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

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,† 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.‡

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 pth power of every operator in G is contained in $\{P\}$.

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

* Presented to the Society April, 25, 1903. Received for publication August 16, 1904, and February 25, 1905.

† *Theory of Groups of a Finite Order*, pp. 75–81.

‡ Transactions, vol. 2 (1901), p. 259, and vol. 3 (1902), p. 383.

I.

	I	II_1	II_2	II_3	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

The number of groups of order p^m, with cyclic subgroups of orders p^m, p^{m-1}, and p^{m-2}, are given in Table II:

II.

	p^m	p^{m-1}	p^{m-2}
$p>2$ $m>5$	1	2*	11†

The number of groups of order p^α, $\alpha = 1, 2, 3, 4, 5$ are given in Table III:

III.

	$\alpha=1$	$\alpha=2$‡	$\alpha=3$‡	$\alpha=4$‡	$\alpha=5$§
$p=2$	1	2	5	14	51
$p=3$	1	2	5	15	66
$p=12k-1$	1	2	5	15	$65+2p$
$p=12k+5$	1	2	5	15	$67+2p$
$p=12k-5$	1	2	5	15	$69+2p$
$p=12k+1$	1	2	5	15	$71+2p$

* BURNSIDE, *Theory of Groups*, Art. 65, p. 75.

† Ibid., Art. 66, p. 77; MILLER, Transactions, vol. 2 (1901), p. 259, and vol. 3 (1902), p. 383.

‡ YOUNG, *On the determination of groups whose order is a power of a prime*, American Journal of Mathematics, vol. 15 (1893), pp. 124-178. COLE and GLOVER, *On groups whose orders are the product of three prime factors*, American Journal of Mathematics, vol. 15 (1893), pp. 191-220. HÖLDER, *Die Gruppen der Ordnungen*, p^3, pq^2, pqr, p^4, Mathematische Annalen, vol. 43 (1893), pp. 301-412.

§ BAGNERA, *La composizione dei gruppi finiti il cui grado è la quinta potenza di un numero primo*, Annali di Matematica, vol. 3 (1898), pp. 137-228.

I give in this paper the whole investigation of Class I, but only the results of Classes II, and III. The investigation as a whole will appear in the Publications of the University of Pennsylvania, Mathematics, no. 3.

Class I.

1. *General notations and relations.* — The group G is generated by the two operators P and Q_1. For brevity we set*

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

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

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

We have the relation

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

There is in G, a subgroup H_1 of order p^{m-2}, which contains $\{P\}$ self-conjugately.† 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 $H_2 = \{Q_1^y, P\}$ of order p^{m-1}, and H_2 is self-conjugate in G.

From these considerations we have the equations

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

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

$$(4) \qquad Q_1^{-1} P\, Q_1 = Q_1^{hp} P^{\alpha_1}.$$

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,

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

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

---

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

† BURNSIDE: *Theory of Groups*, art. 54, p. 64.

‡ BURNSIDE: *Theory of Groups*, art. 56, p. 66.

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

Hence, by (2),

$$\beta\frac{\alpha_1^{p}-1}{\alpha_1-1}p^2 \equiv 0 \pmod{p^3},$$

$$1+\frac{\beta k}{2}\frac{\alpha_1^{p}-1}{\alpha_1-1}p^{m-4}\Big\} + \beta\frac{\alpha_1^{p}-1}{\alpha_1-1}hp^2 \equiv 1 + kp^{m-4} \pmod{p^{m-3}}.$$

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

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

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

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

Equation (3) is now replaced by

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

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

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

A continued use of this equation gives

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

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

$$[-p, 1, p] = [Np, \alpha_1^{p} + Mp^2].$$

From the above equation and (7),

$$\alpha_1^{p} \equiv 1 \pmod{p^2}, \qquad \alpha_1 \equiv 1 \pmod{p}.$$

Set

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

and equation (4) becomes

$$Q_1^{-1} P Q_1 = Q_1^{hp} P^{1+a_2 p}. \tag{9}$$

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,

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

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),

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

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

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

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

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

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

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

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

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

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

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

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

A combination of the last equation with (8) yields

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

From (12) we get

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

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

$$a = a_1 p^\lambda, \; b = b_1 p^\mu,$$

where

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

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

$$G(a, b): \begin{cases} Q^{-1}PQ = Q^{b_1 p^\mu + 1} P^{1 + a_1 p^{m+\lambda-6}}, \\ Q^{p^3} = 1, \; P^{p^{m-3}} = 1. \end{cases}$$

---

*For $m = 7$, $ap^2 - a^2p^3/2 \equiv ap^2 \pmod{p^4}$, $ap^3 \equiv kp^3 \pmod{p^4}$. 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.

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

‡For $m = 8$ it is necessary to add the term $\frac{1}{2}axy\tbinom{s}{2}\left[\frac{1}{3}y(2s-1) - 1\right]p^4$ to the exponent of P, and for $m = 7$ the terms

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

with the extra terms

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

for $p = 3$, to the exponent of P, and the terms

$$\frac{ab}{2}\left\{\frac{2s-1}{3}y - 1\right\}\tbinom{s}{2}xyp^2$$

to the exponent of Q.

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

$$Q_1' = Q'^{y'} P'^{x' p^{m-6}}, \text{ and } P_1' = Q'^{y} P'^{x},$$

with y' and x prime to p.

Since

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

then

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

or in terms of Q', and P'

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

and

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

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

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

$$b_1 p^\mu \equiv b_1' x p^{\mu'} + b_1'^2\binom{x}{2}p^{2\mu'+1} \pmod{p^2},$$

$$a_1 x p^\lambda + b_1 x' p^{\mu+1} \equiv y'\{a_1' x p^{\lambda'} + a_1' b_1'\binom{x}{2}p^{\lambda'+\mu'+1} + a_1' b_1'^2\binom{x}{3}p^{\lambda'+2\mu'+2}\} \pmod{p^3}.$$

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 $\lambda' \geqq \mu + 1 = \mu' + 1$ when we will so choose x' that $\lambda = 3$.

The type groups of Class I for $m > 8$* are then given by

$$\text{(I)} \qquad G(p^\lambda, p^\mu) : Q^{-1}PQ = Q^{p^{1+\mu}} P^{1+p^{m-6+\lambda}},\ Q^{p^3} = 1,\ P^{p^{m-3}} = 1, \qquad \begin{pmatrix} \mu = 0, 1, 2;\ \lambda = 0, 1, 2, \lambda \leqq \mu; \\ \mu = 0, 1, 2;\ \lambda = 3. \end{pmatrix}$$

Of the above groups $G(p^\lambda, p^\mu)$ the groups for $\mu = 2$ have the cyclic sub-

* For $m = 8$ the additional term ayp appears on the left side of congruence (14) and $G(1, p^2)$ and $G(1, p)$ becomes 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 $G(1, p^2)$ become simply isomorphic, also $G(p, p)$ and $G(p, p^2)$.

group $\{P\}$ self-conjugate, while the group $G(p^3, p^2)$ is the abelian group of type $(m-3, 3)$.

Class II.

1. *Sections.* — Class II is divided into three sections.
2. *Types.* — The types of Section I ($m > 5$) are defined by

$$(\mathrm{II}_1)\begin{cases} Q^{-1}PQ = Q^{\beta h}P^{1+\alpha p^{m-5}}, \\ R^{-1}PR = Q^{hp}P^{1+\alpha p^{m-4}}, \\ R^{-1}QR = Q^{1+dp}P^{cp^{m-4}}, \\ R^p = Q^{p^2} = P^{p^{m-3}} = 1, \end{cases}$$

where the constants have the values given in the table below,

(II_1)

	a	b	α	β	c	d		a	b	α	β	c	d
1	0	0	1	0	0	1	10	1	0	p	0	0	0
2	0	0	1	0	0	0	11	0	0	p	1	0	0
3	0	0	1	1	0	0	12	0	0	p	0	1	0
4	0	0	1	0	1	0	13	1	0	p	1	0	0
5	0	1	1	0	κ	0	14	0	1	p	0	κ	0
6	0	0	1	1	1	0	15	0	0	p	1	1	0
7	ω	0	p	0	0	1	16	0	0	0	0	0	0
8	0	0	0	0	0	1	17	0	1	0	0	0	0
9	0	0	p	0	0	0							

$\kappa = 0, 1$, and a non-residue (mod p),

$\omega = 0, 1, 2, \cdots, p-1$.

The types of Section 2 are defined by

$$(\mathrm{II}_2)\begin{cases} R^{-1}PR = P^{1+kp^{m-4}}, \\ Q^{-1}PQ = RP^{1+\epsilon p^{m-5}}, \\ Q^{-1}RQ = Q^{rp}RP^{\epsilon p^{m-4}}, \\ R^p = Q^{p^2} = P^{p^{m-3}} = 1, \end{cases}$$

where the values of the constants are given in the following table:

(II_2)

	k	ϵ	c	e
1	1	1	0	0
2	0	1	1	0
3	0	1	0	ω
4	0	p	ω	0
5	0	p	1	0
6	0	p	0	κ

$\kappa = 0$, 1, and a non-residue (mod p),

$\omega = 0, 1, 2, \cdots, p-1$.

The groups of Section 3 are defined by

$$(\mathrm{II}_3)\begin{cases} Q^{-1}PQ = PR^{\gamma 1+\epsilon p^{m-5}}, \\ Q^{-1}RQ = RP^{\epsilon p^{m-4}}, \\ R^{-1}PR = Q^p P, \\ R^p = Q^{p^2} = P^{p^{m-3}} = 1, \end{cases}$$

with the values $\gamma = 1$ and a non-residue (mod p); $\epsilon = 1$, $e = 0, 1, 2, \cdots, p-1$, and $\epsilon = p$, $e = 0$, 1, and a non-residue (mod p), $2p + 6$ groups in all.

Class III.

Types. — The types of Class III are defined by

$$(\mathrm{III})\begin{cases} Q^{-1}PQ = P^{1+kp^{m-4}}, \\ R^{-1}PR = Q^\beta P, \\ R^{-1}QR = QP^{\alpha p^{m-4}}, \\ S^{-1}PS = R^\gamma Q^\delta P^{1+\epsilon p^{m-4}}, \\ S^{-1}QS = R^c Q, \\ S^{-1}RS = RP^{jp^{m-4}}, \end{cases}$$

where the constants have the values given in the table:

(III)

	α	β	c	γ	δ	k	ϵ	j		α	β	c	γ	δ	k	ϵ	j
1	0	0	0	0	0	0	0	0	10	0	0	0	0	1	1	0	0
2	1	0	0	0	0	0	0	0	11	1	0	0	0	0	0	1	0
3	κ	1	0	0	0	0	0	0	12	κ	1	0	0	0	0	1	0
4*	0	1	0	1	0	0	0	0	13	0	1	0	0	0	0	0	1
5	0	0	1	0	0	0	0	0	14*	0	1	0	1	0	0	0	1
6	0	0	0	0	0	1	0	0	15	0	0	1	0	0	0	0	1
7*	0	1	0	1	0	1	0	0	16*	0	0	1	0	1	0	0	1
8	0	0	1	0	0	1	0	0	17*	0	1	0	κ	0	1	0	1
9*	0	0	1	0	1	1	0	0									

$\kappa = 0$, 1, and a non-residue (mod p).

* These groups for $p = 3$ ($k \neq 0$) are simply isomorphic with groups in Class II.

UNIVERSITY OF PENNSYLVANIA,
February 23, 1905.