1 \pmod{p^{m-3}}$ , which gives  $\alpha_2 \equiv 0 \pmod{p}$ .

Let  $\alpha_2 = \alpha p$  and equations (8) and (7) are now replaced by

$$(9) \quad Q_1^p P Q_1^p = R^\beta P^{1+\alpha p^{m-4}},$$

$$(10) \quad Q_1^{-p} R Q_1^p = R P^{ap^{m-4}}.$$

From these we derive

$$(11) \quad [-yp, 0, x, yp] = \left[0, \beta xy, x + \{\alpha xy + a\beta x \binom{y}{2} + \beta k \binom{x}{2} y\} p^{m-4}\right],$$

$$(12) \quad [-yp, x, 0, yp] = [0, x, axyp^{m-4}].$$

A continued use of (4), (11), and (12) yields

$$(13) \quad [zp, y, x]^s = [szp, sy + U_s, sx + V_s p^{m-4}]$$

where

$$\begin{aligned} U_s &= \beta \binom{s}{2} xz, \\ V_s &= \binom{s}{2} \left\{ \alpha xz + \beta k \binom{s}{2} z + kxy + ayz \right\} + \beta k \binom{s}{3} x^2 z \\ &\quad + \frac{1}{2} a\beta \left\{ \frac{1}{3!} s(s-1)(2s-1)z^2 - \binom{s}{2} z \right\}. \end{aligned}$$

#### 4. Determination of $G$ .

Since  $H_2$  is self-conjugate in  $G_1$  we have

$$(14) \quad Q_1^{-1} P Q_1 = Q_1^{\gamma p} R^\delta P^{\epsilon_1},$$

$$(15) \quad Q_1^{-1} R Q_1 = Q_1^{c p} R^d P^{\epsilon p^{m-4}}.$$

From (14), (15) and (13)

$$[-p, 0, 1, p] = [\lambda p, \mu, \epsilon_1^p + \nu p^{m-4}]$$

and by (9) and (1)

$$\lambda p \equiv 0 \pmod{p^2}, \quad \epsilon_1^p + \nu p^{m-4} + \lambda h p \equiv 1 + \alpha p^{m-4} \pmod{p^{m-3}},$$

from which

$$\epsilon_1^p \equiv 1 \pmod{p^2}, \quad \text{and} \quad \epsilon_1 \equiv 1 \pmod{p} \quad (m > 5).$$

Let  $\epsilon_1 = 1 + \epsilon_2 p$  and equation (14) is replaced by

$$(16) \quad Q_1^{-1} P Q_1 = Q_1^{\gamma p} R^\delta P^{1+\epsilon_2 p}.$$

From (15), (16), and (13)

$$[-p, 1, 0, p] = \left[ c \frac{d^p - 1}{d - 1} p, d^p, K p^{m-4} \right]$$

where

$$K = \frac{d^p - 1}{d - 1} e + \sum_1^{p-1} a c d \frac{d^n (d^n - 1)}{2}.$$

By (10)

$$d^p \equiv 1 \pmod{p}, \quad \text{and} \quad d = 1$$

and by (1)

$$chp^2 \equiv ap^{m-4} \pmod{p^{m-3}}.$$

Equation (15) is now replaced by

$$(17) \quad Q_1^{-1} R Q_1 = Q_1^{cp} R P^{ep^{m-4}}.$$

A combination of (17), (16) and (13) gives

$$[-p, 0, 1, p] = \left[ \left\{ \gamma \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} + c\delta \frac{p-1}{2} \right\} p^2, 0, (1 + \epsilon_2 p)^p \right].$$

By (9)

$$\left\{ \gamma \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} + c\delta \frac{p-1}{2} \right\} h p^2 + (1 + \epsilon_2 p)^p \equiv 1 + \alpha p^{m-4} \pmod{p^{m-3}},$$

$\beta \equiv 0 \pmod{p}$ .

A reduction of the first congruence gives

$$\frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} \{ \epsilon_2 + \gamma h \} p^2 \equiv \left\{ \alpha - a\delta \frac{p-1}{2} \right\} p^{m-4} \pmod{p^{m-3}}$$

and, since

$$\frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} \equiv 1 \pmod{p}, \quad (\epsilon_2 + \gamma h) p^2 \equiv 0 \pmod{p^{m-4}}$$

and

$$(18) \quad (\epsilon_2 + \gamma h) p^2 \equiv \left( \alpha + \frac{a\delta}{2} \right) p^{m-4} \pmod{p^{m-3}}.$$

From (17), (16), (13) and (18)

$$(19) \quad [-y, x, 0, y] = \left[ cxy p, x, \{ exy + ac \binom{x}{2} y \} p^{m-4} \right],$$

$$(20) \quad [-y, 0, x, y] = \left[ x \{ \gamma y + c\delta \binom{y}{2} \} p, \delta xy, x(1 + \epsilon_2 y p) + \theta p^{m-4} \right]$$

where

$$\begin{aligned} \theta = & \left\{ e\delta x + a\delta\gamma x + \epsilon_2 \left( \alpha + \frac{a\delta}{2} \right) x \right\} \binom{y}{2} \\ & + \frac{1}{2} ac \left\{ \frac{1}{3!} y(y-1)(2y-1)\delta^2 - \binom{y}{2} \delta \right\} \\ & + \left\{ \alpha\gamma y + \delta ky + a\delta xy^2 + (ac\delta^2 y + ac\delta) \binom{y}{2} \right\} \binom{x}{2}. \end{aligned}$$



From (19), (20), (4) and (18)

$$\{Q_1 P^x\}^{p^2} = Q_1^{p^2} P^{xp^2} = P^{(h+x)p^2}.$$

If  $x$  be so chosen that

$$h + x \equiv 0 \pmod{p^{m-5}}$$

$Q = Q_1 P^x$  is an operator of order  $p^2$  which will be used in place  $Q_1$  and  $Q^{p^2} = 1$ .

Placing  $h = 0$  in (18) we get

$$\epsilon_2 p^2 \equiv 0 \pmod{p^{m-4}}.$$

Let  $\epsilon_2 = \epsilon p^{m-6}$  and equation (16) is replaced by

$$(21) \quad Q^{-1} P Q = Q^{\gamma p} R^{\delta} P^{1+\epsilon p^{m-5}}$$

The congruence

$$ap^{m-4} \equiv chp^2 \pmod{p^{m-3}}$$

becomes

$$ap^{m-4} \equiv 0 \pmod{p^{m-3}}, \quad \text{and} \quad a \equiv 0 \pmod{p}.$$

Equations (19) and (20) are replaced by

$$(22) \quad [-y, x, 0, y] = [cxyp, x, exyp^{m-4}]$$

$$(23) \quad [-y, 0, x, y] = \left[ \left\{ \gamma y + c\delta \binom{y}{2} \right\} xp, \delta xy, x(1 + \epsilon yp^{m-5}) + \theta p^{m-4} \right]$$

where

$$\theta = \epsilon \delta x \binom{y}{2} + \left\{ \alpha \gamma y + \delta k y + \alpha c \delta \binom{y}{2} \right\} \binom{x}{2}.$$

A formula for any power of an operation of  $G$  is derived from (4), (22) and (23)

$$(24) \quad [z, y, x]^s = [sz + U_s p, sy + V_s, sx + W_s p^{m-5}]$$

where

$$\begin{aligned} U_s &= \binom{s}{2} \{ \gamma x z + c y z \} + \frac{1}{2} c \delta x \left\{ \frac{1}{3!} s(s-1)(2s-1)z^2 - \binom{s}{2} z \right\}, \\ V_s &= \delta \binom{s}{2} x z, \\ W_s &= \binom{s}{2} \left\{ \epsilon x z + [(a\gamma + \delta k) \binom{x}{2} z + e y z + k x y] p \right\} \\ &\quad + \binom{s}{3} \{ \epsilon \gamma x + \epsilon y + \delta k x \} x z p + \frac{1}{2} c \delta \epsilon \left\{ \frac{1}{2} (s-1)z^2 - z \right\} \binom{s}{3} x p \\ &\quad + \frac{1}{2} \{ \delta \epsilon x + \alpha c \delta \binom{x}{2} \} \left\{ \frac{1}{3!} s(s-1)(2s-1)z^2 - \binom{s}{2} z \right\} p. \end{aligned}$$

5. *Transformations of the groups.* Placing  $y = 1$  and  $x = -1$  in (22) we obtain (17) in the form

$$R^{-1} Q R = Q^{1-ep} P^{-ep^{m-4}}.$$

A comparison of the generational equations of the present section with those of Section 1, shows that groups, in which  $\delta \equiv 0 \pmod{p}$ , are simply isomorphic with those in Section 1, so we need consider only those cases in which  $\delta \not\equiv 0 \pmod{p}$ .

All groups of this section are given by

$$(25), (26), (27) \quad G : \begin{cases} R^{-1} P R = P^{1+kp^{m-4}}, \\ Q^{-1} P Q = Q^{\gamma p} R^{\delta} P^{1+\epsilon p^{m-5}}, \\ Q^{-1} R Q = Q^{cp} R P^{\epsilon p^{m-4}}. \end{cases}$$

$R^p = 1$ ,  $Q^{p^2} = 1$ , and  $P^{p^{m-3}} = 1$ , ( $k, \gamma, c, e = 0, 1, 2, \dots, p-1$ ;  $\delta = 1, 2, \dots, p-1$ ;  $\epsilon = 0, 1, 2, \dots, p^2-1$ ).

Not all these groups, however, are distinct. Suppose that  $G$  and  $G'$  of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R'_1, & Q'_1, & P'_1 \end{bmatrix}.$$

Since  $R^p = 1$ ,  $Q^{p^2} = 1$ , and  $P^{p^{m-3}} = 1$ ,  $R'_1{}^p = 1$ ,  $Q'_1{}^{p^2} = 1$  and  $P'_1{}^{p^{m-3}}$ .

The forms of these operators are then

$$\begin{aligned} P'_1 &= Q'^z R'^y P'^x, \\ R'_1 &= Q'^{z'p} R'^{y'} P'^{x'} p^{m-4}, \\ Q'_1 &= Q'^{z''} R'^{y''} P'^{x''} p^{m-5}, \end{aligned}$$

where  $dv[x, p] = 1$ .

Since  $R$  is not contained in  $\{P\}$ , and  $Q^p$  is not contained in  $\{R, P\}$   $R'_1$  is not contained in  $\{P'_1\}$ , and  $Q'^p$  is not contained in  $\{R'_1, P'_1\}$ .

Let

$$R_1^{s'} = P_1^{sp^{m-4}}.$$

This becomes in terms of  $Q'$ ,  $R'$  and  $P'$

$$[s'z'p, s'y', s'x'p^{m-4}] = [0, 0, sxp^{m-4}],$$

and

$$s'y' \equiv 0 \pmod{p}, \quad s'z' \equiv 0 \pmod{p}.$$

Either  $y'$  or  $z'$  is prime to  $p$  or  $s'$  may be taken = 1.

Let

$$Q_1^{s''p} = R_1^{s'} P_1^{s'p^{m-4}},$$

and in terms of  $Q'$ ,  $R'$  and  $P'$

$$[s''z''p, 0, s''x''p^{m-4}] = [s'z'p, s'y', (s'x' + sx)p^{m-4}],$$

from which

$$s''z'' \equiv s'z' \pmod{p}, \quad \text{and} \quad s'y' \equiv 0 \pmod{p}.$$

Eliminating  $s'$  we find

$$s''y'z'' \equiv 0 \pmod{p},$$

$dv[y'z'', p] = 1$  or  $s''$  may be taken = 1. We have then  $z''$ ,  $y'$  and  $x$  prime to  $p$ .

Since  $R$ ,  $Q$  and  $P$  satisfy equations (25), (26) and (27)  $R'_1$ ,  $Q'_1$  and  $P'_1$  do also. These become in terms of  $R'$ ,  $Q'$  and  $P'$ .

$$\begin{aligned} [z + \Phi'_1 p, y, x + \Theta'_1 p^{m-4}] &= [z, y, x(1 + kp^{m-4})], \\ [z + \Phi'_2 p, y + \delta'xz'', x + \Theta'_2 p^{m-5}] &= [z + \Phi_2 p, y + \delta y', x + \Theta_2 p^{m-5}], \\ [(z' + \Phi'_3)p, y', \Theta'_3 p^{m-4}] &= [(z' + \Phi_3)p, y, \Theta_3 p^{m-4}], \end{aligned}$$

where

$$\begin{aligned} \Phi'_1 &= -c'yz', \quad \Theta'_1 = \epsilon'xz' + k'xy' - e'y'z, \\ \Phi'_2 &= \left\{ \gamma'z'' + c'\delta'\binom{z}{2} \right\} x + c'(yz'' - y''z), \\ \Theta'_2 &= \epsilon'xz'' + \left\{ \binom{x}{2} [\alpha'\gamma'z'' + \alpha'c'\delta'\binom{z''}{2}] + \delta'k'z'' \right. \\ &\quad \left. + \delta'e'x\binom{z''}{2} + e'(yz'' - y''z) + k'xy'' \right\} p, \\ \Phi_2 &= \gamma z'' + \delta z' + c'\delta y'z, \quad \Theta_2 \equiv \epsilon x + (\gamma x'' + \delta x + e'\delta y'z)p, \\ \Phi'_3 &= c'y'z'', \quad \Theta'_3 = e'y'z'', \quad \Phi_3 = cz'', \quad \Theta_3 = \epsilon x + cx''. \end{aligned}$$

A comparison of the members of these equations give seven congruences

$$\begin{aligned} \text{(I)} \quad & \Phi'_1 \equiv 0 \pmod{p}, \\ \text{(II)} \quad & \Theta'_1 \equiv kx \pmod{p}, \\ \text{(III)} \quad & \Phi'_2 \equiv \Phi_2 \pmod{p}, \\ \text{(IV)} \quad & \delta'xz'' \equiv \delta y' \pmod{p}, \\ \text{(V)} \quad & \Theta'_2 \equiv \Theta_2 \pmod{p^2}, \\ \text{(VI)} \quad & \Phi'_3 \equiv cz'' \pmod{p}, \\ \text{(VII)} \quad & \Theta'_3 \equiv \Theta_3 \pmod{p}. \end{aligned}$$

The necessary and sufficient condition for the simple isomorphism of  $G$  and  $G'$  is, that these congruences be consistent and admit of solution for the nine indeterminants with  $x$ ,  $y'$ , and  $z''$  prime to  $p$ .

Let  $\kappa = \kappa_1 p^{\kappa_2}$ ,  $dv[\kappa_1, p] = 1$  ( $\kappa = k, \delta, \gamma, \epsilon, c, e$ ).

The groups are divided into three parts and each part is subdivided into 16 cases.

The methods used in discussing the congruences are the same as those used in Section 1.

6. *Reduction to types.* The three parts are given by

I.

	$\epsilon_2$	$\delta_2$
$A$	0	0
$B$	1	0
$C$	2	0

The subdivision into cases and the results of the discussion of the congruences are given in Table II.

II.

	$k_2$	$\gamma_2$	$c_2$	$e_2$	$A$	$B$	$C$
1	1	1	1	1			$B_1$
2	0	1	1	1			$B_2$
3	1	0	1	1	$A_2$	$B_1$	$B_1$
4	1	1	0	1			$B_4$
5	1	1	1	0			$B_5$
6	0	0	1	1	*	$B_2$	$B_2$
7	0	1	0	1	$A_4$		$B_7$
8	0	1	1	0	$A_5$	$B_5$	$B_5$
9	1	0	0	1	$A_4$	$B_4$	$B_4$
10	1	0	1	0	$A_5$	$B_5$	$B_5$
11	1	1	0	0	$A_4$	$B_4$	$B_4$
12	0	0	0	1	$A_4$	$B_7$	$B_7$
13	0	0	1	0	$A_5$	$B_5$	$B_5$
14	0	1	0	0	$A_4$	$B_7$	$B_7$
15	1	0	0	0	$A_4$	$B_4$	$B_4$
16	0	0	0	0	$A_4$	$B_7$	$B_7$

$A_6$  divides into two parts.

The groups of  $A_6$  in which  $\delta k + \epsilon \gamma \equiv 0 \pmod{p}$  are simply isomorphic with the groups of  $A_1$  and those in which  $\delta k + \epsilon \gamma \not\equiv 0 \pmod{p}$  are simply isomorphic with the groups of  $A_2$ . The types are given by equations (25), (26) and (27) where the constants have the values given in Table III.

### III.

	$k$	$\delta$	$\gamma$	$\epsilon$	$c$	$e$
$A_1$	0	1	0	1	0	0
$A_2$	1	1	0	1	0	0
$A_4$	0	1	0	1	1	0
$A_5$	0	1	0	1	0	$\omega$
$B_1$	0	1	0	$p$	0	0
$B_2$	1	1	0	$p$	0	0
$B_4$	0	1	0	$p$	1	0
$B_5$	0	1	0	$p$	0	$\kappa$
$B_7$	1	1	0	$p$	$\omega$	0

$\kappa = 1$ , and a non-residue  $\pmod{p}$ ,  
 $\omega = 1, 2, \dots, p-1$ .

A detailed analysis of several cases is given below, as a general illustration of the methods used.

#### $A_1$ .

The special forms of the congruences for this case are

$$\begin{aligned}
 \text{(II)} \quad & \epsilon'xz' \equiv kx \pmod{p}, \\
 \text{(III)} \quad & \gamma z'' + \delta z' \equiv 0 \pmod{p}, \\
 \text{(IV)} \quad & \delta'xz'' \equiv \delta y' \pmod{p}, \\
 \text{(V)} \quad & \epsilon'xz'' \equiv \epsilon x \pmod{p}, \\
 \text{(VI)} \quad & cz'' \equiv 0 \pmod{p}, \\
 \text{(VII)} \quad & ex \equiv 0 \pmod{p}.
 \end{aligned}$$

Congruence (IV) gives  $\delta \not\equiv 0 \pmod{p}$ , from (II)  $k$  can be  $\equiv 0$  or  $\not\equiv 0 \pmod{p}$ , (III) gives  $\gamma \equiv 0$  or  $\not\equiv 0$ , (V) gives  $\epsilon \not\equiv 0$ , (VI) and (VII) give  $c \equiv e \equiv 0 \pmod{p}$ . Elimination of  $x$ ,  $z'$  and  $z''$  between (II), (III) and (V) gives  $\delta k + \gamma \epsilon \equiv 0 \pmod{p}$ . If  $k \equiv 0$ , then  $\gamma \equiv 0 \pmod{p}$  and if  $k \not\equiv 0$ , then  $\gamma \not\equiv 0 \pmod{p}$ .

#### $A_2$ .

The congruences for this case are

$$\begin{aligned}
 \text{(II)} \quad & \epsilon'xz' + k'xy' \equiv kx \pmod{p}, \\
 \text{(III)} \quad & \gamma x'' + \delta z' \equiv 0 \pmod{p}, \\
 \text{(IV)} \quad & \delta'xz'' \equiv \delta y' \pmod{p}, \\
 \text{(V)} \quad & \epsilon'xz'' \equiv \epsilon x \pmod{p}, \\
 \text{(VI)} \quad & cz'' \equiv 0 \pmod{p}, \\
 \text{(VII)} \quad & ex \equiv 0 \pmod{p}.
 \end{aligned}$$

Congruence (III) gives  $\gamma \equiv 0$  or  $\not\equiv 0$ , (IV) gives  $\delta \not\equiv 0$ , (V)  $\epsilon \not\equiv 0$ , (VI) and (VII) give  $c \equiv e \equiv 0 \pmod{p}$ . Elimination of  $x$ ,  $z'$ , and  $z''$  between (II), (III) and (V) gives

$$\delta k + \gamma \epsilon \equiv k' \delta y' \pmod{p}$$

from which

$$\delta k + \gamma \epsilon \not\equiv 0 \pmod{p}.$$

If  $k \equiv 0$ , then  $\gamma \not\equiv 0$ , and if  $\gamma \equiv 0$  then  $k \not\equiv 0 \pmod{p}$ .

Both  $\gamma$  and  $k$  can be  $\not\equiv 0 \pmod{p}$  provided the above condition is fulfilled.

$A_5$ .

The congruences for this case are

$$\begin{aligned} \text{(II)} \quad & \epsilon' x z' - e' y' z \equiv k x \pmod{p}, \\ \text{(III)} \quad & \gamma z'' + \delta z' \equiv 0 \pmod{p}, \\ \text{(IV)} \quad & \delta' x z'' \equiv \delta y' \pmod{p}, \\ \text{(V)} \quad & \epsilon' x z'' \equiv e x \pmod{p}, \\ \text{(VI)} \quad & c z'' \equiv 0 \pmod{p}, \\ \text{(VII)} \quad & e' y' z'' \equiv e x \pmod{p}. \end{aligned}$$

(II) and (III) are linear in  $z$  and  $z'$  so  $k$  and  $\gamma$  are  $\equiv$  or  $\not\equiv 0 \pmod{p}$  independently, (IV) gives  $\delta \not\equiv 0$ , (V) give  $\epsilon \not\equiv 0$ , (VI)  $c \equiv 0$ , and (VII)  $e \not\equiv 0$ .

Elimination between (IV), (V), and (VII) gives

$$\delta' e' \epsilon^2 \equiv \delta e \epsilon'^2 \pmod{p}.$$

The types are derived by placing  $\epsilon = \delta = 1$ , and  $e = 1, 2, \dots, p-1$ .

$B_5$ .

The congruences for this case are

$$\begin{aligned} \text{(II)} \quad & -e' y' z \equiv k x \pmod{p}, \\ \text{(III)} \quad & \gamma z'' + \delta z' \equiv 0 \pmod{p}, \\ \text{(IV)} \quad & \delta' x z'' \equiv \delta y' \pmod{p}, \\ \text{(V)} \quad & \epsilon'_1 x z'' + \delta' e' x \binom{z''}{2} + e' y z'' \equiv e_1 x + \gamma x'' + \delta x' \pmod{p}, \\ \text{(VI)} \quad & c z'' \equiv 0 \pmod{p}, \\ \text{(VII)} \quad & e' y' z'' \equiv e x \pmod{p}. \end{aligned}$$

(II), and (III) being linear in  $z$  and  $z'$  give  $k \equiv 0$  or  $\not\equiv 0$ , and  $\gamma \equiv 0$  or  $\not\equiv 0 \pmod{p}$ , (IV) gives  $\delta \not\equiv 0$ , (V) being linear in  $x'$  gives  $\epsilon_1 \equiv 0$  or  $\not\equiv 0 \pmod{p}$ , (VI) gives  $c \equiv 0$  and (VII)  $e \not\equiv 0$ .

Elimination of  $x$  and  $y'$  from (IV) and (VII) gives

$$\delta' e' z'^{m^2} \equiv \delta e \pmod{p}.$$

$\delta e$  is a quadratic residue or non-residue  $\pmod{p}$  according as  $\delta' e'$  is a residue or non-residue.

The two types are given by placing  $\delta = 1$ , and  $e = 1$  and a non-residue  $\pmod{p}$ .

### Section 3.

1. *Groups with dependent generators continued.* As in Section 2,  $G$  is here generated by  $Q_1$  and  $P$ , where

$$Q_1^{p^2} = P^{hp^2}.$$

$Q_1^p$  is contained in the subgroup  $H_1$  of order  $p^{m-2}$ ,  $H_1 = \{Q_1^p, P\}$ .

2. *Determination of  $H_1$ .* Since  $\{P\}$  is self-conjugate in  $H_1$

$$(1) \quad Q_1^{-p} P Q_1^p = P^{1+kp^{m-4}}.$$

Denoting  $Q_1^a P^b Q_1^c P^d \dots$  by the symbol  $[a, b, c, d, \dots]$ , we have from (1)

$$(2) \quad [-yp, x, yp] = [0, x(1+kyp^{m-4})] \quad (m > 4).$$

Repeated multiplication with (2) gives

$$(3) \quad [yp, x]^s = [syp, x\{s + k\binom{s}{2}yp^{m-4}\}].$$

3. *Determination of  $H_2$ .* There is a subgroup  $H_2$  of order  $p^{m-1}$  which contains  $H_1$  self-conjugately.<sup>22</sup>  $H_2$  is generated by  $H_1$  and some operator  $R_1$  of  $G$ .  $R_1^p$  is contained in  $H_1$ , in fact in  $\{P\}$ , since if  $R_1^{p^2}$  is the first power of  $R_1$  in  $\{P\}$ , then  $H_2 = \{R_1, P\}$ , which case was treated in Section 1.

$$(4) \quad R_1^p = P^{lp}.$$

Since  $H_1$  is self-conjugate in  $H_2$

$$(5) \quad R_1^{-1} P R_1 = Q_1^{\beta p} P^{\alpha_1},$$

$$(6) \quad R_1^{-1} Q_1^p R_1 = Q_1^{bp} P^{\alpha_1 p}.$$

Using the symbol  $[a, b, c, d, e, f, \dots]$  to denote  $R_1^a Q_1^b P^c R_1^d Q_1^e P^f \dots$ , we have from (5), (6) and (3)

$$(7) \quad [-p, 0, 1, p] = [0, \beta Np, \alpha_1^p + Mp],$$

<sup>22</sup>BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

and by (4)

$$\alpha_1^p \equiv 1 \pmod{p}, \quad \text{and} \quad \alpha_1 \equiv 1 \pmod{p}.$$

Let  $\alpha_1 = 1 + \alpha_2 p$  and (5) is now replaced by

$$(8) \quad R_1^{-1} P R_1 = Q_1^{\beta p} P^{1+\alpha_2 p}.$$

From (6), (8) and (3)

$$[-p, p, 0, p] = [0, b^p p, a_1 \frac{b^p - 1}{b - 1} p + a_1 U p^2],$$

and by (4) and (2)

$$R_1^{-p} Q_1^p R_1^p = Q_1^p$$

and therefore  $b^p \equiv 1 \pmod{p}$ , and  $b = 1$ . Placing  $b = 1$  in the above equation the exponent of  $P$  takes the form

$$a_1 p^2 (1 + U' p) = a_1 \frac{\{1 + (\alpha_2 + \beta h)p\}^p - 1}{(\alpha_2 + \beta h)p^2} p^2$$

from which

$$a_1 p^2 (1 + U' p) \equiv 0 \pmod{p^{m-3}}$$

or

$$a_1 \equiv 0 \pmod{p^{m-5}} \quad (m > 5).$$

Let  $a_1 = a p^{m-5}$  and (6) is replaced by

$$(9) \quad R_1^{-1} Q_1^p R_1 = Q_1^p P^{ap^{m-4}}.$$

(7) now has the form

$$[-p, 0, 1, p] = [0, \beta N p, (1 + \alpha_2 p)^p + M p^2],$$

where

$$N = p \quad \text{and} \quad M = \beta h \left\{ \frac{(1 + \alpha_2 p)^p - 1}{\alpha_2 p^2} - 1 \right\},$$

from which

$$(1 + \alpha_2 p)^p + \frac{(1 + \alpha_2 p)^p - 1}{\alpha_2 p^2} \beta h p^2 \equiv 1 \pmod{p^{m-3}}$$



or

$$\frac{(1 + \alpha_2 p)^p - 1}{\alpha_2 p^2} \{\alpha_2 + \beta h\} p^2 \equiv 0 \pmod{p^{m-3}}$$

and since

$$\frac{(1 + \alpha_2 p)^p - 1}{\alpha_2 p^2} \equiv 1 \pmod{p}$$

$$(10) \quad (\alpha_2 + \beta h) p^2 \equiv 0 \pmod{p^{m-3}}.$$

From (8), (9), (10) and (3)

$$(11) \quad [-y, 0, x, y] = [0, \beta x y p, x(1 + \alpha_2 y p) + \theta p^{m-4}],$$

$$(12) \quad [-y, x p, 0, y] = [0, x p, a x y p^{m-4}],$$

where

$$\theta = a \beta x \binom{y}{2} + \beta k \binom{x}{2} y.$$

By continued use of (11), (12), (2) and (10)

$$(13) \quad [z, y p, x]^s = [s z, (s y + U_s) p, x s + V_s p],$$

where

$$\begin{aligned} U_s &= \beta \binom{s}{2} x z \\ V_s &= \binom{s}{2} \left\{ \alpha_2 x z + [a y z + k x y + \beta k \binom{x}{2} z] p^{m-5} \right\} \\ &\quad + \left\{ \beta \binom{s}{3} x^2 z + \frac{1}{2} a \beta \left[ \frac{1}{3!} s(s-1)(2s-1) z^2 - \binom{s}{2} z \right] x \right\} p^{m-5}. \end{aligned}$$

Placing in this  $y = 0$ ,  $z = 1$  and  $s = p$ ,<sup>23</sup>

$$(R_1 P^x)^p = R_1^p P^{x p} = P^{(x+l)p},$$

determine  $x$  so that

$$x + l \equiv 0 \pmod{p^{m-4}},$$

then  $R = R_1 P^x$  is an operator of order  $p$  which will be used in the place of  $R_1$ ,  $R^p = 1$ .

4. *Determination of  $G$ .* Since  $H_2$  is self-conjugate in  $G$

$$(14) \quad Q_1^{-1} P Q_1 = R^\gamma Q_1^{\delta p} P^{\epsilon_1},$$

$$(15) \quad Q_1^{-1} R Q_1 = R^c Q_1^{d p} P^{\epsilon_1 p}.$$

<sup>23</sup>Terms of the form  $(Ax^2 + Bx)p^{m-4}$  in the exponent of  $P$  for  $p = 3$  and  $m > 5$  do not alter the result.

From (15)

$$(R^c Q_1^{dp} P^{e_1 p})^p = 1,$$

by (13)

$$Q_1^{dp^2} P^{e_1 p^2} = P^{(e_1 + dh)p^2} = 1,$$

and

$$(16) \quad (e_1 + dh)p^2 \equiv 0 \pmod{p^{m-3}}.$$

From (14), (15) and (13)

$$(17) \quad [0, -p, 1, 0, p] = [L, Mp, \epsilon_1^p + Np].$$

By (1)

$$\epsilon_1^p \equiv 1 \pmod{p}, \quad \text{and} \quad \epsilon_1 \equiv 1 \pmod{p}.$$

Let  $\epsilon_1 = 1 + \epsilon_2 p$  and (14) is replaced by

$$(18) \quad Q_1^{-1} P Q_1 = R^\gamma Q_1^{\delta p} P^{1 + \epsilon_2 p}.$$

From (15), (18), and (13)

$$[0, -p, 0, 1, p] = \left[ c_p, \frac{c^p - 1}{c - 1} dp, Kp \right].$$

Placing  $x = 1$  and  $y = -1$  in (12) we have

$$(19) \quad [0, -p, 0, 1, p] = [1, 0, -ap^{m-4}],$$

and therefore  $c^p \equiv 1 \pmod{p}$ , and  $c = 1$ . (15) is now replaced by

$$(20) \quad Q_1^{-1} R Q_1 = R Q_1^{dp} P^{e_1 p}.$$

Substituting  $1 + \epsilon_2 p$  for  $\epsilon_1$  and 1 for  $c$  in (17) gives, by (16)

$$[0, -p, 1, p] = [0, Mp^2, (1 + \epsilon_2 p)^p + Np^2],$$

where

$$M = \gamma d \frac{p-1}{2} + \delta \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2}$$

and

$$N = \frac{e_1 \gamma}{(\epsilon_2 + \delta h)p^2} \left\{ \frac{[1 + (\epsilon_2 + \delta h)p]^p - 1}{(\epsilon_2 + \delta h)p} - p \right\}.$$

By (1)

$$(1 + \epsilon_2 p)^p + (N + Mh)p^2 \equiv 1 + kp^{m-4} \pmod{p^{m-3}},$$

or reducing

$$\psi(\epsilon_2 + \delta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}},$$

where

$$\psi = \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} + N - e_1 \gamma \frac{p-1}{2}.$$

Since

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

$$(21) \quad (\epsilon_2 + \delta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

From (18), (20), (13), (16) and (21)

$$(22) \quad [0, -y, x, 0, y] = [\gamma xy, \theta_1 p, x + \phi_1 p],$$

$$(23) \quad [0, -y, 0, x, y] = [x, dxy p, \phi_2 p],$$

where

$$\begin{aligned} \theta_1 &= d\gamma x \binom{y}{2} + \delta xy + \beta \gamma \binom{x}{2} y, \\ \phi_1 &= \epsilon_2 xy + \alpha_2 \gamma \binom{x}{2} y + e_1 \gamma \binom{y}{2} x + \left\{ x \binom{y}{2} (\epsilon_2 k + \delta \gamma) \right. \\ &\quad \left. + \frac{1}{2} ad \left[ \frac{1}{3!} y(y-1)(2y-1) \gamma^2 - \frac{y}{2} \gamma \right] x + a \gamma^2 dx \frac{1}{3!} y(y+1)(y-1) \right. \\ &\quad \left. + e_1 \gamma k \binom{y}{3} x + \frac{1}{2} a \beta \left[ \frac{1}{3!} x(x-1)(2x-1) \gamma^2 y^2 - \binom{x}{2} \gamma y \right] \right. \\ &\quad \left. + \binom{x}{2} (a+k) [dy \binom{y}{2} + \delta y] + \beta \gamma \binom{x}{3} \right\} p^{m-5}, \\ \phi_2 &= e_1 xy + \left\{ e_1 k \binom{y}{2} + ad \binom{x}{2} y \right\} p^{m-5}. \end{aligned}$$

Placing  $x = 1$  and  $y = p$  in (23) and by (16)

$$Q_1^{-p} R Q_1^p = R,$$

and by (19)

$$a \equiv 0 \pmod{p}.$$

A continued multiplication, with (11), (22), and (23), gives

$$(Q_1 P^x)^{p^2} = Q_1^{p^2} P^{xp^2} = P^{(x+l)p^2}.$$

Let  $x$  be so chosen that

$$(x + l) \equiv 0 \pmod{p^{m-5}},$$

then  $Q = Q_1 P^x$  is an operator of order  $p^2$  which will be used in place of  $Q_1$ ,  $Q^{p^2} = 1$  and

$$h \equiv 0 \pmod{p^{m-5}}.$$

From (21), (10) and (16)

$$\epsilon_2 p^2 \equiv k p^{m-4}, \quad \alpha_2 p^2 \equiv 0 \quad \text{and} \quad e_1 p^2 \equiv 0 \pmod{p^{m-3}}.$$

Let  $\epsilon_2 = \epsilon p^{m-6}$ ,  $\alpha_2 = \alpha p^{m-5}$  and  $e_1 = \epsilon p^{m-5}$ . Then equations (18), (20) and (8) are replaced by

$$(24), (25), (26) \quad G : \begin{cases} Q^{-1} P Q = R^\gamma Q^{\delta p} P^{1+\epsilon p^{m-5}}, \\ Q^{-1} R Q = R Q^{\delta p} P^{\epsilon p^{m-4}}, \\ R^{-1} P R = Q^{\beta p} P^{1+\alpha p^{m-4}}, \end{cases}$$

$$R^p = 1, \quad Q^{p^2} = 1, \quad P^{p^{m-3}} = 1.$$

(11), (22) and (23) are replaced by

$$(27) \quad [-y, 0, x, y] = [0, \beta x y p, x + \phi p^{m-4}],$$

$$(28) \quad [0, -y, x, 0, y] = [\gamma x y, \theta_1 p, x + \phi_1 p^{m-5}],$$

$$(29) \quad [0, -y, 0, x, y] = [x, d x y p, \phi_2 p^{m-4}],$$

where

$$\begin{aligned} \phi &= \alpha x y + \beta k \binom{x}{2} y, \quad \theta_1 = d \gamma \binom{y}{2} x + \delta x y + \beta \gamma \binom{x}{2} y, \\ \phi_1 &= \epsilon x y + \left\{ \epsilon \gamma x \binom{y}{2} + \binom{x}{2} (\alpha \gamma y + d \gamma k \binom{y}{2}) + \delta k y \right\} p, \\ \phi_2 &= \epsilon x y. \end{aligned}$$

A formula for a general power of any operator of  $G$  is derived from (27), (28) and (29)

$$(30) \quad [0, z, 0, y, 0, z]^s = [0, s z + U_s p, 0, s y + V_s, 0, s x + W_s p^{m-5}],$$

where

$$\begin{aligned} U_s &= \binom{s}{2} \{ \delta x z + d y z + \beta x y + \beta \gamma \binom{x}{2} z \} \\ &\quad + \frac{1}{2} d x \left\{ \frac{1}{3!} s(s-1)(2s-1) z^2 - \binom{s}{2} z \right\} x + \beta \gamma \binom{s}{2} x^2 z, \\ V_s &= \gamma \binom{s}{2} x z, \end{aligned}$$

$$\begin{aligned}
W_s = & \binom{s}{2} \{ \epsilon xz + [axy + eyz + (\beta ky + \alpha\beta\gamma + \delta kz) \binom{x}{2}] p \} \\
& + \binom{s}{3} \{ \alpha\gamma x^2 z + dkxyz + \delta kx^2 z + \beta kx^2 y + 2\beta\gamma k \binom{x}{2} xz \} p \\
& + \beta\gamma k \binom{s}{4} x^3 z p + \frac{1}{2} \left\{ \frac{1}{3!} s(s-1)(2s-1)z^2 - \frac{s}{2}z \right\} \{ e\gamma x + d\gamma k \binom{x}{2} \} p \\
& + \frac{1}{2} d\gamma k \left[ \frac{1}{2}(s-1)z^2 - z \right] \binom{s}{3} x^2.
\end{aligned}$$

A comparison of the generational equations of the present section with those of Sections 1 and 2, shows that,  $\gamma \equiv 0 \pmod{p}$  gives groups simply isomorphic with those of Section 1, while  $\beta \equiv 0 \pmod{p}$ , groups simply isomorphic with those of Section 2 and we need consider only the groups in which  $\beta$  and  $\gamma$  are prime to  $p$ .

5. *Transformation of the groups.* All groups of this section are given by equations (24), (25), and (26), where  $\gamma, \beta = 1, 2, \dots, p-1$ ;  $\alpha, \delta, d, e = 0, 1, 2, \dots, p-1$ ; and  $\epsilon = 0, 1, 2, \dots, p^2-1$ .

Not all of these, however are distinct. Suppose that  $G$  is simply isomorphic with  $G'$  and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R'_1, & Q'_1, & P'_1 \end{bmatrix}.$$

An inspection of (30) gives

$$\begin{aligned}
R'_1 &= Q'^{z'p} R'^{y''} P'^{x''p^{m-4}}, \\
Q'_1 &= Q'^{z'} R'^{y'} P'^{x'p^{m-5}}, \\
P'_1 &= Q'^z R'^y P'^x,
\end{aligned}$$

with  $dv[x, p] = 1$ . Since  $Q^p$  is not in  $\{P\}$ , and  $R$  is not in  $\{Q^p, P\}$ ,  $Q'^p_1$  is not in  $\{P'_1\}$  and  $R'_1$  is not in  $\{Q'^p_1, P'_1\}$ . Let

$$Q'^{s'p}_1 = P'^{sp^{m-4}}_1.$$

This is in terms of  $R'$ ,  $Q'$ , and  $P'$ ,

$$[0, s'z'p, s'x'p^{m-4}] = [0, 0, sp^{m-4}].$$

From which

$$s'z'p \equiv 0 \pmod{p^2},$$

and  $z'$  must be prime to  $p$ , since otherwise  $s'$  can = 1. Let

$$R'^{s''}_1 = Q'^{s'p}_1 P'^{sp^{m-4}}_1,$$

or in terms of  $R'$ ,  $Q'$ , and  $P'$ ,

$$[s''y'', s''z''p, s''x''p^{m-4}] = [0, s'z'p, (sx + s'x')p^{m-4}]$$

and

$$s''z'' \equiv s'z' \pmod{p}, \quad s''y'' \equiv 0 \pmod{p},$$

and  $y''$  is prime to  $p$ , since otherwise  $s''$  can = 1. Since  $R$ ,  $Q$ , and  $P$  satisfy equations (24), (25) and (26),  $R'_1$ ,  $Q'_1$ , and  $P'_1$  must also satisfy them. These become when reduced in terms of  $R'$ ,  $Q'$  and  $P'$

$$\begin{aligned} & [0, z + \theta'_1 p, 0, y + \gamma'xz', 0, x + \psi'_1 p^{m-5}] \\ & \quad = [0, z + \theta_1 p, 0, y + \gamma y'', 0, x + \psi_1 p^{m-5}], \\ & [0, (z'' + \theta'_2)p, 0, y'', 0, (x'' + \psi_2)p^{m-4}] \\ & \quad = [0, (z'' + \theta_2)p, 0, y'', 0, (x'' + \psi_2)p^{m-4}], \\ & [0, z + \theta'_3 p, 0, y, 0, x + \psi'_3 p^{m-4}] = [0, z + \theta_3 p, 0, y, 0, x + \psi_3 p^{m-4}], \end{aligned}$$

where

$$\begin{aligned} \theta'_1 &= d'(yz' - y'z) + x \left\{ d'\gamma' \binom{z'}{2} + \delta'z' + \beta'y' \right\} + \beta'\gamma' \binom{x}{2} z', \\ \theta_1 &= \gamma z'' + \delta z' + d'\gamma y'' z, \\ \psi'_1 &= \epsilon'xz' + \left\{ e'\gamma'x \binom{z'}{2} + \binom{x}{2} \left[ \alpha'\gamma'z' + \gamma'\epsilon'd'k' \binom{z'}{2} + \delta'\epsilon k'z' + \beta'k'y' \right] \right. \\ & \quad \left. + \beta'\gamma' \binom{x}{3} z' + e'(yz' - y'z) + \alpha'xy' \right\} p, \\ \psi_1 &= \epsilon x + \{ \delta x' + \gamma x'' + e'\gamma y'' z \} p, \\ \theta'_2 &= d'y''z', \quad \theta_2 = dz', \quad \psi'_2 = e'y''z, \quad \psi_2 = dx' + ex, \\ \theta'_3 &= \beta'xy'' - d'y''z, \quad \theta_3 = \beta z', \\ \psi_3 &= \epsilon'xz'' - e'y''z + \alpha'xy'' + \beta'\epsilon' \binom{x}{2} y'', \quad \psi_3 = \alpha x + \beta x'. \end{aligned}$$

A comparison of the two sides of these equations give seven congruences

$$\begin{aligned} \text{(I)} & \quad \theta'_1 \equiv \theta_1 \pmod{p}, \\ \text{(II)} & \quad \gamma'xz' \equiv \gamma y'' \pmod{p}, \\ \text{(III)} & \quad \psi'_1 \equiv \psi_1 \pmod{p^2}, \\ \text{(IV)} & \quad \theta'_2 \equiv \theta_2 \pmod{p}, \\ \text{(V)} & \quad \psi'_2 \equiv \psi_2 \pmod{p}, \\ \text{(VI)} & \quad \theta'_3 \equiv \theta_3 \pmod{p}, \\ \text{(VII)} & \quad \psi'_3 \equiv \psi_3 \pmod{p}. \end{aligned}$$

(VI) is linear in  $z$  provided  $d' \not\equiv 0 \pmod{p}$  and  $z$  may be so determined that  $\beta \equiv 0 \pmod{p}$  and therefore all groups in which  $d' \not\equiv 0 \pmod{p}$  are simply isomorphic with groups in Section 2.

Consequently we need only consider groups in which  $d' \equiv 0 \pmod{p}$ .

As before we take for  $G'$  the simplest case and associate with it all simply isomorphic groups  $G$ . We then take as  $G'$  the simplest case left and proceed as above.

Let  $\kappa = \kappa_1 p^{\kappa_2}$  where  $dv[\kappa_1, p] = 1, (\kappa = \alpha, \beta, \gamma, \delta, \epsilon, d, e)$ .

For convenience the groups are divided into three sets and each set is subdivided into eight cases.

The sets are given by

$$\begin{aligned} A : \quad & \epsilon_2 = 0, \quad \beta_2 = 0, \quad \gamma_2 = 0, \\ B : \quad & \epsilon_2 = 1, \quad \beta_2 = 0, \quad \gamma_2 = 0, \\ C : \quad & \epsilon_2 = 2, \quad \beta_2 = 0, \quad \gamma_2 = 0. \end{aligned}$$

The subdivision into cases and results of the discussion are given in Table I.

I.

	$\delta_2$	$e_2$	$\alpha_2$	$A$	$B$	$C$
1	1	1	1			$B_1$
2	0	1	1	$A_1$	$B_1$	$B_1$
3	1	0	1			$B_3$
4	1	1	0	$A_1$	$B_1$	$B_1$
5	0	0	1	$A_3$	$B_3$	$B_3$
6	0	1	0	$A_1$	$B_1$	$B_1$
7	1	0	0	$A_3$	$B_3$	$B_3$
8	0	0	0	$A_3$	$B_3$	$B_3$

6. *Reduction to types.* The types of this section are given by equations (24), (25) and (26) with  $\alpha = 0, \beta = 1, \lambda = 1$  or a quadratic non-residue  $\pmod{p}$ ,  $\delta \equiv 0; \epsilon = l, e = 0, 1, 2, \dots, p-1$ ; and  $\epsilon = p, e = 0, 1$ , or a non-residue  $\pmod{p}$ ,  $2p+6$  in all.

The special forms of the congruences for these cases are given below.

$A_1$ .

$$\begin{aligned} \text{(I)} \quad & \beta' \gamma' \binom{x}{2} z' + \beta' x y' \equiv \gamma z'' + \delta z' \pmod{p}, \\ \text{(II)} \quad & \gamma' x z' \equiv \gamma y'' \pmod{p}, \\ \text{(III)} \quad & \epsilon' x z' \equiv \epsilon x \pmod{p}, \\ \text{(IV)} \quad & dz' \equiv 0 \pmod{p}, \\ \text{(V)} \quad & ex \equiv 0 \pmod{p}, \\ \text{(VI)} \quad & \beta' x y'' \equiv \beta z' \pmod{p}, \\ \text{(VII)} \quad & \epsilon' x z'' + \beta' \epsilon' \binom{x}{2} y' \equiv \alpha x + \beta x' \pmod{p}. \end{aligned}$$

(I) is linear in  $z''$  and  $\delta \equiv 0$  or  $\not\equiv 0$ , (II) gives  $\gamma \not\equiv 0$ , (III)  $\epsilon \not\equiv 0$ , (IV) and (V)  $d \equiv e \equiv 0$ , (VI)  $\beta \not\equiv 0$ , (VII) is linear in  $x'$  and  $\alpha \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

Elimination of  $y''$  and  $z'$  between (II) and (VI) gives

$$\beta'\gamma'x^2 \equiv \beta\gamma \pmod{p}$$

and  $\beta\gamma$  is a residue or non-residue  $\pmod{p}$  according as  $\beta'\gamma'$  is a residue or non-residue.

$A_3$ .

$$\begin{aligned} \text{(I)} \quad & \beta'\gamma' \binom{x}{2} z' + \beta'xy' \equiv \gamma z'' + \delta z' \pmod{p}, \\ \text{(II)} \quad & \gamma'xz' \equiv \gamma y'' \pmod{p}, \\ \text{(III)} \quad & \epsilon'z' \equiv \epsilon \pmod{p}, \\ \text{(IV)} \quad & d \equiv 0 \pmod{p}, \\ \text{(V)} \quad & \epsilon'y''z' \equiv ex \pmod{p}, \\ \text{(VI)} \quad & \beta'xy'' \equiv \beta z' \pmod{p}, \\ \text{(VII)} \quad & \epsilon'xz'' - \epsilon'y''z + \beta'\epsilon' \binom{x}{2} y' \equiv \alpha x + \beta x' \pmod{p}. \end{aligned}$$

(I) is linear in  $z''$  and  $\delta \equiv 0$  or  $\not\equiv 0$ . (II) gives  $\gamma \not\equiv 0$ , (III)  $\epsilon \not\equiv 0$ , (V)  $e \not\equiv 0$  and (VI)  $\beta \not\equiv 0$ . (VII) is linear in  $x'$  and  $\alpha \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

Elimination between (II) and (VI) gives

$$\beta'\gamma'x^2 \equiv \beta\gamma \pmod{p},$$

and between (II), (III), and (IV) gives

$$\epsilon'^2\gamma e \equiv \epsilon^2\gamma'e' \pmod{p}.$$

$\beta\gamma$  is a residue, or non-residue, according as  $\beta'\gamma'$  is or is not, and if  $\gamma$  and  $\epsilon$  are fixed,  $e$  must take the  $(p-1)$  values  $1, 2, \dots, p-1$ .

$B_1$ .

$$\begin{aligned} \text{(I)} \quad & \beta'\gamma' \binom{x}{2} z' + \beta'xy' \equiv \gamma z'' + \delta z' \pmod{p}, \\ \text{(II)} \quad & \gamma'xz' \equiv \gamma y'' \pmod{p}, \\ \text{(III)} \quad & \epsilon'_1xz' + \beta'xz' \binom{x}{3} \equiv \epsilon_1x + \delta x' + \gamma x'' \pmod{p}, \\ \text{(IV)} \quad & ex \equiv 0 \pmod{p}, \\ \text{(VI)} \quad & \beta'xy'' \equiv \beta z' \pmod{p}, \\ \text{(VII)} \quad & \alpha x + \beta x' \equiv 0 \pmod{p}. \end{aligned}$$

(I) gives  $\delta \equiv 0$  or  $\not\equiv 0$ , (II)  $\gamma \not\equiv 0$ , (III) is linear in  $x''$  and gives  $\epsilon_1 \equiv 0$  or  $\not\equiv 0$ , (V)  $e = 0$ , (VI)  $\beta \not\equiv 0$  and (VII) is linear in  $x'$  and gives  $\alpha \equiv 0$  or  $\not\equiv 0$ .

Elimination between (II) and (VI) gives

$$\beta'\gamma'x^2 \equiv \beta\gamma \pmod{p}.$$



$B_3$ .

$$\begin{aligned}
\text{(I)} \quad & \beta' \gamma' \binom{x}{2} z' + \beta' x y' \equiv \gamma \beta'' + \delta z' \pmod{p}, \\
\text{(II)} \quad & \gamma' x z' \equiv \gamma y' \pmod{p}, \\
& \epsilon'_1 x z' + e' \gamma' x \binom{z'}{2} + \beta' \gamma' \binom{x}{3} + e' (y z' - y' z) \\
\text{(III)} \quad & \equiv \epsilon_1 x + \delta x' + \gamma x'' + e' \gamma z y'' \pmod{p}, \\
\text{(V)} \quad & e' y'' z' \equiv e x \pmod{p}, \\
\text{(VI)} \quad & \beta' x y'' \equiv \beta z' \pmod{p}, \\
\text{(VII)} \quad & -e' y'' z \equiv \alpha x + \beta x' \pmod{p}.
\end{aligned}$$

(I) gives  $\delta \equiv 0$  or  $\not\equiv 0$ , (II)  $\gamma \not\equiv 0$ , (III) is linear in  $x''$  and gives  $\epsilon_1 \equiv 0$  or  $\not\equiv 0$ , (V)  $e \not\equiv 0$ , (VI)  $\beta \not\equiv 0$ , (VII) is linear in  $x'$  and gives  $\alpha \equiv 0$  or  $\not\equiv 0 \pmod{p}$ . Elimination of  $y''$  and  $z'$  between (II) and (VI) gives

$$\beta' \gamma' x^2 \equiv \beta \gamma \pmod{p},$$

and between (V) and (VI) gives

$$\beta' e' y''^2 \equiv \beta e \pmod{p}$$

and  $\beta \gamma$  and  $\beta e$  are residues or non-residues, independently, according as  $\beta' \gamma'$  and  $\beta' e'$  are residues or non-residues.

### Class III.

1. *General relations.* In this class, the  $p$ th power of every operator of  $G$  is contained in  $\{P\}$ . There is in  $G$  a subgroup  $H_1$  of order  $p^{m-2}$ , which contains  $\{P\}$  self-conjugately.<sup>24</sup>

2. *Determination of  $H_1$ .*  $H_1$  is generated by  $P$  and some operator  $Q_1$  of  $G$ .

$$Q_1^p = P^{hp}.$$

Denoting  $Q_1^a P^b Q_1^c P^d \dots$  by the symbol  $[a, b, c, d, \dots]$ , all operators of  $H_1$  are included in the set  $[y, x]; (y = 0, 1, 2, \dots, p-1, x = 0, 1, 2, \dots, p^{m-3} - 1)$ .

Since  $\{P\}$  is self-conjugate in  $H_1$ <sup>25</sup>

$$(1) \quad Q_1^{-1} P Q_1 = P^{1+kp^{m-4}}.$$

<sup>24</sup>BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

<sup>25</sup>*Ibid.*, Art. 56, p. 66.

Hence

$$(2) \quad [-y, x, y] = [0, x(1 + kyp^{m-4})] \quad (m > 4).$$

and

$$(3) \quad [y, x]^s = [sy, x \{s + ky \binom{s}{2} p^{m-4}\}].$$

Placing  $y = 1$  and  $s = p$  in (3), we have,

$$[Q_1 P^x]^p = Q_1^p P^{xp} = P^{(x+h)p}$$

and if  $x$  be so chosen that

$$(x + h) \equiv 0 \pmod{p^{m-4}},$$

$Q = Q_1 P^x$  will be an operator of order  $p$  which will be used in place of  $Q_1$ ,  $Q^p = 1$ .

3. *Determination of  $H_2$ .* There is in  $G$  a subgroup  $H_2$  of order  $p^{m-1}$ , which contains  $H_1$  self-conjugately.  $H_2$  is generated by  $H_1$ , and some operator  $R_1$  of  $G$ .

$$R_1^p = P^{lp}.$$

We will now use the symbol  $[a, b, c, d, e, f, \dots]$  to denote  $R_1^a Q^b P^c R_1^d Q^e P^f \dots$ .

The operations of  $H_2$  are given by  $[z, y, x]$ ; ( $z, y = 0, 1, \dots, p-1$ ;  $x = 0, 1, \dots, p^{m-3} - 1$ ). Since  $H_1$  is self-conjugate in  $H_2$

$$(4) \quad R_1^{-1} P R_1 = Q_1^\beta P^{\alpha_1},$$

$$(5) \quad R_1^{-1} Q R_1 = Q_1^{b_1} P^{\alpha_2 p^{m-4}}.$$

From (4), (5) and (3)

$$[-p, 0, 1, p] = \left[ 0, \frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1} \beta, \alpha_1^p + \theta p^{m-4} \right] = [0, 0, 1],$$

where

$$\theta = \frac{\alpha_1^p \beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} + a\beta \left\{ \frac{\alpha_1^p - 1}{\alpha_1 - b_1} p - \frac{\alpha_1^p - b_1^p}{(\alpha_1 - b_1)^2} \right\}.$$

Hence

$$(6) \quad \frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1} \beta \equiv 0 \pmod{p}, \quad \alpha_1^p + \theta p^{m-4} \equiv 1 \pmod{p^{m-3}},$$

and  $\alpha_1^p \equiv 1 \pmod{p^{m-4}}$ , or  $\alpha_1 \equiv 1 \pmod{p^{m-5}}$  ( $m > 5$ ),  $\alpha_1 = 1 + \alpha_2 p^{m-5}$ . Equation (4) is replaced by

$$(7) \quad R_1^{-1} P R_1 = Q^\beta P^{1 + \alpha_2 p^{m-5}},$$

From (5), (7) and (3).

$$[-p, 1, 0, p] = \left[ 0, b_1^p, a \frac{b_1^p - 1}{b - 1} p^{m-4} \right].$$

Placing  $x = lp$  and  $y = 1$  in (2) we have  $Q^{-1}P^{lp}Q = P^{lp}$ , and

$$b_1^p \equiv 1 \pmod{p}, \quad a \frac{b_1^p - 1}{b_1 - 1} \equiv 0 \pmod{p}.$$

Therefore,  $b_1 = 1$ .

Substituting 1 for  $b_1$  and  $1 + \alpha_2 p^{m-5}$  for  $\alpha_1$  in congruence (6) we find

$$(1 + \alpha_2 p^{m-5})^p \equiv 1 \pmod{p^{m-3}}, \quad \text{or} \quad \alpha_2 \equiv 0 \pmod{p}.$$

Let  $\alpha_2 = \alpha p$  and equations (7) and (5) are replaced by

$$(8) \quad R_1^{-1} P R_1 = Q^\beta P^{1+\alpha p^{m-4}},$$

$$(9) \quad R_1^{-1} Q R_1 = Q P^{\alpha p^{m-4}}.$$

From (8), (9) and (3)

$$(10) \quad [-y, 0, x, y] = \left[ 0, \beta xy, x + \{ \alpha xy + a\beta x \binom{y}{2} + \beta ky \binom{x}{2} \} p^{m-4} \right],$$

$$(11) \quad [-y, x, 0, y] = [0, x, axyp^{m-4}].$$

From (2), (10), and (11)

$$(12) \quad [z, y, x]^s = [sz, sy + U_s, sx + V_s p^{m-4}],$$

where

$$\begin{aligned} U_s &= \beta \binom{s}{2} xz, \\ V_s &= \binom{s}{2} \{ \alpha xz + kxy + ayz + \beta k \binom{x}{2} z \} \\ &\quad + \beta k \binom{s}{3} x^2 z + \frac{1}{2} a \beta \binom{s}{2} \left\{ \frac{1}{3!} (2s-1)z - 1 \right\} xz. \end{aligned}$$

Placing  $z = 1$ ,  $y = 0$ , and  $s = p$  in (12)<sup>26</sup>

$$[R_1 P^x]^p = R_1^p P^{xp} = P^{(x+l)p}.$$

If  $x$  be so chosen that

$$x + l \equiv 0 \pmod{p^{m-4}}$$

then  $R = R_1 P^x$  is an operator of order  $p$  which will be used in place of  $R_1$ , and  $R^p = 1$ .

<sup>26</sup>The terms of the form  $(Ax + Bx^2)p^{m-4}$  which appear in the exponent of  $P$  for  $p = 3$  do not alter the conclusion for  $m > 5$ .

4. *Determination of G.*  $G$  is generated by  $H_2$  and some operation  $S_1$ .

$$S_1^p = P^{\lambda p}.$$

Denoting  $S_1^a R^b Q^c P^d \dots$  by the symbol  $[a, b, c, d, \dots]$  all the operators of  $G$  are given by

$$[v, z, y, x]; (v, z, y = 0, 1, \dots, p-1; x = 0, 1, \dots, p^{m-3} - 1).$$

Since  $H_2$  is self-conjugate in  $G$

$$(13) \quad S_1^{-1} P S_1 = R^\gamma Q^s P^{\epsilon_1},$$

$$(14) \quad S_1^{-1} Q S_1 = R^c Q^d P^{\epsilon p^{m-4}},$$

$$(15) \quad S_1 R S_1 = R^f Q^g P^{j p^{m-4}}.$$

From (13), (14), (15), and (12)

$$[-p, 0, 0, 1, p] = [0, L, M, \epsilon_1^p + N p^{m-4}] = [0, 0, 0, 1]$$

and

$$\epsilon_1^p \equiv 1 \pmod{p^{m-4}} \quad \text{or} \quad \epsilon_1 \equiv 1 \pmod{p^{m-5}} \quad (m > 5).$$

Let  $\epsilon_1 = 1 + \epsilon_2 p^{m-5}$ . Equation (13) is now replaced by

$$(16) \quad S_1^{-1} P S_1 = R^\gamma Q^\delta P^{1+\epsilon_2 p^{m-5}}.$$

If  $\lambda = 0 \pmod{p}$  and  $\lambda = \lambda' p$ ,

$$\begin{aligned} [1, 0, 0, 1]^p &= [p, 0, 0, p + \epsilon \binom{p}{2} p^{m-5} + W p^{m-4}] \\ &= [0, 0, 0, p + \lambda' p^2 + W' p^{m-4}] \end{aligned}$$

and for  $m > 5$   $S_1 P$  is of order  $p^{m-3}$ . We will take this in place of  $S_1$  and assume  $dv[\lambda, p] = 1$ .

$$S_1^{p^{m-3}} = 1.$$

There is in  $G$  a subgroup  $H'_1$  of order  $p^{m-2}$  which contains  $\{S_1\}$  self-conjugately.  $H'_1 = \{S_1, S_1^y R^z Q^y P^x\}$  and the operator  $T = R^z Q^y P^x$  is in  $H'_1$ .

There are two cases for discussion.

1°. Where  $x$  is prime to  $p$ .

$T$  is an operator of  $H_2$  of order  $p^{m-3}$  and will be taken as  $P$ . Then

$$H'_1 = \{S_1, P\}.$$

Equation (16) becomes

$$S_1^{-1} P S_1 = P^{1+\epsilon p^{m-4}}.$$

There is in  $G$  a subgroup  $H'_2$  of order  $p^{m-1}$  which contains  $H'_1$  self-conjugately.

$$H'_2 = \{H'_1, S_1^{y'} R^{z'} Q^{y'} P^{x'}\}.$$

$T' = R^{z'} Q^{y'}$  is in  $H'_2$  and also in  $H_2$  and is taken as  $Q$ , since  $\{P, T'\}$  is of order  $p^{m-2}$ .

$H'_2 = \{H'_1, Q\} = \{S_1, H_1\}$  and in this case  $c$  may be taken  $\equiv 0 \pmod{p}$ .

2°. Where  $x = x_1 p$ .  $P^p$  is in  $\{S_1\}$  since  $\lambda$  is prime to  $p$ . In the present case  $R^z Q^y$  is in  $H'_1$  and also in  $H_2$ . If  $z \not\equiv 0 \pmod{p}$  take  $R^z Q^y$  as  $R$ ; if  $z \equiv 0 \pmod{p}$  take it as  $Q$ .

$$H'_1 = \{S_1, R\} \quad \text{or} \quad \{S_1, Q\},$$

and

$$R^{-1} S_1 R = S_1^{1+k'p^{m-4}} \quad \text{or} \quad Q^{-1} S_1 Q = S_1^{1+k''p^{m-4}}.$$

On rearranging these take the forms

$$S_1^{-1} R S_1 = R S_1^{n'p^{m-4}} = R P^{j'p^{m-4}} \quad \text{or} \quad S_1^{-1} Q S_1 = Q S_1^{n''p^{m-4}} = Q P^{e'p^{m-4}},$$

and either  $c$  or  $g$  may be taken  $\equiv 0 \pmod{p}$ ,

$$(17) \quad cg \equiv 0 \pmod{p}.$$

From (14), (15), (16), (12) and (17)

$$[-p, 0, 1, 0, p] = \left[ 0, c \frac{d^p - f^p}{d - f}, d^p, W p^{m-4} \right].$$

Place  $x = \lambda p$  and  $y = 1$  in (12)

$$Q^{-1} P^{\lambda p} Q = P^{\lambda p} \quad \text{or} \quad S_1^p Q S_1^p = Q,$$

and

$$d^p \equiv 1 \pmod{p}, \quad d = 1.$$

Equation (14) is replaced by

$$(18) \quad S_1^{-1} Q S_1 = R^c Q P^{e'p^{m-4}}.$$

From (15), (18), (17), (16) and (12)

$$[-p, 1, 0, 0, p] = \left[ 0, f^p, \frac{d^p - f^p}{d - f} g, W' p^{m-4} \right].$$

Placing  $x = \lambda p$ ,  $y = 1$  in (10)

$$R^{-1} P^{\lambda p} R = P^{\lambda p},$$

and  $f^p \equiv 1 \pmod{p}$ ,  $f = 1$ . Equation (15) is replaced by

$$(19) \quad S_1^{-1} R S_1 = R Q^g P^j p^{m-4}.$$

From (16), (18), (19) and (12)

$$S_1^{-p} P S_1^p = P^{1+\epsilon_2 p^{m-4}} = P$$

and  $\epsilon_2 \equiv 0 \pmod{p}$ . Let  $\epsilon_2 = \epsilon p$  and (16) is replaced by

$$(20) \quad S_1^{-1} P S_1 = R^\gamma Q^\delta P^{1+\epsilon p^{m-4}}.$$

Transforming both sides of (1), (8) and (9) by  $S_1$

$$\begin{aligned} S_1^{-1} Q^{-1} S_1 \cdot S_1^{-1} P S_1 \cdot S_1^{-1} Q S_1 &= S_1^{-1} P^{1+k p^{m-4}} S_1, \\ S_1^{-1} R^{-1} S_1 \cdot S_1^{-1} P S_1 \cdot S_1^{-1} R S_1 &= S_1^{-1} Q^\beta S_1 \cdot S_1^{-1} P^{1+\alpha p^{m-4}} S_1, \\ S_1^{-1} R^{-1} S_1 \cdot S_1^{-1} Q S_1 \cdot S_1^{-1} R S_1 &= S_1^{-1} Q S_1 \cdot S_1^{-1} P^{a p^{m-4}} S_1. \end{aligned}$$

Reducing these by (18), (19), (20) and (12) and rearranging

$$\begin{aligned} &[0, \gamma, \delta + \beta c, 1 + \{\epsilon + \alpha c + k + a c \delta + a \beta \binom{c}{2} - a \gamma\} p^{m-4}] \\ &= [0, \gamma, \delta, 1 + (\epsilon + k) p^{m-4}]. \\ &[0, \gamma, \beta + \delta, 1 + \{k g + \epsilon + \alpha + a \delta - a \gamma g\} p^{m-4}] \\ &= [0, \gamma + \beta c, \beta + \delta, 1 + \{\epsilon + \alpha + \beta e + \alpha \binom{\beta}{2} c + a \beta \gamma\} p^{m-4}], \\ &[0, c, 1, (e + a) p^{m-4}] = [0, c, 1, (e + a) p^{m-4}]. \end{aligned}$$

The first gives

$$(21) \quad \beta c \equiv 0 \pmod{p},$$

$$(22) \quad a c + a c \delta - a \gamma \equiv 0 \pmod{p}.$$

Multiplying this last by  $g$

$$(23) \quad a g \gamma \equiv 0 \pmod{p}.$$

From the second equation above

$$(24) \quad g k + \alpha \delta \equiv \beta e + a \beta \gamma \pmod{p}.$$

Multiplying by  $c$

$$(25) \quad a c \delta \equiv 0 \pmod{p}.$$

These relations among the constants *must be satisfied* in order that our equations should define a group.

From (20), (19), (18) and (12)

$$(26) \quad [-y, 0, 0, x, y] = [0, \gamma xy + \chi_1(x, y), \delta xy + \phi_1(x, y), x + \Theta_1(x, y)p^{m-4}],$$

$$(27) \quad [-y, 0, x, 0, y] = [0, cxy, x, \Theta_2(x, y)p^{m-4}],$$

$$(28) \quad [-y, x, 0, 0, y] = [0, x, gxy, \Theta_3(x, y)p^{m-4}],$$

where

$$\chi_1(x, y) = c\delta x \binom{y}{2},$$

$$\phi_1(x, y) = \gamma gx \binom{y}{2} + \beta \gamma \binom{x}{2} y,$$

$$\begin{aligned} \Theta_1(x, y) = \epsilon xy + \binom{y}{2} [\gamma jx + e\delta x + a\delta\gamma + (\alpha\gamma + k\delta) \binom{x}{2}] \\ + \binom{y}{3} [c\delta j + e\gamma\gamma]x + \binom{x}{2} [\alpha\gamma y + \delta ky + a\delta\gamma y^2] + \beta\gamma k \binom{x}{3} y^2, \end{aligned}$$

$$\Theta_2(x, y) = \epsilon xy + cjx \binom{y}{2} + ac \binom{x}{2} y,$$

$$\Theta_3(x, y) = jxy + egx \binom{y}{2} + ag \binom{x}{2} y.$$

Let a general power of any operator be

$$(29) \quad [v, z, y, x]^s = [sv, sz + U_s, sy + V_s, sx + W_s p^{m-4}].$$

Multiplying both sides by  $[v, z, y, x]$  and reducing by (2), (10), (11), (26), (27) and (28), we find

$$U_{s+1} \equiv U_s + (cy + \gamma x)sv + c\delta \binom{sv}{2} x \pmod{p},$$

$$V_{s+1} \equiv V_s + (gz + \delta x)sv + \gamma g \binom{sv}{2} x + \beta \gamma \binom{x}{2} sv + \beta (sz + U_s)x \pmod{p},$$

$$\begin{aligned} W_{s+1} \equiv W_s + \Theta_1(x, sv) + \{ey + jz + a\gamma xy + ac \binom{y}{2} + ag \binom{z}{2}\} sv \\ + \{\alpha x + \beta k \binom{x}{2} + ay + a\delta sx + \alpha gsvz\} sz + ksxy \\ + \binom{sv}{2} \{c jy + egz\} + U_s \{\alpha x + \beta k \binom{x}{2} + ay + a(\delta x + gz)sv\} \\ + a\beta \binom{sz+U_s}{2} x + kV_s x \pmod{p}. \end{aligned}$$

From (29)

$$U_1 \equiv 0, \quad V_1 \equiv 0, \quad W_1 \equiv 0 \pmod{p}.$$

A continued use of the above congruences give

$$U_s \equiv (cy + \gamma x) \binom{s}{2} v + \frac{1}{2} c\delta xv \left\{ \frac{1}{3} (2s-1)v - 1 \right\} \binom{s}{2} \pmod{p},$$

$$V_s \equiv \{[gz + \delta x + \beta \gamma \binom{x}{2}]v + \beta xz\} \binom{s}{2}$$

$$+ \frac{1}{2} \gamma gxv \left\{ \frac{1}{3} (2s-1)v - 1 \right\} \binom{s}{2} + \beta \gamma \binom{s}{3} x^2 v \pmod{p},$$

$$\begin{aligned}
W_s \equiv \binom{s}{2} & \left\{ \epsilon xv + egv + (\alpha\gamma + \delta kv + \beta kz) \binom{s}{2} + \beta\gamma k \binom{x}{3} v + ac \binom{y}{2} v \right. \\
& + jvz + ag \binom{z}{2} v + \alpha xz + kxy + a\gamma xyv + ayz \left. \right\} + \binom{s}{3} \left\{ \alpha cxyv \right. \\
& + \alpha\gamma x^2 v + 2\beta\gamma k \binom{x}{2} xv + gkxzv + \delta kx^2 v + \beta kx^2 z + acvy^2 \\
& + a\gamma xvy \left. \right\} + \beta k \gamma \binom{s}{4} x^3 v + \binom{s}{2} \frac{2s-1}{3} \left\{ a\delta\gamma \binom{x}{2} v^2 + a\delta xzv \right. \\
& + agvz^2 \left. \right\} + \frac{1}{2} v \binom{s}{2} \left\{ \frac{1}{3} (2s-1)v - 1 \right\} \left\{ \gamma jx + e\delta x + a\delta\gamma x \right. \\
& + \alpha c\delta \binom{x}{2} + \gamma gk \binom{x}{2} + c jy + egz \left. \right\} + \frac{1}{6} \binom{s}{2} \left\{ \binom{s}{2} v^2 - (2s-1)v \right. \\
& + 2 \left. \right\} \left\{ c\delta jx + eg\gamma x \right\} v + \frac{1}{2} \binom{s}{3} \left\{ \frac{1}{2} (s-1)v - 1 \right\} \left\{ \alpha c\delta \right. \\
& + \gamma gk \left. \right\} x^2 v + \frac{1}{2} a\beta x \binom{s}{2} \left\{ \frac{1}{3} (2s-1)z - 1 \right\} z \\
& + \frac{1}{2} a\delta\gamma x^2 v \binom{s}{3} \frac{1}{2} (3s-1) \pmod{p}
\end{aligned}$$

Placing  $v = 1$ ,  $z = y = s = p$  in (29)<sup>27</sup>

$$[S_1 P^x]^p = S_1^p P^{xp} = P^{(\lambda+x)p} \quad (p > 3).$$

If  $x$  be so chosen that

$$x + \lambda \equiv 0 \pmod{p^{m-4}}.$$

$S = S_1 P^x$  is an operator of order  $p$  and is taken in place of  $S_1$ .

$$S^p = 1.$$

The substitution of  $S$  for  $S_1$  leaves congruence (17) invariant.

5. *Transformation of the groups.* All groups of this class are given by

$$(30) \quad G : \begin{cases} Q^{-1} P Q = P^{1+kp^{m-4}}, \\ R^{-1} P R = Q^\beta P^{1+\alpha p^{m-4}}, \\ R^{-1} Q R = Q P^{\alpha p^{m-4}}, \\ S^{-1} P S = R^\gamma Q^\delta P^{1+\epsilon p^{m-4}}, \\ S^{-1} Q S = R^c Q P^{\epsilon p^{m-4}}, \\ S^{-1} R S = R Q^g P^{j p^{m-4}}, \end{cases}$$

with

$$P^{p^{m-3}} = 1, \quad Q^p = R^p = S^p = 1,$$

<sup>27</sup>For  $p = 3$  and  $c\delta \equiv \gamma g \equiv \beta\gamma \equiv 0 \pmod{p}$  there are terms of the form  $(A + Bx + Cx^2 + Dx^3)p^{m-4}$  in the exponent of  $P$ . For  $m > 5$  these do not vitiate our conclusion. For  $p = 3$  and  $c\delta, \gamma g$ , or  $\beta\gamma$  prime to  $p$ ,  $[S_1 P^x]^p$  is not contained in  $\{P\}$  and the groups defined belong to Class II.



( $k, \beta, \alpha, a, \gamma, \delta, \epsilon, c, e, g, j = 0, 1, 2, \dots, p-1$ ).

These constants are however subject to conditions (17), (21), (22), (23), (24) and (25). Not all these groups are distinct. Suppose that  $G$  and  $G'$  of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} S, & R, & Q, & P \\ S'_1, & R'_1, & Q'_1, & P'_1 \end{bmatrix}.$$

Inspection of (29) gives

$$\begin{aligned} S'_1 &= S'^{v'''} R'^{z'''} Q'^{y'''} P'^{x'''} p^{m-4}, \\ R'_1 &= S'^{v''} R'^{z''} Q'^{y''} P'^{x''} p^{m-4}, \\ Q'_1 &= S'^{v'} R'^{z'} Q'^{y'} P'^{x'} p^{m-4}, \\ P'_1 &= S'^v R'^z Q'^y P'^x, \end{aligned}$$

in which  $x$  and one out of each of the sets  $v', z', y', x'; v'', z'', y'', x''; v''', z''', y''', x'''$  are prime to  $p$ .

Since  $S, R, Q$ , and  $P$  satisfy equations (30),  $S'_1, R'_1, Q'_1$  and  $P'_1$  also satisfy them. Substituting these operators and reducing in terms of  $S', R', Q'$ , and  $P'$  we get the six equations

$$(31) \quad [V'_\kappa, Z'_\kappa, Y'_\kappa, X'_\kappa] = [V_\kappa, Z_\kappa, Y_\kappa, X_\kappa] \quad (\kappa = 1, 2, 3, 4, 5, 6),$$

which give the following twenty-four congruences

$$(32) \quad \begin{cases} V'_\kappa \equiv V_\kappa \pmod{p}, \\ Z'_\kappa \equiv Z_\kappa \pmod{p}, \\ Y'_\kappa \equiv Y_\kappa \pmod{p}, \\ X'_\kappa \equiv X_\kappa \pmod{p^{m-3}}, \end{cases}$$

where

$$\begin{aligned} V'_1 &= v, \quad V_1 = v, \\ Z'_1 &= Z + c'(yv' - y'v) + \gamma'xv' + c\delta x \binom{v'}{2}, \quad Z_1 = z, \\ Y'_1 &= y + g'(zv' - z'v) + \delta'xv' + \gamma'g'x \binom{v'}{2} + \beta'xz', \quad Y_1 = y, \\ X'_1 &= x + \left\{ \epsilon'xv' + (\gamma'j'x + e'\delta'x + a'\delta'\gamma'x) \binom{v'}{2} + c'\delta'j' \binom{v'}{3} + (\alpha'\gamma'v' + \delta'k'v' \right. \\ &\quad + a'\delta'\gamma'v^2 + \beta'k'z') \binom{x}{2} + j'(zv' - z'v) + e'g'[z \binom{v'}{2} - z' \binom{v'}{2}] \\ &\quad + a'g'[(\frac{z}{2})v' + (\frac{z'}{2})v - zz'v] + e'(yv' - y'v) + c'j'[y \binom{v'}{2} - y' \binom{v'}{2}] \\ &\quad + a'c'[(\frac{y}{2})v' + v \binom{-y'}{2}] - yy'v + a'(yz' - y'z) - a'\beta'xz'^2 + \alpha'xz' \\ &\quad \left. + \alpha'\beta'x \binom{z'}{2} + a'\gamma'x(y - y')v' + k'xy' \right\} p^{m-4}, \\ X_1 &= x + kxp^{m-4}, \end{aligned}$$

$$\begin{aligned}
V_2' &= v, & V_2 &= v + \beta v', \\
Z_2' &= z + c'(yv'' - y''v) + \gamma' xv'' + e'\delta'(v_2''), & Z_2 &= z + \beta z' + c'\beta y'v, \\
Y_2' &= y + g'(zv'' - z''v) + \delta' xv'' + \gamma' g'x(v_2'') + \beta'\gamma'(x_2)v'' + \beta'xz'', \\
Y_2 &= y + \beta y' + g'\beta z'v, \\
X_2' &= x + \left\{ \Theta_1'(x, v'') + j'(zv'' - z''v) + e'g'[z(v_2'') - z''(v_2')] + a'g'[(x_2)v'' \right. \\
&\quad + (-z_2'')v - zz''v] + e'(yv'' - y''v) + c'j'[y(v_2'') - y''(v_2')] + a'c'[(y_2)v'' \\
&\quad + (-y_2'')v - yy''v''] + a'g'(zv'' - z''v)z'' + a'(yz'' - y''z) + a'\delta'v''z'' \\
&\quad \left. + a'\gamma'(y - y'')v''x + \alpha'xz'' + a'\beta'x(z_2'') + \beta'k'(x_2)z'' + k'xy'' \right\} p^{m-4}, \\
X_2 &= x + \left\{ \alpha x + \beta x' + a'(\beta_2)y'z' + e'\beta v y' + (c'j'\beta + e'g'\beta z')(v_2) \right. \\
&\quad \left. + a'c'(\beta_2 y')v + j'\beta v z' + a'g'(\beta_2 z') + a'\beta(g'z'v + y')z \right\} p^{m-4}, \\
V_3' &= v', & V_3 &= v', \\
Z_3' &= z' + c'(y'v'' - y''v'), & Z_3 &= z', \\
Y_3' &= y' + g'(z'v'' - z''v'), & Y_3 &= y', \\
X_3' &= \left\{ x' + j'(z'v'' - z''v') + e'g'[(v_2'')z' - (v_2')z''] + a'g'[(z_2')v'' + (-z_2'')v' \right. \\
&\quad - z'z''v'] + e'(y'v'' - y''v') + c'j'[y'(v_2'') - y''(v_2')] + a'c'[(y_2')v'' + (-y_2'')v' \\
&\quad \left. - y''y'v''] + a'(y'z'' - y''z') \right\} p^{m-4}, \\
X_4 &= (x' + a'x)p^{m-4}, \\
V_4' &= v, & V_4 &= v + \gamma v'' + \delta v', \\
Z_4' &= z + c'(yv''' - y'''v) + \gamma' xv''' + c'\delta'x(v_2'''), \\
Z_4 &= z + \gamma z'' + \delta z' + c'[(z_2'')v''y'' + (z_2')v'y'] + c'(\gamma y'' + \delta y')v + c'\gamma \delta y''v, \\
Y_4' &= y + g'(zv''' - z'''v) + \delta' xv''' + \gamma' g'x(v_2''') + \beta'\gamma'(x_2)v''' + \beta'xz''', \\
Y_4 &= y + \gamma y'' + \delta y' + g'[(z_2'')v''z'' + (z_2')v'z'] + g'(\gamma z'' + \delta z')v + g'\delta \gamma v'z'', \\
X_4' &= x + \left\{ \Theta_1'(x, v''') + j'(zv''' - z'''v) + e'g'[(v_2''')z - (v_2'')z'''] + a'g'[(z_2'')v''' \right. \\
&\quad + (-z_2''')v - zz'''v] + e'(yv''' - y'''v) + c'j'[y(v_2''') - y'''(v_2')] \\
&\quad + a'c'[(y_2'')v''' + (-y_2''')v - yy'''v'''] + a'g'(v'''z - vz''')z''' \\
&\quad + a'(yz''' - y'''z) + a'\delta'xz'''v''' + a'\gamma'x(y - y''')v''' + \alpha'xz''' \\
&\quad \left. + a'\beta'x(z_2''') + \beta'k'z'''(x_2) + k'xy''' \right\} p^{m-4}.
\end{aligned}$$

$$\begin{aligned}
X_4 = x + & \left\{ \epsilon x + \delta x' + \gamma x'' + \binom{\gamma}{2} [a'c' \binom{y''}{2} v'' + a'y''z'' + e'v''y'' + j'v''z'' \right. \\
& + a'g' \binom{z''}{2} v'' + (c'j'v''y'' + e'g'v''z'')(v + \delta v') + a'(z + \delta z')v''z'' \\
& + \frac{2\gamma - 1}{3} a'g'v''z''^2 + \frac{1}{2} \left[ \frac{1}{3} (2\gamma - 1)v'' - 1 \right] (c'j'y'' + e'g'z'')v'' \\
& + \binom{\gamma}{3} a'c'v''y'' + \binom{\delta}{2} [a'c' \binom{y'}{2} v' + a'y'z' + e'v'y' + j'v'z' \\
& + a'g' \binom{z'}{2} v' + j'c'v'v'y' + e'g'v'v'z' + a'g'v'zz' + a'c'\gamma y'y'v' \\
& + \frac{2\delta - 1}{3} a'g'v'z'^2 + \frac{1}{2} \left\{ \frac{1}{3} (2\delta - 1)v' - 1 \right\} (c'j'y' + e'g'z') \\
& + \binom{\delta}{3} a'c'v'y'^2 + (v + \delta v') [j'\gamma z'' + \binom{\gamma z''}{2} a'g' + e'\gamma y'' + \binom{\gamma y''}{2} a'c' \\
& + a'g'(z + \delta z')] + \binom{v + \delta v'}{2} [e'g'\gamma z'' + c'j'\gamma y''] + \delta [(e'g'z' \\
& + c'j'y') \binom{v}{2} + e'v'y' + j'z' + a'zy + a'g'vzz' + a'\gamma z'y'' + a'c'\gamma v'y'y''] \\
& \left. + a'g' \binom{\delta z'}{2} v + a'c' \binom{\delta y'}{2} v + a'\gamma zy'' \right\} p^{m-4},
\end{aligned}$$

$$V'_5 = v', \quad V_5 = v' + cv'',$$

$$Z'_5 = z' + c'(y'v''' - y'''v'), \quad Z_5 = z' + cz'' + c'cy''v,$$

$$Y'_5 = y' + g'(z'v''' - z'''v'), \quad Y_5 = y' + cy'' + g'cv'z'',$$

$$\begin{aligned}
X'_5 = & \left\{ x' + j'(z'v''' - z'''v') + e'g' \left[ \binom{v'''}{2} z' - \binom{v'}{2} z'''' \right] + a'g' \left[ \binom{z'}{2} v''' \right. \right. \\
& + \binom{-z'''}{2} v' - z'z'''v' \left. \right] + c'(y'v''' - y'''v') + c'j' [y' \binom{\delta'''}{2} - y''' \binom{v'}{2}] \\
& \left. + a'c' \left[ \binom{y'}{2} v'''' + \binom{-y'''}{2} v' - y'y''''v'' \right] + a'(y'z'''' - y''''z') \right\} p^{m-4},
\end{aligned}$$

$$\begin{aligned}
X_5 = & \left\{ x' + \epsilon x + \delta x' + \gamma x'' + a' \binom{c}{2} y''z'' + j'cv'z'' + (e'g'cz'' + c'cj'y'') \binom{v'}{2} + e'cy''v \right. \\
& \left. + a'cy''z' + a'g'z'v' + a'g' \binom{cz''}{2} + a'c' \binom{cy''}{2} \right\} p^{m-4},
\end{aligned}$$

$$V'_6 = v'', \quad V_6 = v'' + gv',$$

$$Z'_6 = z'' + c'(y''v''' - y'''v''), \quad Z_6 = z'' + gz',$$

$$Y'_6 = y'' + g'(z''v''' - z'''v''), \quad Y_6 = y'' + gy',$$

$$\begin{aligned}
X'_6 = & \left\{ x'' + j'(z''v''' - z'''v'') + e'g' \left[ \binom{v'''}{2} z'' - \binom{v''}{2} z'''' \right] + a'g' \left[ \binom{z''}{2} v'''' \right. \right. \\
& + \binom{-z'''}{2} v'' - z''z'''v'' \left. \right] + e'(y''v''' - y'''v'') + c'j' [y'' \binom{v'''}{2} - y'''' \binom{v''}{2}] \\
& \left. + a'c' \left[ \binom{y''}{2} v'''' + \binom{-y'''}{2} v'' - y''y''''v'' \right] + a'(y''z'''' - y''''z'') \right\} p^{m-4},
\end{aligned}$$

$$X_6 = \{x'' + jx + gx' + a'gy''z'\} p^{m-4}.$$

The necessary and sufficient condition for the simple isomorphism of the two groups  $G$  and  $G'$  is that congruences (32) shall be consistent and admit of solution subject to conditions derived below.

6. *Conditions of transformation.* Since  $Q$  is not contained in  $\{P\}$ ,  $R$  is not contained in  $\{Q, P\}$ , and  $S$  is not contained in  $\{R, Q, P\}$ , then  $Q'_1$  is not

contained in  $\{P'_1\}$ ,  $R'_1$  is not contained in  $\{Q'_1, P'_1\}$ , and  $S'_1$  is not contained in  $\{R'_1, Q'_1, P'_1\}$ .

Let

$$Q_1^{s'} = P_1^{s'p^{m-4}}.$$

This equation becomes in terms of  $S'$ ,  $R'$ ,  $Q'$  and  $P'$

$$[s'v', s'z' + c' \binom{s'}{2} v'y', s'y' + g' \binom{s'}{2} v'z', Dp^{m-4}] = [0, 0, 0, sxp^{m-4}],$$

and

$$s'v' \equiv s'z' \equiv s'y' \equiv 0 \pmod{p}.$$

At least one of the three quantities  $v'$ ,  $z'$  or  $y'$  is prime to  $p$ , since otherwise  $s'$  may be taken = 1.

Let

$$R_1^{s''} = Q_1^{s'} P_1^{s'p^{m-4}},$$

or in terms of  $S'$ ,  $R'$ ,  $Q'$  and  $P'$

$$\begin{aligned} [s''v'', s''z'' + c' \binom{s''}{2} v''y'', s''y'' + g' \binom{s''}{2} v''z'', Ep^{m-4}] \\ = [s'v', s'z' + c' \binom{s'}{2} v'y', s'y' + g' \binom{s'}{2} v'z', E_1p^{m-4}], \end{aligned}$$

and

$$\begin{aligned} s''v'' &\equiv s'v' \pmod{p}, \\ s''z'' + c' \binom{s''}{2} v''y'' &\equiv s'z' + c' \binom{s'}{2} v'y' \pmod{p}, \\ s''y'' + g' \binom{s''}{2} v''z'' &\equiv s'y' + g' \binom{s'}{2} v'z' \pmod{p}. \end{aligned}$$

Since  $c'g' \equiv 0 \pmod{p}$ , suppose  $g' \equiv 0 \pmod{p}$ . Elimination of  $s'$  between the last two give by means of the congruence  $Z'_3 \equiv Z_3 \pmod{p}$ ,

$$s''\{2(y'z'' - y''z') + c'y'y''(v' - v'')\} \equiv 0 \pmod{p},$$

between the first two

$$s''\{2(v'z'' - v''z') + c'v'v''(y' - y'')\} \equiv 0 \pmod{p},$$

and between the first and last

$$s''(y'v'' - y''v') \equiv 0 \pmod{p}.$$

At least one of the three above coefficients of  $s''$  is prime to  $p$ , since otherwise  $s''$  may be taken = 1.

Let

$$S_1^{s'''} = R_1^{s''} Q_1^{s'} P_1^{s'p^{m-4}}$$

or, in terms of  $S'$ ,  $R'$ ,  $Q'$ , and  $P'$

$$\begin{aligned} & [s'''v''', s'''z''' + c' \binom{s'''}{2} v'''y''', s'''y''' + g' \binom{s'''}{2} v'''z''', E_2p^{m-4}] \\ & = [s''v'' + s'v', s''z'' + s'z' + c' \{ \binom{s''}{2} v''y'' + \binom{s'}{2} v'y' + s's''y''v' \}, \\ & \quad s''y'' + s'y' + g' \{ \binom{s''}{2} v''z'' + \binom{s'}{2} v'z' + s's''v'z'' \}, E_3p^{m-4}] \end{aligned}$$

and

$$\begin{aligned} s'''v''' & \equiv s''v'' + s'v' \pmod{p}, \\ s'''z''' + c' \binom{s'''}{2} v'''y''' & \equiv s''z'' + s'z' + c' \{ \binom{s''}{2} v''y'' + \binom{s'}{2} v'y' + s's''y''v' \} \pmod{p}, \\ s'''y''' + g' \binom{s'''}{2} v'''z''' & \equiv s''y'' + s'y' + g' \{ \binom{s''}{2} v''z'' + \binom{s'}{2} v'z' + s's''z''v' \} \pmod{p}. \end{aligned}$$

If  $g' \equiv 0$  and  $c' \not\equiv 0 \pmod{p}$  the congruence  $Z'_3 \equiv Z_3 \pmod{p}$  gives

$$(y'v'' - y''v') \equiv 0 \pmod{p}.$$

Elimination in this case of  $s''$  between the first and last congruences gives

$$s'''(y''v''' - y'''v'') \equiv 0 \pmod{p}.$$

Elimination of  $s''$  between the first and second, and between the second and third, followed by elimination of  $s'$  between the two results, gives

$$s''' \left( z''^2 - c'y''z''v' + \frac{c'^2}{4} y''v'' \right) (y'v''' - y'''v') \equiv 0 \pmod{p}.$$

Either  $(y''v''' - y'''v'')$ , or  $(y'v''' - y'''v')$  is prime to  $p$ , since otherwise  $s'''$  may be taken = 1.

A similar set of conditions holds for  $c' \equiv 0$  and  $g' \not\equiv 0 \pmod{p}$ .

When  $c' \equiv g' \equiv 0 \pmod{p}$  elimination of  $s'$  and  $s''$  between the three congruences gives

$$s''' \Delta \equiv s''' \begin{vmatrix} v' & v'' & v''' \\ y' & y'' & y''' \\ z' & z'' & z''' \end{vmatrix} \equiv 0 \pmod{p}$$

and  $\Delta$  is prime to  $p$ , since otherwise  $s'''$  may be taken = 1.

7. *Reduction to types.* In the discussion of congruences (32), the group  $G'$  is taken from the simplest case and we associate with it all simply isomorphic groups  $G$ .

I.

A.							B.					
	$a_2$	$\beta_2$	$c_2$	$g_2$	$\gamma_2$	$\delta_2$		$k_2$	$\alpha_2$	$\epsilon_2$	$e_2$	$j_2$
<b>1</b>	1	1	1	1	1	1	<b>1</b>	1	1	1	1	1
<b>2</b>	0	1	1	1	1	1	<b>2</b>	0	1	1	1	1
<b>3</b>	0	0	1	1	1	1	<b>3</b>	1	0	1	1	1
<b>4</b>	0	0	1	1	1	0	<b>4</b>	1	1	0	1	1
<b>5</b>	0	0	1	0	1	1	<b>5</b>	1	1	1	0	1
<b>6</b>	0	0	1	0	1	0	<b>6</b>	1	1	1	1	0
<b>7</b>	0	1	0	1	1	1	<b>7</b>	0	0	1	1	1
<b>8</b>	0	1	0	1	0	1	<b>8</b>	0	1	0	1	1
<b>9</b>	0	1	1	0	1	1	<b>9</b>	0	1	1	0	1
<b>10</b>	0	1	1	0	1	0	<b>10</b>	0	1	1	1	0
<b>11</b>	1	0	1	1	1	1	<b>11</b>	1	0	0	1	1
<b>12</b>	1	0	1	0	1	1	<b>12</b>	1	0	1	0	1
<b>13</b>	1	0	1	1	0	1	<b>13</b>	1	0	1	1	0
<b>14</b>	1	0	1	1	1	0	<b>14</b>	1	1	0	0	1
<b>15</b>	1	0	1	0	0	1	<b>15</b>	1	1	0	1	0
<b>16</b>	1	0	1	0	1	0	<b>16</b>	1	1	1	0	0
<b>17</b>	1	0	1	1	0	0	<b>17</b>	0	0	0	1	1
<b>18</b>	1	0	1	0	0	0	<b>18</b>	0	0	1	0	1
<b>19</b>	1	1	0	1	1	1	<b>19</b>	0	0	1	1	0
<b>20</b>	1	1	0	1	0	1	<b>20</b>	0	1	0	0	1
<b>21</b>	1	1	0	1	1	0	<b>21</b>	0	1	0	1	0
<b>22</b>	1	1	0	1	0	0	<b>22</b>	0	1	1	0	0
<b>23</b>	1	1	1	0	1	1	<b>23</b>	1	0	0	0	1
<b>24</b>	1	1	1	1	0	1	<b>24</b>	1	0	0	1	0
<b>25</b>	1	1	1	1	1	0	<b>25</b>	1	0	1	0	0
<b>26</b>	1	1	1	0	0	1	<b>26</b>	1	1	0	0	0
<b>27</b>	1	1	1	0	1	0	<b>27</b>	0	0	0	0	1
<b>28</b>	1	1	1	1	0	0	<b>28</b>	0	0	0	1	0
<b>29</b>	1	1	1	0	0	0	<b>29</b>	0	0	1	0	0
							<b>30</b>	0	1	0	0	0
							<b>31</b>	1	0	0	0	0
							<b>32</b>	0	0	0	0	0

II.

A.

	1	2	3	4	5	6	7	8	9	10
<b>1</b>	×	×	×		$19_6$		$19_6$		$19_6$	
<b>2</b>	×	$2_1$	$3_1$			$19_6$	$19_6$			$19_6$
<b>3</b>	$1_2$	$2_1$	$3_1$		$19_6$			$19_6$	$19_6$	
<b>4</b>	$1_2$	×	×		$19_6$		$19_6$		$19_6$	
<b>5</b>	$2_1$	$2_1$		*		$19_6$	$19_6$		$19_6$	
<b>6</b>	$2_1$	$2_1$	$3_1$		$19_6$		$19_6$		$19_6$	
<b>7</b>	$1_2$	$2_1$	$3_1$			$19_6$		$19_6$		$19_6$
<b>8</b>	$1_2$	$2_4$	$3_4$			$19_6$	$19_6$			$19_6$
<b>9</b>	$2_1$	$2_1$		*	$19_6$	$19_6$	$19_6$			$19_6$
<b>10</b>	$2_4$	$2_4$	$3_4$			$19_6$	$19_6$			$19_6$
<b>11</b>	$1_2$	$2_4$	$3_4$		$19_6$			$19_6$	$19_6$	
<b>12</b>	$2_4$	$2_4$		*		$19_6$		$19_6$	$19_6$	
<b>13</b>	$2_1$	$2_1$	$3_1$		$19_6$			$19_6$	$19_6$	
<b>14</b>	$2_1$	$2_4$		*		$19_6$	$19_6$		$19_6$	
<b>15</b>	$2_1$	$2_4$	$3_4$		$19_6$		$19_6$		$19_6$	
<b>16</b>	$2_1$	$2_1$		*		$19_6$	$19_6$		$19_6$	
<b>17</b>	$1_2$	$2_4$	$3_4$			$19_6$		$19_6$		$19_6$
<b>18</b>	$2_4$	$2_4$		*	$19_6$	$19_6$		$19_6$		$19_6$
<b>19</b>	$2_4$	$2_4$	$3_4$			$19_6$		$19_6$		$19_6$
<b>20</b>	$2_1$	$2_4$		*	$19_6$	$19_6$	$19_6$			$19_6$
<b>21</b>	$2_4$	*	*			$19_6$	$19_6$			$19_6$
<b>22</b>	$2_4$	$2_4$		*	$19_6$	$19_6$	$19_6$			$19_6$
<b>23</b>	$2_4$	*		*		$19_6$		$19_6$	$19_6$	
<b>24</b>	$2_1$	$2_4$	$3_4$			$19_6$			$19_6$	$19_6$
<b>25</b>	$2_4$	$2_4$		*		$19_6$		$19_6$	$19_6$	
<b>26</b>	$2_1$	$2_4$		*		$19_6$	$19_6$		$19_6$	
<b>27</b>	$2_4$	*		*	$19_6$	$19_6$		$19_6$		$19_6$
<b>28</b>	$2_4$	*	*			$19_6$		$19_6$		$19_6$
<b>29</b>	*	*		*	$19_6$	$19_6$		$19_6$		$19_6$
<b>30</b>	$2_4$	*		*	$19_6$	$19_6$	$19_6$			$19_6$
<b>31</b>	$2_4$	*		*		$19_6$		$19_6$	$19_6$	
<b>32</b>	*	*		*	$19_6$	$19_6$		$19_6$		$19_6$

B.

II. (continued)

A.

	11	12	13	14	15	16	17	18	19
<b>1</b>	×	19 <sub>1</sub>	×	11 <sub>1</sub>	19 <sub>1</sub>	19 <sub>1</sub>	13 <sub>1</sub>	19 <sub>1</sub>	×
<b>2</b>	25 <sub>2</sub>		×	25 <sub>2</sub>			13 <sub>2</sub>		×
<b>3</b>	11 <sub>1</sub>	19 <sub>2</sub>	13 <sub>1</sub>	24 <sub>2</sub>	21 <sub>2</sub>	19 <sub>2</sub>	13 <sub>1</sub>	21 <sub>2</sub>	
<b>4</b>	24 <sub>2</sub>	19 <sub>2</sub>	13 <sub>1</sub>	24 <sub>2</sub>	19 <sub>1</sub>	19 <sub>2</sub>	13 <sub>1</sub>	19 <sub>1</sub>	19 <sub>2</sub>
<b>5</b>									19 <sub>1</sub>
<b>6</b>	×	19 <sub>2</sub>	×	11 <sub>6</sub>	21 <sub>2</sub>	19 <sub>2</sub>	13 <sub>6</sub>	21 <sub>2</sub>	×
<b>7</b>	25 <sub>2</sub>		13 <sub>2</sub>	25 <sub>2</sub>			13 <sub>2</sub>		
<b>8</b>	25 <sub>2</sub>		13 <sub>2</sub>	25 <sub>2</sub>			13 <sub>2</sub>		19 <sub>2</sub>
<b>9</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	19 <sub>2</sub>
<b>10</b>	25 <sub>10</sub>		×	25 <sub>10</sub>			13 <sub>10</sub>		19 <sub>6</sub>
<b>11</b>	24 <sub>2</sub>	19 <sub>2</sub>	13 <sub>1</sub>	*	21 <sub>2</sub>	19 <sub>2</sub>	13 <sub>1</sub>	21 <sub>2</sub>	
<b>12</b>									
<b>13</b>	11 <sub>6</sub>	*	13 <sub>6</sub>	11 <sub>6</sub>	*	19 <sub>2</sub>	13 <sub>6</sub>	*	
<b>14</b>									19 <sub>2</sub>
<b>15</b>	11 <sub>6</sub>	19 <sub>2</sub>	13 <sub>6</sub>	11 <sub>6</sub>	21 <sub>2</sub>	19 <sub>2</sub>	13 <sub>6</sub>	21 <sub>2</sub>	19 <sub>6</sub>
<b>16</b>									19 <sub>6</sub>
<b>17</b>	25 <sub>2</sub>		13 <sub>2</sub>	25 <sub>2</sub>			13 <sub>2</sub>		
<b>18</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	
<b>19</b>	25 <sub>10</sub>		13 <sub>10</sub>	25 <sub>10</sub>			13 <sub>10</sub>		
<b>20</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	19 <sub>2</sub>
<b>21</b>	25 <sub>10</sub>		13 <sub>10</sub>	25 <sub>10</sub>			13 <sub>10</sub>		19 <sub>6</sub>
<b>22</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	19 <sub>6</sub>
<b>23</b>									
<b>24</b>		11 <sub>6</sub>	19 <sub>2</sub>	13 <sub>6</sub>	11 <sub>6</sub>	*	*	13 <sub>6</sub>	*
<b>25</b>									
<b>26</b>									19 <sub>6</sub>
<b>27</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	
<b>28</b>	25 <sub>10</sub>		13 <sub>10</sub>	25 <sub>10</sub>			13 <sub>10</sub>		
<b>29</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	
<b>30</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	19 <sub>6</sub>
<b>31</b>									
<b>32</b>		19 <sub>6</sub>			21 <sub>6</sub>	19 <sub>6</sub>		21 <sub>6</sub>	

B.



II. (concluded)

	A.									
	20	21	22	23	24	25	26	27	28	29
<b>1</b>	19 <sub>1</sub>	19 <sub>1</sub>	19 <sub>1</sub>	19 <sub>1</sub>	11 <sub>1</sub>	11 <sub>1</sub>	19 <sub>1</sub>	19 <sub>1</sub>	11 <sub>1</sub>	19 <sub>1</sub>
<b>2</b>	19 <sub>2</sub>	×	21 <sub>2</sub>		×	×			25 <sub>2</sub>	
<b>3</b>				19 <sub>2</sub>	25 <sub>2</sub>	24 <sub>2</sub>	21 <sub>2</sub>	19 <sub>2</sub>	25 <sub>2</sub>	21 <sub>2</sub>
<b>4</b>	19 <sub>2</sub>	19 <sub>1</sub>	19 <sub>1</sub>	19 <sub>2</sub>	11 <sub>1</sub>	11 <sub>1</sub>	19 <sub>1</sub>	19 <sub>2</sub>	11 <sub>1</sub>	19 <sub>1</sub>
<b>5</b>	19 <sub>2</sub>	19 <sub>1</sub>	19 <sub>1</sub>	19 <sub>6</sub>	11 <sub>6</sub>	3 <sub>1</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>1</sub>	21 <sub>6</sub>
<b>6</b>	19 <sub>6</sub>	×	21 <sub>6</sub>	19 <sub>1</sub>	3 <sub>1</sub>	11 <sub>6</sub>	19 <sub>1</sub>	19 <sub>2</sub>	3 <sub>1</sub>	19 <sub>1</sub>
<b>7</b>					25 <sub>2</sub>	25 <sub>2</sub>			*	
<b>8</b>	19 <sub>2</sub>	21 <sub>2</sub>	21 <sub>2</sub>		24 <sub>2</sub>	25 <sub>2</sub>			25 <sub>2</sub>	
<b>9</b>	19 <sub>2</sub>	21 <sub>2</sub>	21 <sub>2</sub>		11 <sub>6</sub>	3 <sub>1</sub>			3 <sub>1</sub>	
<b>10</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>		3 <sub>4</sub>	×			3 <sub>4</sub>	
<b>11</b>				19 <sub>2</sub>	25 <sub>2</sub>	24 <sub>2</sub>	21 <sub>2</sub>	19 <sub>2</sub>	25 <sub>2</sub>	21 <sub>2</sub>
<b>12</b>				19 <sub>6</sub>	25 <sub>10</sub>	3 <sub>4</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>4</sub>	21 <sub>6</sub>
<b>13</b>				19 <sub>2</sub>	3 <sub>1</sub>	11 <sub>6</sub>	21 <sub>2</sub>	19 <sub>2</sub>	3 <sub>1</sub>	21 <sub>2</sub>
<b>14</b>	*	19 <sub>1</sub>	19 <sub>1</sub>	19 <sub>6</sub>	11 <sub>6</sub>	3 <sub>1</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>1</sub>	21 <sub>6</sub>
<b>15</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>	19 <sub>2</sub>	3 <sub>1</sub>	11 <sub>6</sub>	19 <sub>1</sub>	*	3 <sub>1</sub>	19 <sub>1</sub>
B. <b>16</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>1</sub>	3 <sub>1</sub>	21 <sub>6</sub>	19 <sub>6</sub>	*	21 <sub>6</sub>
<b>17</b>					25 <sub>2</sub>	25 <sub>2</sub>			*	
<b>18</b>					25 <sub>10</sub>	3 <sub>4</sub>			3 <sub>4</sub>	
<b>19</b>					3 <sub>4</sub>	25 <sub>10</sub>			3 <sub>4</sub>	
<b>20</b>	19 <sub>2</sub>	21 <sub>2</sub>	21 <sub>2</sub>		11 <sub>6</sub>	3 <sub>1</sub>			3 <sub>1</sub>	
<b>21</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>		3 <sub>4</sub>	25 <sub>10</sub>			3 <sub>4</sub>	
<b>22</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>		3 <sub>4</sub>	3 <sub>4</sub>			*	
<b>23</b>				19 <sub>6</sub>	25 <sub>10</sub>	3 <sub>4</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>4</sub>	21 <sub>6</sub>
<b>24</b>				19 <sub>2</sub>	3 <sub>1</sub>	11 <sub>6</sub>	21 <sub>2</sub>	19 <sub>2</sub>	3 <sub>1</sub>	21 <sub>2</sub>
<b>25</b>		21 <sub>6</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>4</sub>	3 <sub>4</sub>	21 <sub>6</sub>	19 <sub>6</sub>	*	21 <sub>6</sub>
<b>26</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>	19 <sub>6</sub>	3 <sub>1</sub>	3 <sub>1</sub>	21 <sub>6</sub>	19 <sub>6</sub>	*	21 <sub>6</sub>
<b>27</b>					25 <sub>10</sub>	3 <sub>4</sub>			3 <sub>4</sub>	
<b>28</b>					3 <sub>4</sub>	25 <sub>10</sub>			3 <sub>4</sub>	
<b>29</b>					*	*			*	
<b>30</b>	19 <sub>6</sub>	21 <sub>6</sub>	21 <sub>6</sub>		3 <sub>4</sub>	3 <sub>4</sub>			*	
<b>31</b>				19 <sub>6</sub>	3 <sub>4</sub>	3 <sub>4</sub>	21 <sub>6</sub>	19 <sub>6</sub>	*	21 <sub>6</sub>
<b>32</b>					*	*			*	

For convenience the groups are divided into cases.

The double Table I gives all cases consistent with congruences (17), (21), (23) and (25). The results of the discussion are given in Table II. The cases in Table II left blank are inconsistent with congruences (22) and (24), and therefore have no groups corresponding to them.

Let  $\kappa = \kappa_1 p^{k_2}$  where  $dv[\kappa_1, p] = 1$  ( $\kappa = a, \beta, c, g, \gamma, d, k, \alpha, \epsilon, e, j$ ).

In explanation of Table II the groups in cases marked  $\boxed{r_s}$  are simply isomorphic with groups in  $A_r B_s$ .

The group  $G'$  is taken from the cases marked  $\boxed{\times}$ . The types are also selected from these cases.

The cases marked  $\boxed{*}$  divide into two or more parts. Let

$$\begin{aligned}
a\epsilon - \alpha e + jk &= I_1, & a\epsilon - jk &= I_2, \\
a\delta(a - e) + 2I_1 &= I_3, & \alpha g - \beta j &= I_4, \\
\alpha\delta - \beta\epsilon &= I_5, & \epsilon g - \delta j &= I_6, \\
c\epsilon - e\gamma &= I_7, & \alpha e - jk &= I_8, \\
\delta e + \gamma j &= I_9, & \alpha\gamma + \delta k &= I_{10}.
\end{aligned}$$

The parts into which these groups divide, and the cases with which they are simply isomorphic, are given in Table III.

### III.

$A_{1,2}B^*$	$dv[I_1, p] = p$	$2_1$	$dv[I_1, p] = 1$	$2_4$
$A_3B^*$	$dv[I_2, p] = p$	$3_1$	$dv[I_2, p] = 1$	$3_4$
$A_4B^*$	$dv[I_3, p] = p$	$3_1$	$dv[I_3, p] = 1$	$3_4$
$A_{12}B_{13}$	$dv[I_4, p] = p$	$19_1$	$dv[I_4, p] = 1$	$19_2$
$A_{14}B_{11}$	$dv[I_5, p] = p$	$11_1$	$dv[I_5, p] = 1$	$24_2$
$A_{15,18}B^*$	$dv[I_4, p] = p$	$19_1$	$dv[I_4, p] = 1$	$21_2$
$A_{16}B_{24}$	$dv[I_6, I_5, p] = p$	$19_1$	$dv[I_6, I_5, p] = 1$	$19_2$
$A_{20}B_{14}$	$dv[I_7, p] = p$	$19_1$	$dv[I_7, p] = 1$	$19_2$
$A_{24,25}B^*$	$dv[I_8, p] = p$	$3_1$	$dv[I_8, p] = 1$	$3_4$
$A_{27}B_{15}$	$dv[I_6, p] = p$	$19_1$	$dv[I_6, p] = 1$	$19_2$
$A_{29}B_{7,17}$	$dv[I_{10}, p] = p$	$24_2$	$dv[I_{10}, p] = 1$	$25_2$
$A_{29}B_{16,26}$	$dv[I_9, p] = p$	$11_6$	$dv[I_9, p] = 1$	$3_1$
$A_{29}B_{22,25,30,31}$	$dv[I_9, p] = p$	$25_{10}$	$dv[I_9, p] = 1$	$3_4$
$A_{29}B_{29,32}$	$dv[I_8, I_9, p] = p$	$11_6$	$[I_8, p] = p, [I_9, p] = 1$	$3_1$
$A_{29}B_{29,32}$	$[I_8, p] = 1, [I_9, p] = p$	$25_{10}$	$[I_8, p] = 1, [I_9, p] = 1$	$3_4$

8. *Types.* The types for this class are given by equations (30) where the constants have the values given in Table IV.

IV.

	$a$	$\beta$	$c$	$g$	$\gamma$	$\delta$	$k$	$\alpha$	$\epsilon$	$e$	$j$
$1_1$	0	0	0	0	0	0	0	0	0	0	0
$2_1$	1	0	0	0	0	0	0	0	0	0	0
$3_1$	$\kappa$	1	0	0	0	0	0	0	0	0	0
$11_1$	0	1	0	0	0	0	0	0	0	0	0
* $13_1$	0	1	0	0	1	0	0	0	0	0	0
$19_1$	0	0	1	0	0	0	0	0	0	0	0
$1_2$	0	0	0	0	0	0	1	0	0	0	0
* $13_2$	0	1	0	0	1	0	1	0	0	0	0
$19_2$	0	0	1	0	0	0	1	0	0	0	0
* $21_2$	0	0	1	0	0	1	1	0	0	0	0
$24_2$	0	0	0	0	1	0	1	0	0	0	0
$25_2$	0	0	0	0	0	1	1	0	0	0	0
$2_4$	1	0	0	0	0	0	0	0	1	0	0
$3_4$	$\kappa$	1	0	0	0	0	0	0	1	0	0
$11_6$	0	1	0	0	0	0	0	0	0	0	1
* $13_6$	0	1	0	0	1	0	0	0	0	0	1

$\kappa = 1$ , and a non-residue (mod  $p$ ).

\*For  $p = 3$  these groups are isomorphic in Class II.

A detailed analysis of congruences (32) for several cases is given below as a general illustration of the methods used.

$A_3B_1$ .

The special forms of the congruences for this case are

- (II)  $\beta'xz' \equiv 0 \pmod{p}$ ,
- (III)  $a'(yz' - y'z) \equiv kx \pmod{p}$ ,
- (IV),(V),(VI)  $\beta v' \equiv 0, \quad \beta z' \equiv 0, \quad \beta y' \equiv \beta'xz'' \pmod{p}$ ,
- (VII)  $a'(yz'' - y''z) + a'\beta'x\binom{z''}{2} \equiv \alpha x + \beta x' + a'\beta y'z \pmod{p}$ ,
- (X)  $a'(y'z'' - y''z') \equiv ax \pmod{p}$ ,
- (XI)  $\gamma v'' + \delta v' \equiv 0 \pmod{p}$ ,
- (XII)  $\gamma z'' + \delta z' \equiv 0 \pmod{p}$ ,
- (XIII)  $\gamma y'' + \delta y' \equiv \beta'xz'' \pmod{p}$ ,
- (XIV)  $a'(yz''' - y'''z) + a'\beta'x\binom{z'''}{2} \equiv \epsilon x + \gamma x'' + \delta x + a'\delta y'z$   
 $+ a'\gamma y''z + a'\binom{\gamma}{2}y''z'' \pmod{p}$ ,
- (XV),(XVI),(XVII)  $cv'' \equiv 0, \quad cz'' \equiv 0, \quad cy'' \equiv 0 \pmod{p}$ ,
- (XVIII)  $a'(y'z''' - y'''z') \equiv ex \pmod{p}$ ,

$$\begin{aligned}
& \text{(XIX),(XX),(XXI)} & gv' \equiv 0, & \quad gz' \equiv 0, & \quad gy' \equiv 0 \pmod{p}, \\
& \text{(XXII)} & a'(y''z''' - y'''z'') \equiv jx \pmod{p},
\end{aligned}$$

From (II)  $z' \equiv 0 \pmod{p}$ .

The conditions of isomorphism give

$$\Delta \equiv \begin{vmatrix} v' & v'' & v''' \\ y' & y'' & y''' \\ z' & z'' & z''' \end{vmatrix} \not\equiv 0 \pmod{p}.$$

Multiply (IV), (V), (VI) by  $\gamma$  and reduce by (XII),  $\beta\gamma v' \equiv 0$ ,  $\beta\gamma z' \equiv 0$ ,  $\beta\gamma y' \equiv 0 \pmod{p}$ . Since  $\Delta \not\equiv 0 \pmod{p}$ , one at least of the quantities,  $v'$ ,  $z'$  or  $y'$  is  $\not\equiv 0 \pmod{p}$  and  $\beta\gamma \equiv 0 \pmod{p}$ .

From (XV), (XVI) and (XVII)  $c \equiv 0 \pmod{p}$ , and from (XIX), (XX) and (XXI)  $g \equiv 0 \pmod{p}$ .

From (IV), (V), (VI) and (X) if  $a \equiv 0$ , then  $\beta \equiv 0$  and if  $a \not\equiv 0$ , then  $\beta \not\equiv 0 \pmod{p}$ .

At least one of the three quantities  $\beta$ ,  $\gamma$  or  $\delta$  is  $\not\equiv 0 \pmod{p}$  and one, at least, of  $a$ ,  $e$  or  $j$  is  $\not\equiv 0 \pmod{p}$ .

$A_3$ : Since  $z''' \equiv 0 \pmod{p}$ , (XVIII) gives  $e \equiv 0$ . Elimination between (III), (X), (XIV) and (XXII) gives  $a\epsilon - kj \equiv 0 \pmod{p}$ . Elimination between (VI) and (X) gives  $a'\beta'z''^2 \equiv a\beta \pmod{p}$  and  $a\beta$  is a quadratic residue or non-residue according as  $a'\beta'$  is or is not, and there are two types for this case.

$A_4$ : Since  $y'$  and  $z''$  are  $\not\equiv 0 \pmod{p}$ ,  $e \not\equiv 0 \pmod{p}$ . Elimination between (VI), (X), (XIII) and (XVIII) gives  $a\delta - \beta e \equiv 0 \pmod{p}$ .

This is a special form of (24).

Elimination between (III), (VII), (X), (XIII), (XIV), (XVIII) and (XXII) gives

$$2jk + a\delta(a - e) + 2(a\epsilon - \alpha e) \equiv 0 \pmod{p}.$$

$A_{24}$ : Since from (XI), (XII) and (XIII)  $y''$  and  $z''' \not\equiv 0 \pmod{p}$ , and  $z'' \equiv v'' \equiv 0 \pmod{p}$ , (xxii) gives  $j \not\equiv 0 \pmod{p}$ .

Elimination between (III), (X), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod{p}.$$

$A_{25}$ : (XI), (XII) and (XIII) give  $v' \equiv z' \equiv 0$  and  $y', z''' \not\equiv 0 \pmod{p}$  and this with (XVIII) gives  $e \not\equiv 0$ .

Elimination between (III), (VII), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod{p}.$$

$A_{28}$ : Since  $a \equiv 0$  then  $e$  or  $j \not\equiv 0 \pmod{p}$ .

Elimination between (III), (VII), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod{p}.$$

Multiply (XIII) by  $a'z'''$  and reduce

$$\delta e + \gamma j \equiv a' \beta' z''^2 \not\equiv 0 \pmod{p}.$$

$$A_{11}B_1.$$

The special forms of the congruences for this case are

$$\begin{aligned} \text{(II)} & \quad \beta' x z' \equiv 0 \pmod{p}, \\ \text{(III)} & \quad kx \equiv 0 \pmod{p}, \\ \text{(IV),(V),(VI)} & \quad \beta v' \equiv \beta z' \equiv 0, \quad \beta y' \equiv \beta' x z'', \\ \text{(VII)} & \quad \alpha x + \beta x' \equiv 0 \pmod{p}, \\ \text{(X)} & \quad ax \equiv 0 \pmod{p}, \\ \text{(XI)} & \quad \gamma v'' + \delta v \equiv 0 \pmod{p}, \\ \text{(XII)} & \quad \gamma z'' + \delta z \equiv 0 \pmod{p}, \\ \text{(XIII)} & \quad \gamma y'' + \delta y \equiv \beta' x z''' \pmod{p}, \\ \text{(XIV)} & \quad \epsilon x + \gamma x'' + \delta x' \equiv 0 \pmod{p}, \\ \text{(XV),(XVI),(XVII)} & \quad cv'' \equiv cz'' \equiv cy'' \equiv 0 \pmod{p}, \\ \text{(XVIII)} & \quad ex \equiv 0 \pmod{p}, \\ \text{(XIX),(XX),(XXI)} & \quad gv' \equiv gz' \equiv gy' \equiv 0 \pmod{p}, \\ \text{(XXII)} & \quad jx \equiv 0 \pmod{p}, \end{aligned}$$

(II) gives  $z' = 0$ , (III) gives  $k \equiv 0$ , (X) gives  $a \equiv 0$ , (XV), (XVI), (XVII) give  $c \equiv 0$  ( $\Delta \neq 0$ ), (XVIII) gives  $e \equiv 0$ , (XIX), (XX), (XXI) give  $g \equiv 0$ , (XXII) gives  $j \equiv 0$ . One of the two quantities  $z''$  or  $z''' \not\equiv 0 \pmod{p}$ , and by (VI) and (XIII) one of the three quantities  $\beta$ ,  $\gamma$  or  $\delta$  is  $\neq 0$ .

$A_{11}$ : (XIV) gives  $\epsilon \equiv 0 \pmod{p}$ . Multiplying (IV), (V), (VI) by  $\gamma$  gives, by (XII),  $\beta\gamma v' \equiv \beta\gamma z' \equiv \beta\gamma y' \equiv 0 \pmod{p}$ , and  $\beta\gamma \equiv 0 \pmod{p}$ .

$A_{14}$ : Elimination between (VII) and (XIV) gives  $\alpha\delta - \beta\epsilon \equiv 0 \pmod{p}$ .

$A_{24}$ : (VII) gives  $\alpha \equiv 0 \pmod{p}$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{25}$ : (VII) gives  $\alpha \equiv 0 \pmod{p}$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{28}$ : (VII) gives  $\alpha \equiv 0 \pmod{p}$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{19}B_1$ .

The special forms of the congruences for this case are

- (I)  $c'(yv' - y'v) \equiv 0 \pmod{p}$ ,
- (III)  $kx \equiv 0 \pmod{p}$ ,
- (IV),(V),(VI)  $\beta v \equiv 0, \beta z \equiv c'(yv'' - y''v), \beta y' \equiv 0 \pmod{p}$ ,
- (VII)  $\alpha x + \beta x' \equiv 0 \pmod{p}$ ,
- (VIII)  $c'(y'v'' - y''v') \equiv 0 \pmod{p}$ ,
- (X)  $ax \equiv 0 \pmod{p}$ ,
- (XI)  $\gamma v'' + \delta v' \equiv 0 \pmod{p}$ ,
- (XII)  $\gamma z'' + \delta z' + c'\gamma\delta y''v + c'(\binom{\delta}{2})v'y' + c'(\binom{\gamma}{2})v''y'' \equiv c'(yv''' - y'''v) \pmod{p}$ ,
- (XIII)  $\gamma y'' + \delta y' \equiv 0 \pmod{p}$ ,
- (XIV)  $\epsilon x + \gamma x'' + \delta x' \equiv 0 \pmod{p}$ ,
- (XV),(XVI),(XVII)  $cv'' \equiv 0, cz'' \equiv c'(y'v''' - y'''v'), cy'' \equiv 0 \pmod{p}$ ,
- (XVIII)  $ex + cx'' \equiv 0 \pmod{p}$ ,
- (XIX),(XX),(XXI)  $gv' \equiv 0, gz' \equiv c'(y''v''' - y'''v''), gy' \equiv 0 \pmod{p}$ ,
- (XXII)  $jx + gx' \equiv 0 \pmod{p}$ .

(III) gives  $k \equiv 0$ , (X) gives  $a \equiv 0$ .

Since  $dv[(y'v''' - y'''v'), (y''v''' - y'''v''), p] = 1$  then  $dv[c, g, p] = 1$ .

If  $c \not\equiv 0, v'' \equiv y'' \equiv 0 \pmod{p}$  and therefore  $g \equiv 0 \pmod{p}$  and if  $g \not\equiv 0$ , then  $c \equiv 0 \pmod{p}$ .

$A_{12}$ : (XVIII) gives  $e \equiv 0 \pmod{p}$ . Elimination between (VII) and (XXII) gives  $\alpha g - \beta j \equiv 0 \pmod{p}$ , (XIV) gives  $\epsilon \equiv 0 \pmod{p}$ .

$A_{15}$ : (XVIII) gives  $e \equiv 0 \pmod{p}$ . Elimination between (VII) and (XXII) gives  $\alpha g - \beta j \equiv 0 \pmod{p}$ , (XIV) gives  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{16}$ : (XVIII) gives  $e \equiv 0$ . Elimination between (XIV) and (XXII) gives  $\epsilon g - \delta j \equiv 0 \pmod{p}$ , between (VII) and (XIV) gives  $\alpha\delta - \beta\epsilon \equiv 0$ .

$A_{18}$ : (XVIII) gives  $e \equiv 0 \pmod{p}$ . Elimination between (VII) and (XXII) gives  $\alpha g - \beta j \equiv 0 \pmod{p}$ , (XIV) gives  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{19}$ : (VII) gives  $\alpha \equiv 0 \pmod{p}$ , (XIV) gives  $\epsilon \equiv 0$ , (XXII) gives  $j \equiv 0 \pmod{p}$ , (XVIII) gives  $e \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{20}$ : (VII) gives  $\alpha \equiv 0$ , (XXII) gives  $j \equiv 0$ . Elimination between (XIV) and (XVIII) gives  $\epsilon c - e\gamma \equiv 0 \pmod{p}$ .

$A_{21}$ : (VII) gives  $\alpha \equiv 0$ , (XIV) gives  $\epsilon \equiv 0$  or  $\not\equiv 0 \pmod{p}$ , (XVIII) gives  $e \equiv 0$ , or  $\not\equiv 0$ , and (XXII) gives  $j \equiv 0 \pmod{p}$ .

$A_{22}$ : (VII) gives  $\alpha \equiv 0$ , (XIV) gives  $\epsilon \equiv 0$  or  $\not\equiv 0$ , (XVIII) gives  $\epsilon \equiv 0$  or  $\not\equiv 0$ , (XXII) gives  $j \equiv 0 \pmod{p}$ .

$A_{23}$ : (VII) gives  $\alpha \equiv 0$ , (XIV) gives  $\epsilon \equiv 0$ , (XVIII) gives  $\epsilon \equiv 0$ , (XXII) gives  $j \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{26}$ : (VII)  $\alpha \equiv 0$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0$ , (XVIII)  $\epsilon \equiv 0$ , (XXII)  $j \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

$A_{27}$ : (VII)  $\alpha \equiv 0$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0$ , (XVIII)  $\epsilon \equiv 0$ , (XXII)  $j \equiv 0$  or  $\not\equiv 0 \pmod{p}$ . Elimination between (XIV) and (XXII) gives  $\epsilon g - \delta j \equiv 0 \pmod{p}$ .

$A_{29}$ : (VII)  $\alpha \equiv 0$ , (XIV)  $\epsilon \equiv 0$  or  $\not\equiv 0$ , (XVIII)  $\epsilon \equiv 0$ , (XXII)  $j \equiv 0$  or  $\not\equiv 0 \pmod{p}$ .

End of the Project Gutenberg EBook of Groups of Order  $p^m$  Which Contain  
Cyclic Subgroups of Order  $p^{(m-3)}$ , by Lewis Irving Neikirk

\*\*\* END OF THE PROJECT GUTENBERG EBOOK GROUPS OF ORDER  $P^M$  \*\*\*

This file should be named grdpm10p.pdf or grdpm10p.zip  
Corrected EDITIONS of our eBooks get a new NUMBER, grdpm11p.pdf  
VERSIONS based on separate sources get new LETTER, grdpm10ap.pdf

Produced by Cornell University, Joshua Hutchinson, Lee Chew-Hung,  
John Hageron, and the Online Distributed Proofreading Team.

Project Gutenberg eBooks are often created from several printed  
editions, all of which are confirmed as Public Domain in the US  
unless a copyright notice is included. Thus, we usually do not  
keep eBooks in compliance with any particular paper edition.

We are now trying to release all our eBooks one year in advance  
of the official release dates, leaving time for better editing.  
Please be encouraged to tell us about any error or corrections,  
even years after the official publication date.

Please note neither this listing nor its contents are final til  
midnight of the last day of the month of any such announcement.  
The official release date of all Project Gutenberg eBooks is at  
Midnight, Central Time, of the last day of the stated month. A  
preliminary version may often be posted for suggestion, comment  
and editing by those who wish to do so.

Most people start at our Web sites at:  
<http://gutenberg.net> or  
<http://promo.net/pg>

These Web sites include award-winning information about Project  
Gutenberg, including how to donate, how to help produce our new  
eBooks, and how to subscribe to our email newsletter (free!).

Those of you who want to download any eBook before announcement  
can get to them as follows, and just download by date. This is  
also a good way to get them instantly upon announcement, as the  
indexes our cataloguers produce obviously take a while after an  
announcement goes out in the Project Gutenberg Newsletter.

<http://www.ibiblio.org/gutenberg/etext03> or  
<ftp://ftp.ibiblio.org/pub/docs/books/gutenberg/etext03>



Or /etext02, 01, 00, 99, 98, 97, 96, 95, 94, 93, 92, 91 or 90

Just search by the first five letters of the filename you want,  
as it appears in our Newsletters.

Information about Project Gutenberg (one page)

We produce about two million dollars for each hour we work. The time it takes us, a rather conservative estimate, is fifty hours to get any eBook selected, entered, proofread, edited, copyright searched and analyzed, the copyright letters written, etc. Our projected audience is one hundred million readers. If the value per text is nominally estimated at one dollar then we produce \$2 million dollars per hour in 2002 as we release over 100 new text files per month: 1240 more eBooks in 2001 for a total of 4000+ We are already on our way to trying for 2000 more eBooks in 2002 If they reach just 1-2% of the world's population then the total will reach over half a trillion eBooks given away by year's end.

The Goal of Project Gutenberg is to Give Away 1 Trillion eBooks! This is ten thousand titles each to one hundred million readers, which is only about 4% of the present number of computer users.

Here is the briefest record of our progress (\* means estimated):

eBooks Year Month

1	1971	July
10	1991	January
100	1994	January
1000	1997	August
1500	1998	October
2000	1999	December
2500	2000	December
3000	2001	November
4000	2001	October/November
6000	2002	December*
9000	2003	November*
10000	2004	January*

The Project Gutenberg Literary Archive Foundation has been created to secure a future for Project Gutenberg into the next millennium.

We need your donations more than ever!

As of February, 2002, contributions are being solicited from people and organizations in: Alabama, Alaska, Arkansas, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Illinois,

Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

We have filed in all 50 states now, but these are the only ones that have responded.

As the requirements for other states are met, additions to this list will be made and fund raising will begin in the additional states. Please feel free to ask to check the status of your state.

In answer to various questions we have received on this:

We are constantly working on finishing the paperwork to legally request donations in all 50 states. If your state is not listed and you would like to know if we have added it since the list you have, just ask.

While we cannot solicit donations from people in states where we are not yet registered, we know of no prohibition against accepting donations from donors in these states who approach us with an offer to donate.

International donations are accepted, but we don't know ANYTHING about how to make them tax-deductible, or even if they CAN be made deductible, and don't have the staff to handle it even if there are ways.

Donations by check or money order may be sent to:

Project Gutenberg Literary Archive Foundation  
PMB 113  
1739 University Ave.  
Oxford, MS 38655-4109

Contact us if you want to arrange for a wire transfer or payment method other than by check or money order.

The Project Gutenberg Literary Archive Foundation has been approved by the US Internal Revenue Service as a 501(c)(3) organization with EIN [Employee Identification Number] 64-622154. Donations are tax-deductible to the maximum extent permitted by law. As fund-raising requirements for other states are met, additions to this list will be made and fund-raising will begin in the additional states.

We need your donations more than ever!

You can get up to date donation information online at:

<http://www.gutenberg.net/donation.html>

\*\*\*

If you can't reach Project Gutenberg,  
you can always email directly to:

Michael S. Hart <hart@pobox.com>

Prof. Hart will answer or forward your message.

We would prefer to send you information by email.

**\*\*The Legal Small Print\*\***

(Three Pages)

**\*\*\*START\*\*THE SMALL PRINT!\*\*FOR PUBLIC DOMAIN EBOOKS\*\*START\*\*\***  
Why is this "Small Print!" statement here? You know: lawyers. They tell us you might sue us if there is something wrong with your copy of this eBook, even if you got it for free from someone other than us, and even if what's wrong is not our fault. So, among other things, this "Small Print!" statement disclaims most of our liability to you. It also tells you how you may distribute copies of this eBook if you want to.

**\*BEFORE!\* YOU USE OR READ THIS EBOOK**

By using or reading any part of this PROJECT GUTENBERG-tm eBook, you indicate that you understand, agree to and accept this "Small Print!" statement. If you do not, you can receive a refund of the money (if any) you paid for this eBook by sending a request within 30 days of receiving it to the person you got it from. If you received this eBook on a physical medium (such as a disk), you must return it with your request.

**ABOUT PROJECT GUTENBERG-TM EBOOKS**

This PROJECT GUTENBERG-tm eBook, like most PROJECT GUTENBERG-tm eBooks, is a "public domain" work distributed by Professor Michael S. Hart through the Project Gutenberg Association (the "Project"). Among other things, this means that no one owns a United States copyright on or for this work, so the Project (and you!) can copy and distribute it in the United States without permission and without paying copyright royalties. Special rules, set forth below, apply if you wish to copy and distribute this eBook under the "PROJECT GUTENBERG" trademark.

Please do not use the "PROJECT GUTENBERG" trademark to market any commercial products without permission.

To create these eBooks, the Project expends considerable efforts to identify, transcribe and proofread public domain works. Despite these efforts, the Project's eBooks and any medium they may be on may contain "Defects". Among other things, Defects may take the form of incomplete, inaccurate or corrupt data, transcription errors, a copyright or other intellectual property infringement, a defective or damaged disk or other eBook medium, a computer virus, or computer codes that damage or cannot be read by your equipment.

#### LIMITED WARRANTY; DISCLAIMER OF DAMAGES

But for the "Right of Replacement or Refund" described below, [1] Michael Hart and the Foundation (and any other party you may receive this eBook from as a PROJECT GUTENBERG-tm eBook) disclaims all liability to you for damages, costs and expenses, including legal fees, and [2] YOU HAVE NO REMEDIES FOR NEGLIGENCE OR UNDER STRICT LIABILITY, OR FOR BREACH OF WARRANTY OR CONTRACT, INCLUDING BUT NOT LIMITED TO INDIRECT, CONSEQUENTIAL, PUNITIVE OR INCIDENTAL DAMAGES, EVEN IF YOU GIVE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

If you discover a Defect in this eBook within 90 days of receiving it, you can receive a refund of the money (if any) you paid for it by sending an explanatory note within that time to the person you received it from. If you received it on a physical medium, you must return it with your note, and such person may choose to alternatively give you a replacement copy. If you received it electronically, such person may choose to alternatively give you a second opportunity to receive it electronically.

THIS EBOOK IS OTHERWISE PROVIDED TO YOU "AS-IS". NO OTHER WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ARE MADE TO YOU AS TO THE EBOOK OR ANY MEDIUM IT MAY BE ON, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimers of implied warranties or the exclusion or limitation of consequential damages, so the above disclaimers and exclusions may not apply to you, and you may have other legal rights.

#### INDEMNITY

You will indemnify and hold Michael Hart, the Foundation, and its trustees and agents, and any volunteers associated with the production and distribution of Project Gutenberg-tm

texts harmless, from all liability, cost and expense, including legal fees, that arise directly or indirectly from any of the following that you do or cause: [1] distribution of this eBook, [2] alteration, modification, or addition to the eBook, or [3] any Defect.

DISTRIBUTION UNDER "PROJECT GUTENBERG-tm"

You may distribute copies of this eBook electronically, or by disk, book or any other medium if you either delete this "Small Print!" and all other references to Project Gutenberg, or:

- [1] Only give exact copies of it. Among other things, this requires that you do not remove, alter or modify the eBook or this "small print!" statement. You may however, if you wish, distribute this eBook in machine readable binary, compressed, mark-up, or proprietary form, including any form resulting from conversion by word processing or hypertext software, but only so long as \*EITHER\*:
  - [\*] The eBook, when displayed, is clearly readable, and does \*not\* contain characters other than those intended by the author of the work, although tilde (~), asterisk (\*) and underline (\_) characters may be used to convey punctuation intended by the author, and additional characters may be used to indicate hypertext links; OR
  - [\*] The eBook may be readily converted by the reader at no expense into plain ASCII, EBCDIC or equivalent form by the program that displays the eBook (as is the case, for instance, with most word processors); OR
  - [\*] You provide, or agree to also provide on request at no additional cost, fee or expense, a copy of the eBook in its original plain ASCII form (or in EBCDIC or other equivalent proprietary form).
- [2] Honor the eBook refund and replacement provisions of this "Small Print!" statement.
- [3] Pay a trademark license fee to the Foundation of 20% of the gross profits you derive calculated using the method you already use to calculate your applicable taxes. If you don't derive profits, no royalty is due. Royalties are payable to "Project Gutenberg Literary Archive Foundation" the 60 days following each date you prepare (or were legally required to prepare) your annual (or equivalent

periodic) tax return. Please contact us beforehand to let us know your plans and to work out the details.

WHAT IF YOU \*WANT\* TO SEND MONEY EVEN IF YOU DON'T HAVE TO?  
Project Gutenberg is dedicated to increasing the number of public domain and licensed works that can be freely distributed in machine readable form.

The Project gratefully accepts contributions of money, time, public domain materials, or royalty free copyright licenses. Money should be paid to the:  
"Project Gutenberg Literary Archive Foundation."

If you are interested in contributing scanning equipment or software or other items, please contact Michael Hart at:  
hart@pobox.com

[Portions of this eBook's header and trailer may be reprinted only when distributed free of all fees. Copyright (C) 2001, 2002 by Michael S. Hart. Project Gutenberg is a TradeMark and may not be used in any sales of Project Gutenberg eBooks or other materials be they hardware or software or any other related product without express permission.]

\*END THE SMALL PRINT! FOR PUBLIC DOMAIN EBOOKS\*Ver.02/11/02\*END\*