TOPICS IN THE ISOMORPHISM OF GROUP RINGS

by

ALI AKBAR MEHRVARZ

Presented for the Degree of

Doctor of Philosophy in Mathematics

University of Stirling,
Stirling

May, 1979

CONTENTS

ACKNOWLEDGEMENTS

I am indebted to Professor D A R Wallace, who was my Supervisor during my years as a research student, for his assistance, patience and encouragement. I shall always be grateful.

I wish to thank the entire members of the Department of Mathematics for useful discussions and friendly dispositions. I should like to thank the University of Tabriz for granting me study leave for a period of three years.

My thanks are also due to the members of my family for their patience.

I wish to thank Mrs May Abrahamson for the skill and patience with which she typed this thesis.

INTRODUCTION

Let R be a ring and let G be a group. The group ring $R(G)$ of G over R is the free left R-module over the set of elements of G as a basis in which the multiplication induced by G is extended linearly to $R(G)$, [12].

A twisted group ring $R^{\gamma}(G)$ of G over R is an R-algebra with basis $\{\overline{g} | g \in G\}$ and with an associative multiplication $\overline{g}\,\overline{h} = \gamma(g, h)\,\overline{gh}$ for all $g, h \in G$, where $\gamma(g, h)$ is a unit in the centre of R, [13].

In [5] Higman proved that the only units of finite order in the group ring $R(G)$, where R is the ring of rational integers and G is a finite abelian group, are $\pm g$, $g \in G$. In [16] Sehgal proved that the only units of finite order in the group ring $R(G)$, where R is the ring of rational integers and G is an arbitrary abelian group, are $\pm t$ where t is a torsion element of G. Moreover in [16] he proved that the units of $R(G)$, where R is an integral domain and G is a torsion-free abelian group, are of the form $r g$ where r is a unit in R and $g \in G$. Also in [15] he proved that the units of $R(<x>)$, where R is a commutative ring with no non-zero nilpotents and no non-trivial idempotents and $<x>$ is an infinite cyclic group, are of the form $r g$ where r is a unit in R and $g \in <x>$.

In [17] Zariski and Samuel studied R-automorphisms of the polynomial rings $R[x]$, (that is, automorphisms of $R[x]$ which restrict to the identity mapping on R) where R is an integral domain. In [3] Gilmer determined R-automorphisms of the polynomial rings R[x] where R is a commutative ring. In [2] Coleman and Enochs studied the corresponding results in general. In [9] Parmenter studied R-automorphisms of the group ring R(<x>) where <x> is an infinite cyclic group and he determined necessary and sufficient conditions that $x \to \Sigma a_i x^i$ induces an R-automorphism of R(<x>) . He also studied the units of R(G) where R is a commutative ring and G is a right-ordered group.

This thesis consists of five chapters. Chapter 1 contains some well known results and definitions that are needed in this thesis. In Chapter 2 we extend some ideas of [9] to a twisted group ring $R^{\gamma}(<x>)$ where <x> is an infinite cyclic group and we determine a necessary and sufficient condition that $\bar{x} \to \Sigma a_i \overline{x^i}$ induces an R-automorphism of $R^{\gamma}(<x>)$. Chapter 3 studies R-automorphism of R(G) where R is either a field or a ring with a unique proper ideal and G is a finitely generated torsion-free abelian group. In Chapter 4 we determine the units and study the K-automorphisms of K(<x> × <y>) where K is a field and <x> is an infinite cyclic group, $y^2 = 1$. In [10] Passman proved that the group algebras of all non-isomorphic p-groups of order at most p^4 over the prime field of p elements are non-isomorphic. In Chapter 5 we attempt to find the corresponding results for the p-groups of order p^5 , but the problem is still open.

CHAPTER 1

In this chapter we present certain well-known definitions and general results which are needed in this thesis. Throughout this thesis we understand by the word 'ring', an associative ring with a multiplicative identity 1 . We use multiplicative notation for groups and we write 1 for the identity element of a group.

Definitions 1.1

Let R be a ring and $r \in R$. Then,

(i) r is said to be an idempotent if $r^2 = r$, [7, 8] .

(ii) r is said to be nilpotent if there exists a positive integer n such that $r^n = 0$, [7, 8] .

(iii) r is said to be a proper divisor of zero if $r \neq 0$ and either there exists $s \in R$, $s \neq 0$, such that $rs = 0$ or there exists $t \in R$, $t \neq 0$, such that $tr = 0$, [8] .

(iv) r is said to be a unit if there exists $s \in R$ such that $rs = sr = 1$. Then s is determined uniquely by r and we write $s = r^{-1}$, [8]

Lemma 1.2

Let R be a ring. If $r \in R$ is nilpotent, then $1 - r$, $1 + r$ are units.

Proof

Since the proof for the case $1 - r$ is similar to the proof for the case $1 + r$ we consider the case $1 + r$. Let $r^n = 0$ for some positive integer n . Then we have

$$(1 + r) \sum_{k=0}^{n-1} (-1)^k r^k = 1 + (-1)^{n-1} r^n = 1 . \qquad \Delta$$

Definitions 1.3

Here we make the standard definitions with regard to ideals of a ring R. We should remark that throughout this thesis '$x \subseteq y$' means that x is a subset of y and '$x \subset y$' means that x is a proper subset of y.

(i) I is a prime ideal of R if whenever A, B ideals of R such that $AB \subseteq I$, then $A \subseteq I$ or $B \subseteq I$, [8].

(ii) I is a maximal (right, left) ideal of R if $I \neq R$ and there exists no (right, left) ideal A in R such that $I \subset A \subset R$, [8].

(iii) I is a nil ideal of R if every element of I is nilpotent, [7, 8].

(iv) If I is an ideal of R such that $I^n = (0)$ for some positive integer n, I is said to be a nilpotent ideal [1].

Definition 1.4

Let R be a ring. Then the smallest positive integer n such that $n1 = 0$, is called the characteristic of R. If no such positive integer exists R is said to have characteristic zero.

As is well known, the characteristic of an integral domain is either zero or prime [8].

Definition 1.5

The intersection of all prime ideals of a ring R is called the prime radical of R, [1, 7].

Lemma 1.6

Let R be a commutative ring. Then the proper ideal P of R is prime if and only if R/P is an integral domain [1, 7].

Lemma 1.7

The prime radical of a commutative ring R consists of all nilpotent elements of R , [7].

Lemma 1.8

Let R be a commutative ring. Then the proper ideal M of R is maximal if and only if R/M is a field [1, 7].

Definition 1.9

The intersection of all maximal right ideals of a ring R is called the Jacobson radical $\mathcal{J}(R)$, [7].

Definition 1.10

The group ring R(G) of a group G over a ring R is the free left R-module over the set of elements of G as a basis in which the multiplication induced by G is extended linearly to R(G) .

Thus if $\sum_{i=1}^{m} \alpha_i g_i$, $\sum_{j=1}^{n} \beta_j h_j$ $(\alpha_i, \beta_j \in R ; g_i, h_j \in G)$ are typical elements of R(G) then their product is defined by:

$$\sum_{i=1}^{m} \alpha_i g_i \quad \sum_{j=1}^{n} \beta_j h_j \quad = \quad \sum_{i,j} \alpha_i \beta_j \, (g_i h_j) \qquad [11] \qquad .$$

The notion of group ring extends to that of a twisted group ring as follows.

Definition 1.11

Let R be a ring and let G be a group. Then a twisted group ring $R^{\gamma}(G)$ of G over R is an R-algebra with basis $\{\overline{g} \mid g \in G\}$ and with an associative multiplication defined as follows:

$$\overline{g}\,\overline{h} = \gamma(g, h)\,\overline{gh} \quad \text{for all } g, h \in G ,$$

for some unit $\gamma(g, h)$ in the centre of R, [11, 12].

The associativity condition $x(y\,z) = (x\,y)z \quad (x, y, z \in G)$ implies that

$$\gamma(x, yz)\,\gamma(y, z) = \gamma(x, y)\,\gamma(xy, z) \qquad (x, y, z \in G) .$$

Taking $y = 1$ in the last identity we have
$\gamma(x, z)\,\gamma(1, z) = \gamma(x, 1)\,\gamma(x, z)$ whence

$$\gamma(1, z) = \gamma(x, 1) \qquad (z, x \in G) .$$

Taking $x = 1$ we have $\gamma(1, z) = \gamma(1, 1)$ for all $z \in G$ and so we have

$$\gamma(1, 1) = \gamma(1, z) = \gamma(x, 1) \qquad (z, x \in G) .$$

Also by taking $x = 1$ in $\overline{x}\,\overline{y} = \gamma(x, y)\,\overline{xy}$ we have
$\overline{1}\,\overline{y} = \gamma(1, y)\,\overline{1y} = \gamma(1, y)\overline{y}$ and this implies that

$$(\gamma(1, 1))^{-1}\,\overline{1}\,\overline{y} = \overline{y} , \qquad (y \in G) .$$

Again by taking $y = 1$ in $\overline{x}\,\overline{y} = \gamma(x, y)\,\overline{xy}$ we have
$\overline{x}\,\overline{1} = \gamma(x, 1)\,\overline{x1} = \gamma(1, 1)\overline{x}$. This implies that $\overline{x}[(\gamma(1, 1))^{-1}\,\overline{1}] = \overline{x}$.
Hence we conclude that $(\gamma(1, 1))^{-1}\,\overline{1}$ is the identity element of the twisted group ring $R^{\gamma}(G)$ of G over R. We write $(\gamma(1, 1))^{-1}$ briefly as $\gamma(1,1)^{-1}$.

Now let $g \in G$. Then from $\overline{g}\,\overline{g^{-1}} = \gamma(g, g^{-1})\overline{1}$ and
$\overline{g^{-1}}\,\overline{g} = \gamma(g^{-1}, g)\overline{1}$ we conclude that
$\overline{g}[\gamma(1, 1)^{-1}\,\gamma(g, g^{-1})^{-1}\,\overline{g^{-1}}] = \gamma(1, 1)^{-1}\,\overline{1}$, and
$[\gamma(1, 1)^{-1}\,\gamma(g^{-1}, g)^{-1}\,\overline{g^{-1}}]\overline{g} = \gamma(1, 1)^{-1}\,\overline{1}$. But $\gamma(1, 1)^{-1}\,\overline{1}$ is

the identity element of $R^{\gamma}(G)$ and so

$$\gamma(1, 1)^{-1}\ \gamma(g, g^{-1})^{-1}\ \overline{g^{-1}} = \gamma(1, 1)^{-1}\ \gamma(g^{-1}, g)^{-1}\ \overline{g^{-1}}\ ,$$

the inverse of $\bar{g}$. Also this implies that $\gamma(g, g^{-1}) = \gamma(g^{-1}, g)$ for all $g \in G$.

Furthermore, let I be an ideal of R and let $\bar{R} = R/I$. Let a bar $\bar{\ }$ denote a residue class (mod I) i.e.

$$\bar{a} = a + I \qquad (a \in R)\ .$$

Then from $\gamma(x, yz)\ \gamma(y, z) = \gamma(x, y)\ \gamma(xy, z)$, $(x, y, z \in G)$ we have $\overline{\gamma(x, yz)}\ \overline{\gamma(y, z)} = \overline{\gamma(x, y)}\ \overline{\gamma(xy, z)}$.

Consequently we may construct the twisted group ring $\bar{R}^{\bar{\gamma}}(G) = (R/I)^{\bar{\gamma}}(G)$ by defining

$$\bar{x}\ \bar{y} = \overline{\gamma(x, y)}\ \overline{xy}\ .$$

Now we define $\phi : R^{\gamma}(G) \to \bar{R}^{\gamma}(G)$ by

$$\phi\left(\sum_g \alpha_g\ \bar{g}\right) = \sum_g \bar{\alpha}_g\ \bar{g}\ .$$

It is straightforward to check that ϕ is a ring-epimorphism. From this we conclude that if $\sum_g \alpha_g\ \bar{g} \in R^{\gamma}(G)$ is a unit in $R^{\gamma}(G)$, then $\sum_g \bar{\alpha}_g\ \bar{g}$ is a unit in $\bar{R}^{\bar{\gamma}}(G)$.

<u>Lemma 1.12</u>

Let R be a ring and let $\langle x \rangle$ be an infinite cyclic group. Let $R^{\gamma}(\langle x \rangle)$ be a twisted group ring of $\langle x \rangle$ over R . then $\overline{x^m}\ \overline{x^n} = \overline{x^n}\ \overline{x^m}$, (m, n integers).

Proof

To prove the lemma it is enough to prove $\gamma(x^m, x^n) = \gamma(x^n, x^m)$. By (1.11) we have

$$\gamma(w, yz)\ \gamma(y, z) = \gamma(w, y)\ \gamma(wy, z), \qquad (w, y, z \in \langle x \rangle)\ . \tag{1}$$

$$\gamma(1, z) = \gamma(y, 1) = \gamma(1, 1), \qquad (z, y \in \langle x \rangle)\ . \tag{2}$$

$$\gamma(y, y^{-1}) = \gamma(y^{-1}, y), \qquad (y \in \langle x \rangle)\ . \tag{3}$$

First we prove by mathematical induction that $\gamma(x, x^m) = \gamma(x^m, x)$, m positive integer. For $m = 1$ there is nothing to prove. Assume $m = 2$, by taking $w = y = z = x$ in (1) we have $\gamma(x, x^2)\ \gamma(x, x) = \gamma(x, x)\ \gamma(x^2, x)$. This implies $\gamma(x, x^2) = \gamma(x^2, x)$ because $\gamma(x, x)$ is a central unit in R . Now we assume that $\gamma(x, x^m) = \gamma(x^m, x)$, m positive integer, by taking $w = x$, $y = x^m$, $z = x$ in (1) we conclude that $\gamma(x, x^{m+1})\ \gamma(x^m, x) = \gamma(x, x^m)\ \gamma(x^{m+1}, x)$. From this we conclude that $\gamma(x, x^{m+1}) = \gamma(x^{m+1}, x)$. Hence our claim has been established.

Now we prove that $\gamma(x^2, x^m) = \gamma(x^m, x^2)$, m positive integer. For $m = 1$ we have proved this in the last paragraph. For $m = 2$ there is nothing to prove. Assume $m = 3$ by taking $w = x^2$, $y = x$, $z = x^2$ in (1) we have $\gamma(x^2, x^3)\ \gamma(x, x^2) = \gamma(x^2, x)\ \gamma(x^3, x^2)$. Since $\gamma(x, x^2) = \gamma(x^2, x)$ we conclude that $\gamma(x^2, x^3) = \gamma(x^3, x^2)$. Now we assume $\gamma(x^2, x^k) = \gamma(x^k, x^2)$ for $k = 1, 2, \ldots, m$, then we prove that $\gamma(x^2, x^{m+1}) = \gamma(x^{m+1}, x^2)$. By taking $w = x^2$, $y = x^{m-1}$, $z = x^2$ in (1) we have

$$\gamma(x^2, x^{m+1})\ \ \gamma(x^{m-1}, x^2) = \gamma(x^2, x^{m-1})\ \gamma(x^{m+1}, x^2)\ .$$

This implies that $\gamma(x^2, x^{m+1}) = \gamma(x^{m+1}, x^2)$. Hence our claim has been established.

Finally we assume $\gamma(x^r, x^m) = \gamma(x^m, x^r)$ for $1 \leq r \leq n$, and $n \geq m$. Then by taking $w = x^m$, $y = x^{n+1-m}$, $z = x^m$ in (1) we have $\gamma(x^m, x^{n+1}) \ \gamma(x^{n+1-m}, x^m) = \gamma(x^m, x^{n+1-m}) \ \gamma(x^{n+1}, x^m)$. This implies that $\gamma(x^{n+1}, x^m) = \gamma(x^m, x^{n+1})$. Hence $\gamma(x^m, x^n) = \gamma(x^n, x^m)$

Now we prove that $\gamma(x^{-m}, x^{-n}) = \gamma(x^{-n}, x^{-m})$ for all positive integer, m, n. By (1.11) we know that $(\overline{x^m})^{-1}$ exists. Then from $\overline{x^m}\ \overline{x^{-m}} = \gamma(x^m, x^{-m})\ \overline{1}$ we obtain $\overline{x^{-m}} = \gamma(x^m, x^{-m})(\overline{x^m})^{-1}\ \overline{1}$. Since $\overline{1}$ is central and $\overline{x^m}\ \overline{x^n} = \overline{x^n}\ \overline{x^m}$ $(m, n \geq 0)$ we have

$$\begin{aligned}
\overline{x^{-m}}\ \overline{x^{-n}} &= [\gamma(x^m, x^{-m})(\overline{x^m})^{-1}\ \overline{1}]\ [\gamma(x^n, x^{-n})\ (\overline{x^n})^{-1}\ \overline{1}] \\
&= \gamma(x^m, x^{-m})\ \gamma(x^n, x^{-n})\ (\overline{x^m})^{-1}\ (\overline{x^n})^{-1}\ \overline{1}\ \overline{1} \\
&= \gamma(x^m, x^{-m})\ \ \gamma(x^n, x^{-n})\ (\overline{x^n}\ \overline{x^m})^{-1}\ \overline{1}\ \overline{1} \\
&= \gamma(x^m, x^{-m})\ \ \gamma(x^n, x^{-n})\ (\overline{x^m}\ \overline{x^n})^{-1}\ \overline{1}\ \overline{1} = \overline{x^{-n}}\ \overline{x^{-m}}\ . \quad \Delta
\end{aligned}$$

Definition 1.13

(I) A non-empty set x is said to be linearly ordered if there exists a relation $<$ on x such that the following two conditions hold:

(i) For all $a, b \in x$ exactly one of the following holds:

$a < b$ or $a = b$ or $b < a$.

(ii) For all $a, b, c \in x$, $a < b$ and $b < c$ imply that $a < c$.

(II) A group G on which there is defined a linear ordering $<$ is said to be a right-ordered group if for $a, b, c \in G$ $a < b$ implies that $ac < bc$, [11].

Throughout this thesis by $b > a$ we understand that $a < b$.

Example 1.13 (I)

Let $<x>$ be an infinite cyclic group and let $x^m, x^n \epsilon <x>$, we define $x^m < x^n$ if and only if $m < n$. Then $<x>$ is a right-ordered group.

Example 1.13 (II)

Let $G = <x_1> \times <x_2> \times \dots \times <x_n>$ where $\langle x_i \rangle$, $1 \le i \le n$, is an infinite cyclic group. Let

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} , x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} \epsilon G .$$

We define

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} < x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$$

if and only if either

(1) $\alpha_1 < \beta_1$, or

(2) $\alpha_1 = \beta_1 , \dots, \alpha_i = \beta_i , \alpha_{i+1} < \beta_{i+1}$, $1 \le i \le n-1$.

Thus G is a right-ordered group.

Lemma 1.14 (Lifting idempotents)

Let R be a ring and let N be a nil ideal of R . Let $\tau : R \to R/N$ be the natural homomorphism. Let $a \epsilon R$ be such that $\tau(a)$ an idempotent. Then there exists $b \epsilon R$ such that $e = aba$ is an idempotent with $\tau(e) = \tau(a)$. [11, page 49].

Proof

Let $a \epsilon R$ and $\tau(a) = \bar{a}$. By assumption we have $\tau(a - a^2) = \tau(a) - (\tau(a))^2 = \bar{a} - (\bar{a})^2 = \bar{a} - \bar{a} = 0$. This implies that $a - a^2 \in N$. Since N is nil for some positive integer K we have $(a - a^2)^k = 0$. If $k = 1$, then $a - a^2 = 0$ and we let $b = a$ to obtain the result. Now let $k \geq 2$. Since we have $(1 - a)^k = 1 - ad$ where

$$d = \sum_{t=1}^{k} (-1)^{t-1} \binom{k}{t} a^{t-1} \in R .$$

Hence $a^k(1 - ad) = (a - a^2)^k = 0$ and $ad = da$. But $\bar{a}$ is an idempotent, and so $1 - \bar{a}$ is also an idempotent. Since τ is onto, then $\tau(1) = 1$. Thus we have

$$1 - \tau(ad) = \tau[(1 - a)^k] = [1 - \tau(a)]^k = (1 - \bar{a})^k = 1 - \bar{a} .$$

This implies that $\tau(ad) = \bar{a}$.

Now from $0 = (a - a^2)^k = a^k(1 - a)^k = a^k(1 - ad)$ we have that $a^k = a^k(ad)$. This implies that $a^k = a^k(ad) = [a^k(ad)](ad) = a^k(ad)^2$. By induction on i, we have $a^k = a^k(ad)^i$ for any positive integer i. Since $ad = da$ we have in particular $a^k = a^k(ad)^k = a^{2k} d^k$.

From this we conclude that $(ad)^k = a^k d^k = (a^{2k} d^k) d^k = a^{2k} d^{2k} = [(ad)^k]^2$ i.e., $(ad)^k$ is an idempotent. Since $(ad)^k$ is an idempotent and $\tau(ad) = \bar{a}$ is also an idempotent we have,

$$\tau(e) = \tau[(ad)^k] = (\bar{a})^k = \bar{a} = \tau(a) .$$

But we know that $k \geq 2$, and so $(ad)^k = aba$ for some $b \in R$. Δ

<u>Lemma 1.15</u>

Let R be a ring and let $<x>$ be an infinite cyclie group. Let $R^{\gamma}(<x>)$ be a twisted group ring of $<x>$ over R. Then for any integer $m > 1$ we have

(i) $(\bar{x})^m = \gamma(x, x)\, \gamma(x^2, x) \ldots \gamma(x^{m-1}, x)\, \overline{x^m}$

$\quad = \gamma(x, x)\ \gamma(x, x^2) \ldots \gamma(x, x^{m-1})\overline{x^m}$.

(ii) $$\overline{(x^{-1})}^{m} = \gamma(x^{-1}, x^{-1})\ \gamma(x^{-2}, x^{-1})\ \dots\ \gamma(x^{-m+1}, x^{-1})\ \overline{x^{-m}}$$

$$= \gamma(x^{-1}, x^{-1})\ \gamma(x^{-1}, x^{-2})\ \dots\ \gamma(x^{-1}, x^{-m+1})\ \overline{x^{-m}}\ .$$

Proof

To prove (i) we proceed by induction. For $m = 2$ we have $(\bar{x})^2 = \bar{x}\,\bar{x} = \gamma(x, x)\overline{x^2}$. Suppose (i) holds for m . We prove the corresponding result for $m + 1$. We have

$$(\bar{x})^{m+1} = (\bar{x})^{m},\ \bar{x} = [\gamma(x, x)\ \gamma(x^2, x)\ \dots\ \gamma(x^{m-1}, x)\overline{x^m}]\bar{x}$$

$$= \gamma(x, x)\ \ \gamma(x^2, x)\ \dots\ \gamma(x^{m-1}, x)\ [\overline{x^m}\ \bar{x}]$$

$$= \gamma(x, x)\ \gamma(x^2, x)\ \dots\ \gamma(x^{m-1}, x)\ \gamma(x^m, x)\overline{x^{m+1}}\ .$$

From this result and using (1.12) the proof of (i) is complete. Since the proof of (ii) is similar to the proof of (i) we omit it. Δ

Lemma 1.16

Let R be a ring and let $G = \langle x_1\rangle \times \langle x_2\rangle \times \dots \times \langle x_n\rangle$ be an abelian group. Let $\langle x\rangle$ be an infinite cyclic group and let $R^{\gamma}(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R . Then

(i) Every endomorphism of G is determined by its effect on a set of generators of G .

(ii) Every homomorphism of G into $R(G)$ is determined by its effect on a set of generators of G .

(iii) Every homomorphism of G into $R(G)$ can be extended to an R-endomorphism of $R(G)$.

(iv) A mapping $\bar{\theta} : R^{\gamma}(\langle x\rangle) \to R^{\gamma}(\langle x\rangle)$ is defined by $\bar{\theta}[(\bar{x})^j] = [\sum_i a_i\ \overline{x^i}]^j$ and extended by linearity to $R^{\gamma}(\langle x\rangle)$.

Then $\bar{\theta}$ is an R-endomorphism of $R^{\gamma}(\langle x\rangle)$.

Proof

Let θ be an endomorphism of G and $\theta(x_i)$ for $1 \le i \le n$ be determined. Since every element of G is of the form $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ we have

$$\theta(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) = (\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \dots (\theta(x_n))^{\alpha_n} .$$

Hence (i) and (ii) have been proved.

Let θ be a homomorphism of G into $R(G)$ we define $\phi : R(G) \to R(G)$ by ,

$$\phi(\sum a_{\alpha_1\alpha_2 \dots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) = \sum a_{\alpha_1\alpha_2 \dots \alpha_n}$$

$$(\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \dots (\theta(x_n))^{\alpha_n} .$$

By this definition we have,

$$\phi[(\sum a_{\alpha_1\alpha_2 \dots \alpha_n} x_1^{\alpha_1}x_2^{\alpha_2} \dots x_n^{\alpha_n}) (\sum b_{\beta_1\beta_2 \dots \beta_n} x_1^{\beta_1}x_2^{\beta_2} \dots x_n^{\beta_n})]$$

$$= \phi(\sum a_{\alpha_1\alpha_2 \dots \alpha_n} b_{\beta_1\beta_2 \dots \beta_n} x_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \dots x_n^{\alpha_n+\beta_n})$$

$$= \sum a_{\alpha_1\alpha_2 \dots \alpha_n} b_{\beta_1\beta_2 \dots \beta_n} (\theta(x_1))^{\alpha_1+\beta_1} (\theta(x_2))^{\alpha_2+\beta_2} \dots (\theta(x_n))^{\alpha_n+\beta_n}$$

$$= [\sum a_{\alpha_1\alpha_2 \dots \alpha_n} (\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \dots (\theta(x_n))^{\alpha_n}]$$

$$[\sum b_{\beta_1\beta_2 \dots \beta_n} (\theta(x_1))^{\beta_1}(\theta(x_2))^{\beta_2} \dots (\theta(x_n))^{\beta_n}]$$

$$= \phi([\sum a_{\alpha_1\alpha_2 \dots \alpha_n} x_1^{\alpha_1}x_2^{\alpha_2} \dots x_n^{\alpha_n}) \phi(\sum b_{\beta_1\beta_2 \dots \beta_n} x_1^{\beta_1}x_2^{\beta_2} \dots x_n^{\beta_n}) .$$

Proof

Let θ be an endomorphism of G and $\theta(x_i)$ for $1 \leq i \leq n$ be determined. Since every element of G is of the form $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ we have

$$\theta(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = (\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \ldots (\theta(x_n))^{\alpha_n} .$$

Hence (i) and (ii) have been proved.

Let θ be a homomorphism of G into $R(G)$ we define $\phi : R(G) \to R(G)$ by ,

$$\phi(\sum a_{\alpha_1\alpha_2 \ldots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = \sum a_{\alpha_1\alpha_2 \ldots \alpha_n}$$

$$(\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \ldots (\theta(x_n))^{\alpha_n} .$$

By this definition we have,

$$\phi[(\sum a_{\alpha_1\alpha_2 \ldots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) (\sum b_{\beta_1\beta_2 \ldots \beta_n} x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n})]$$

$$= \phi(\sum a_{\alpha_1\alpha_2 \ldots \alpha_n} b_{\beta_1\beta_2 \ldots \beta_n} x_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \ldots x_n^{\alpha_n+\beta_n})$$

$$= \sum a_{\alpha_1\alpha_2 \ldots \alpha_n} b_{\beta_1\beta_2 \ldots \beta_n} (\theta(x_1))^{\alpha_1+\beta_1} (\theta(x_2))^{\alpha_2+\beta_2} \ldots (\theta(x_n))^{\alpha_n+\beta_n}$$

$$= [\sum a_{\alpha_1\alpha_2 \ldots \alpha_n} (\theta(x_1))^{\alpha_1}(\theta(x_2))^{\alpha_2} \ldots (\theta(x_n))^{\alpha_n}]$$

$$[\sum b_{\beta_1\beta_2 \ldots \beta_n} (\theta(x_1))^{\beta_1}(\theta(x_2))^{\beta_2} \ldots (\theta(x_n))^{\beta_n}]$$

$$= \phi([\sum a_{\alpha_1\alpha_2 \ldots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) \phi(\sum b_{\beta_1\beta_2 \ldots \beta_n} x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}) .$$

Hence ϕ is a R-endomorphism of $R(G)$ and (iii) has been proved.

By (1.15) we know that $\{(\overline{x})^j \mid j \in \mathbb{Z}\}$ is a basis for $R^\gamma(<x>)$ and so to prove (iv) we define $\tilde{\theta} : R^\gamma(<x>) \to R^\gamma(<x>)$ by

$$\tilde{\theta}(\sum_j b_j(\overline{x})^j) = \sum_j b_j(\overline{\theta}(\overline{x}))^j .$$

Since by (1.12) $\overline{x^i}\,\overline{x^j} = \overline{x^j}\,\overline{x^i}$ then as in (iii) we conclude that θ is an R-endomorphism of $R^\gamma(<x>)$. Δ

Lemma 1.17

Let R be a commutative ring and let G be a group. Let $R^\gamma(G)$ be a twisted group ring of G over R . Let $u + \sum_m^n a_i\overline{g_i}$ $(g_i \in G)$ be an element of $R^\gamma(G)$ such that u is a unit in $R^\gamma(G)$ and all a_i are nilpotents in R . Then for every integer k ,

$$[u + \sum_m^n a_i\overline{g_i}]^k = u^k + N \text{ where } N \text{ is nilpotent in } R^\gamma(G) .$$

Proof

Let T be the ideal of R generated by $\{a_i \mid m \le i \le n\}$. Then T is nilpotent. Since u is a unit in $R^\gamma(G)$ and $\gamma(1, 1)^{-1}\,\overline{1}$ is the identity element of $R^\gamma(G)$, (1.11) we can write

$$u + \sum_m^n a_i\overline{g_i} = [\gamma(1, 1)^{-1}\,\overline{1} + (\sum_m^n a_i\overline{g_i})\,u^{-1}]u .$$

Furthermore $(\sum_m^n a_i\overline{g_i})u^{-1}$ is nilpotent in $R^\gamma(G)$, because R is commutative. Let $w = (\sum_m^n a_i\overline{g_i})u^{-1}$ with $w^s = 0$ for some positive integer s . Then

$$([\gamma(1,1)^{-1}\,\overline{1} + w]u)(u^{-1}[\gamma(1,1)^{-1}\,\overline{1} - w + w^2 + \dots + (-1)^{s-1}(w)^{s-1}])$$

$$= \gamma(1,1)^{-1}\,\overline{1} .$$

Hence

$$[u + \sum_{m}^{n} a_i\overline{g_i}]^{-1} = u^{-1}[\gamma(1,1)^{-1}\,\overline{1} - w + w^2 + \dots + (-1)^{s-1}(w)^{s-1}] = u^{-1} + N_1$$

where N_1 is nilpotent in $R^{\gamma}(G)$.

Finally, for $k \geq 0$ it is evident that $[u + \sum_{m}^{n} a_i\overline{g_i}]^k = u^k + N_2$ where N_2 is nilpotent in $R^{\gamma}(G)$. But for $k < 0$ we have

$$[u + \sum_{m}^{n} a_i\overline{g_i}]^k = ([u + \sum_{m}^{n} a_i\overline{g_i}]^{-1})^{-k} = [u^{-1} + N_1]^{-k} = (u^{-1})^{-k} + N_3 = u^k + N_3$$

where N_3 is nilpotent in $R^{\gamma}(G)$. ▲

Definition 1.18

A ring R is said to be a (Von Neumann)regular ring if for every element $r \in R$ there exists an element $s \in R$ such that $rsr = r$, [7, 9].

Lemma 1.19

In a commutative regular ring every prime ideal is maximal [7].

Proof

Let P be a prime ideal of R . Then $\overline{R} = R/P$ is a commutative regular ring which is an integral domain (1.6). Now suppose $\overline{0} \neq \overline{a} \in \overline{R}$. Since $\overline{R}$ is regular there exists $\overline{b} \in \overline{R}$ such that $\overline{a}\,\overline{b}\,\overline{a} = \overline{a}$. This implies that $\overline{b} \neq \overline{0}$ and $\overline{a}\,\overline{b}\,\overline{a}\,\overline{b} = \overline{a}\,\overline{b}$. From $\overline{a}\,\overline{b}\,\overline{a}\,\overline{b} = \overline{a}\,\overline{b}$ we conclude that $\overline{a}\,\overline{b} = \overline{1}$ and $\overline{b}\,\overline{a} = \overline{1}$ because $\overline{1}$ is the identity element of $\overline{R}$. Thus $\overline{R}$ is a field. ▲

The following lemma is well known [11] but we include a Proof of a special case for the sake of completeness.

Lemma 1.20

Let $G = \langle x_1\rangle \times \langle x_2\rangle \times \ldots \times \langle x_n\rangle$ where $\langle x_i\rangle$ is an infinite cyclic group $(i = 1, 2, \ldots, n)$. Let R be an integral domain. Then $R(G)$ is an integral domain.

Proof

We prove the lemma for $n = 1$ and the proof of the lemma for $n > 1$ is similar to the proof of the lemma for $n = 1$. Let $G = \langle x\rangle$ where $\langle x\rangle$ is infinite cyclic group and let $\sum_{\alpha}^{\beta} a_i x^i$, $\sum_{m}^{n} b_j x^j$ be non-zero elements of $R(\langle x\rangle)$ where $a_\beta \neq 0$, $b_n \neq 0$. In the product

$$\left(\sum_{i=\alpha}^{i=\beta} a_i x^i\right)\left(\sum_{j=m}^{j=n} b_j x^j\right)$$

the coefficient of $x^{\beta+n}$ is $a_\beta b_n$ which is non-zero. Δ

Definition 1.21

Let G be a group and let K be a field. Then

$$\text{aug } K(G) = \{\sum_i \alpha_i g_i \in K(G) \mid \sum \alpha_i = 0\},$$

which is an ideal of $K(G)$, is called the augmentation ideal of $K(G)$, [11].

Lemma 1.22

Let $G = \langle g_i : i \in I\rangle$ and let K be a field. Then

$$\text{aug } K(G) = \sum_i (K(G))\,(1 - g_i)\,.$$

Proof

As aug $K(G)$ is an ideal of $K(G)$ and $1 - g_i \in \text{aug } K(G)$ for every i it follows that $\sum_i (K(G))(1 - g_i) \subseteq \text{aug } K(G)$.

Now we prove that $\text{aug } K(G) \subseteq \sum_i (K(G))(1 - g_i)$. For this we suppose that $\sum_{j=1}^{m} \beta_j x_j \in \text{aug } K(G)$, then $\sum \beta_j = 0$. This implies that $\sum_{j=1}^{m} \beta_j x_j = \sum_{j=1}^{m} \beta_j - \sum_{j=1}^{m} \beta_j (1 - x_j) = - \sum_{j=1}^{m} \beta_j (1 - x_j)$. We prove that $1 - x_j \in \sum_i (K(G))(1 - g_i)$. Since $x_j \in G$ we have $x_j = g_{j_1} g_{j_2} \ldots g_{j_r}$ where $j_u \in I$ $(u = 1, 2, \ldots, r)$.

We proceed by mathematical induction on the number of factors in $x_j = g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_r}^{\pm 1}$, to prove $1 - x_j \in \sum_i (K(G))(1 - g_i)$.

We know that $1 - g_{j_i} \in (K(G))(1 - g_{j_i})$ so we have $1 - g_{j_i} \in \sum_i (K(G))(1 - g_i)$. *Moreover* $1 - g_{j_i}^{-1} = -g_{j_i}^{-1}(1 - g_{j_i}) \in K(G)(1 - g_{j_i})$. Let $1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1} \in \sum_i (K(G))(1 - g_i)$ for $1 \leq \sigma < r$. Since we have

$$1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1} g_{j_{(\sigma+1)}}^{\pm 1} = -(1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1})(1 - g_{j_{(\sigma+1)}}^{\pm 1})$$
$$+ (1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1}) + (1 - g_{j_{(\sigma+1)}}^{\pm 1}) ,$$

and $(1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1})(1 - g_{j_{(\sigma+1)}}^{\pm 1})$, $1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \ldots g_{j_\sigma}^{\pm 1}$, $1 - g_{j_{(\sigma+1)}}^{\pm 1}$ belong to $\sum_i (K(G))(1 - g_i)$ we conclude that

$1 - g_{j_1}^{\pm 1} g_{j_2}^{\pm 1} \cdots g_{j_\sigma}^{\pm 1} g_{j_{(\sigma+1)}}^{\pm 1}$ belongs to $\sum_i (K(G))(1-g_i)$ Thus

$$\text{aug } K(G) \subseteq \sum_i (K(G))(1 - g_i) \ . \ \Delta$$

Lemma 1.23

Let G be a group and let K be a field. Let I be an ideal of $K(G)$. Let θ be a K-automorphism of $K(G)$ such that $\theta(I) = I$. Then $\tilde{\theta} : K(G) \to K(G)/I$ defined by $\tilde{\theta}(\sum_i a_i g_i) = \sum_i a_i \theta(g_i) + I$ is an epimorphism and its kernel is I .

Lemma 1.24

Let $G = \langle x \rangle \times \langle y \rangle$ be an abelian group where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2 . Then

$$(K(G)) \text{ aug } K(\langle y \rangle) = (K(G))(1 + y) = k(\langle x \rangle)(1 + y) \ .$$

Proof

By (1.21) we have $\text{aug } K(\langle y \rangle) = K(\langle y \rangle)(1 + y)$ because by the hypothesis of the lemma $-y = y$. This implies that $K(G) \text{ aug } K(\langle y \rangle) = (K(G))[K(\langle y \rangle)(1 + y)] = (K(G))(1 + y)$. Now we prove that $(K(G))(1 + y) = (K(\langle x \rangle))(1 + y)$. It is evident that $(K(\langle x \rangle))(1 + y) \subseteq (K(G))(1 + y)$ and so we show that $(K(G))(1 + y) \subseteq (K(\langle x \rangle))(1 + y)$. Let

$$[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j) y] \ (1 + y) \in (K(G))(1 + y) \ .$$

Then we have

$$[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j) y] \ (1 + y) = [\sum_i \alpha_i x^i + \sum_j \beta_j x^j](1 + y) \in (K(\langle x \rangle))(1 + y))$$

because $y + y^2 = 1 + y$. Hence $(K(G))(1 + y) = (K(\langle x \rangle))(1 + y) \ . \ \Delta$

Notation 1.25

Let G be a group and let K be a field.

(1) In G, $(x, y) = x^{-1}y^{-1}xy$, the commutator of elements of x, y of G.

(2) $<\ldots> =$ the subgroup of G generated by the elements and subgroups indicated within the brackets.

(3) If $X \subseteq G$, $Y \subseteq G$ then $(X, Y) = <(x, y) : x \in X, y \in Y>$ in particular, (G, G) is the commutator subgroup G' of G.

(4) $I^n =$ the nth power of the ideal I of $K(G)$.

(5) $S^{(p)} =$ the set of pth powers of the elements of the subspace S of $K(G)$.

(6) The M-series of G is defined inductively [6] as follows,

$M_1 = G$.

$M_i = <(M_{i-1}, G), M^{(p)}_{(i/p)}>$ for $i > 1$, where (i/p) is the least integer not less than i/p and $M^{(p)}_{\lambda}$ is the set of pth powers of M_{λ}.

(7) We say an abelian p-group A is of type $(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_k})$. If A is the direct product of cyclic subgroups of A of orders $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_k}$.

(8) In $K(G)$, $[\alpha, \beta] = \alpha\beta - \beta\alpha$, the Lie product of elements α and β, $[K(G), K(G)] =$ the commutator subspace of $K(G)$.

Lemma 1.26

Let p be a prime and let G be a finite p-group. Let K be a field of characteristic p. Then $JK(G) = \text{aug } K(G)$.

Proof

We prove that aug $K(G)$ is nilpotent and so is nil. Then aug $K(G) \subseteq JK(G)$ by lemma 1.2.2 of [4]. Let $|G| = p^{\alpha}$ for some positive integer α. Then we proceed by induction on α. Suppose $\alpha = 1$ then G is a cyclic group say $G = \langle g \rangle$. Hence by (1.22) we have aug $K(G) = (K(G))(1 - g)$. Since $g^p = 1$ and characteristic of K is p and G is abelian we have $(\text{aug } K(G))^p = [K(G)(1 - g)]^p = K(G)(1 - g^p) = 0$.

Now suppose for every p-group of order $|G| \leq p^{\alpha}$ we have $(\text{aug } K(G))^{p^{\alpha}} = 0$ then we prove the corresponding result for the group G of order $p^{\alpha+1}$. Since $Z(G) \neq 1$ we may suppose $Z(G)$ is of order p^t for some $t \geq 1$. Hence there exists an element $1 \neq z \in Z(G)$ such that $z^p = 1$ and so $\langle z \rangle$ is a subgroup of G. Let $\phi : G \rightarrow G/\langle z \rangle$ be a natural homomorphism defined by $\phi(g) = g\langle z \rangle$. Then ϕ induces a homomorphism $\theta : K(G) \rightarrow K(G/\langle z \rangle)$ defined by $\theta(\sum_i \alpha_i g_i) = \sum \alpha_i (g_i \langle z \rangle)$. The kernel of θ is $K(G)$ aug $K(\langle z \rangle)$.

Suppose $\sum_i \alpha_i g_i \in \text{aug } K(G)$ then we have $\theta(\sum_i \alpha_i g_i) = \sum_i \alpha_i (g_i \langle z \rangle)$

where $\sum_i \alpha_i = 0$. This implies that aug $K(G)$ is mapped into aug $K(G/\langle z \rangle)$. But $|G/\langle z \rangle| = p^{\alpha}$ and so by assumption we have $(\text{aug } K(G/\langle z \rangle))^{p^{\alpha}} = 0$. Since $(\text{aug } K(G))^{p^{\alpha}}$ is mapped into

aug $k(G/\langle z \rangle)^{p^{\alpha}}$ then $(\text{aug } K(G))^{p^{\alpha}} \subseteq \ker\theta = K(G) \text{ aug } K(\langle z \rangle)$.

From this we conclude that

$$[(\text{aug } K(G))^{p^{\alpha}}]^p \subseteq [K(G) \text{ aug } K(\langle z \rangle)]^p = K(G) \ [\text{aug } K(\langle z \rangle)]^p = 0 .$$

Thus our claim has been established and so aug $K(G) \subseteq JK(G)$. But aug $K(G)$ has a basis of elements $g_i - 1$ $(1 \neq g_i \in G)$ and so is a maximal ideal. Hence aug $K(G) = JK(G)$. Δ

Lemma 1.27

Let p be a prime and let K be a field of characteristic p. Let G be a finite p-group in which every conjugacy class has 1 or p elements, and let $A = \{\sum_i \alpha_i u_i \mid \alpha_i \in K$ and u_i is a p element class sum in $K(G)\}$. Then

$$JK(G) \cap Z(K(G)) = \text{aug } K(Z) + A .$$

Proof

By (1.26) $JK(G) = \text{aug } K(G)$ and so it is enough to prove $\text{aug } K(G) \cap Z\, K(G) = \text{aug } K(Z) + A$.

Let $\{g_1, g_2, \ldots, g_p\}$ be a conjugacy class of G of p elements. Then $g_1 + g_2 + \ldots + g_p \in Z(K(G))$. On the other hand we have

$$\begin{aligned} g_1 + g_2 + \ldots + g_p &= g_1 + g_2 + \ldots + g_p - p \\ &= (g_1 - 1) + (g_2 - 1) + \ldots + (g_p - 1) \in \text{aug } K(G) . \end{aligned}$$

Hence $A \subseteq \text{aug } K(G) \cap Z(K(G))$.

Now let $\sum_i \alpha_i (z_i - 1) \in \text{aug } K(Z)$. We have $\sum_i \alpha_i (z_i - 1) \in \text{aug } K(G)$ and $\sum_i \alpha_i (z_i - 1) \in Z(K(G))$ i.e. $\text{aug } K(Z) \subseteq \text{aug } K(G) \cap Z(K(G))$.

Hence we have

$$\text{aug } K(Z) + A \subseteq \text{aug } K(G) \cap Z(K(G)) . \qquad (1)$$

Conversely let $x \in \text{aug } K(G) \cap Z(K(G))$. Then we can write $x = \sum_i \beta_i (g_i - 1) = \sum_i \beta_i g_i - (\sum_i \beta_i) 1$. Since $x \in Z(K(G))$ and $(\sum_i \beta_i) 1 \in Z(K(G))$ we have $\sum_i \beta_i g_i \in Z(K(G))$. But the centre of $K(G)$ is spanned by all the class sums of G and so we can divide

$\sum_i \beta_i g_i$ into two parts say $\sum_\lambda \beta_{i_\lambda} g_{i_\lambda} + \sum_\mu \beta_{i_\mu} g_{i_\mu}$. Where all $g_{i_\lambda} \in Z$ and every g_{i_μ} belongs to one of the class sums of G that have p elements. Since $\sum_\mu \beta_{i_\mu} g_{i_\mu} \in Z(K(G))$, the number of terms in $\sum_\mu \beta_{i_\mu} g_{i_\mu}$ is a multiple of p and for every β_{i_μ} there are $p - 1$ other coefficients that are equal to β_{i_μ} . Thus $\sum_\mu \beta_{i_\mu} g_{i_\mu} \in A$. Moreover $x = \sum_i \beta_i(g_i - 1) = \sum_\lambda \beta_{i_\lambda}(g_{i_\lambda} - 1) + \sum_\mu \beta_{i_\mu} g_{i_\mu}$ because $\sum_\mu \beta_{i_\mu} = 0$. Hence $x \in \text{aug } K(Z) + A$ and so $\text{aug } K(G) \cap Z(K(G)) \subseteq \text{aug } K(Z) + A$. Δ

Lemma 1.28

Let N be any ideal of group ring $K(G)$ where K is a field. Let $a, b \in G$ such that $a - 1 \in N^i$, $b - 1 \in N^j$ $(1 \le i \le j)$. Then

(1) $(ab - 1) \equiv (a - 1) + (b - 1) \bmod N^{i+1}$.

(2) $(a^n - 1) \equiv n(a - 1) \bmod N^{i+1}$ (n positive integer).

(3) $(b - 1)(a - 1) \equiv (a - 1)(b - 1) + (c - 1) \bmod N^{i+j+1}$, where $c = (b, a) = b^{-1} a^{-1} ba$, [10].

Proof

The proof of (1) follows from

$$(ab - 1) = (a - 1)(b - 1) + (a - 1) + (b - 1)$$

and (2) is a special case of (1). Since

$$(b - 1)(a - 1) - (a - 1)(b - 1) = ab(b^{-1}a^{-1}ba - 1) = ab(c - 1)$$

we conclude that $(c - 1) \in N^{i+j}$. Hence (3) follows from

$$(b - 1)(a - 1) - (a - 1)(b - 1) = (ab - 1)(c - 1) + (c - 1) . \quad \Delta$$

Definition 1.29

An element a of a ring R is said to be right-quasi-regular if there exists $a' \in R$ such that $a + a' + aa' = 0$. We call a' right-quasi-inverse of a , [4].

Definition 1.30

We say that a right ideal I of a ring R is right-quasi-regular if for every element a of I there exists $a' \in R$ such that $a + a' + aa' = 0$, [4].

Lemma 1.31

The Jacobson radical of a ring R is the unique maximal right-quasi-regular right ideal of R , [4].

Lemma 1.32

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field. Let $u \in K(\langle x\rangle)$ and let u be a unit in $K(G)$. Then u is a unit in $K(\langle x\rangle)$.

Proof

Since $u1$ is a unit in $K(G)$ there exist $A, B \in K(\langle x\rangle)$ such that $u1(A + By) = 1$. This implies that $uA = 1$ and $uB = 0$. Δ

CHAPTER 2

In this chapter we extend some ideas of [9] for twisted group rings that M.M. Parmenter has obtained for group rings. We follow his method of proof.

<u>Lemma 2.1</u>

Let R be a commutative ring and let G be a right-ordered group. Let $R^{\gamma}(G)$ be a twisted group ring of G over R and let $U(R^{\gamma}(G))$ denote the units of $R^{\gamma}(G)$. Then the following two statements are equivalent:

(i) $U(R^{\gamma}(G)) = \{\sum_g \alpha_g \overline{g} \mid$ there exist $\beta_g \in R$ with

$\sum_g \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1}$, and $\alpha_g \beta_h = 0$

whenever $gh \neq 1\}$.

(ii) R has no non-zero nilpotent elements.

<u>Proof</u>

We assume first that (i) holds. Let $a \in R$ be nilpotent with $a^K = 0$ for some positive integer K. Let $1 \neq g \in G$. Then by (1.2) $\gamma(1, 1)^{-1}\, \overline{1} + a\overline{g}$ is a unit in $R^{\gamma}(G)$.

Let $\alpha_1 \overline{1} + \alpha_g \overline{g} = \gamma(1, 1)^{-1}\, \overline{1} + a\overline{g}$, where $\alpha_1 = \gamma(1, 1)^{-1}$ $\alpha_g = a$. By (i) there exist $\beta_1, \beta_{g^{-1}} \in R$ such that

$$\gamma(1, 1)^{-1}\beta_1\, \gamma(1, 1) + \alpha_g \beta_{g^{-1}}\, \gamma(g, g^{-1}) = \gamma(1, 1)^{-1}\,. \qquad (1)$$

$$\alpha_1 \beta_{g^{-1}} = 0\,. \qquad (2)$$

$$\alpha_g \beta_1 = 0\,. \qquad (3)$$

But $\alpha_1 = \gamma(1, 1)^{-1}$ is a central unit in R and so (2) implies that $\beta_{g^{-1}} = 0$. From this and (1) we conclude that

$$\beta_1 = \gamma(1, 1)^{-1} . \qquad (4)$$

From (4) and (3) we obtain ,

$$\alpha_g \gamma(1, 1)^{-1} = \alpha_g \beta_1 = 0 .$$

This implies that $a = \alpha_g = 0$, which we wished to prove.

Now we assume that (ii) holds. To prove (i) let $\sum_{i=1}^{m} \alpha_i \overline{g_i}$ be a unit in $R^{\gamma}(G)$. Then for some $\sum_{j=1}^{n} \beta_j \overline{h_j} \in R^{\gamma}(G)$ we have

$$\left(\sum_{i=1}^{m} \alpha_i \overline{g_i}\right)\left(\sum_{j=1}^{n} \beta_j \overline{h_j}\right) = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} \alpha_i \beta_j \, \gamma(g_i, h_j) \overline{g_i h_j} = \gamma(1, 1)^{-1} \, \overline{1} . \qquad (5)$$

We shall show in (5) that, $\alpha_i \beta_j = 0$ whenever $g_i h_j \neq 1$ and from this we shall conclude that $\sum \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1}$.

Since G is a right-ordered group (1.13) under the relation $<$ we may impose in a natural manner an ordering, also denoted by $<$, on the set $S = \{\overline{x} \mid x \in G\}$ by defining

$$\overline{x} < \overline{y} \text{ if and only if } x < y .$$

We now suppose the numbering is chosen so that

$$g_1 < g_2 < \dots < g_m \quad \text{and} \quad h_1 < h_2 < \dots < h_n .$$

Then we have

$$\begin{array}{l} g_1 h_1 < g_2 h_1 < \dots < g_m h_1 , \\ g_1 h_2 < g_2 h_2 < \dots < g_m h_2 , \\ \;\;\dots \qquad\;\; \dots \qquad\;\; \dots \\ g_1 h_n < g_2 h_n < \dots < g_m h_n . \end{array}$$

From these relations it follows immediately that

$$\overline{g_1h_1} < \overline{g_2h_1} < \dots < \overline{g_mh_1} \ ,$$

$$\overline{g_1h_2} < \overline{g_2h_2} < \dots < \overline{g_mh_2} \ ,$$

$$\dots \quad \dots \quad \dots$$

$$\overline{g_1h_n} < \overline{g_2h_n} < \dots < \overline{g_mh_n} \ .$$

The maximal element of $\{\overline{g_ih_j} \mid i = 1, 2, \dots, m \ , \ j = 1, 2, \dots, n\}$ must occur in the set $\{\overline{g_mh_j} \mid j = 1, 2, \dots, n\}$, and for the sake of argument, we suppose $\overline{g_mh_{j_1}}$ is the maximal element of this set. By 1.13(I) the maximal element $\overline{g_mh_{j_1}}$ occurs precisely once in

$$\{\overline{g_ih_j} \mid i = 1, 2, \dots, m, \ j = 1, 2, \dots, n\} \ .$$

Hence $\overline{g_mh_{j_1}}$ is unique.

To prove that $\alpha_i\beta_j = 0$ whenever $g_ih_j \neq 1$ we need to prove $\alpha_i\beta_j = 0$ whenever $g_ih_j < 1$ or $g_ih_j > 1$. We know that it is false that $g_mh_{j_1} < 1$, because if $g_mh_{j_1} < 1$, then $(\sum_{i=1}^{m} \alpha_i\overline{g_i})(\sum_{j=1}^{n} \beta_j\overline{h_j}) = \gamma(1, 1)^{-1}\,\overline{1}$ does not hold. If $g_mh_{j_1} = 1$, then we prove $\alpha_i\beta_j = 0$ whenever $g_ih_j < 1$, because there is no element g_ih_j such that $g_ih_j > 1$.

Let us assume that $g_mh_{j_1} > 1$. Since $g_mh_{j_1}$ is maximal and unique in $\{g_ih_j \mid i = 1, 2, \dots, m, \ j = 1, 2, \dots, n\}$ it follows from

$$(\sum_{i=1}^{m} \alpha_i\overline{g_i})(\sum_{j=1}^{n} \beta_j\overline{h_j}) = \sum_{\substack{1\le i\le m \\ 1\le j\le n}} \alpha_i\beta_j\,\gamma(g_i, h_j)\overline{g_ih_j} = \gamma(1, 1)^{-1}\,\overline{1} \ ,$$

that $\alpha_mh_{j_1}\,\gamma(g_m, h_{j_1}) = 0$. But $\gamma(g_m, h_{j_1})$ is a unit in R and so we have $\alpha_m\beta_{j_1} = 0$.

Now we proceed to prove that $\alpha_i \beta_j = 0$ whenever $g_i h_j > 1$. Assume that $\alpha_r \beta_s = 0$ whenever there exists $p > 1$ such that

$$g_r h_s > g_{\varepsilon_1} h_{k_1} = g_{\varepsilon_2} h_{k_2} = \ldots = g_{\varepsilon_p} h_{k_p} > 1 \qquad (6)$$

Where $g_{\varepsilon_\nu} h_{k_\nu}$ $(\nu = 1, 2, \ldots, p)$ are all of the elements equal to $g_{\varepsilon_1} h_{k_1}$. Hence from

$$\sum_{i=1}^{m} \alpha_i \overline{g_i} \sum_{j=1}^{n} \beta_j \overline{h_j} = \gamma(1, 1)^{-1} \overline{1}$$

we have

$$\alpha_{\varepsilon_1} \beta_{k_1} \gamma(g_{\varepsilon_1}, h_{k_1}) + \alpha_{\varepsilon_2} \beta_{k_2} \gamma(g_{\varepsilon_2}, h_{k_2}) + \ldots + \alpha_{\varepsilon_p} \beta_{k_p} \gamma(g_{\varepsilon_p}, h_{k_p}) = 0 \qquad (7)$$

Suppose we have arranged the notation such that $\varepsilon_1 < \varepsilon_2 < \ldots < \varepsilon_p$. Then by multiplying (7) by α_{ε_p} we have

$$\alpha_{\varepsilon_1} \beta_{k_1} \alpha_{\varepsilon_p} \gamma(g_{\varepsilon_1}, h_{k_1}) + \alpha_{\varepsilon_2} \beta_{k_2} \alpha_{\varepsilon_p} \gamma(g_{\varepsilon_2}, h_{k_2}) + \ldots$$

$$+ \alpha_{\varepsilon_p} \beta_{k_p} \alpha_{\varepsilon_p} \gamma(g_{\varepsilon_p}, h_{k_p}) = 0 . \qquad (8)$$

But $1 \leq t < p$ implies that $\varepsilon_t < \varepsilon_p$ and this in turn implies that $g_{\varepsilon_t} h_{k_t} < g_{\varepsilon_p} h_{k_t}$. Since $g_{\varepsilon_t} h_{k_t} > 1$ for $1 \leq t \leq p$, we have $g_{\varepsilon_p} h_{k_t} > g_{\varepsilon_t} h_{k_t} > 1$. From this and the hypothesis for (6) we have $\alpha_{\varepsilon_p} \beta_{k_t} = 0$ for $1 \leq t < p$. Hence from (8) we conclude that $\alpha_{\varepsilon_p} \beta_{k_p} \alpha_{\varepsilon_p} = 0$. This implies that

$$\alpha_{\varepsilon_p} \beta_{k_p} \alpha_{\varepsilon_p} \beta_{k_p} = (\alpha_{\varepsilon_p} \beta_{k_p})^2 = 0 .$$

But R has no non-zero nilpotent elements and so $(\alpha_{\varepsilon_p} \beta_{k_p})^2 = 0$ implies that $\alpha_{\varepsilon_p} \beta_{k_p} = 0$. In this way we deduce that $\alpha_{\varepsilon_t} \beta_{k_t} = 0$ for $1 \leq t \leq p$. Hence $\alpha_i \beta_j = 0$ whenever $g_i h_j > 1$. Similarly we prove $\alpha_i \beta_j = 0$ whenever $g_i h_j < 1$. Δ

We now utilise the previous lemma to extend the results to rings with nilpotent elements.

<u>Lemma 2.2</u>

Let R be a commutative ring and let G be a right-ordered group. Let $R^{\gamma}(G)$ be a twisted group ring of G over R . Then $\sum_g \alpha_g \overline{g}$ is a unit in $R^{\gamma}(G)$ if and only if there exist $\beta_g \in R$ such that $\sum_g \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1}$ and $\alpha_g \beta_h$ is nilpotent whenever $gh \neq 1$.

<u>Proof</u>

We assume first that $\sum_g \alpha_g \overline{g}$ is a unit in $R^{\gamma}(G)$. Let P be the prime radical (1.5) of R . Then by (1.11) $\sum_g \overline{\alpha_g}\, \overline{g}$ $(\overline{\alpha_g} \in R/P)$ is a unit in $(R/P)^{\overline{\gamma}}(G)$. Since R/P has no non-zero nilpotent elements by lemma (2.1) there exist $\overline{\delta_g} \in R/P$ such that

$$\sum_g \overline{\alpha_g}\, \overline{\delta_{g^{-1}}}\, \overline{\gamma(g, g^{-1})} = \overline{\gamma(1, 1)^{-1}} \quad \text{and} \quad \overline{\alpha_g}\, \overline{\delta_h}\, \overline{\gamma(g, h)} = 0$$

whenever $gh \neq 1$. From this we conclude that

$$\sum_g \alpha_g \delta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1} + n ,$$

where n is nilpotent in R and $\alpha_g \delta_h \gamma(g, h)$ is nilpotent in R whenever $gh \neq 1$. By (1.2) we conclude that $\sum_g \alpha_g \delta_{g^{-1}} \gamma(g, g^{-1})$ is a unit. Let $(\sum_g \alpha_g \delta_{g^{-1}} \gamma(g, g^{-1}))^{-1} = w$. Since $\alpha_g \delta_h \gamma(g, h)$ is nilpotent whenever $gh \neq 1$ and R is commutative $\alpha_g \delta_h \gamma(g, h)w$ is also nilpotent in R whenever $gh \neq 1$. Thus by letting $\beta_g = \delta_g w$ the 'only if' part of the lemma has been established.

Now, we suppose there exist β_g in R such that $\sum \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1}$ and $\alpha_g \beta_h$ is nilpotent in R whenever $gh \neq 1$. This means that there exists $\sum \beta_h \bar{h} \in R^{\gamma}(G)$ such that $(\sum_g \alpha_g \bar{g})(\sum_h \beta_h \bar{h}) = \gamma(1, 1)^{-1} \bar{1} + \sum_{\substack{g,h \\ gh\neq 1}} \alpha_g \beta_h \gamma(g, h)\overline{gh}$

where $\alpha_g \beta_h$ is nilpotent when $gh \neq 1$. Hence $\sum_{\substack{g,h \\ gh\neq 1}} \alpha_g \beta_h \gamma(g, h)\overline{gh}$

is nilpotent and so by (1.2), $(\sum_g \alpha_g \bar{g})(\sum_h \beta_h \bar{h})$ is a unit. This implies that $\sum_g \alpha_g \bar{g}$ is a unit. Δ

Corollary 2.3

Let R be a commutative ring with no non-trivial idempotents. Let G be a right-ordered group and let $R^{\gamma}(G)$ be a twisted group ring of G over R. Then $\sum_g \alpha_g \bar{g}$ is a unit in $R^{\gamma}(G)$ if and only if α_λ is a unit in R for some λ, and all other α_g's are nilpotent in R.

Proof

By lemma (2.2) $\sum_g \alpha_g \bar{g}$ is a unit in $R^\gamma(G)$ if and only if there exist $\beta_g \in R$ such that

$$\sum_g \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1}) = \gamma(1, 1)^{-1} , \tag{1}$$

and $\alpha_g \beta_h$ is nilpotent in R whenever $gh \neq 1$.

In (1) for fixed ν we have,

$$\alpha_\nu \beta_{\nu^{-1}} \alpha_\nu \gamma(\nu, \nu^{-1}) = \gamma(1, 1)^{-1} \alpha_\nu + n , \tag{2}$$

where n is nilpotent in R . We multiply (2) by $\beta_{\nu^{-1}} \gamma(\nu, \nu^{-1}) \gamma(1, 1)^2$; then we have

$$\alpha_\nu \beta_{\nu^{-1}} \alpha_\nu \beta_{\nu^{-1}} \gamma(\nu, \nu^{-1})^2 \gamma(1, 1)^2 = \gamma(\nu, \nu^{-1}) \gamma(1, 1) \alpha_\nu \beta_{\nu^{-1}} + n_1$$

where n_1 is nilpotent in R . For convenience, let $w = \gamma(\nu, \nu^{-1}) \gamma(1, 1)$ and so we have

$$(w \alpha_\nu \beta_{\nu^{-1}})^2 = w \alpha_\nu \beta_{\nu^{-1}} + n_1 .$$

Now, let P be the prime radical of R (1.5). Then modulo P , $w \alpha_\nu \beta_{\nu^{-1}}$ is an idempotent. Since by (1.7) P is a nil ideal of R and by (1.14) idempotents can be lifted modulo P , there exists an idempotent $f \in R$ such that

$$w \alpha_\nu \beta_{\nu^{-1}} \equiv f \pmod{P} .$$

But R has no non-trivial idempotents so either $f = 0$, or $f = 1$. Then we have

$$w \alpha_\nu \beta_{\nu^{-1}} \equiv 0 \pmod{P} . \tag{3}$$

or

$$w \alpha_\nu \beta_{\nu^{-1}} \equiv 1 \pmod{P} . \tag{4}$$

Suppose (3) holds. Then

$$\gamma(\nu,\ \nu^{-1})\ \gamma(1,\ 1)\ \alpha_\nu\ \beta_{\nu^{-1}} = w\ \alpha_\nu\ \beta_{\nu^{-1}} \in P\ ,$$

whence

$$\gamma(\nu,\ \nu^{-1})\ \ \gamma(1,\ 1)\ \alpha_\nu\ \beta_{\nu^{-1}}\ \alpha_\nu \in P\ . \qquad (5)$$

Furthermore, by multiplying (2) by $\gamma(1,\ 1)$ we have,

$$\gamma(\nu,\ \nu^{-1})\ \gamma(1,\ 1)\ \alpha_\nu\ \beta_{\nu^{-1}}\ \alpha_\nu = \alpha_\nu + \gamma(1,\ 1)\ n\ . \qquad (6)$$

By using (5), (6) and the fact that $\gamma(1,1)\ n \in P$ we conclude that $\alpha_\nu \in P$, i.e. α_ν is nilpotent.

If (3) holds for every ν , then $\sum_g \alpha_g\ \bar{g}$ is nilpotent. But this is false because $\sum_g \alpha_g\ \bar{g}$ is a unit. Hence (4) holds for some ν , say $w\ \alpha_\lambda\ \beta_{\lambda^{-1}} \equiv 1 \pmod P$. Let $n_2 = w\ \alpha_\lambda\ \beta_{\lambda^{-1}} - 1$. Then $n_2 \in P$. Let $\alpha_\varepsilon\ \bar{\varepsilon}$ be any term in $\sum \alpha_g\ \bar{g}$ other $\alpha_\lambda\ \ \bar{\lambda}$. Then by multiplying n_2 by α_ε we have

$$w\ \alpha_\lambda\ \beta_{\lambda^{-1}}\ \alpha_\varepsilon - \alpha_\varepsilon = \alpha_\varepsilon\ n_2\ .$$

By (2.2) $\alpha_\varepsilon\ \beta_{\lambda^{-1}} \in P$ because $\varepsilon\ \lambda^{-1} \neq 1$, and so $w\ \alpha_\lambda\ \beta_{\lambda^{-1}}\ \alpha_\varepsilon \in P$. Also $n_2 \in P$ implies that $\alpha_\varepsilon\ n_2 \in P$, hence from $w\ \alpha_\lambda\ \beta_{\lambda^{-1}}\ \alpha_\varepsilon - \alpha_\varepsilon = \alpha_\varepsilon\ n_2$ we conclude that $\alpha_\varepsilon \in P$. Thus all α_g's other than α_λ are nilpotent.

Again by (2.2) we have $\sum_g \alpha_g\ \beta_{g^{-1}}\ \gamma(g,\ g^{-1}) = \gamma(1,\ 1)^{-1}$. Since all α_g's other than α_λ are nilpotent we have

$$\alpha_\lambda\ \beta_{\lambda^{-1}}\ \gamma(\lambda,\ \lambda^{-1}) + \sum_{g\neq\lambda} \alpha_g\ \beta_{g^{-1}}\ \gamma(g,\ g^{-1}) = \gamma(1,\ 1)^{-1}$$

where

$$\sum_{g\neq\lambda} \alpha_g\ \beta_{g^{-1}}\ \gamma(g,\ g^{-1})$$

is nilpotent in $R^{\gamma}(G)$. Thus we have $\alpha_{\lambda} \beta_{\lambda^{-1}} \gamma(\lambda, \lambda^{-1}) = \gamma(1, 1)^{-1} + n_3$ where $n_3 = - \sum_{g \neq \lambda} \alpha_g \beta_{g^{-1}} \gamma(g, g^{-1})$. But, since $\gamma(1, 1)^{-1}$ is a unit in R , then $\gamma(1, 1)^{-1}$ is a unit in $R^{\gamma}(G)$. Hence by using lemma (1.2) $\gamma(1, 1)^{-1} + n_3$ is a unit in $R^{\gamma}(G)$. This implies that $\alpha_{\lambda} \beta_{\lambda^{-1}} \gamma(\lambda, \lambda^{-1})$ is a unit in $R^{\gamma}(G)$ and so α_{λ} is a unit in $R^{\gamma}(G)$. Thus α_{λ} is a unit in R . Δ

Corollary 2.4

Let R be a commutative ring with no non-zero nilpotents and no non-trivial idempotents. Let G be a right-ordered group and let $R^{\gamma}(G)$ be a twisted group ring of G over R . Then the only units of $R^{\gamma}(G)$ are of the form $r\,\overline{g}$ where r is a unit in R and $g \in G$.

Proof

Since R has no non-trivial idempotents by Corollary (2.3) $\sum \alpha_g \overline{g}$ is a unit in $R^{\gamma}(G)$ if and only if α_{λ} is a unit in R for some λ and all other α_g's are nilpotent in R . Since R has no non-zero nilpotents then $\sum_g \alpha_g \overline{g}$ is a unit in $R^{\gamma}(G)$ if and only if α_{λ} is a unit in R for some λ and all other α_g's are zero. Δ

Before starting to extend theorem (2.1) of [9] we prove some lemmas on group rings of infinite cyclic groups.

Lemma 2.5

Let R be a ring and let $<x>$ be an infinite cyclic group. Let $R^{\gamma}(<x>)$ be a twisted group ring of $<x>$ over R . Let $Z(R)$ be the centre of R and let $Z(R^{\gamma}(<x>))$ be the centre of $R^{\gamma}(<x>)$. Then,

$$Z(R^{\gamma}(<x>)) = (Z(R))^{\gamma}(<x>) \ .$$

Proof

By (1.12) we know that for any integer m , $\overline{x^m} \in Z(R^{\gamma}(\langle x\rangle))$. It follows from this that $(Z(R))^{\gamma}(\langle x\rangle) \subseteq Z(R^{\gamma}(\langle x\rangle))$.

To prove $Z(R^{\gamma}(\langle x\rangle)) \subseteq (Z(R))^{\gamma}(\langle x\rangle)$ we assume that $\sum a_i \overline{x^i}$ is an arbitrary element of $Z(R^{\gamma}(\langle x\rangle))$ and b is also an arbitrary element of R . Then we have

$$(\sum a_i \overline{x^i})(b\,\overline{1}) = (b\,\overline{1})(\sum a_i \overline{x^i}) .$$

This implies that

$$a_i\, b\ \gamma(x^i, 1) = b\, a_i\, \gamma(1, x^i) ,$$

for all i .

By (1.11), $\gamma(x^i, 1) = \gamma(1, x^i) = \gamma(1, 1)$ is a central unit in R and so we have $a_i b = b a_i$ for all i . This implies that $a_i \in Z(R)$ for all i , and hence $Z(R^{\gamma}(\langle x\rangle)) \subseteq (Z(R))^{\gamma}(\langle x\rangle)$.Δ

Lemma 2.6

Let R be a commutative ring and let $\langle x\rangle$ be an infinite cyclic group. Let $R^{\gamma}(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R . Let $\sum a_i \overline{x^i}$ be a unit in $R^{\gamma}(\langle x\rangle)$ and let $\sum b_j \overline{x^j}$ be its inverse in $R^{\gamma}(\langle x\rangle)$. Then, $a_\varepsilon a_\nu$ and $b_\varepsilon b_\nu$ are nilpotent in R whenever $\varepsilon \neq \nu$.

Proof

By example 1.13(I) , $\langle x\rangle$ is a right-ordered group and by using (2.2) we have $\sum a_i b_{-i}\, \gamma(x^i, x^{-i}) = \gamma(1, 1)^{-1}$. Also $a_i b_j$ is nilpotent in R whenever $i + j \neq 0$.

Let P_0 be a given prime ideal of R . Then by (1.11) $\sum \overline{a_i}\, \overline{x^i}$ ($\overline{a_i} \in R/P_0$) is a unit in $(R/P_0)^{\overline{\gamma}}(\langle x\rangle)$. But by (1.6)

R/P_0 is an integral domain and therefore has no non-trivial idempotents. Hence by (2.3) for some i_0 depending on P_0, $\bar{a}_{i_0}$ is a unit in R/P_0 and $\overline{a_i} = \bar{0}$ for all $i \neq i_0$. Also for some j_0 depend on P_0, $\bar{b}_{j_0}$ is a unit in R/P_0 and $\overline{b_j} = \bar{0}$ for all $j \neq j_0$. This implies that exactly one a_i and exactly one b_j do not lie in P_0. In fact, $i_0 = -j_0$ because $\sum \bar{a}_i \bar{b}_{-i} \overline{\gamma(x^i, x^{-i})} = \overline{\gamma(1, 1)^{-1}}$.

Finally we wish to prove that $a_\varepsilon a_\nu$ $(\varepsilon \neq \nu)$ is nilpotent. For this let p be an arbitrary prime ideal of R. Since exactly one a_i does not lie in p we conclude that either a_ε or a_ν belongs to p and then $a_\varepsilon a_\nu$ belong to p. This implies that $a_\varepsilon a_\nu$ belong to all prime ideals of R and then by (1.7) $a_\varepsilon a_\nu$ is nilpotent. Δ

Lemma 2.7

Let R be a commutative ring and let $\langle x\rangle$ be an infinite cyclic group. Let $R^\gamma(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R. Let $\sum a_i \overline{x^i}$ be a unit in $R^\gamma(\langle x\rangle)$ and let a_i be nilpotent for $i \neq 1, -1$. Let there exist $c_t \in R$ such that $\sum_{t=-u}^{\nu} c_t (\sum_i a_i \overline{x^i})^t = 0$. Then c_t is nilpotent for all t.

Proof

Let $(\sum a_i \overline{x^i})^{-1} = \sum b_j \overline{x^j}$, and $\mathfrak{P}$ be a prime ideal of R. Then by (1.11) $\sum_{t=-u}^{\nu} \bar{c}_t (\sum_i \bar{a}_i \overline{x^i})^t = 0$, $(\bar{c}_t, \bar{a}_i \in R/P)$. Since a_i is nilpotent for $i \neq 1, -1,$ we conclude from (1.6) that all

R/P_0 is an integral domain and therefore has no non-trivial idempotents. Hence by (2.3) for some i_0 depending on P_0, $\bar{a}_{i_0}$ is a unit in R/P_0 and $\overline{a_i} = \bar{0}$ for all $i \neq i_0$. Also for some j_0 depend on P_0, $\bar{b}_{j_0}$ is a unit in R/P_0 and $\overline{b_j} = \bar{0}$ for all $j \neq j_0$. This implies that exactly one a_i and exactly one b_j do not lie in P_0. In fact, $i_0 = - j_0$ because $\sum \bar{a}_i \bar{b}_{-i} \overline{\gamma(x^i, x^{-i})} = \overline{\gamma(1, 1)^{-1}}$.

Finally we wish to prove that $a_\varepsilon a_\nu$ $(\varepsilon \neq \nu)$ is nilpotent. For this let p be an arbitrary prime ideal of R. Since exactly one a_i does not lie in p we conclude that either a_ε or a_ν belongs to p and then $a_\varepsilon a_\nu$ belong to p. This implies that $a_\varepsilon a_\nu$ belong to all prime ideals of R and then by (1.7) $a_\varepsilon a_\nu$ is nilpotent. Δ

<u>Lemma 2.7</u>

Let R be a commutative ring and let $\langle x\rangle$ be an infinite cyclic group. Let $R^\gamma(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R. Let $\sum a_i \overline{x^i}$ be a unit in $R^\gamma(\langle x\rangle)$ and let a_i be nilpotent for $i \neq 1, -1$. Let there exist $c_t \in R$ such that $\sum_{t=-u}^{\nu} c_t (\sum_i a_i \overline{x^i})^t = 0$. Then c_t is nilpotent for all t.

<u>Proof</u>

Let $(\sum a_i \overline{x^i})^{-1} = \sum b_j \overline{x^j}$, and $\mathbf{P}$ be a prime ideal of R. Then by (1.11) $\sum_{t=-u}^{\nu} \bar{c}_t (\sum_i \bar{a}_i \overline{x^i})^t = 0$, $(\bar{c}_t, \bar{a}_i \in R/P)$. Since a_i is nilpotent for $i \neq 1, -1$, we conclude from (1.6) that all

$\overline{a_i}$ except $\overline{a_1}$, $\overline{a_{-1}}$ are zero. Furthermore, $\sum a_i \overline{x^i}$ is a unit in $R^\gamma(<x>)$ so by (1.11) $\overline{a_i}\ \overline{x^i}$ is a unit in $(R/P)^{\overline{\gamma}}(<x>)$. Hence by (1.6) and (2.4) we conclude that one of $\overline{a_1}$, $\overline{a_{-1}}$ must be zero and the other one must be a unit in R/P . Thus there are two cases as follows:

(i) $\overline{a_1}$ is a unit in R/P and $\overline{a_{-1}}$ is zero.

(ii) $\overline{a_{-1}}$ is a unit in R/P and $\overline{a_1}$ is zero.

Since the proofs for (i), (ii) are similar we assume, for convenience, that (i) holds.

By example 1.13(I) $<x>$ is a right-ordered group. Then by using (2.2) we have $\sum a_i b_{-i} \gamma(x^i, x^{-i}) = \gamma(1, 1)^{-1}$. From this and the fact that $\overline{a_i} = 0$ for all $i \neq 1$ we obtain $\overline{a_1}\ \overline{b_{-1}}\ \overline{\gamma(x, x^{-1})} = \overline{\gamma(1, 1)^{-1}}$. This implies that $\overline{b_{-1}}$ is also a unit in R/P because $\overline{\gamma(1, 1)^{-1}}$, $\overline{\gamma(x, x^{-1})}$, $\overline{a_1}$ are units in R/P . But $\sum b_j \overline{x^j}$ is a unit in $R^\gamma(<x>)$, hence by (1.11) $\sum \overline{b_j}\ \overline{x^j}$ is a unit in $(R/P)^{\overline{\gamma}}(<x>)$. Thus by (1.6) and (2.4) exactly one $\overline{b_j}$ must be a unit in R/P and all the other $\overline{b_j}$'s must be zero. Since $\overline{b_{-1}}$ is a unit in R/P we conclude that $\overline{b_j} = 0$ for all $j \neq -1$.

Since $\overline{a_1}$ is a unit and $\overline{a_i} = 0$ for $i \neq 1$ we deduce from

$$\sum_{t=-u}^{t=v} \overline{c_t}\ (\sum_i \overline{a_i}\ \overline{x^i})^t = 0$$

that

$$\sum \overline{c_t}\ (\overline{a_1}\ \overline{x})^t = 0$$

i.e.

$$\sum \overline{c_t}\ \overline{a_1}^t\ \overline{x}^t = 0 .$$

This implies that $\overline{c_t} = 0$ for all t , i.e. $c_t \in P$ for all t . But P is an arbitrary prime ideal and so each c_t belongs to all prime ideals of R . This implies by (1.5) and (1.7) that all c_t are nilpotent in R . Δ

We shall in lemma (2.8) obtain a stronger result.

Lemma 2.8

Let R be a commutative ring and let $\langle x\rangle$ be an infinite cyclic group. Let $R^{\gamma}(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R. Let $\sum a_i \overline{x^i}$ be a unit in $R^{\gamma}(\langle x\rangle)$ and let a_i for $i \neq 1, -1$ be nilpotent. Let there exist $c_t \in R$ such that

$$\sum_{t=-u}^{\nu} c_t \left(\sum_i a_i \overline{x^i}\right)^t = 0 \ , \ u \ , \ \nu \quad \text{positive integers.}$$

Then all $c_t = 0$.

Proof

Let $(\sum a_i \overline{x^i})^{-1} = \sum b_j \overline{x^j}$. By (2.6) $a_\varepsilon a_\nu$ and $b_\varepsilon b_\nu$ are nilpotents whenever $\varepsilon \neq \nu$. By (2.7) all c_t are nilpotent.

Let T be the ideal of R generated by,

$$\{c_t\} \cup \{a_i \mid a_i \text{ is nilpotent}\} \cup \{b_j \mid b_j \text{ is nilpotent}\}$$
$$\cup \{a_\varepsilon a_\nu \mid \varepsilon \neq \nu\} \cup \{b_\varepsilon b_\nu \mid \varepsilon \neq \nu\}$$

Then T is nilpotent. Let all $c_t \in T^k$ for some $k > 0$, but some c_t does not belong to T^{k+1} . Let $\overline{R} = R/T^{k+1}$. In $\overline{R}^{\gamma}(\langle x\rangle)$ we have

$$\sum_{t=-u}^{\nu} \overline{c_t} \left(\sum_i \overline{a_i}\, \overline{x^i}\right)^t = 0 \ .$$

We can write

$$\sum_{t=-u}^{\nu} \overline{c_t} \left(\sum_i \overline{a_i}\, \overline{x^i}\right)^t = \sum_{t=-u}^{-1} \overline{c_t}\left(\sum_i \overline{a_i}\, \overline{x^i}\right)^t + \overline{c_0} + \sum_{t=1}^{\nu} \overline{c_t} \left(\sum_i \overline{a_i}\, \overline{x^i}\right)^t$$

$$= \sum_{t=1}^{u} \overline{c_{-t}} \left(\sum_i \overline{a_i}\, \overline{x^i}\right)^{-t} + \overline{c_0} + \sum_{t=1}^{\nu} \overline{c_t}\left(\sum_i \overline{a_i}\, \overline{x^i}\right)^t = 0 \ ,$$

that is

$$\sum_{t=1}^{u} \overline{c_{-t}} \left(\sum_j \overline{b_j}\, \overline{x^j}\right)^t + \overline{c_0} + \sum_{t=1}^{\nu} \overline{c_t}\left(\sum \overline{a_i}\, x^i\right)^t = 0 \qquad (1)$$

Since all $c_t \in T^k$ and $a_i \in T$, $b_i \in T$ when $i \neq 1, -1$ we have

$$\sum_{t=1}^{u} \overline{c_{-t}}(\overline{b_{-1}}\ \overline{x^{-i}} + \overline{b_1}\ \overline{x})^t + \overline{c_0} + \sum_{t=1}^{\nu} \overline{c_t}(\overline{a_1}\ \overline{x} + \overline{a_{-1}}\ \overline{x^{-1}})^t = 0 . \qquad (2)$$

By equating the coefficients of $(\overline{x})^t$ for $t > 0$ in (2) we conclude that

$$\overline{c_{-t}}\ (\overline{b_1})^t + \overline{c_t}(\overline{a_1})^t = 0 , \qquad t > 0 . \qquad (3)$$

By using the fact that all $c_t \in T^k$ and $b_1\ b_{-1} \in T$ we multiply (3) by $\overline{b_{-1}}$ and we have

$$\overline{c_t}\ (\overline{a_1})^t\ \overline{b_{-1}} = 0 , \qquad t > 0 . \qquad (4)$$

Two cases arise:

(1) $t = 1$.

(2) $t > 1$.

In case (1) we have $\overline{c_1}\ \overline{a_1}\ \overline{b_{-1}} = 0$.

In case (2) we prove that $\overline{c_t}\ \overline{a_1} = 0$.

By (2.2) we know that $\sum a_i\ b_{-i}\ \gamma(x^i, x^{-i}) = \gamma(1, 1)^{-1}$. From this we obtain

$$\sum \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^i, x^{-i})} = \overline{\gamma(1, 1)^{-1}} . \qquad (5)$$

From (5) we conclude that

$$\overline{a_1}\ \overline{b_{-1}}\ \overline{\gamma(x, x^{-1})} = \overline{\gamma(1, 1)^{-1}} - \overline{a_{-1}}\ \overline{b_1}\ \overline{\gamma(x^{-1}, x)}$$

$$- \sum_{i \neq 1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^i, x^{-i})} . \qquad (6)$$

By multiplying (4) by $\overline{\gamma(x, x^{-1})}$ we have

$$\overline{c_t}(\overline{a_1})^{t-1} (\overline{a_1}\ \overline{b_{-1}})\ \overline{\gamma(x, x^{-1})} = 0 , \quad t > 1 . \qquad (7)$$

Now by multiplying (6) by $\overline{c_t}(\overline{a_1})^{t-1}$ $(t > 1)$, and using (7) we conclude that

$$0 = \overline{c_t}(\overline{a_1})^{t-1} (\overline{a_1}\ \overline{b_{-1}})\ \overline{\gamma(x, x^{-1})}$$

$$= \overline{c_t}(\overline{a_1})^{t-1} [\overline{\gamma(1, 1)^{-1}} - \overline{a_{-1}}\ \overline{b_1}\ \gamma(x^{-1}, x) - \sum_{i\neq 1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^{i}, x^{-i})}] \quad (8)$$

But $\overline{c_t}\ (\overline{a_i})^{t-1} \sum_{i\neq 1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^{i}, x^{-i})} = 0$, because all $c_t \in T^{k}$ and a_i belong to T for $i \neq 1, -1$. Also $\overline{c_t}\ (\overline{a_1})^{t-1}\ \overline{a_{-1}}\ \overline{b_1}\ \overline{\gamma(x^{-1}, x)} = 0$ because $t > 1$ and by (2.6) $a_1\ a_{-1} \in T$. Thus from (8) we have $\overline{c_t}\ (\overline{a_1})^{t-1}\ \overline{\gamma(1, 1)^{-1}} = 0$. This implies that $\overline{c_t}\ (\overline{a_1})^{t-1} = 0$ because $\overline{\gamma(1, 1)^{-1}}$ is a unit in ${}^{R}/_{T^{k+1}}$.

By repeating in this manner we obtain $\overline{c_t}\ \overline{a_1} = 0$ $(t > 1)$. Similarly we prove that $\overline{c_1}\ \overline{a_{-1}}\ \overline{b_1} = 0$ and $\overline{c_t}\ \overline{a_{-1}} = 0$ $(t > 1)$.

Thus we have $\overline{c_1}\ \overline{a_1}\ \overline{b_{-1}} = 0$, $\overline{c_1}\ \overline{a_{-1}}\ \overline{b_1} = 0$, and also $\overline{c_t}\ \overline{a_1} = 0$, $\overline{c_t}\ \overline{a_{-1}} = 0$ for $t > 1$. By using these results and multiplying $\sum \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^{i}, x^{-i})} = \overline{\gamma(1, 1)^{-1}}$ by $\overline{c_t}$ $(t \geq 1)$ we have

$$0 = \overline{c_t}[\overline{a_1}\ \overline{b_{-1}}\ \overline{\gamma(x, x^{-1})} + \overline{a_{-1}}\ \overline{b_1}\ \overline{\gamma(x^{-1}, x)} + \sum_{i\neq 1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^{i}, x^{-i})}]$$

$$= \overline{c_t}\ \overline{\gamma(1, 1)^{-1}}$$

This implies that $\overline{c_t}\,\overline{\gamma(1,\ 1)^{-1}} = 0$ i.e., $\overline{c_t} = 0$ because $\overline{\gamma(1,\ 1)^{-1}}$ is a unit. Hence $c_t \in T^{k+1}$ for $t \geq 1$.

Now we show that all c_t , $(t \leq -1)$ beong to T^{k+1} . For this we multiply $\overline{c_{-t}}\,(\overline{b_1})^t + \overline{c_t}(\overline{a_1})^t = 0$, $(t > 0)$ by $\overline{a_{-1}}$, and since $c_t(a_1)^t a_{-1} \in T^{k+1}$ we have

$$\overline{c_{-t}}\,(\overline{b_1})^t\,\overline{a_{-1}} = 0\ , \qquad t > 0\ . \tag{9}$$

Two cases arise:

(5) $t = 1$.

(6) $t > 1$.

In case (5) we have $\overline{c_{-1}}\,\overline{b_1}\,\overline{a_{-1}} = 0$.

In case (6) we show that $\overline{c_t}\,\overline{b_1} = 0$, $t < -1$. For this from $\sum \overline{a_i}\,\overline{b_{-i}}\ \overline{\gamma(x^i,\ x^{-i})} = \overline{\gamma(1,\ 1)^{-1}}$ we conclude that

$$\overline{a_{-1}}\,\overline{b_1}\ \overline{\gamma(x^{-1},\ x)} = \overline{\gamma(1,\ 1)^{-1}} - \overline{a_1}\,\overline{b_{-1}}\ \overline{\gamma(x,\ x^{-1})} - \sum_{i=1,-1} \overline{a_i}\,\overline{b_{-i}}\ \overline{\gamma(x^i,\ x^{-i})} \tag{10}$$

Also from (9) we obtain

$$\overline{c_{-t}}\ (\overline{b_1})^{t-1}(\overline{b_1}\ \overline{a_{-1}})\overline{\gamma(x^{-1},\ x)} = 0\ , \qquad t > 1\ . \tag{11}$$

By (10) and (11) we conclude that

$$0 = \overline{c_{-t}}(\overline{b_1})^{t-1}(\overline{b_1}\ \overline{a_{-1}})\overline{\gamma(x^{-1},\ x)}$$

$$= \overline{c_{-t}}(\overline{b_1})^{t-1}\ [\overline{\gamma(1,\ 1)^{-1}} - \overline{a_1}\ \overline{b_{-1}}\ \overline{\gamma(x,\ x^{-1})} - \sum_{i=1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^i,\ x^{-i})}]\ . \tag{12}$$

But we know that all $c_t \in T^k$ and $a_i \in T$ for $i \neq 1, -1$. Also $t > 1$ and $b_1\ b_{-1} \in T$. Hence from (12) we obtain

$\overline{c_{-t}}(\overline{b_1})^{t-1}\ \overline{\gamma(1,\ 1)^{-1}} = 0$ and this implies that $\overline{c_{-t}}(\overline{b_1})^{t-1} = 0$ because $\overline{\gamma(1,\ 1)^{-1}}$ is a unit in R/T^{k+1}. By repeating in this manner we have $\overline{c_{-t}}\ \overline{b_1} = 0$, $t > 1$. Hence $\overline{c_t}\ \overline{b_1} = 0$, $t < -1$. Similarly we prove that $\overline{c_{-1}}\ \overline{b_{-1}}\ \overline{a_1} = 0$ and $\overline{c_t}\ \overline{b_{-1}} = 0$ $(t < -1)$.

Thus we proved that, $\overline{c_{-1}}\ \overline{b_1}\ \overline{a_{-1}} = 0$, $\overline{c_{-1}}\ \overline{b_{-1}}\ \overline{a_1} = 0$. Also $\overline{c_t}\ \overline{b_1} = 0$, $\overline{c_t}\ \overline{b_{-1}} = 0$ for $t < -1$. By using these results and multiplying

$$\sum \overline{a_i}\ \overline{b_{-i}}\,\overline{\gamma(x^i,\ x^{-i})} = \overline{\gamma(1,\ 1)^{-1}}$$

by $\overline{c_t}$ $(t \le -1)$ we conclude that

$$0 = \overline{c_t}\ [\overline{a_1}\ \overline{b_{-1}}\ \overline{\gamma(x,\ x^{-1})} + \overline{a_{-1}}\ \overline{b_1}\ \overline{\gamma(x^{-1},\ x)} + \sum_{i\neq 1,-1} \overline{a_i}\ \overline{b_{-i}}\ \overline{\gamma(x^i,\ x^{-i})}]$$

$$= \overline{c_t}\ \overline{\gamma(1,\ 1)^{-1}} .$$

This implies that $\overline{c_t} = 0$ for $t \le -1$.

Now we proved that $\overline{c_t} = 0$ for $t \ge 1$ and $\overline{c_t} = 0$ for $t \le -1$. By these results and

$$\sum_{t=-u}^{v} \overline{c_t}\ (\sum_i \overline{a_i}\ \overline{x^i})^t = 0$$

we conclude that $\overline{c_0} = 0$. Hence all c_t belong to T^{k+1}, contrary to assumption. Consequently all c_t lie in arbitrary large powers of T. Since T is nilpotent all $c_t = 0$. Δ

Now we are in a position to extend Theorem (2.1) of [9]. Since the proof is long we split it into two lemmas.

Lemma 2.9

Let R be a ring and let $\langle x\rangle$ be an infinite cyclic group. Let $R^{\gamma}(\langle x\rangle)$ be a twisted group ring of $\langle x\rangle$ over R and let $Z(R^{\gamma}(\langle x\rangle))$ be the centre of $R^{\gamma}(\langle x\rangle)$. Let $Z(R)$ be the centre of R and let $\overline{\theta} : \overline{x} \to \sum_i a_i \overline{x^i}$ induce an R-automorphism of $R^{\gamma}(\langle x\rangle)$.

Then the following two conditions hold:

(i) $\sum a_i \overline{x^i}$ is a unit in $(Z(R))^{\gamma}(\langle x\rangle)$.

(ii) If $i \neq 1, -1$, then a_i is nilpotent.

Proof

By (2.5) $Z(R^{\gamma}(\langle x\rangle)) = (Z(R))^{\gamma}(\langle x\rangle)$ and by (1.12) $\overline{x}$ is a central unit in $R^{\gamma}(\langle x\rangle)$. Since $\overline{\theta}$ is an R-automorphism of $R^{\gamma}(\langle x\rangle)$ we conclude that $\sum_i a_i \overline{x^i}$ is a unit in

$(Z(R))^{\gamma}(\langle x\rangle) = Z(R^{\gamma}(\langle x\rangle))$ and (i) holds.

Now we prove (ii). $\sum_i a_i \overline{x^i}$ is a unit in $(Z(R))^{\gamma}(\langle x\rangle)$.

Then $(\sum_i a_i \overline{x^i})^{-1}$ exists and belongs to $(Z(R))^{\gamma}(\langle x\rangle)$. Let

$$(\sum_i a_i \overline{x^i})^{-1} = \sum_j b_j \overline{x^j} .$$

Hence we conclude that $a_i, b_j \in Z(R)$ for all i, j . Since

$\overline{\theta} : \overline{x} \to \sum_i a_i \overline{x^i}$ is an R-automorphism of $R^{\gamma}(<x>)$, $\{(\sum_i a_i \overline{x^i})^t : t \in \mathbb{Z}\}$ is an R-basis of $R^{\gamma}(<x>)$ and so there exist $c_t \in Z(R)$ such that

$$\overline{x} = \sum_{t=-\varepsilon}^{\delta} c_t \, (\sum_i a_i \overline{x^i})^t \text{ , } \varepsilon \text{ , } \delta \text{ positive integers.}$$

By applying

$$(\sum_i a_i \overline{x^i})^{-t} = (\sum_j b_j \overline{x^j})^t \text{ , } \quad (t > 0)$$

we have

$$\begin{aligned} \overline{x} = c_{-\varepsilon} (\sum_i a_i \overline{x^i})^{-\varepsilon} + \ldots + c_{-1} (\sum_i a_i \overline{x^i})^{-1} + c_0 + c_1 (\sum_i a_i \overline{x^i}) \\ + \ldots + c_{\delta} (\sum_i a_i \overline{x^i})^{\delta} = c_{-\varepsilon} (\sum_j b_j \overline{x^j})^{\varepsilon} \\ + \ldots + c_{-1} (\sum_j b_j \overline{x^j}) + c_0 + c_1 (\sum_i a_i \overline{x^i}) \\ + \ldots + c_{\delta} (\sum_i a_i \overline{x^i})^{\delta} \text{ .} \qquad (1) \end{aligned}$$

The coefficient of $\overline{x}$ on the left hand side of (1) is 1 .

The coefficient of $\overline{x}$ in $c_{-1}(\sum_j b_j \overline{x^j})$ is $c_{-1} b_1$ and the coefficient of $\overline{x}$ in $c_1(\sum_i a_i \overline{x^i})$ is $c_1 a_1$.

But by (2.6) all $a_{\mu} a_{\nu}$ and $b_{\mu} b_{\nu}$ for $\mu \neq \nu$ are nilpotent in $Z(R)$, and so the coefficient of $\overline{x}$ in $c_k(\sum_i a_i \overline{x^i})^k$ for either $k > 1$ or $k < -1$ is nilpotent.

Hence by equating the coefficients of $\overline{x}$ in (1) we have

$$1 = c_{-1} b_1 + c_1 a_1 + n \ , \qquad (2)$$

where n is nilpotent in $Z(R)$.

Let P be an arbitrary prime ideal of $Z(R)$. If $a_1 \in P$ and $b_1 \in P$ then by using (2) we have $1 \in P$, because n is nilpotent, and then $P = Z(R)$. Hence for any prime ideal P of $Z(R)$, $a_1 \in P$ implies that $b_1 \notin P$.

By example 1.13 (I), $<x>$ is a right-ordered group and then by (2.2) we have

$$\sum a_i \, b_{-i} \, \gamma(x^i, x^{-i}) = \gamma(1, 1)^{-1} \ , \qquad (3)$$

and $a_i b_j$ is nilpotent in $Z(R)$ whenever $i + j \neq 0$. From this and multiplying (3) by b_1 we obtain

$$b_1 \, a_{-1} \, b_1 \, \gamma(x^{-1}, x) = b_1 \ \gamma(1, 1)^{-1} + n_1 \ , \qquad (4)$$

where n_1 is nilpotent in $Z(R)$.

It follows from (4) that if a_{-1} belongs to any prime ideal P of $Z(R)$, then b_1 also belongs to P , because n_1 is nilpotent. Suppose there exists a prime ideal P of $Z(R)$ such that $a_1 \in P$ and $a_{-1} \in P$. We wish to show that P cannot exist. By above paragraphs $a_1 \in P$ implies that $b_1 \notin P$ and $a_{-1} \in P$ implies that $b_1 \in P$ which is impossible. Thus for any prime ideal P of $Z(R)$, $a_1 \in P$ implies that $a_{-1} \notin P$.

Finally, consider a_t , $t \neq \pm 1$. We wish to show that a_t belongs to all prime ideals of $Z(R)$. For the sake of argument suppose Q is a prime ideal of $Z(R)$ such that $a_t \notin Q$. Since $\sum_i a_i \overline{x}^i$ is a unit in $(Z(R))^{\gamma}(<x>)$ by (1.11)

$$\sum \overline{a_i} \, \overline{x}^i \ (\overline{a_i} = a_i + Q)$$

is a unit. By using (2.4) and the fact that $\overline{a_t} \neq \overline{0}$ we conclude that $\overline{a_t}$ is a unit in R/Q and $\overline{a_\lambda} = \overline{0}$ for all $\lambda \neq t$. In particular $\overline{a_1} = \overline{0}$, $\overline{a_{-1}} = \overline{0}$ and then $a_1 \in Q$, $a_{-1} \in Q$ which is false. Hence for any prime ideal P of $Z(R)$, $a_t \in P$ whenever $t \neq \pm 1$; i.e. a_t is nilpotent whenever $t \neq \pm 1$. Δ

<u>Lemma 2.10</u>

Let R be a ring and let $<x>$ be an infinite cyclic group. Let $R^\gamma(<x>)$ be a twisted group ring of $<x>$ over R and let $Z(R^\gamma(<x>))$ be the centre of $R^\gamma(<x>)$. Let $Z(R)$ be the centre of R .

Suppose that

(i) $\sum a_i \overline{x^i}$ is a unit in $(Z(R))^\gamma(<x>)$.

(ii) If $i \neq 1, -1,$ then a_i is nilpotent.

Then the map $\overline{\theta} : \overline{x}^j \to (\sum_i a_i \overline{x^i})^j$ induces an R-automorphism of $R^\gamma(<x>)$.

<u>Proof</u>

Let $(\sum_i a_i \overline{x^i})^{-1} = \sum_j b_j \overline{x^j}$.

First by (2.5) we know that $Z(R^\gamma(<x>)) = (Z(R))^\gamma(<x>)$. Now we define $\tilde{\theta} : (Z(R))^\gamma(<x>) \to (Z(R))^\gamma(<x>)$ by

$$\tilde{\theta}(\sum_\lambda d_\lambda (\overline{x})^\lambda) = \sum_\lambda d_\lambda (\overline{\theta}(\overline{x}))^\lambda = \sum_\lambda d_\lambda (\sum a_i \overline{x^i})^\lambda .$$

By (1.16) $\tilde{\theta}$ is an Z(R)-endomorphism of $(Z(R))^\gamma(<x>)$ and we prove that $\tilde{\theta}$ is 1-1 and onto, i.e. $\tilde{\theta}$ is an Z(R)-automorphism of $(Z(R))^\gamma(<x>)$.

Assume $\sum_t c_t (\overline{x})^t \in (Z(R))^\gamma(<x>)$ such that $\tilde{\theta}[\sum_t c_t (\overline{x})^t] = 0$.

Then we have $\sum_t c_t(\sum_i a_i \overline{x^i})^t = 0$. By (2.8) we conclude that all $c_t = 0$ and hence $\tilde{\theta}$ is 1-1 .

Now we prove that $\tilde{\theta}$ is onto. Since by condition (ii) all a_i for $i \neq 1, -1$ are nilpotent, from

$$\sum_i a_i b_{-i} \gamma(x^i, x^{-i}) = \gamma(1, 1)^{-1}$$

we conclude that

$$a_1 b_{-1} \gamma(x, x^{-1}) + a_{-1} b_1 \gamma(x^{-1}, x) = \gamma(1, 1)^{-1} + n_1 \qquad (2)$$

where n_1 is nilpotent in $(Z(R))^{\gamma}(<x>)$.

Since $\gamma(1, 1)^{-1} \bar{1}$ is the identity element of $(Z(R))^{\gamma}(<x>)$ we have

$$[\gamma(x, x^{-1})b_{-1} (\sum a_i \overline{x^i}) + \gamma(x^{-1}, x)a_{-1} (\sum b_j \overline{x^j})] \bar{1}$$

$$= [\gamma(x, x^{-1})b_{-1}a_1\bar{x} + \gamma(x, x^{-1})b_{-1}(\sum_{i\neq 1} a_i\overline{x^i}) + \gamma(x^{-1},x)a_{-1}b_1\bar{x} + \gamma(x^{-1}, x)a_{-1} (\sum_{j\neq 1} b_j\overline{x^j})]\bar{1}$$

$$= [\gamma(x, x^{-1})b_{-1}a_1 + \gamma(x^{-1}, x)a_{-1}b_1]\bar{1}\,\bar{x} + n_2$$

where n_2 is nilpotent in $(Z(R))^{\gamma}(<x>)$. From this and (2) we have

$$[\gamma(x, x^{-1})b_{-1} (\sum_i a_i \overline{x^i}) + \gamma(x^{-1}, x)a_{-1} (\sum_j b_j \overline{x^j})]\bar{1}$$

$$= [\gamma(1, 1)^{-1} + n_1]\bar{1}\bar{x} + n_2 = \gamma(1, 1)^{-1} \bar{1}\,\bar{x} + n_1 \bar{1}\,\bar{x} + n_2$$

$$= \gamma(1, 1)^{-1} \bar{1}\,\bar{x} + n_3 = \bar{x} + n_3$$

where $n_3 = n_1 \bar{1}\,\bar{x} + n_2$ is nilpotent in $(Z(R))^{\gamma}(<x>)$.

Let $n_3 = \sum_\mu d_\mu \overline{x^\mu}$. Then each d_μ is nilpotent. Let N be the ideal of $Z(R)$ generated by all d_μ . Then N is a nilpotent ideal of $Z(R)$.

By (1.17) we have $(\bar{x} + n_3)^\mu = (\bar{x})^\mu + n_4$ where $n_4 \in N\,(<x>)$. Also by (1.15) we have $(\bar{x})^\mu = \xi_\mu \overline{x^\mu}$ where ξ_μ is a unit in $Z(R)$. Hence we conclude that $\bar{x} + n_3 - \sum_\mu d_\mu \xi_\mu^{-1} (\bar{x} + n_3)^\mu = \bar{x} + n_5$ where $n_5 = -\sum_\mu d_\mu \xi_\mu^{-1} m_\mu \in N^2\,(<x>)$, say $n_5 = \sum_\sigma \psi_\sigma \overline{x^\sigma}$ with $\psi_\sigma \in N^2$.

Again by (1.17) and (1.15) we have

$$\bar{x} + n_5 - \sum_\sigma \psi_\sigma f_\sigma^{-1} (\bar{x} + n_5)^\sigma = \bar{x} + n_6$$

where $(\bar{x})^\sigma = f_\sigma \overline{x^\sigma}$ and $n_6 \in N^3\,(<x>)$.

Since N is nilpotent by repeating in this manner a finite number of times we have

$$[\gamma(x, x^{-1}) b_{-1} \bar{1} (\sum_i a_i \overline{x^i}) + \gamma(x^{-1}, x) a_{-1} \bar{1} (\sum_j b_j \overline{x^j})]$$

$$- \sum d_\mu \xi_\mu^{-1} [\gamma(x, x^{-1}) b_{-1} \bar{1} (\sum_i a_i \overline{x^i}) + \gamma(x^{-1}, x) a_{-1} \bar{1} (\sum_j b_j \overline{x^j}))]^\mu$$

$$- \sum \psi_\sigma f_\sigma^{-1} \{[\gamma(x, x^{-1}) b_{-1} \bar{1} (\sum_i a_i \overline{x^i}) + \gamma(x^{-1}, x) a_{-1} \bar{1} (\sum_j b_j \overline{x^j})]$$

$$- \sum d_\mu \xi_\mu^{-1} [\gamma(x, x^{-1}) b_{-1} \bar{1} (\sum_i a_i \overline{x^i}) + \gamma(x^{-1}, x) a_{-1} \bar{1} (\sum_j b_j \overline{x^j}))]^\mu\}^\sigma + \ldots = \bar{x} .$$

This means we obtain $\bar{x}$ as a linear combination of powers of $\sum a_i \overline{x^i}$. Hence $\tilde{\theta}$ is onto and $\bar{\theta} : \bar{x} \to \sum a_i \overline{x^i}$ induces a $Z(R)$-automorphism of $(Z(R))^\gamma(<x>)$.

Now we define $\tilde{\tilde{\theta}} : R^{\gamma}(<x>) \to R^{\gamma}(<x>)$ by

$$\tilde{\tilde{\theta}}|_{(Z(R))^{\gamma}(<x>)} = \tilde{\theta} \quad \text{and} \quad \tilde{\tilde{\theta}}(r) = r\ , \quad r \in R\ .$$

$\tilde{\tilde{\theta}}$ is an endomorphism of $R^{\gamma}(\ x\ )$ because $\tilde{\theta}$ is an $Z(R)$-automorphism of $(Z(R))^{\gamma}(<x>)$ and by (1.12) $\overline{x^i} \in (Z(R))^{\gamma}(<x>)$.

We show that $\tilde{\tilde{\theta}}$ is onto and 1-1 .

To prove $\tilde{\tilde{\theta}}$ is 1-1 we define $\phi : R^{\gamma}(<x>) \to R^{\gamma}(<x>)$ by,

$$\phi|_{(Z(R))^{\gamma}(<x>)} = \tilde{\theta}^{-1}\ , \quad \text{and} \quad \phi(r) = r\ , \quad r \in R\ .$$

As before ϕ is an endomorphism of $R^{\gamma}(<x>)$ and we have

$$\tilde{\tilde{\theta}}\,\phi[\textstyle\sum a_i\,\overline{x^i}] = \tilde{\tilde{\theta}}[\sum a_i(\tilde{\theta}^{-1}\ (\overline{x^i}))] = \sum a_i\,\tilde{\theta}(\tilde{\theta}^{-1}\ (\overline{x^i})) = \sum a_i\,\overline{x^i}\ .$$

Hence $\tilde{\tilde{\theta}}\,\phi$ is the identity mapping of $R^{\gamma}(<x>)$.

Also we have

$$\phi\,\tilde{\tilde{\theta}}[\textstyle\sum a_i\,\overline{x^i}] = \phi[\sum a_i(\tilde{\theta}(\overline{x^i}))] = \sum a_i\,\tilde{\theta}^{-1}\ (\tilde{\theta}(\overline{x^i})) = \sum a_i\,\overline{x^i}\ .$$

This implies that $\phi\,\tilde{\tilde{\theta}}$ is the identity mapping of $R^{\gamma}(<x>)$. Thus $\tilde{\tilde{\theta}}$ is invertible, i.e. $\tilde{\tilde{\theta}}$ is 1-1 . Since $\phi\,\tilde{\tilde{\theta}}$ is the identity mapping of $R^{\gamma}(<x>)$, $\tilde{\tilde{\theta}}$ is onto. Δ

Combining lemmas (2.9) and (2.10) we have:

<u>Theorem I</u>

Let R be a ring and let $<x>$ be an infinite cyclic group. Let $R^{\gamma}(<x>)$ be a twisted group ring of $<x>$ over R and let $Z(R^{\gamma}(<x>))$ be the centre of $R^{\gamma}(<x>)$. Let $Z(R)$ be the centre of R . Then $\overline{\theta} : \overline{x} \to \sum a_i\,\overline{x^i}$ induces an R-automorphism of $R^{\gamma}(<x>)$ if and only if the following two conditions hold:

(i) $\sum a_i\,\overline{x^i}$ is a unit in $(Z(R))^{\gamma}(<x>)$.

(ii) if $i \neq 1, -1$, then a_i is nilpotent.

CHAPTER 3

In this chapter we study the automorphisms of the group rings of finitely generated abelian groups. These automorphisms were studied by M. M. Parmenter for infinite cyclic groups but the presence of more than one independent generator makes for a complex problem with unpleasant notation. In order to avoid notational difficulties we consider mainly abelian groups with two free generators. The general case follows this particular case quite closely.

Lemma 3.1

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ and $\langle y \rangle$ are infinite cyclic groups. Let θ be the endomorphism of G determined by:

$$\theta(x) = x^{\alpha} y^{\beta} \qquad \alpha , \beta \quad \text{integers,}$$
$$\theta(y) = x^{\gamma} y^{\delta} \qquad \gamma , \delta \quad \text{integers.}$$

Then θ is an automorphism of G if and only if $\alpha\delta - \beta\gamma = \pm 1$.

Proof

By (1.16) we know that every endomorphism of G is determined by its effect on a set of generators.

Let θ be an endomorphism of G with $\alpha\delta - \beta\gamma = \pm 1$. Then

$$\theta(x^{\delta} y^{-\beta}) = (\theta(x))^{\delta} (\theta(y))^{-\beta} = (x^{\alpha} y^{\beta})^{\delta} (x^{\gamma} y^{\delta})^{-\beta}$$

$$= x^{\alpha\delta-\beta\gamma} y^{\beta\delta-\delta\beta} = x^{\alpha\delta-\beta\gamma} = x^{\pm 1} .$$

Also we have,

$$\theta(x^{\gamma}\ y^{-\alpha}) = (\theta(x))^{\gamma}\ (\theta(y))^{-\alpha} = (x^{\alpha}\ y^{\beta})^{\gamma}\ (x^{\gamma}\ y^{\delta})^{-\alpha}$$

$$= x^{\alpha\gamma-\gamma\alpha}\ y^{\beta\gamma-\delta\alpha} = y^{\beta\gamma-\delta\alpha} = y^{\mp 1} .$$

Hence θ is onto. Now we prove that θ is 1-1. For this we suppose $\theta(x^{m}\ y^{n}) = \theta(x^{u}\ y^{v})$ for some integer, m, n, u, v . This implies that

$$x^{\alpha m+\gamma n}\ y^{\beta m+\delta n} = x^{\alpha u+\gamma v}\ y^{\beta u+\delta v} . \qquad (1)$$

It follows from (1) that

$$\alpha m + \gamma n = \alpha u + \gamma v$$

$$\beta m + \delta n = \beta u + \delta v \quad , \text{ equivalently}$$

$$\alpha(m - u) + \gamma(n - v) = 0$$

$$\beta(m - u) + \delta(n - v) = 0 .$$

Since $\alpha\delta - \beta\gamma = \pm 1$ the only solution is $m - u = 0$ and $n - v = 0$. Hence $m = u$ and $n = v$ and therefore θ is 1-1 .

Conversely we suppose that θ is an automorphism of G and then we prove that $\alpha\delta - \beta\gamma = \pm 1$.

Since θ is an automorphism of G there exist integers m and n such that $\theta(x^{m}\ y^{n}) = x$, also there exist integers u and v such that $\theta(x^{u}\ y^{v}) = y$. From $\theta(x^{m}\ y^{n}) = x$ we conclude that $x^{\alpha m+\gamma n}\ y^{\beta m+\delta n} = x$, and this implies that

$$\alpha m + \gamma n = 1$$

$$\beta m + \delta n = 0 . \qquad (2)$$

Also from $\theta(x^u y^v) = y$ we conclude that $x^{\alpha u+\gamma v} y^{\beta u+\delta v} = y$ and this implies that

$$\beta u + \delta v = 1$$

$$\alpha u + \gamma v = 0 \ . \qquad (3)$$

Now $\alpha\delta - \beta\gamma$ must be non-zero, as otherwise there is no solution for (2) and (3).

From (2) we have $m = \delta(\alpha\delta - \beta\gamma)^{-1}$ and $n = -\beta(\alpha\delta - \beta\gamma)^{-1}$. Since m, n are integers $\alpha\delta - \beta\gamma$ divides δ and β , and therefore $\alpha\delta - \beta\gamma$ divides the greatest common divisor of δ and β . But in (3) we have $\beta u + \delta v = 1$ and then the greatest common divisor of δ and β is ± 1 .

This implies that $\alpha\delta - \beta\gamma = \pm 1$. Δ

<u>Lemma 3.2</u>

Let R be a commutative ring and let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$, $\langle y\rangle$ are infinite cyclic groups. Let θ be an endomorphism of G such that

$$\theta(x) = x^{\alpha} y^{\beta} \quad \text{and} \quad \theta(y) = x^{\gamma} y^{\delta} \ ,$$

with $\alpha\delta - \beta\gamma = \pm 1$. Let $\tilde{\theta} : R(G) \to R(G)$ be defined by

$\theta(\sum a_{ij} x^i y^j) = \sum a_{ij} \theta(x^i y^j)$. Then $\tilde{\theta}$ is an R-automorphism of $R(G)$.

<u>Proof</u>

By (1.16) $\tilde{\theta}$ is an endomorphism of $R(G)$. Since θ is onto it is evident that $\tilde{\theta}$ is also onto. Thus we need to prove $\tilde{\theta}$ is 1-1 . For this we define $\phi : R(G) \to R(G)$ by,

$\phi(\sum a_{ij} x^i y^j) = \sum a_{ij} \theta^{-1}(x^i y^j)$.

As before ϕ is an endomorphism of $R(G)$. Moreover we have

$$\tilde{\theta}\phi(\sum a_{ij}\; x^i y^j) = \tilde{\theta}(\sum a_{ij}\; \theta^{-1}(x^i y^j)) = \sum a_{ij}\; \theta(\theta^{-1}\; (x^i y^j)) = \sum a_{ij}\; x^i y^j \;.$$

Also we have

$$\phi\tilde{\theta}(\sum a_{ij}\; x^i y^j) = \phi(\sum a_{ij}\; \theta(x^i\; y^j)) = \sum a_{ij}\; \theta^{-1}(\theta(x^i\; y^j) = \sum a_{ij}\; x^i y^j \;.$$

Thus $\tilde{\theta}\phi$ and $\phi\tilde{\theta}$ are the identity mapping of $R(G)$ i.e. $\tilde{\theta}$ is onto and 1-1 . Δ

Lemma 3.3

Let R be a commutative ring and $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$, $\langle y\rangle$ are infinite cyclic groups. Let $\theta : R(G) \to R(G)$ be defined by $\theta(\sum a_{ij}\; x^i y^j) = \sum a_{ij}\; (bx)^i (cy)^j$ where b, c are units in R . Then θ is an R-automorphism of $R(G)$.

Proof

Assume $\sum \alpha_{ij}\; x^i y^j$, $\sum \beta_{mn}\; x^m y^n \in R(G)$, then,

$$\begin{aligned}\theta[(\sum \alpha_{ij}\; x^i y^j)(\sum \beta_{mn}\; x^m y^n)] &= \theta[\sum \alpha_{ij}\; \beta_{mn}\; x^{i+m}\; y^{j+n}] = \\ &= \sum \alpha_{ij}\; \beta_{mn}\; (bx)^{i+m}(cy)^{j+n} \\ &= \sum \alpha_{ij}\; \beta_{mn}[(bx)^i (cy)^j][(bx)^m (cy)^n] \\ &= \theta(\sum \alpha_{ij}\; x^i y^j)\; \theta(\sum \beta_{mn}\; x^m y^n) \;.\end{aligned}$$

Hence θ is an endomorphism of $R(G)$.

Now we define $\phi : R(G) \to R(G)$ by,

$$\phi(\sum \alpha_{ij}\; x^i\; y^j) = \sum \alpha_{ij}\; (b^{-1}x)^i (c^{-1}y)^j \;.$$

As before ϕ is an endomorphism of $R(G)$ and we have

$$\phi\theta(\sum \alpha_{ij}\ x^i y^j) = \phi[\sum \alpha_{ij}\ (bx)^i (cy)^j] = \phi[\sum \alpha_{ij}\ b^i c^j x^i y^j]$$

$$= \sum \alpha_{ij}\ b^i c^j\ (b^{-1}x)^i\ (c^{-1}y)^j = \sum \alpha_{ij}\ x^i y^j\ .$$

Also we have

$$\theta\phi(\sum \alpha_{ij}\ x^i y^j) = \theta[\sum \alpha_{ij}\ (b^{-1}x)^i (c^{-1}y)^j] = \theta[\sum \alpha_{ij}\ b^{-i} c^{-j} x^i y^j]$$

$$= \sum \alpha_{ij}\ b^{-i} c^{-j}\ (bx)^i (cy)^j = \sum \alpha_{ij}\ x^i y^j\ .$$

Hence $\phi\theta$ and $\theta\phi$ are the identity mappings of $R(G)$ i.e. θ is onto and 1-1 . Δ

Lemma 3.4

Let R be a commutative ring and let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$, $\langle y\rangle$ are infinite cyclic groups. Let $\theta : R(G) \to R(G)$ be defined as follows,

$$\theta(x) = a_{\alpha\beta}\ x^\alpha y^\beta \quad \text{and} \quad \theta(y) = b_{\gamma\delta}\ x^\gamma y^\delta\ ,$$

where $a_{\alpha\beta}$ and $b_{\gamma\delta}$ are units in R . Then θ induces an R-automorphism of $R(G)$ if and only if $\alpha\delta - \beta\gamma = \pm 1$.

Proof

Assume θ is an R-automorphism of $R(G)$. We define $\phi : R(G) \to R(G)$ as follows, $\phi(\sum \alpha_{ij}\ x^i y^j) = \sum \alpha_{ij} (a_{\alpha\beta}^{-1}\ x)^i (b_{\gamma\delta}^{-1}\ y)^j$.

By (3.3) ϕ is an R-automorphism of $R(G)$, and we have

$$\phi(x) = a_{\alpha\beta}^{-1}\ x\ , \qquad \phi(y) = b_{\gamma\delta}^{-1}\ y\ .$$

Since θ and ϕ are R-automorphisms of $R(G)$, $\theta\phi$ is also an R-automorphism of $R(G)$ and we have

$$\theta\phi(x) = \theta(a_{\alpha\beta}^{-1}\ x) = a_{\alpha\beta}^{-1}\ \theta(x) = a_{\alpha\beta}^{-1}\ (a_{\alpha\beta}\ x^\alpha\ y^\beta) = x^\alpha y^\beta\ ,$$

and

$$\theta\phi(y) = \theta(b_{\gamma\delta}^{-1}\ y) = b_{\gamma\delta}^{-1}\ \theta(y) = b_{\gamma\delta}^{-1}\ (b_{\gamma\delta}\ x^\gamma\ y^\delta) = x^\gamma y^\delta.$$

Hence $\theta\phi$ is an automorphism of G , by (3.1) we have $\alpha\delta - \beta\gamma = \pm 1$.

Conversely we suppose that $\alpha\delta - \beta\gamma = \pm 1$. By (3.3) we know $\sum c_{ij} x^i y^j \to \sum c_{ij} (a_{\alpha\beta} x)^i (b_{\gamma\delta} y)^j$ is an R-automorphism of $R(G)$. Also by (3.2) we know that

$$\sum c_{ij} a^i_{\alpha\beta} b^j_{\gamma\delta} x^i y^j \to \sum c_{ij} a^i_{\alpha\beta} b^j_{\gamma\delta} (x^\alpha y^\beta)^i (x^\gamma y^\delta)^j$$

$$= \sum c_{ij} (a_{\alpha\beta} x^\alpha y^\beta)^i (b_{\gamma\delta} x^\gamma y^\delta)^j$$

is an R-automorphism of $R(G)$. Hence

$$\sum c_{ij} x^i y^j \to \sum c_{ij} (a_{\alpha\beta} x^\alpha y^\beta)^i (b_{\gamma\delta} x^\gamma y^\delta)^j$$

is an R-automorphism of $R(G)$. Δ

<u>Lemma 3.5</u>

Let R be a commutative ring with a unique maximal ideal M which is nilpotent. Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$, $\langle y \rangle$ are infinite cyclic groups. Let θ be the mapping $\theta : R(G) \to R(G)$ where

$$\theta(x) = \sum a_{ij} x^i y^j , \qquad \theta(y) = \sum b_{hk} x^h y^k ,$$

and let θ induce an R-automorphism of $R(G)$. Then we have that

(i) $\sum a_{ij} x^i y^j$ and $\sum b_{hk} x^h y^k$ are units in $R(G)$.

(ii) For some integers α, β, γ, δ, $a_{\alpha\beta}$ and $b_{\gamma\delta}$ are units in R but all a_{ij} for $(i, j) \neq (\alpha, \beta)$ and all b_{hk} for $(h, k) \neq (\gamma, \delta)$ are nilpotent.

(iii) $\alpha\delta - \beta\gamma = \pm 1$.

Proof

Since θ induces an R-automorphism of $R(G)$ and x, y are units in $R(G)$ then $\sum a_{ij} x^i y^j$ and $\sum b_{hk} x^h y^k$ must be units in $R(G)$. Hence (i) has been established.

By (1.8) R/M is a field and by (1.6) M is the prime radical of R . Also by (1.11) and (i)

$$\sum \overline{a_{ij}} x^i y^j , \sum \overline{b_{hk}} x^h y^k \quad (\overline{a_{ij}} = a_{ij} + M, \overline{b_{hk}} = b_{hk} + M)$$

are units in $(R/M)(G)$. Moreover by (1.13)(II) $G = \langle x \rangle \times \langle y \rangle$ is a right-ordered group. Hence by Corollary (1.4) of [9] $\overline{a}_{\alpha\beta}$ for some integer, α, β is a unit in R/M and all $\overline{a_{ij}}$ for $(i, j) \neq (\alpha, \beta)$ are zero. Similarly $\overline{b}_{\gamma\delta}$ for some integer γ, δ is a unit in R/M and all $\overline{b_{hk}}$ for $(h, k) \neq (\gamma, \delta)$ are zero. Thus (ii) has been established.

To prove (iii) we define $\theta_1 : R(G) \rightarrow (R/M)(G)$ by ,

$$\theta_1(\sum a_{rs} x^r y^s) = \sum \overline{a_{rs}} x^r y^s \quad (\overline{a_{rs}} = a_{rs} + M) .$$

By (1.11) θ_1 is an epimorphism. Since by hypothesis θ is an R-automorphism of $R(G)$ we conclude that $\theta_1\theta$ is an epimorphism of $R(G)$ onto $(R/M)(G)$.

By using (ii) we have

$$\theta_1\theta(\sum c_{mn} x^m y^n) = \sum \overline{c_{mn}} (\sum \overline{a_{ij}} x^i y^j)^m (\sum \overline{b_{hk}} x^h y^k)^n$$

$$= \sum \overline{c_{mn}} (\overline{a_{\alpha\beta}} x^\alpha y^\beta)^m (\overline{b_{\gamma\delta}} x^\gamma y^\delta)^n .$$

The kernel of $\theta_1\theta$ is $M(G) = \{\sum d_{ij} x^i y^j \mid d_{ij} \in M\}$. Hence $R(G)/M(G) \cong (R/M)(G)$. This implies that $\theta_2 : R(G)/M(G) \rightarrow (R/M)(G)$ defined by

$\theta_2(\sum c_{mn} x^m y^n + M(G)) = \sum \overline{c_{mn}}(\overline{a_{\alpha\beta}} x^\alpha y^\beta)^m (\overline{b_{\gamma\delta}} x^\gamma y^\delta)^n$ is an isomorphism. On the other hand $\theta_3 : (R/M)(G) \rightarrow R(G)/M(G)$ defined by $\theta_3(\sum \overline{c_{mn}} x^m y^n) = \sum c_{mn} x^m y^n + M(G)$ is an isomorphism. Hence $\theta_2\theta_3 : (R/M)(G) \rightarrow (R/M)(G)$ by,

$$\theta_2\theta_3(\sum \overline{c_{mn}} x^m y^n) = \sum \overline{c_{mn}}(\overline{a_{\alpha\beta}} x^\alpha y^\beta)^m (\overline{b_{\gamma\delta}} x^\gamma y^\delta)^n$$

is an R/M-automorphism of $(R/M)(G)$. Since R/M is a field, we conclude from (3.4) that $\alpha\delta - \beta\gamma = \pm 1$. Δ

Lemma 3.6

Let R be a commutative ring with a unique maximal ideal M which is nilpotet. Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$, $\langle y \rangle$ are infinite cyclic groups. Let $\theta : R(G) \rightarrow R(G)$ where $\theta(x) = \sum a_{ij} x^i y^j$ and $\theta(y) = \sum b_{kh} x^h y^k$ satisfy the following three conditions:

(i) $\sum a_{ij} x^i y^j$ and $\sum b_{hk} x^h y^k$ are units in $R(G)$.

(ii) For some integers $\alpha, \beta, \gamma, \delta$, $a_{\alpha\beta}$ and $b_{\gamma\delta}$ are units in R but all a_{ij} for $(i, j) \neq (\alpha, \beta)$ and all b_{hk} for $(h, k) \neq (\gamma, \delta)$ are nilpotent .

(iii) $\alpha\delta - \beta\gamma = \pm 1$.

Then θ induces an R-automorphism of $R(G)$.

Proof

By (1.16) the map $\tilde{\theta} : R(G) \rightarrow R(G)$ defined by $\tilde{\theta}(\sum d_{uv} x^u y^v) = \sum d_{uv} (\theta(x))^u (\theta(y))^v$ is an endomorphism of $R(G)$. We prove that $\tilde{\theta}$ is onto and 1-1 .

First we prove $\tilde{\theta}$ is onto. Since $\theta(x)$ and $\theta(y)$ are units in $R(G)$, $(\theta(x))^{-1}$ and $(\theta(y))^{-1}$ exist. For the sake of argument we suppose $\alpha\delta - \beta\gamma = 1$, the proof for $\alpha\delta - \beta\gamma = -1$ is similar to the proof for $\alpha\delta - \beta\gamma = 1$. By assumption $a_{\alpha\beta}$ and

$b_{\gamma\delta}$ are units in R and, by this and (1.17) we have

$$\begin{aligned}
[a_{\alpha\beta}^{-1}\,\theta(x)]^{\delta}\,[b_{\gamma\delta}^{-1}\,\theta(y)]^{-\beta} &= [a_{\alpha\beta}^{-1}\,(a_{\alpha\beta}\,x^{\alpha}y^{\beta} + \sum_{(i,j)\neq(\alpha,\beta)} a_{ij}\,x^{i}y^{j})]^{\delta} \\
&\quad \times [b_{\gamma\delta}^{-1}\,(b_{\gamma\delta}x^{\gamma}y^{\delta} + \sum_{(h,k)\neq(\gamma,\delta)} b_{hk}\,x^{h}y^{k})]^{-\beta} \\
&= [x^{\alpha}y^{\beta} + \sum_{(i,j)\neq(\alpha,\beta)} a_{\alpha\beta}^{-1}\,a_{ij}\,x^{i}y^{j}]^{\delta} \\
&\quad\ [x^{\gamma}y^{\delta} + \sum_{(h,k)\neq(\gamma,\delta)} b_{\gamma\delta}^{-1}\,b_{hk}\,x^{h}y^{k}]^{-\beta} \\
&= (x^{\alpha\delta}y^{\beta\delta} + n_1)(x^{-\gamma\beta}\,y^{-\delta\beta} + n_2) \\
&= x^{\alpha\delta-\beta\gamma}\,y^{\beta\delta-\beta\delta} + n_3 \\
&= x + n_3
\end{aligned}$$

where n_1, n_2, n_3 are nilpotent in $R(G)$.

Similarly we have $[a_{\alpha\beta}^{-1}\,\theta(x)]^{-\gamma}[b_{\gamma\delta}^{-1}\,\theta(y)]^{\alpha} = y + n_4$ where n_4 is nilpotent in $R(G)$.

Let $n_3 = \sum \eta_{rs}\,x^{r}y^{s}$ and $n_4 = \sum \mu_{pq}\,x^{p}y^{q}$ where all η_{rs} and all μ_{pq} are nilpotent in R . Let T be the ideal of R generated by $\{\eta_{rs}\} \cup \{\mu_{pq}\}$. Then T is nilpotent. By using (1.17) we have

$$x + \sum \eta_{rs}\,x^{r}y^{s} - \sum \eta_{rs}[x + \sum \eta_{rs}\,x^{r}y^{s}]^{r}\,[y + \sum \mu_{pq}\,x^{p}y^{q}]^{s} = x + n_5$$

where $\sum \lambda_{\nu\varepsilon}\,x^{\nu}y^{\varepsilon} = n_5$ is nilpotent in $R(G)$ with all $\lambda_{\nu\varepsilon} \in T^2$.

Again by using (1.17) we have

$$y + \sum \mu_{pq}\,x^{p}y^{q} - \sum \mu_{pq}[x + \sum \eta_{rs}\,x^{r}y^{s}]^{p}\,[y + \sum \mu_{pq}\,x^{p}y^{q}]^{q} = y + n_6$$

where $\sum f_{\tau\sigma}\,x^{\tau}y^{\sigma} = n_6$ is nilpotent in $R(G)$ with all $f_{\tau\sigma} \in T^2$.

Hence we have

$$[a_{\alpha\beta}^{-1}\ \theta(x)]^{\delta}\ [b_{\gamma\delta}^{-1}\ \theta(y)]^{-\beta} - \sum \eta_{rs}\{[a_{\alpha\beta}^{-1}\ \theta(x)]^{\delta}\ [b_{\gamma\delta}^{-1}\ \theta(y)]^{-\beta}\}^{r}$$

$$\times\{[a_{\alpha\beta}^{-1}\ \theta(x)]^{-\gamma}\ [b_{\gamma\delta}^{-1}\ \theta(y)]^{\alpha}\}^{s} = x + n_5 \ .$$

$$[a_{\alpha\beta}^{-1}\ \theta(x)]^{-\gamma}\ [b_{\alpha\delta}^{-1}\ \theta(y)]^{\alpha} - \sum \mu_{pq}\{[a_{\alpha\beta}^{-1}\ \theta(x)]^{\delta}\ [b_{\gamma\delta}^{-1}\ \theta(y)]^{-\beta}\}^{p}$$

$$\times\{[a_{\alpha\beta}^{-1}\ \theta(x)]^{-\gamma}\ [b_{\gamma\delta}^{-1}\ \theta(y)]^{\alpha}\}^{q} = y + n_6 \ .$$

Since T is nilpotent by continuing in this manner a finite number of times we get x, y as a linear combination of powers of $\theta(x) = \sum a_{ij}\ x^i y^j$ and $\theta(y) = \sum b_{hk}\ x^h y^k$. Hence $\tilde{\theta}$ is onto.

Now we prove that θ is 1-1 . For this we suppose there exist $c_{mn} \in R$ such that $\sum c_{mn}(\theta(x))^m\ (\theta(y))^n = 0$. Then we show that all $c_{mn} = 0$. From $\sum c_{mn}(\theta(x))^m(\theta(y))^n = 0$ we have modulo M , $\sum \overline{c_{mn}}(\ \overline{a_{ij}}\ x^i y^j)^m\ (\sum \overline{b_{hk}}\ x^h y^k)^n = 0$. Since a_{ij} for $(i, j) \neq (\alpha, \beta)$ and b_{hk} for $(h, k) \neq (\gamma, \delta)$ are nilpotent we have

$$\sum \overline{c_{mn}}(\overline{a_{\alpha\beta}}\ x^{\alpha}y^{\beta} + \sum_{(i,j)\neq(\alpha,\beta)} \overline{a_{ij}}\ x^i y^j)^m\ (\overline{b_{\gamma\delta}}\ x^{\gamma}y^{\delta} + \sum_{(h,k)\neq(\gamma,\delta)} \overline{b_{hk}}\ x^h y^k)^n$$

$$= \sum \overline{c_{mn}}(\overline{a_{\alpha\beta}}\ x^{\alpha}y^{\beta})^m\ (\overline{b_{\gamma\delta}}\ x^{\gamma}y^{\delta})^n = \sum \overline{c_{mn}}(\overline{a_{\alpha\beta}})^m\ (\overline{b_{\gamma\delta}})^n\ x^{\alpha m+\gamma n}\ y^{\beta m+\delta n} = 0 \ .$$

In this identity each term in x, y occurs at most once because $x^{\alpha m+\gamma n}\ y^{\beta m+\delta n} = x^{\alpha m'+\gamma n'}\ y^{\beta m'+\delta n'}$ and $\alpha\delta - \beta\gamma = 1$ implies that $m = m'$ and $n = n'$. From this result and $\sum \overline{c_{mn}}(\overline{a}_{\alpha\beta})^m\ (\overline{b}_{\gamma\delta})^n\ x^{\alpha m+\gamma n}\ y^{\beta m+\delta n} = 0$ we conclude that $\overline{c_{mn}}(\overline{a}_{\alpha\beta})^m\ (\overline{b}_{\gamma\delta})^n = 0$ for all m, n . But $\overline{a}_{\alpha\beta}$ and $\overline{b}_{\gamma\delta}$ are units in R/M and so we have $\overline{c_{mn}} = 0$ for all m, n. This implies that $c_{mn} \in M$ for all m, n i.e. all c_{mn} are nilpotent.

Now let N be the ideal of R generated by $\{c_{mn}\} \cup \{a_{ij} \mid (i, j) \neq (\alpha, \beta)\} \cup \{b_{hk} \mid (h, k) \neq (\gamma, \delta)\}$. Then N is nilpotent. Assume all c_{mn} belong to N^w for some positive integer w but some of them do not belong to N^{w+1}.

From $\sum c_{mn}(\sum a_{ij} x^i y^j)^m (\sum b_{hk} x^h y^k)^n = 0$ we have $\sum \overline{c_{mn}} (\sum \overline{a_{ij}} x^i y^j)^m (\overline{\sum b_{hk}} x^h y^k)^n = 0$ in $(R/N^{w+1})(G)$. Since all $c_{mn} \in N^w$ and all a_{ij} for $(i, j) \neq (\alpha, \beta)$ and all b_{hk} for $(h, k) \neq (\gamma, \delta)$ belong to N we conclude that $\sum \overline{c_{mn}} (\overline{a_{\alpha\beta}} x^\alpha y^\beta)^m (\overline{b_{\gamma\delta}} x^\gamma y^\delta)^n = 0$. By using $\alpha\delta - \beta\gamma = 1$ and the fact that $\overline{a_{\alpha\beta}}, \overline{b_{\gamma\delta}}$ are units in R/N^{w+1} we have $\overline{c_{mn}} = 0$ for all m, n. This implies that $c_{mn} \in N^{w+1}$ contrary to assumption. Hence each c_{mn} lies in N^w for all integers $w > 0$. Since N is nilpotent we conclude that $c_{mn} = 0$ for all m, n. Hence $\tilde{\theta}$ is 1-1. Δ

Combining lemmas (3.5) and (3.6) we have:

Theorem II

Let R be a commutative ring with a unique maximal ideal M which is nilpotent. Let $G = \langle x \rangle \times \langle y \rangle$ where x, y are infinite cyclic groups. Let θ be the mapping $\theta : R(G) \to R(G)$ where $\theta(x) = \sum a_{ij} x^i y^j$, $\theta(y) = \sum b_{hk} x^h y^k$. Then θ induces an R-automorphism of $R(G)$ if and only if the following three conditions hold:

(i) $\sum a_{ij} x^i y^j$, $\sum b_{hk} x^h y^k$ are units in R(G) .

(ii) For some integers α, β, γ, and δ , $a_{\alpha\beta}$ and $b_{\gamma\delta}$ are units in R but all a_{ij} for $(i, j) \neq (\alpha, \beta)$ and all b_{hk} for $(h, k) \neq (\gamma, \delta)$ are nilpotent.

(iii) $\alpha\delta - \beta\gamma = \pm 1$.

CHAPTER 4

In this chapter we shall be concerned to find the automorphisms of $K(G)$, where K is a field and G is a finitely generated abelian group of the form $G = \langle x\rangle \times \langle y\rangle$ where x is an infinite cyclic group and $y^2 = 1$.

Lemma 4.1

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field and let $u, v \in K(\langle x\rangle)$. Then $u + vy$ is a unit in $K(G)$ if and only if $u - vy$ is a unit in $K(G)$.

Proof

Suppose $u + vy$ is a unit in $K(G)$. Then there exist r , $s \in K(\langle x\rangle)$ such that $(u + vy)(r + sy) = 1$. This implies that

$$\begin{aligned} ur + vs &= 1 \\ us + vr &= 0 \quad . \qquad (1) \end{aligned}$$

From (1) we have $(u - vy)(r - sy) = (ur + vs) - (us + vr)y = 1$. Thus $u - vy$ is a unit in $K(G)$.

Now by replacing v by $-v$, we see that conversely if $u - vy$ is a unit then $u + vy$ is a unit. Δ

Lemma 4.2

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field and $u, v \in K(\langle x\rangle)$. Then we have

(i) $u + vy$ is a unit in $K(G)$ if and only if $u^2 - v^2$ is a unit in $K(\langle x\rangle)$.

(ii) If characteristic $K \neq 2$, then the units of $K(G)$ are the elements of the form $(\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y$ where $\alpha, \beta \in K - \{0\}$ and m, n are integers.

Proof

Suppose $u + vy$ is a unit in $K(G)$. Then by (4.1) $u - vy$ is also a unit in $K(G)$. This implies that $(u + vy)(u - vy) = (u^2 - v^2)1$ is a unit in $K(G)$ and consequently $u^2 - v^2$ is a unit in $K(\langle x\rangle)$, (1.32).

Now we suppose that $u^2 - v^2$ is a unit in $K(\langle x\rangle)$. Then we have $(u + vy)[(u^2 - v^2)^{-1} u - (u^2 - v^2)^{-1} vy] = (u^2 - v^2)(u^2 - v^2)^{-1} = 1$. Hence $u + vy$ is a unit in $K(G)$ and then (i) has been established.

To prove (ii) we suppose that $u + vy$ is a unit in $K(G)$. Then by (i) $u^2 - v^2 = (u + v)(u - v)$ is a unit in $K(\langle x\rangle)$. This implies that $u + v$ and $u - v$ are units in $K(\langle x\rangle)$. By 1.13 (I) $\langle x\rangle$ is a right-ordered group, hence by using Corollary (1.4) of [9] we have

$$u + v = \gamma x^m \qquad 0 \neq \gamma \in K , \quad m \text{ integer.} \qquad (1)$$

$$u - v = \delta x^n \qquad 0 \neq \delta \in K , \quad n \text{ integer.} \qquad (2)$$

It follows from (1) and (2) that $u = 2^{-1} \gamma x^m + 2^{-1} \delta x^n$ and $v = 2^{-1} \gamma x^m - 2^{-1} \delta x^n$.

On the other hand if $\alpha, \beta \in K - \{0\}$ then we have

$$[(\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y][(4\alpha\beta x^{m+n})^{-1}(\alpha x^m + \beta x^n) - (4\alpha\beta x^{m+n})^{-1}(\alpha x^m - \beta x^n)y]$$

$= (4\alpha\beta x^{m+n})(4\alpha\beta x^{m+n})^{-1} = 1$. Hence $(\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y$ is a unit in $K(G)$. Δ

Lemma 4.3

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic $\neq 2$. Let $u + vy = (\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y$ ($\alpha, \beta \in K$; m, n integers) be a unit in $K(G)$. Then for all $w \in \mathbb{Z}$ we have,

$$(u + vy)^w = 2^{w-1}[(\alpha x^m)^w + (\beta x^n)^w + ((\alpha x^m)^w - (\beta x^n)^w)y] .$$

Proof

We consider the case $w \geq 0$ and we proceed by mathematical induction. For convenience let $A = \alpha x^m$ and $B = \beta x^n$. If $w = 0, 1$, then there is nothing to prove so we suppose $w > 1$. Assume $(u + vy)^w = [(A + B) + (A - B)y]^w = 2^{w-1}[(A^w + B^w) + (A^w - B^w)y]$. This implies that

$$\begin{aligned}(u + vy)^{w+1} &= [(A + B) + (A - B)y]^w[(A + B) + (A - B)y] \\ &= 2^{w-1}[(A^w + B^w) + (A^w - B^w)y]\ [(A + B) + (A - B)y] \\ &= 2^{w-1}[2(A^{w+1} + B^{w+1}) + 2(A^{w+1} - B^{w+1})y] \\ &= 2^w[(A^{w+1} + B^{w+1}) + (A^{w+1} - B^{w+1})y] .\end{aligned}$$

This completes the induction steps and so our assertion has been established for $w \geq 0$.

Now assume $w = -1$. Since

$$2^{-2}[(A + B) + (A - B)y]\ \ [(A^{-1} + B^{-1}) + (A^{-1} - B^{-1})y] = 1 ,$$

we conclude that

$$(u + vy)^{-1} = [(A + B) + (A - B)y]^{-1} = 2^{-2}[(A^{-1} + B^{-1}) + (A^{-1} - B^{-1})y] .$$

Finally we suppose that $w < -1$ and let $t = -w$. Since t is positive we have

$$(u + vy)^w = [(u + vy)^{-1}]^t = (2^{-2})^t[(A^{-1} + B^{-1}) + (A^{-1} - B^{-1})y]^t =$$

$$2^{-t-1}[(A^{-t} + B^{-t}) + (A^{-t} - B^{-t})y] = 2^{-t-1}[(A^{-t} + B^{-t}) + (A^{-t} - B^{-t})y]$$

$$= 2^{w-1}[(A^w + B^w) + (A^w - B^w)y .$$ ◁

Lemma 4.4

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic $\neq 2$. Let $\theta : K(G) \to K(G)$ be defined by

$$\theta(x) = (\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y ,$$

$$\theta(y) = (\gamma x^p + \delta x^q) + (\gamma x^p - \delta x^q)y ,$$

where $\alpha, \beta, \gamma, \delta \in K - \{0\}$ and m, n, p, q integers. If θ is a K-automorphism of $K(G)$, then $m = \pm 1$, $n = \pm 1$, $\gamma x^p = \pm \frac{1}{2}$, $\delta x^q = \mp \frac{1}{2}$.

Proof

In order to simplify the proof let $\alpha x^m = A$, $\beta x^n = B$, $\gamma x^p = C$, $\delta x^q = D$. Since $y^2 = 1$ we have

$$\theta(y^2) = [(C + D) + (C - D)y]^2 = [(C + D)^2 + (C - D)^2] + 2(C + D)(C - D)y = 1 .$$

It follows from this that

$$(C + D)^2 + (C - D)^2 = 1$$

$$(C + D)(C - D) = 0 . \qquad (1)$$

By using (1.20) we conclude from (1) that either $C + D = 0$ or $C - D = 0$.

If $C + D = 0$, then $(C + D)^2 + (C - D)^2 = 1$ implies that $C - D = \pm 1$ and then $\theta(y) = (C + D) + (C - D)y = \pm y$. From $C - D = 0$ and $(C + D)^2 + (C - D)^2 = 1$ we have $C + D = \pm 1$ and then we have $\theta(y) = (C + D) + (C - D)y = \pm 1$ which is not true, because θ is an automorphism and $y \neq 1, -1$. Hence $C + D = 0$, $C - D = \pm 1$ and $\theta(y) = \pm y$. From $C + D = 0$ and $C - D = \pm 1$ we conclude that $C = \pm \frac{1}{2}$ and $D = \mp \frac{1}{2}$. For the sake of argument we suppose that $\theta(y) = y$; we remark that the proof of $\theta(y) = -y$ is the same as the proof for $\theta(y) = y$, and therefore we omit it.

Now, since θ is an K-automorphism of $K(G)$ there exist $a_i, b_j \in K$ such that $\theta[\sum a_i x^i + (\sum b_j x^j)y] = x$. By using (4.3) we have

$$\theta(\sum a_i x^i) + \theta(\sum b_j x^j)\ \theta(y) = \sum a_i(\theta(x))^i + [\sum b_j(\theta(x))^j]y$$

$$= \sum a_i\ 2^{i-1}[(A^i + B^i) + (A^i - B^i)y] + \sum b_j\ 2^{j-i}[(A^j + B^j) + (A^j - B^j)y]y = x\ .$$

From this equality it follows that

$$\sum 2^{i-1}\ a_i(A^i + B^i) + \sum 2^{j-1}\ b_j\ (A^j - B^j) = x\ . \qquad (2)$$

$$\sum 2^{i-1}\ a_i(A^i - B^i) + \sum 2^{j-1}\ b_j\ (A^j + B^j) = 0\ . \qquad (3)$$

From (2) and (3) we conclude that

$$\sum 2^{i-1}\ a_i(A^i - A^i + 2B^i) + \sum 2^{j-1}\ b_j(A^j - A^j - 2B^j)$$

$$= \sum 2^i\ a_i\ B^i - \sum 2^j\ b_j\ B^j = \sum 2^i(a_i - b_i)B^i = x\ . \qquad (4)$$

Also from (2) and (3) we have

$$\sum 2^i\ a_i\ A^i + \sum 2^j\ b_j\ A^j = \sum 2^i(a_i + b_i)A^i = x\ . \qquad (5)$$

By using the fact that $B = \beta x^n$ ($\beta \in K$, n integer) we conclude that (4) cannot be valid for $|n| > 1$ or for $n = 0$. Also (5) cannot be valid for $|m| > 1$ or for $m = 0$. Hence $m = \pm 1$, $n = \pm 1$. Δ

Lemma 4.5

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic $\neq 2$. Let $\theta : K(G) \to K(G)$ be the K-linear mapping defined by

$$\theta(x) = (\alpha x^{\pm 1} + \beta x^{\pm 1}) + (\alpha x^{\pm 1} - \beta x^{\pm 1})y \qquad \alpha, \beta \in K - \{0\}, \text{ and}$$

$$\theta(y) = \pm\ y\ .$$

Then θ induces an K-automorphism of $K(G)$.

Proof

In order to simplify the proof we assume that $\theta(x) = (\alpha x + \beta x) + (\alpha x - \beta x)y$ and $\theta(y) = y$. The proof for other cases is similar to the proof of this particular case.

We prove that θ is onto and 1-1 . By hypothesis we have $\theta[2^{-2}(\alpha^{-1} + \beta^{-1})x + 2^{-2}(\alpha^{-1} - \beta^{-1})xy] = x$ and $\theta(y) = y$. Hence θ is onto.

Now we prove that θ is 1-1 . Let $\sum a_i x^i + (\sum b_j x^j)y$ be an element of $K(G)$ such that $\theta[\sum a_i x^i + (\sum b_j x^j)y] = 0$. Then we show that all a_i and all b_j are zero. For convenience let $A = \alpha x$ and $B = \beta x$. Arguing exactly as in the proof of (4.4) we have

$$\sum 2^i a_i A^i + \sum 2^j b_j A^j = \sum 2^i (a_i + b_i) A^i = 0 . \qquad (1)$$

$$\sum 2^i a_i B^i - \sum 2^j b_j B^j = \sum 2^i (a_i - b_i) B^i = 0 . \qquad (2)$$

Since $A = \alpha x$ and $B = \beta x$, it follows from (1) and (2) that

$$a_i + b_i = 0 , \quad \text{for all} \quad i .$$

$$a_i - b_i = 0 , \quad \text{for all} \quad i .$$

Hence all a_i and all b_j are zero i.e. θ is 1-1 . Δ

Theorem III

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic $\neq 2$. Let $\theta : K(G) \to K(G)$ be defined by

$$\theta(x) = (\alpha x^m + \beta x^n) + (\alpha x^m - \beta x^n)y \ ,$$

$$\theta(y) = (\gamma x^p + \delta x^q) + (\gamma x^p - \delta x^q)y \ ,$$

where $\alpha, \beta, \gamma, \delta \in K - \{0\}$ and m, n, p, q integers.

Then θ is an K-automorphism of $K(G)$ if and only if $m = \pm 1$, $n = \pm 1$, $\gamma x^p = \pm \frac{1}{2}$, $\delta x^q = \mp \frac{1}{2}$.

In the rest of this chapter we are dealing with the fields of characteristic 2 .

Lemma 4.6

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2 . Let $u \in K(\langle x \rangle)$ and let $\lambda \in K$. Then for all integers ε we have

(i) $[\lambda x^{\pm 1} + u(1 + y)]^{2\varepsilon} = (\lambda x^{\pm 1})^{2\varepsilon}$.

(ii) $[\lambda x^{\pm 1} + u(1 + y)^{2\varepsilon+1} = (\lambda x^{\pm 1})^{2\varepsilon+1} + (\lambda x^{\pm 1})^{2\varepsilon} u(1 + y)$.

Proof

Since $(1 + y)^2 = 0$ we have

$$[\lambda n^{\pm 1} + u(1 + y)]^2 = (\lambda x^{\pm 1})^2 + 2(\lambda x^{\pm 1})\, u(1 + y) + (1 + y)^2 = (\lambda x^{\pm 1})^2 .$$

From this we conclude that

$$[\lambda x^{\pm 1} + u(1 + y)]^{2\varepsilon} = \{[\lambda x^{\pm 1} + u(1 + y)]^2\}^{\varepsilon} = [(\lambda x^{\pm 1})^2]^{\varepsilon} = (\lambda x^{\pm 1})^{2\varepsilon} .$$

Hence (i) has been established. To prove (ii) we have

$$\begin{aligned}[\lambda x^{\pm 1} + u(1 + y)]^{2\varepsilon+1} &= [\lambda x^{\pm 1} + u(1 + y)]^{2\varepsilon}[\lambda x^{\pm 1} + u(1 + y)] \\ &= (\lambda x^{\pm 1})^{2\varepsilon}[\lambda x^{\pm 1} + u(1 + y)] \\ &= (\lambda x^{\pm 1})^{2\varepsilon+1} + (\lambda x^{\pm 1})^{2\varepsilon}\, u(1 + y) . \quad \Delta\end{aligned}$$

Lemma 4.7

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2. Let $\phi : K(G) \to K(G/\langle y\rangle)$ be the natural homomorphism. Let $JK(G)$ be the Jacobson radical of $K(G)$. Then $\ker\phi = JK(G)$.

Proof

Let $X = \langle x\rangle$ and $Y = \langle y\rangle$. Since ϕ is an epimorphism and its kernel is $K(G)$ aug $K(Y)$ we have $K(G)/K(G)$ aug $K(Y) \simeq K(G/Y)$. By (1.24) and using the fact that the characteristic of K is 2 we have $K(G)$ aug $K(Y) = (K(G))(1 + y) = (K(X))(1 + y)$. But $(1 + y)^2 = 0$ so $(K(G))(1 + y)$ is nilpotent. This implies that $(K(G))(1 + y) \subseteq JK(G)$. Hence there is an ideal I of $JK(G/Y)$ such that $JK(G)/K(G)$ aug $K(Y) = JK(G)/(K(G))(1 + y) \simeq I \subseteq JK(G/Y) \simeq JK(X)$ because $G/Y \simeq X$. Since X is an infinite cyclic group we have $JK(X) = 0$ (see [11]). This implies that

$JK(G) = (K(G))$ aug $K(Y) = (K(G))(1 + y) = (K(\langle x\rangle))(1 + y)$. Δ

Lemma 4.8

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2. Then the units of $K(G)$ are the elements $\lambda x^m + u(1 + y)$ where $0 \neq \lambda \in K$, m is an integer and $u \in K(\langle x \rangle)$.

Proof

Let $a, b \in K(\langle x \rangle)$ and suppose that $a + by$ is a unit in $K(\langle x \rangle)$. Since the characteristic of K is 2 we have $a + by = a + b + b + by = (a + b) + b(1 + y)$. Thus $(a + b) + b(1 + y)$ is a unit in $K(G)$ and then $[(a + b) + b(1 + y)]^2 = (a + b)^2$ is a unit in $K(G)$. This implies that $a + b$ is a unit in $K(G)$. Thus by (1.32) $a + b$ is a unit in $K(\langle x \rangle)$. Thus by Corollary (1.4) of [9] $a + b$ is of the form λx^m where $0 \neq \lambda \in K$ and m integer. Hence $a + by$ is of the form $\lambda x^m + b(1 + y)$ where $b \in K(\langle x \rangle)$.

Now suppose $\lambda x^m + b(1 + y) \in K(G)$ where $0 \neq \lambda \in K$, m is an integer and $b \in K(\langle x \rangle)$. Since $(1 + y)^2 = 0$ we have, $[\lambda x^m + b(1 + y)][(\lambda x^m)^{-1} - (\lambda x^m)^{-2} b(1 + y)] = 1$. This implies that $\lambda x^m + b(1 + y)$ is a unit of $K(G)$. Δ

Lemma 4.9

Let $G = \langle x \rangle \times \langle y \rangle$ where $\langle x \rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2. If θ is a K-automorphism of $K(G)$ then there exist $\lambda \in K - \{0\}$ and $u, v \in K(\langle x \rangle)$ such that v is a unit and

$$\theta(x) = \lambda x^{\pm 1} + u(1 + y) ,$$
$$\theta(y) = 1 + v(1 + y) .$$

Proof

Let $\langle y\rangle = y$, and let $JK(G)$ be the Jacobson radical of $K(G)$. Since θ is an K-automorphism of $K(G)$ then θ permutes all maximal right ideals of $K(G)$. This implies that θ fixes the intersection of the maximal right ideals $JK(G)$. But by (4.7), $JK(G) = (K(G))(1 + y) = (K(\langle x\rangle))(1 + y)$. It follows from this that $\theta(1 + y) \in (K(\langle x\rangle))(1 + y)$. Hence $1 + \theta(y) = \theta(1 + y) = v(1 + y)$ where $0 \neq v \in K(\langle x\rangle)$, because $v = 0$ implies that $y = 1$. From this result we conclude that $\theta(y) = 1 + v(1 + y)$.

Now, by (1.23) θ induces an K-automorphism $\tilde{\theta}$ of $K(G)/JK(G)$. Also by (4.7) we have $K(G)/JK(G) \cong K(G/Y) \cong K(\langle x\rangle)$. Thus θ induces an K-automorphism $\approx\atop{\theta}$ of $K(\langle x\rangle)$. By using this result and theorem (2.1) of [9] we conclude that $\overset{\approx}{\theta}(x) = \lambda x^{\pm 1}$ where $0 \neq \lambda \in K$. This implies that $\theta(x) = \lambda x^{\pm 1} + u(1 + y)$ where $u \in K(\langle x\rangle)$.

Since θ is a K-automorphism of $K(G)$ there exists $\sum \eta_i x^i + (\sum \delta_j x^j)y \in K(G)$ such that $\theta[\sum \eta_i x^i + (\sum \delta_j x^j)y] = y$.

Finally, for convenience we distinguish even and odd powers of x in $\sum\limits_i \eta_i x^i$ and $\sum\limits_j \delta_j x^j$. Thus we write

$$\sum_i \eta_i x^i = \sum_r \eta_{2r} x^{2r} + \sum_s \eta_{2s+1} x^{2s+1} \quad .$$

$$\sum_j \delta_j x^j = \sum \delta_{2\psi} x^{2\psi} + \sum \delta_{2\pi+1} x^{2\pi+1} \quad . \qquad (1)$$

By (4.6) and (1) we have

$$\theta[\sum_i \eta_i x^i + (\sum_j \delta_j x^j)y] = \sum_r \eta_{2r}(\lambda x^{\pm 1})^{2r} + \sum_s \eta_{2s+1}[(\lambda x^{\pm 1})^{2s+1} + (\lambda x^{\pm 1})^{2s} u(1 + y)]$$

$$+ (\sum \delta_{2\psi}(\lambda x^{\pm 1})^{2\psi} + \sum \delta_{2\pi+1}[(\lambda x^{\pm 1})^{2\pi+1} + (\lambda x^{\pm 1})^{2\pi} u(1 + y)])[1 + v(1 + y)] = y \ .$$

By using $(1 + y)^2 = 0$ we have

$$[\sum_r \eta_{2r}(\lambda x^{\pm 1})^{2r} + \sum_s \eta_{2s+1}(\lambda x^{\pm 1})^{2s+1} + \sum_s \eta_{2s+1}(\lambda x^{\pm 1})^{2s}u + \sum_\psi \delta_{2\psi}(\lambda x^{\pm 1})^{2\psi}$$

$$+ \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi+1} + \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi}u$$

$$+ \sum_\psi \delta_{2\psi}(\lambda x^{\pm 1})^{2\psi}v + \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi+1}v]$$

$$+ [\sum_s \eta_{2s+1}(\lambda x^{\pm 1})^{2s}u + \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi}u + \sum_\psi \delta_{2\psi}(\lambda x^{\pm 1})^{2\psi}v + \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi+1}v]y = y .$$

By using (1) and the fact that $u, v \in K(\langle x\rangle)$ we have

$$\sum_i \eta_i(\lambda x^{\pm 1})^i + (\sum_j \delta_j(\lambda x^{\pm 1})^j)(1 + v) + \sum_s \eta_{2s+1}(\lambda x^{\pm 1})^{2s}u$$

$$+ \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi}u = 0 .$$

$$\sum_j \delta_j(\lambda x^{\pm 1})^j + (\sum_j \delta_j(\lambda x^{\pm 1})^j)(1 + v) + \sum_s \eta_{2s+1}(\lambda x^{\pm 1})^{2s}u$$

$$+ \sum_\pi \delta_{2\pi+1}(\lambda x^{\pm 1})^{2\pi}u = 1 . \qquad (3)$$

By adding these equalities we obtain

$$\sum_i \eta_i(\lambda x^{\pm 1})^i + \sum_j \delta_j(\lambda x^{\pm 1})^j = 1 . \qquad (4)$$

This implies that $\eta_0 + \delta_0 = 1$ and $\eta_i = \delta_i$ for all $i \neq 0$. By using this result and using the equality (3) we have $(\sum_j \delta_j(\lambda x^{\pm 1}))v = 1$. Hence v is a unit in $K(\langle x\rangle)$. Δ

Lemma 4.10

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2 .

Let $\lambda \in K - \{0\}$ and let $\delta \in \{-1, 1\}$. Let $u \in K(\langle x\rangle)$ and let v be a unit in $K(\langle x\rangle)$. Let θ be the K-endomorphism of $K(G)$ such that

$$\theta(x) = \lambda x^{\delta} + u(1 + y) \quad ,$$

$$\theta(y) = 1 + v(1 + y).$$

Then θ is a K-automorphism of $K(G)$.

Proof

By (1.16) $\theta : K(G) \to K(G)$ by

$$\theta[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j)y] = \sum_i \alpha_i(\theta(x)^i + \sum_j \beta_j(\theta(x)^j\ \theta(y)$$

is an endomorphism of $K(G)$. We prove that θ is onto and 1-1 . First we show that θ is onto. By Corollary (1.4) of [9] $v = px^m$ for some $p \in K - \{0\}$ and m integer. Let $u = v(\sum_\varepsilon b_\varepsilon x^\varepsilon)$ where $\sum_\varepsilon b_\varepsilon x^\varepsilon \in K(\langle x\rangle)$. Then by using (4.6) we have

$$\theta[(\sum_\varepsilon \lambda^{-\varepsilon-1} b_\varepsilon x^\varepsilon)(1 + y) + \lambda^{-1}x] = [\sum_\varepsilon \lambda^{-\varepsilon-1} b_\varepsilon(\lambda x + u(1 + y)^\varepsilon][1 + 1 + v(1 + y]$$

$$+ \lambda^{-1}[\lambda x + u(1 + y)] = [\sum_\varepsilon \lambda^{-\varepsilon-1} b_\varepsilon(\lambda x)^\varepsilon + \Omega_1(1 + y)][v(1 + y)]$$

$$+ \lambda^{-1}[\lambda x + u(1 + y)]$$

where $\Omega_1 \in K(\langle x\rangle)$. Since $(1 + y)^2 = 0$ we have

$$\theta[(\sum_\varepsilon \lambda^{-\varepsilon-1} b_\varepsilon x^\varepsilon)(1 + y) + \lambda^{-1}x] = [\sum_\varepsilon \lambda^{-\varepsilon-1} b_\varepsilon(\lambda x)^\varepsilon]v(1 + y) + x + \lambda^{-1}u(1 + y) .$$

But we know that $u = v \sum b_\varepsilon x^\varepsilon$ and so we have

$$\theta[(\sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} x^{\varepsilon})(1 + y) + \lambda^{-1}x] = [\sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} (\lambda x)^{\varepsilon}] v(1 + y) + x$$

$$+ \lambda^{-1} v(\sum_{\varepsilon} b_{\varepsilon} x^{\varepsilon})(1 + y)$$

$$= (\sum_{\varepsilon} \lambda^{-1} b_{\varepsilon} x^{\varepsilon}) v(1 + y) + x + (\sum_{\varepsilon} \lambda^{-1} b_{\varepsilon} x^{\varepsilon}) v(1 + y) = x \ .$$

Also by using (4.6) we have

$$\theta[1 + (\lambda^{m} p^{-1} x^{-m})(1 + y)] = 1 + \lambda^{m} p^{-1} [\lambda x + u(1 + y)]^{-m} [1 + 1 + px^{m}(1 + y)]$$

$$= 1 + \lambda^{m} p^{-1} [(\lambda x)^{-m} + \Omega_2(1 + y)][px^{m}(1 + y)] \text{ where } \Omega_2 \in K(<x>)$$

$$\therefore \ \theta[1 + (\lambda^{m} p^{-1} x^{-m})(1 + y)] = 1 + \lambda^{m} p^{-1} (\lambda x)^{-m} px^{m}(1 + y) = 2 + y = y \ .$$

Hence θ is onto when $\delta = 1$. Now suppose that $\delta = -1$. In order to simplify the proof, let $v = px^{m}$ where $0 \neq p \in K$ and m integer. Let $u = x^{-2} v(\sum_{\varepsilon} b_{\varepsilon}(x^{-1})^{\varepsilon})$ where $\sum_{\varepsilon} b_{\varepsilon}(x^{-1})^{\varepsilon} \in K(<x>)$. Then by (4.6) we have

$$\theta[(\sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} x^{\varepsilon})(1 + y) + \lambda x^{-1}] = \sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} [\lambda x^{-1} + u(1 + y)]^{\varepsilon} [(1 + 1 + v(1 + y)]$$

$$+ \lambda[\lambda x^{-1} + u(1 + y)]^{-1} = \sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} [(\lambda x^{-1})^{\varepsilon} + \Omega_3(1 + y)][(v(1 + y)]$$

$$+ \lambda[(\lambda x^{-1})^{-1} - (\lambda x^{-1})^{-2} u(1 + y)] \text{ where } \Omega_3 \in K(<x>) \ .$$

Since $(1 + y)^{2} = 0$ and $u = x^{-2} v(\sum_{\varepsilon} b_{\varepsilon}(x^{-1})^{\varepsilon})$ we have

$$\theta[(\sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} x^{\varepsilon})(1 + y) + \lambda x^{-1}] = \sum_{\varepsilon} \lambda^{-\varepsilon-1} b_{\varepsilon} (\lambda x^{-1})^{\varepsilon} v(1 + y) + x - \lambda^{-1} x^{2} u(1 + y)$$

$$= \sum_{\varepsilon} \lambda^{-1} b_{\varepsilon} (x^{-1})^{\varepsilon} v(1 + y) + x - \lambda^{-1} x^{2} [x^{-2} v \sum_{\varepsilon} b_{\varepsilon} (x^{-1})^{\varepsilon}](1 + y)$$

$$= \sum_{\varepsilon} \lambda^{-1} b_{\varepsilon} (x^{-1})^{\varepsilon} v(1 + y) + x - \sum_{\varepsilon} \lambda^{-1} b_{\varepsilon} (x^{-1})^{\varepsilon} v(1 + y) = x \ .$$

Also by using (4.6) we have

$$\theta[1 + \lambda^{-m} p^{-1} x^{m} (1 + y)] = 1 + \lambda^{-m} p^{-1} [\lambda x^{-1} + u(1 + y)]^{m} [1 + 1 + v(1 + y)]$$

$$= 1 + \lambda^{-m} p^{-1} [(\lambda x^{-1})^{m} + \Omega_4(1 + y)][(v(1 + y)]$$

where $\Omega_4 \in K(<x>)$.

Since $(1 + y)^2 = 0$ and $v = px^m$ we have

$$\theta[1 + \lambda^{-m}p^{-1}x^m(1 + y)] = 1 + \lambda^{-m}p^{-1}[\lambda^m(x^{-1})^m](px^m)(1 + y) = 2 + y = y .$$

Hence θ is also onto when $\delta = -1$.

Finally we prove that θ is 1-1 . Suppose $\sum_i \alpha_i x^i + (\sum_j \beta_j x^j)y$ is a member of $K(G)$ such that $\theta[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j)y] = 0$. Then we show that all α_i and all β_j are zero.

It is convenient to distinguish even and odd powers of x in $\sum_i \alpha_i x^i$ and $\sum_j \beta_j x^j$. Thus let

$$\sum_i \alpha_i x^i = \sum_\nu \alpha_{2\nu} x^{2\nu} + \sum_\sigma \alpha_{2\sigma+1} x^{2\sigma+1} .$$

$$\sum_j \beta_j x^j = \sum_\mu \beta_{2\mu} x^{2\mu} + \sum_\xi \beta_{2\xi+1} x^{2\xi+1} . \qquad (1)$$

By (1) and using (4.6) we have

$$\theta[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j)y] = \sum_\nu \alpha_{2\nu}(\lambda x^{\pm 1})^{2\nu} + \sum_\sigma \alpha_{2\sigma+1}[(\lambda x^{\pm 1})^{2\sigma+1} + (\lambda x^{\pm 1})^{2\sigma} u(1 + y)]$$

$$+ (\sum_\mu \beta_{2\mu}(\lambda x^{\pm 1})^{2\mu} + \sum_\xi \beta_{2\xi+1}[(\lambda x^{\pm 1})^{2\xi+1} + (\lambda x^{\pm 1})^{2\xi} u(1 + y)])$$

$$[1 + v(1 + y)] = 0 .$$

In order to simplify let $A = \sum_\sigma \alpha_{2\sigma+1}(\lambda x^{\pm 1})^{2\sigma} u,$ $B = \sum_\xi \beta_{2\xi+1}(\lambda x^{\pm 1})^{2\xi} u$, we have

$$\theta[\sum_i \alpha_i x^i + (\sum_j \beta_j x^j)y] = \sum_i \alpha_i (\lambda x^{\pm 1})^i + A(1 + y) + \sum_j \beta_j (\lambda x^{\pm 1})^j + B(1 + y)$$

$$+ [\sum_j \beta_j (\lambda x^{\pm 1})^j] v(1 + y) = 0 . \qquad (2)$$

By multiplying (2) by $1 + y$ and using $(1 + y)^2 = 0$ we obtain

$$[\sum_i \alpha_i(\lambda x^{\pm 1})^i + \sum_j \beta_j(\lambda x^{\pm 1})^j](1 + y) = 0 \text{ .} \qquad (3)$$

This implies that

$$\sum_i \alpha_i(\lambda x^{\pm 1})^i + \sum_j \beta_j(\lambda x^{\pm})^j = 0 \text{ .} \qquad (4)$$

Since $\lambda \neq 0$, it follows from (4) that $\alpha_i = \beta_i$ for all i and this implies that $A = B$. From this result and (2) we conclude that $\sum_j \beta_j(\lambda x^{\pm 1})^j v(1 + y) = 0$. But v is a unit and so $\sum_j \beta_j(\lambda x^{\pm 1})^j (1 + y) = 0$. This implies that $\beta_j = 0$ for all j because $\lambda \neq 0$. Thus $\alpha_i = \beta_i = 0$ for all i i.e. θ is 1-1 . Δ

Combining lemmas (4.9) and (4.10) we have:

<u>Theorem IV</u>

Let $G = \langle x\rangle \times \langle y\rangle$ where $\langle x\rangle$ is an infinite cyclic group and $y^2 = 1$. Let K be a field of characteristic 2 . Then θ is a K-automorphism of $K(G)$ if and only if there exist $\lambda \in K - \{0\}$ and $u, v \in K(\langle x\rangle)$ such that v is a unit and

$$\theta(x) = \lambda x^{\pm 1} + u(1 + y) \text{ .}$$

$$\theta(y) = 1 + v(1 + y) \text{ .}$$

CHAPTER 5

Let $K = GF(p)$, the Galois field with p elements. In [10] D.S. Passman proved that the group rings of all non-isomorphic p-groups of order at most p^4 over K are non-isomorphic. Our aim in this chapter is to investigate the corresponding property for non-isomorphic p-groups of order p^5 $(p > 3)$; unfortunately this problem is still open.

We use Schreier's classification of groups of order p^5 $(p > 3)$ in [14]. As far as possible we retain his notations but, for convenience in accordance with present-day usage, we replace his Gothic letters by capital Roman letters, his capital letters for groups elements by small letters, and E by 1 .

The groups of order p^5 $(p > 3)$ as characterised by Schreier, are divided into ten types, each type being again sub-divided into various sub-types of non-isomorphic groups.

Our techniques are based on the results of Jennings in [6] and Passman in [10]. We also use the notations found in (1.25). We say two groups G_1 and G_2 are distinguished if $K(G_1) \ncong K(G_2)$.

Since there are few details given in [10] for finding the properties of groups of order p^2, p^3 and p^4 we insert details for some of them before pursuing the main aim. For example we find the properties of groups of type (X), (XI), (XII) and (XIII) given in [10] of order p^4 $(p \geq 3)$.

For convenience we replace letters P, Q, and R by letters a, b, and c respectively.

Group X

This group is given by the relations,

$$G = \langle a,b,c \mid a^{p^2} = 1,\ b^p = 1,\ c^p = 1,\ c^{-1}ac = ab,\ b^{-1}ab = a,\ c^{-1}bc = b\rangle .$$

Observe that $b \in Z(G)$. Also $c^{-1}ac = ab$ implies that $ac = cab$ so every element of G is of the form $c^\gamma a^\alpha b^\beta$.

From $c^{-1}ac = ab$ and $b \in Z(G)$ we conclude that, $c^{-1}a^nc = (c^{-1}ac)^n = (ab)^n = a^nb^n$. This implies that $cb^{-n} = a^{-n}ca^n$ and from this and $b \in Z(G)$ we have $c^tb^{-tn} = (cb^{-n})^t = (a^{-n}ca^n)^t = a^{-n}c^ta^n$. Hence we have

$$a^nc^t = c^ta^nb^{nt} \quad . \tag{1}$$

Now we prove by induction that for $K \geq 1$,

$$(c^\gamma a^\alpha b^\beta)^K = c^{K\gamma}a^{K\alpha}b^{K\beta + \frac{K(K-1)}{2}\alpha\gamma} \tag{2}$$

For $K = 1$ there is nothing to prove. Suppose that (2) is valid for K : then by using (1) we have

$$(c^\gamma a^\alpha b^\beta)^{K+1} = (c^\gamma a^\alpha b^\beta)^K(c^\gamma a^\alpha b^\beta) = [c^{K\gamma}a^{K\alpha}b^{K\beta + \frac{K(K-1)}{2}\alpha\gamma}](c^\gamma a^\alpha b^\beta)$$

$$= c^{K\gamma}a^{K\alpha}c^\gamma a^\alpha b^{(K+1)\beta + \frac{K(K-1)}{2}\alpha\gamma} = c^{K\gamma}(c^\gamma a^{K\alpha}b^{K\alpha\gamma})a^\alpha b^{(K+1)\beta + \frac{K(K-1)}{2}\alpha\gamma} .$$

$$= c^{(K+1)\gamma}a^{(K+1)\alpha}b^{(K+1)\beta + K\alpha\gamma + \frac{K(K-1)}{2}\alpha\gamma}$$

$$= c^{(K+1)\gamma}a^{(K+1)\alpha}a^{(K+1)\beta + \frac{(K+1)K}{2}\alpha\gamma} \quad .$$

Hence our claim has been provedand in particular we have

$$(c^\gamma a^\alpha b^\beta)^p = c^{p\gamma}a^{p\alpha}b^{p\beta + \frac{p(p-1)}{2}\alpha\gamma} = a^{p\alpha} \tag{3}$$

Now we calculate $Z(G)$. Since $b \in Z(G)$, $c^\gamma a^\alpha b^\beta \in Z(G)$ if and only if $(c^\gamma a^\alpha)a = a(c^\gamma a^\alpha)$ and $(c^\gamma a^\alpha)c = c(c^\gamma a^\alpha)$. Hence if $c^\gamma a^\alpha b^\beta \in Z(G)$ then it follows from (1) that $b^\gamma = 1$ and $b^\alpha = 1$.

Therefore $\gamma = wp$, $\alpha = \varepsilon p$. Hence every element of $Z(G)$ is of form $c^{wp}a^{\varepsilon p}b^{\beta} = a^{\varepsilon p}b^{\beta}$. This implies that $Z(G) = \{a^{\varepsilon p}b^{\beta}\} = \langle a^p\rangle \times \langle b\rangle$, so $Z(G)$ is of order p^2 and of type (p, p) .

Now $G/\langle b\rangle$ is an abelian group of type (p^2, p) . In particular, $G' \subseteq \langle b\rangle$. Since G is non-abelian, $G' = \langle b\rangle$.

Finally we calculate the M-series.

$M_1 = G$. By using (3) we have

$$M_2 = \langle (G, G), M^{(p)}_{(2/p)}\rangle = \langle G', G^{(p)}\rangle = \langle\langle b\rangle, \langle a^p\rangle\rangle = \langle b\rangle \times \langle a^p\rangle .$$

Since $b, a^p \in Z(G)$ we have

$$M_3 = \langle (M_2, G), M^{(p)}_{(3/p)}\rangle = \langle\langle 1\rangle, \langle a^p\rangle\rangle = \langle a^p\rangle \ .$$

Also we have

$$M_3 = M_4 = \ldots = M_p = \langle a^p\rangle .$$

$$M_{p+1} = \langle (M_p, G), M^{(p)}_{(p+1/p)}\rangle = \langle\langle 1\rangle, M_2^{(p)}\rangle = \langle a^{p^2}\rangle = \langle 1\rangle .$$

Thus $M_1/M_2 = \langle cM_2\rangle \times \langle aM_2\rangle$, abelian group (p, p) , $|M_2/M_3| = p$,

$M_i/M_{i+1} = 1 \ (i = 3, \ldots, p - 1)$, $M_p/M_{p+1} = p$.

Groups (XI),(XII), (XIII)

These groups are given by the relations

$$G = \langle a,b,c \mid a^{p^2} = 1,\ b^p = 1,\ c^p = a^{\psi p},\ b^{-1}ab = a^{1+p},\ c^{-1}ac = ab,\ c^{-1}bc = b\rangle$$

where $\psi = 0, 1$, and any non-residue modulo p respectively.

We begin with results common to these groups.

From $b^{-1}ab = a^{1+p}$ we conclude that $ab = ba^{1+p}$, from this and $c^{-1}ac = ab$ we have $ac = cab = cba^{1+p}$. Since $bc = cb$ so every element of G is of form $c^\gamma b^\beta a^\alpha$.

Also we have $b^{-1}a^t b = (b^{-1}ab)^t = (a^{1+p})^t = a^{t(1+p)}$. In particular we have $b^{-1}a^p b = a^{p(1+p)} = a^p a^{p^2} = a^p$, then $a^p b = ba^p$.

Again from $b^{-1}a^t b = a^{t(1+p)}$ we conclude that $b = a^{-t}ba^t a^{tp}$ and this with $a^p b = ba^p$ implies that $b^n = a^{-t}b^n a^t a^{ntp}$. Hence we have

$$a^t b^n = b^n a^t a^{ntp} . \qquad (4)$$

Now we prove by induction that $c^{-K}ac^K = ab^K$. For $K = 1$ there is nothing to prove. Let $c^{-K}ac^K = ab^K$ then we have
$c^{-(K+1)}ac^{K+1} = c^{-1}[c^{-K}ac^K]c = c^{-1}(ab^K)c = (c^{-1}ac)b^K = (ab)b^K = ab^{K+1}$
because $bc = cb$.

By using (4) and $c^{-K}ac^K = ab^K$ we have $c^{-K}ac^K = b^K a^{1+Kp}$. Also by induction we prove that

$$c^{-K}a^n c^K = b^{nK} a^{n + \frac{n(n+1)}{2}Kp} \qquad (5)$$

For $n = 1$ our assertion is true. Let

$$c^{-K}a^n c^K = b^{nK} a^{n + \frac{n(n+1)}{2}Kp} .$$

By (4) and $a^pb = ba^p$ we have

$$c^{-K}a^{n+1}c^{K} = (c^{-K}ac^{K})^{n+1} = (c^{-K}ac^{K})^{n}(c^{-K}ac^{K}) = [b^{nK}a^{n + \frac{n(n+1)}{2}Kp}](c^{-K}ac^{K})$$

$$= [b^{nK}a^{n + \frac{n(n+1)}{2}Kp}](ab^{K}) = b^{nK}a^{n+1}b^{K}a^{\frac{n(n+1)}{2}Kp}$$

$$= b^{nK}(b^{K}a^{n+1}a^{K(n+1)p})\,a^{\frac{n(n+1)}{2}Kp} = b^{(n+1)K}a^{n+1}a^{\frac{(n+1)(n+2)}{2}Kp}$$

$$= b^{(n+1)K}a^{(n+1) + \frac{(n+1)(n+2)}{2}Kp} .$$

In particular we have $c^{-K}a^{p}c^{K} = b^{pK}a^{p + \frac{p(p+1)}{2}Kp} = a^{p}$ because $b^{p} = 1$ and $a^{p^{2}} = 1$. From this we have $a^{p}c = ca^{p}$. By this result and $a^{p}b = ba^{p}$ we conclude that $a^{p} \in Z(G)$ the centre of G .

Now we prove by induction that

$$(c^{\gamma}b^{\beta}a^{\alpha})^{n} = c^{n\gamma}\,b^{n\beta + \frac{n(n-1)}{2}\alpha\gamma}$$

$$a^{n\alpha + \frac{n(n-1)}{2}\alpha\beta p + [\frac{\alpha(\alpha+1)}{2} + \frac{2\alpha(2\alpha+1)}{2} + \dots + \frac{(n-1)\alpha[(n-1)\alpha+1]}{2}]\gamma p} \qquad (6)$$

For $n = 1$ there is nothing to prove. Let

$$A = \frac{\alpha(\alpha+1)}{2} + \frac{2\alpha(2\alpha+1)}{2} + \dots + \frac{(n-1)\alpha[(n-1)\alpha+1]}{2} .$$

By using $a^{p} \in Z(G)$, $bc = cb$, (4) and (5) we have,

$$(c^{\gamma}b^{\beta}a^{\alpha})^{n+1} = [c^{n\gamma}\,b^{n\beta + \frac{n(n-1)}{2}\alpha\gamma}\,a^{n\alpha + \frac{n(n-1)}{2}\alpha\beta p + A\gamma p}](c^{\gamma}b^{\beta}a^{\alpha})$$

$$= [c^{n\gamma}\,b^{n\beta + \frac{n(n-1)}{2}\alpha\gamma}\,a^{n\alpha}](c^{\gamma}b^{\beta}a^{\alpha})\,a^{\frac{n(n-1)}{2}\alpha\beta p + A\gamma p}$$

$$= c^{n\gamma}\,b^{n\beta + \frac{n(n-1)}{2}\alpha\gamma}\,(c^{\gamma}\,b^{n\alpha\gamma}\,a^{n\alpha + \frac{n\alpha(n\alpha+1)}{2}\gamma p})b^{\beta}a^{\alpha}\,a^{\frac{n(n-1)}{2}\alpha\beta p+A\gamma p}$$

$$= c^{(n+1)\gamma} b^{n\beta + \frac{n(n-1)}{2}\alpha\gamma + n\alpha\gamma} a^{n\alpha} b^{\beta} a^{\alpha} a^{\frac{n\alpha(n\alpha+1)}{2}\gamma p + \frac{n(n-1)}{2}\alpha\beta p + A\gamma p}$$

$$= c^{(n+1)\gamma} b^{n\beta + \frac{(n+1)n}{2}\alpha\gamma} (b^{\beta} a^{n\alpha} a^{n\alpha\beta p}) a^{\alpha} a^{\frac{n\alpha(n\alpha+1)}{2}\gamma p + \frac{n(n-1)}{2}\alpha\beta p + A\gamma p}$$

$$= c^{(n+1)\gamma} b^{(n+1)\beta + \frac{(n+1)n}{2}\alpha\gamma}$$

$$a^{(n+1)\alpha + \frac{(n+1)n}{2}\alpha\beta p + [\frac{\alpha(\alpha+1)}{2} + \frac{2\alpha(2\alpha+1)}{2} + \ldots + \frac{n\alpha(n\alpha+1)}{2}]\gamma p} .$$

In particular we have,

$$(c^{\gamma} b^{\beta} a^{\alpha})^{p} = c^{p\gamma} a^{p\alpha + [\frac{\alpha(\alpha+1)}{2} + \frac{2\alpha(2\alpha+1)}{2} + \ldots + \frac{(p-1)\alpha[(p-1)\alpha+1]}{2}]\gamma p}$$

$$= a^{\psi p\gamma + p\alpha + [\frac{\alpha(\alpha+1)}{2} + \frac{2\alpha(2\alpha+1)}{2} + \ldots + \frac{(p-1)\alpha[(p-1)\alpha+1]}{2}]\gamma p} .$$

This implies that $<G^{(p)}> = <a^{p}>$.

By $a^{p} \in Z(G)$, $bc = cb$ and repeating (4), (5) we have $(c^{\gamma}b^{\beta}a^{\alpha})^{-1}(c^{r}b^{s}a^{t})^{-1}(c^{\gamma}b^{\beta}a^{\alpha})(c^{r}b^{s}a^{t}) = b^{\alpha r - t\gamma} a^{up}$ (u integer). Hence we have $G' = <\{b^{\alpha r - t\gamma} a^{up}\}> = <b> \times <a^{p}>$. This implies that

$${}^{G}/_{G'} = <\{c^{\gamma}b^{\beta}a^{\alpha}(<b> \times <a^{p}>)\}> = <c(<b> \times <a^{p}>)> \times <a(<b> \times <a^{p}>)> .$$

Thus ${}^{G}/_{G'}$ is of order p^{2} and of type (p, p) .

Now we calculate $Z(G)$. $c^{\gamma}b^{\beta}a^{\alpha} \in Z(G)$ if and only if $(c^{\gamma}b^{\beta}a^{\alpha})a = a(c^{\gamma}b^{\beta}a^{\alpha})$, $(c^{\gamma}b^{\beta}a^{\alpha})b = b(c^{\gamma}b^{\beta}a^{\alpha})$ and $(c^{\gamma}b^{\beta}a^{\alpha})c = c(c^{\gamma}b^{\beta}a^{\alpha})$.

By using (4), (5) and $(c^{\gamma}b^{\beta}a^{\alpha})a = a(c^{\gamma}b^{\beta}a^{\alpha})$ we have, $c^{\gamma}b^{\beta}a = ac^{\gamma}b^{\beta} = (c^{\gamma}b^{\gamma}a^{1+p\gamma})b^{\beta} = c^{\gamma}b^{\gamma}(b^{\beta}a^{1+p\gamma}a^{\beta(1+p\gamma)p}) = c^{\gamma}b^{\gamma+\beta}a^{1+p\gamma+p\beta}$. This implies that $1 = b^{\gamma}a^{p\gamma+p\beta}$ so we obtain $\gamma = \varepsilon p$ and $\beta = \sigma p$.

Also by $cb = bc$, (4) and $(c^\gamma b^\beta a^\alpha)b = b(c^\gamma b^\beta a^\alpha)$ we have $a^\alpha b = ba^\alpha$ or we have $ba^\alpha a^{\alpha p} = ba^\alpha$ and this implies that $a^{\alpha p} = 1$ so $\alpha = \lambda p$.

From $(c^\gamma b^\beta a^\alpha)c = c(c^\gamma b^\beta a^\alpha)$ as above we conclude that $\alpha = \lambda p$. Hence every element of $Z(G)$ is of form $c^{\varepsilon p}\, b^{\sigma p}\, \alpha^{\lambda p} = a^{\lambda p}$ and this implies that $Z(G) = \langle a^p\rangle$. Hence $Z(G)$ is of order p and of type (p) .

Finally we calculate the M-series.

$M_1 = G$.

$M_2 = \langle G', G^{(p)}\rangle = \langle\langle b\rangle \times \langle a^p\rangle, \langle a^p\rangle\rangle = \langle b\rangle \times \langle a^p\rangle$.

Now we calculate (M_2, G) . Since $a^p \in Z(G)$ we have $(c^\gamma b^\beta a^\alpha)^{-1} b^{-t} (c^\gamma b^\beta a^\alpha) b^t = a^{-\alpha} b^{-\beta} c^{-\gamma} b^{-t} c^\gamma b^\beta a^\alpha b^t = a^{-\alpha} b^{-t} a^\alpha b^t$ because $bc = cb$. But by (4) we have $a^{-\alpha} b^{-t} a^\alpha b^t = a^{-\alpha} b^{-t} (b^t a^\alpha a^{\alpha t p}) = a^{\alpha t p}$. Hence we have

$M_3 = \langle (M_2, G), M^{(p)}_{(3/p)}\rangle = \langle\langle a^p\rangle, G^{(p)}\rangle = \langle a^p\rangle$.

$M_3 = M_4 = \ldots = M_p = \langle a^p\rangle$.

$M_{p+1} = \langle (M_p, G), M^{(p)}_{(p+1/p)}\rangle = \langle\langle 1\rangle, \langle a^{p^2}\rangle\rangle = \langle 1\rangle$.

Thus we have,

$M_1/M_2 = \langle cM_2\rangle \times \langle aM_2\rangle$, abelian group (p, p) , $|M_2/M_3| = p$,

$M_i/M_{i+1} = 1$ $(i = 3, \ldots, p-1)$, $|M_p/M_{p+1}| = p$.

Let N be the Jacobson radical of $K(G)$. Then we calculate the kernel of $\phi : N/N^2 \to N^3/N^4$ for $p = 3$. Since

$M_1/M_2 = \langle cM_2 \rangle \times \langle aM_2 \rangle$ it follows from [6] that, $c - 1$ and $a - 1$ have weight 1 . Also since $M_2/M_3 = \langle bM_3 \rangle$, $b - 1$ has weight 2 .

Finally since $M_3/M_4 = \langle a^3M_4 \rangle$, $a^3 - 1$ has weight 3 . Hence every element of N/N^2 is of the form $[m(a - 1) + n(c - 1)] + N^2$ where $m, n \in K$, and then we have

$$[m(a-1) + n(c-1)]^3 = m^3(a-1)^3 + m^2n(a-1)(c-1)(a-1) + m^2n(c-1)(a-1)^2$$
$$+ mn^2(c-1)^2(a-1) + m^2n(a-1)^2(c-1) + mn^2(a-1)(c-1)^2$$
$$+ mn^2(c-1)(a-1)(c-1) + n^3(c-1)^3 \quad .$$

By using lemma (1.28) we have

$(a-1)(c-1)(a-1) \equiv (a-1)[(a-1)(c-1) + (c^{-1}a^{-1}ca-1)] \bmod N^4$. Since $b^3 = 1$ and $c^{-1}ac = ab$ we have

$c^{-1}a^{-1}ca - 1 = b^{-1} -1 = b^2 - 1 = (b - 1)^2 + 2(b - 1)$.

Hence we have

$(a-1)(c-1)(a-1) \equiv (a-1)^2(c-1) + (a-1)(b-1)^2 + 2(a-1)(b-1) \bmod N^4$.

But $(b-1)^2 \in N^4$ because $b - 1$ has weight 2 and then we have

$$(a-1)(c-1)(a-1) \equiv (a-1)^2(c-1) + 2(a-1)(b-1) \bmod N^4 . \qquad (7)$$

By the above we also have

$(c-1)(a-1)^2 \equiv [(a-1)(c-1) + (b-1)^2 + 2(b-1)](a-1) \bmod N^4$. We have

$(c-1)(a-1)^2 \equiv (a-1)(c-1)(a-1) + (b-1)^2(a-1) + 2(b-1)(a-1) \bmod N^4$.

Since $(a-1)(c-1)(a-1) \equiv (a-1)^2(c-1) + 2(a-1)(b-1) \bmod N^4$ and $(b-1)^2 \in N^4$ we have

$$(c-1)(a-1)^2 \equiv (a-1)^2(c-1) + 2(a-1)(b-1) + 2(b-1)(a-1) \bmod N^4 . \qquad (8)$$

As before we have

$$(c-1)^2(a-1) \equiv (c-1)(a-1)(c-1) + (c-1)(b-1)^2 + 2(c-1)(b-1) \bmod N^4 .$$

Since $(b-1)^2 \in N^4$ we have

$$(c-1)^2(a-1) \equiv (c-1)(a-1)(c-1) + 2(c-1)(b-1) \bmod N^4 . \qquad (9)$$

But we have

$$(c-1)(a-1)(c-1) \equiv (a-1)(c-1)^2 + (b-1)^2(c-1) + 2(b-1)(c-1) \bmod N^4 .$$

Since $(b-1)^2 \in N^4$ we have

$$(c-1)(a-1)(c-1) \equiv (a-1)(c-1)^2 + 2(b-1)(c-1) \bmod N^4 . \qquad (10)$$

By using (7), (8), (9) and (10) we have

$$\begin{aligned}[m(a-1) + n(c-1)]^3 \equiv\ & m^3(a-1)^3 + m^2n[(a-1)^2(c-1) + 2(a-1)(b-1)] \\ & + m^2n[(a-1)^2(c-1) + 2(a-1)(b-1) + 2(b-1)(a-1)] \\ & + mn^2[(a-1)(c-1)^2 + 2(b-1)(c-1) + 2(c-1)(b-1)] + m^2n(a-1)^2(c-1) \\ & + mn^2(a-1)(c-1)^2 + mn^2[(a-1)(c-1)^2 + 2(b-1)(c-1)] + n^3(c-1)^3 \bmod N^4 .\end{aligned}$$

Since the characteristic of K is 3 , and $bc = cb$ we have

$$\begin{aligned}[m(a-1) + n(c-1)]^3 \equiv\ & m^3(a^3 - 1) + m^2n(a-1)(b-1) + 2m^2n(b-1)(a-1) \\ & + n^3(c^3-1) \bmod N^4 . \qquad (11)\end{aligned}$$

Since $p = 3$ we have $b^{-1}ab = a^{1+p} = a^4$. This implies that $(b-1)(a-1) = (a-1)(b-1) + ba(1-a^{-1}b^{-1}ab)$. We have $(b-1)(a-1) = (a-1)(b-1) + ba(1-a^3)$. We have

$$(b-1)(a-1) = (a-1)(b-1) + (ba-1+1)(1-a^3) = (a-1)(b-1) + (ba-1)(1-a^3) + (1-a^3) .$$

Since $a^3 - 1$ has weight 3 we have

$$(b-1)(a-1) \equiv (a-1)(b-1) + (1-a^3) \bmod N^4 . \qquad (12)$$

By using (11), (12) and $c^3 = a^{3\psi}$ we have

$$[m(a-1) + n(c-1)]^3 \equiv m^3(a^3-1) + 2m^2n(1-a^3) + n^3(a^{3\psi}-1) \bmod N^4 . \quad (13)$$

By using lemma (1.28) and the fact that a^3-1 has weight 3 we have $a^{3\psi} - 1 \equiv \psi(a^3-1) \bmod N^4$. Hence we have

$$[m(a-1) + n(c-1)]^3 \equiv m^3(a^3-1) + m^2n(a^3-1) + \psi n^3(a^3-1) \bmod N^4 .$$

Or we have $[m(a-1) + n(c-1)]^3 \equiv (m^3 + m^2n + \psi n^3)\,(a^3-1) \bmod N^4$. (14)

It follows from (14) that $[m(a-1) + n(c-1)] + N^2 \in \ker \phi$ if and only if $m^3 + m^2n + \psi n^3 = 0$.

We now have to consider the three groups separately.

Group (XI)

In this case $\psi = 0$ and then we have $m^3 + m^2n = 0$. This implies that $m^2(m + n) = 0$. Since K is the prime field of three elements we have one of the following:

$$\begin{matrix} m = 0 \\ n = 0 \end{matrix} , \quad \begin{matrix} m = 0 \\ n = 1 \end{matrix} , \quad \begin{matrix} m = 0 \\ n = 2 \end{matrix} , \quad \begin{matrix} m = 1 \\ n = 2 \end{matrix} , \quad \text{and} \quad \begin{matrix} m = 2 \\ n = 1 \end{matrix} .$$

Hence in this case the kernel of ϕ consists of five elements.

Group (XII)

In this case $\psi = 1$ and then we have $m^3 + m^2n + n^3 = 0$.

This implies that

$$\begin{matrix} m = 0 \\ n = 0 \end{matrix} , \quad \begin{matrix} m = 1 \\ n = 1 \end{matrix} , \quad \text{and} \quad \begin{matrix} m = 2 \\ n = 2 \end{matrix} .$$

Hence in this case the kernel of ϕ consists of three elements.

Group (XIII)

In this case $\psi = 2$ because 2 is a non-residue modulo 3 . Thus we have $m^3 + m^2n + 2n^3 = 0$ and the only solution is $\begin{matrix} m = 0 \\ n = 0 \end{matrix}$.

Hence in this case the kernel of ϕ consists of one element. Thus we have the following table.

Group number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 $p>3$ type	M_p/M_{p+1} type	Kernel size ($p = 3$)
X	(p, p)	(p^2, p)	(p, p)	(p)	(1)	(p)	
XI	(p)	(p, p)	(p, p)	(p)	(1)	(p)	5
XII	(p)	(p, p)	(p, p)	(p)	(1)	(p)	3
XIII	(p)	(p, p)	(p, p)	(p)	(1)	(p)	1

This table shows that the groups (XI), (XII), and (XIII) for $p = 3$ are distinguished. For $p > 3$ we have the following lemmas found in [10].

Before starting to write the lemmas we note that by (1.28) we have $(a-1)$ and $(c-1)$ have weight 1 , $b - 1$ has weight 2 , and $a^p - 1$ has weight p . Since $p > 3$ we have $a^p-1 \in N^4$. Hence by (1.28) we have

$$(a-1)(c-1) \equiv (c-1)(a-1) + (b-1) \bmod N^3 \qquad \text{(I)}$$

$$(a-1)(b-1) \equiv (b-1)(a-1) + (a^p-1) \bmod N^{p+1} \qquad \text{(II)}$$

$$(a-1)(b-1) \equiv (b-1)(a-1) \bmod N^4 \qquad \text{(III)}$$

$$(c-1)(b-1) = (b-1)(c-1) \quad \text{because} \quad bc = cb \qquad \text{(IV)}$$

$$(a^{\psi p}-1) \equiv \psi(a^p-1) \bmod N^{p+1} \quad . \qquad \text{(V)}$$

Lemma 5.1

The natural map $\phi : N/N^2 \to N^p/N^{p+1}$ is given by $\{m(a-1) + n(c-1)\}^p \equiv (m + \psi n)(a^p-1) \bmod N^{p+1}$.

Proof

By (I) we have $[m(a-1), n(c-1)] \equiv mn(b-1) \bmod N^3$. By (III) and (IV) , $m(a-1)$ and $n(c-1)$ commute with $mn(b-1)$ modulo N^4 . Hence $m(a-1), n(c-1)$ commute with $[m(a-1), n(b-1)]$ modulo N^4 . Since $p > 3$ by lemma 2 of [10] we have $\{m(a-1) + n(c-1)\}^p \equiv m^p(a-1)^p + n^p(c-1)^p \bmod N^{p+1}$. By (IV), $c^p = a^{\psi p}$, and the fact that K is a prime field of p elements we have

$$\{m(a-1) + n(c-1)\}^p \equiv (m + \psi n)(a^p-1) \bmod N^{p+1} . \qquad \Delta$$

Lemma 5.2

Let $S = \langle (b-1), (b-1)^2, \dots, (b-1)^{(p-1)/2}, N^p \rangle$. Let $\phi : N/N^2 \to N^p/N^{p+1}$ be the natural homomorphism. Let $N^{p+1} \subseteq T \subseteq N^p$ with $T/N^{p+1} = \phi(N/N^2)$. Let $U = \{u \in N \mid \forall x \in N , xu - ux \in T\}$. Then $S = U$.

Proof

By (5.1) it is evident that $T = \langle a^p-1, N^{p+1} \rangle$.

Let $x \in S$. Then $x = \alpha_1(b-1) + \alpha_2(b-1)^2 + \dots + \alpha_{p-1/2}(b-1)^{p-1/2} + w$ where $\alpha_i \in K$ $(i = 1, 2, \dots, p-1/2)$ and $w \in N^p$. Let $u \in N$. Then we write u in terms of the Jennings basis modulo N^p i.e.

$$u = \sum \beta_{i,j,K}(a-1)^i(b-1)^j(c-1)^K + \sigma \quad \text{where} \quad 1 \le i + 2j + K \le p - 1 .$$

By using (II) and $a^p-1 \in \overset{p}{N}$ we have

$$(a-1)(b-1)^\mu \equiv (b-1)^\mu(a-1) \bmod N^{p+1} \quad (\mu > 1) . \qquad (4)$$

$$(a-1)^\mu(b-1) \equiv (b-1)(a-1)^\mu \bmod N^{p+1} \quad (\mu > 1) \qquad (5)$$

Hence by using (4) and (5) we have

$$ux - xu = [\sum \beta_{i,j,K}(a-1)^{i}(b-1)^{j}(c-1)^{K} + \sigma]$$

$$\times\ [\alpha_1(b-1) + \alpha_2(b-1)^2 + \ldots + \alpha_{p-1/2}(b-1)^{\frac{p-1}{2}} + w]$$

$$-\ [\alpha_1(b-1) + \alpha_2(b-1)^2 + \ldots + \alpha_{p-1/2}(b-1)^{\frac{p-1}{2}} + w]$$

$$\times\ [\sum \beta_{i,j,K}(a-1)^{i}(b-1)^{j}(c-1)^{K} + \sigma]$$

$$\equiv [\beta_{1,0,0}\,\alpha_1(a-1)(b-1) - \alpha_1\beta_{1,0,0}(b-1)(a-1)] + \eta\ ,$$

where $\eta \in N^{p+1}$.

By using (II) we deduce that $ux - xu \equiv \alpha_1\beta_{1,0,0}(a^{p}-1) + \Omega$, where $\Omega \in N^{p+1}$. This implies that $ux - xu \in T$ and then $x \in U$, i.e. $S \subseteq U$.

Now we prove that $U \subseteq S$. If not we choose $u \in U\backslash S$ and we write u in terms of Jennings basis. Since $(b-1)^{j}$ for $2j < p$ belongs to S we assume that no terms of the form $(b-1)^{j}$ with $2j < p$ occur in the representation of u . Now we prove by induction on t that $u \in N^{t}$ for $t \leq p$. For $t = 1$ there is nothing to prove because $u \in N$. Let $u \in N^{t}$ with $t < p$. Then we prove as follows that $u \in N^{t+1}$. Now we can write

$$u \equiv \sum \alpha_{i,j,K}(a-1)^{i}(b-1)^{j}(c-1)^{K} \bmod N^{t+1}$$

where $i + 2j + K = t$ and $\alpha_{0,j,0} = 0$. Since $u \in U$, $a-1 \in N$ and $c-1 \in N$ we have

$$[(a-1),\ u] \in T\ , \qquad [(c-1),\ u] \in T\ , \qquad \text{and}$$

$$[(a-1),\ u] \in T + N^{t+2}\ , \qquad [(c-1),\ u] \in T + N^{t+2}\ .$$

Now we prove by induction on $K (K \geq 1)$ that

$$[(a-1),\ u] \equiv \sum_{K\geq 1} K\ \alpha_{i,j,K}(a-1)^{i}(b-1)^{j+1}(c-1)^{K-1} \bmod N^{t+2}\ . \qquad (6)$$

$$[(c-1),\ u] \equiv -\sum_{i\geq 1} i\ \alpha_{i,j,K}(a-1)^{i-1}(b-1)^{j+1}(c-1)^{K} \bmod N^{t+2}\ . \qquad (7)$$

By (II) and $t < p$ we know that $(a-1)$ commutes with $(b-1)$ modulo N^{t+1} . Hence to prove (6) it is enough to prove

$$[(a-1),\ (c-1)^{K}] \equiv K(b-1)(c-1)^{K-1} \bmod N^{K+2} \qquad (8)$$

By using (I) there is nothing to prove when $K = 1$. Suppose (8) holds for K . Then we wish to prove the corresponding result for $K + 1$. We have

$$[(a-1),\ (c-1)^{K+1}] = (a-1)(c-1)^{K+1} - (c-1)^{K+1}(a-1)$$

$$= [(a-1)(c-1)^{K}](c-1) - (c-1)^{K+1}(a-1)$$

$$= \{(c-1)^{K}(a-1) + K(b-1)(c-1)^{K-1} + \theta_1\}(c-1) - (c-1)^{K+1}(a-1)$$

where $\theta_1 \in N^{K+2}$.

From this and (1), (3) we conclude that

$$[(a-1),\ (c-1)^{K+1}] = (c-1)^{K}[(c-1)(a-1) + (b-1) + \theta_2] + K(b-1)(c-1)^{K} + \theta_1(c-1) - (c-1)^{K+1}(a-1)$$

Where $\theta_2 \in N^3$ by (I) Page 84. Thus

$$[(a-1),\ (c-1)^{K+1}] = (c-1)^{K}(b-1) + (c-1)^{K}\theta_2 + K(b-1)(c-1)^{K} + \theta_1(c-1)$$

$$= (K+1)(b-1)(c-1)^{K} + \theta_3$$

where $\theta_3 = (c-1)^{K}\theta_2 + \theta_1(c-1) \in N^{K+3}$. Hence (8) has been established and so (6) has been established.

The proof of (7) is similar to the proof of (6) and so we omit it.

By using (6), (7), $[(a-1), u] \in T + N^{t+2} = \langle N^{t+2}, a^p - 1\rangle$ $[(c-1), u] \in T + N^{t+2} = \langle N^{t+2}, a^p-1\rangle$ we conclude that

$$\sum_{K\geq 1} K\, \alpha_{i,j,K}(a-1)^i(b-1)^{j+1}(c-1)^{K-1} = 0 \qquad (9)$$

$$\sum_{i\geq 1} i\, \alpha_{i,j,K}(a-1)^{i-1}(b-1)^{j+1}(c-1)^K = 0 \qquad (10)$$

because $i + 2(j+1) + (k-1) = (i + 2j + K) + 1 = t + 1$, $(i-1) + 2(j+1) + K = t + 1$, and $1 \leq i, j \leq t < p$. This implies that $\alpha_{i,j,K = 0}$ and then $u \equiv 0 \bmod N^{t+1}$. Hence $u \in N^p \subseteq S$ which is false, i.e. $S = U$. Δ

We remark that, on the one hand, sub-space S is determined by a particular basis in terms of the group elements and that, on the other hand, U is determined solely by the ring-theoretic structure. Thus this lemma shows that S is itself determined solely by the ring-theoretic structure.

Now we choose an element $x \in N\backslash N^2$ with $\phi(x + N^2) = 0$, and we choose $y \in N$ with $\phi(y + N^2) \neq 0$. By (5.1) and the fact that $a^p-1 \in N^p$ we can write

$$x = \lambda[\Psi(a-1) - (c-1)] + n,$$

$$y = \rho[\Psi(a-1) - (c-1)] + \mu(a-1) + m,$$

where $n, m \in N^2$ and $\lambda, \mu \neq 0$. But by using (I) we have $[x, y] \equiv \mu\lambda(b-1) \bmod N^3$. Thus, if $s \equiv \mu\lambda(b-1) + \sum_{i\geq 2} b_i(b-1)^i \bmod N^P$, then $s \in S$ and $[x, y] \equiv s \bmod N^3$.

By using (II), (III) we have $[x, (b-1)^i] \in N^{p+1}$ for $i \geq 2$ and $[n, s] \in N^{p+1}$. Hence we have

$$[x, s] \equiv \mu\lambda^2[\{\psi(a-1) - (c-1)\}, b-1] \equiv \mu\lambda^2\psi(a^p-1) \bmod N^{p+1}.$$

By using (6), (7), $[(a-1), u] \in T + N^{t+2} = \langle N^{t+2}, a^{p} - 1\rangle$ $[(c-1), u] \in T + N^{t+2} = \langle N^{t+2}, a^{p}-1\rangle$ we conclude that

$$\sum_{K\geq 1} K\,\alpha_{i,j,K}(a-1)^{i}(b-1)^{j+1}(c-1)^{K-1} = 0 \qquad (9)$$

$$\sum_{i\geq 1} i\,\alpha_{i,j,K}(a-1)^{i-1}(b-1)^{j+1}(c-1)^{K} = 0 \qquad (10)$$

because $i + 2(j+1) + (k-1) = (i + 2j + K) + 1 = t + 1$, $(i-1) + 2(j+1) + K = t + 1$, and $1 \leq i, j \leq t < p$. This implies that $\alpha_{i,j,K} = 0$ and then $u \equiv 0 \bmod N^{t+1}$. Hence $u \in N^{p} \subseteq S$ which is false, i.e. $S = U$. Δ

We remark that, on the one hand, sub-space S is determined by a particular basis in terms of the group elements and that, on the other hand, U is determined solely by the ring-theoretic structure. Thus this lemma shows that S is itself determined solely by the ring-theoretic structure.

Now we choose an element $x \in N\backslash N^{2}$ with $\phi(x + N^{2}) = 0$, and we choose $y \in N$ with $\phi(y + N^{2}) \neq 0$. By (5.1) and the fact that $a^{p}-1 \in N^{p}$ we can write

$x = \lambda[\Upsilon(a-1) - (c-1)] + n$,

$y = \rho[\Upsilon(a-1) - (c-1)] + \mu(a-1) + m$,

where $n, m \in N^{2}$ and $\lambda, \mu \neq 0$. But by using (I) we have $[x, y] \equiv \mu\lambda(b-1) \bmod N^{3}$. Thus, if $s \equiv \mu\lambda(b-1) + \sum_{i\geq 2} b_{i}(b-1)^{i} \bmod N^{P}$, then $s \in S$ and $[x, y] \equiv s \bmod N^{3}$.

By using (II), (III) we have $[x, (b-1)^{i}] \in N^{p+1}$ for $i \geq 2$ and $[n, s] \in N^{p+1}$. Hence we have

$[x, s] \equiv \mu\lambda^{2}[\{\psi(a-1) - (c-1)\}, b-1] \equiv \mu\lambda^{2}\psi(a^{P}-1) \bmod N^{p+1}$.

If $\psi = 0$, then $[x, s] \equiv 0 \bmod N^{p+1}$. Therefore the group for $\psi = 0$ is distinguished from the other two.

Suppose $\psi \neq 0$. By lemma (5.1) we have
$y^p - [x, s] \equiv (\mu - \mu\lambda^2\psi)(a^p - 1) \bmod N^{p+1}$, because $\mu^p = \mu$.

If $\psi = 1$ we may choose x so that $y^p - [x, s] \equiv 0 \bmod N^{p+1}$.
If ψ is not a quadratic residue, then for all choices of x
$y^p - [x, s] \not\equiv 0 \bmod N^{p+1}$. Thus the three groups are distinguished.

Now we start with type I of groups of order p^5 $(p > 3)$.

Type I

The groups of this type are given by the following relations,

$$G = \langle a, b_1, b_2 \mid a^p = 1,\ b_1^{p^3} = a^{\alpha_1},\ b_2^p = a^{\alpha_2},\ ab_i = b_ia\ (i = 1, 2),$$
$$b_2^{-1}\, b_1\, b_2 = b_1 a \rangle,$$

of which there are three sub-types given by

α_1	1	0	0
α_2	0	1	0

.

We denote these sub-types by (I, 1), (I, 2), (I, 3) respectively. Observe $a \in Z(G)$ and we have

$$b_1^n\, b_2^t = b_2^t\, b_1^n\, a^{nt} . \qquad (1)$$

The elements of this type are of the form $a^\alpha\, b_2^\beta\, b_1^\gamma$ and we have

$$(a^\alpha\, b_2^\beta\, b_1^\gamma)^m = a^{m\alpha + \frac{m(m-1)}{2}\beta\gamma}\, b_2^{m\beta}\, b_1^{m\gamma} .$$

Now we calculate $Z(G)$. $a^\alpha\, b_2^\beta\, b_1^\gamma \in Z(G)$ if and only if $(b_2^\beta\, b_1^\gamma)b_1 = b_1(b_2^\beta\, b_1^\gamma)$ and $(b_2^\beta\, b_1^\gamma)b_2 = b_2(b_2^\beta\, b_1^\gamma)$. Hence if $a^\alpha\, b_2^\beta\, b_1^\gamma \in Z(G)$ then it follows from (1) that $a^\beta = 1$ and $a^\gamma = 1$. Therefore $\beta = \varepsilon p$ and $\gamma = \sigma p$. Hence $Z(G) = \{a^\alpha\, b_2^{\varepsilon p}\, b_1^{\sigma p}\}$. Also we know that $G' = \langle a \rangle$.

Sub-type (I, 1)

For this sub-type we have $\alpha_1 = 1$, $\alpha_2 = 0$. Hence $Z(G) = \langle b_1^p \rangle$.

$M_1 = G$.

$M_i = \langle b_1^p \rangle \; (i = 2, 3, \ldots, p)$.

$M_j = \langle b_1^{p^2} \rangle \; (j = p + 1, \ldots, p^2)$.

$M_K = \langle a \rangle \quad (K = p^2 + 1, \ldots, p^3)$.

$M_{p^3+1} = \langle 1 \rangle$.

Sub-type (I, 2)

Since $\alpha_1 = 0$, $\alpha_2 = 1$ we have

$Z(G) = \langle a \rangle \times \langle b_1^p \rangle$.

$M_1 = G$.

$M_i = \langle a \rangle \times \langle b_1^p \rangle \quad (i = 2, \ldots, p)$.

$M_j = \langle b_1^{p^2} \rangle \quad (j = p+1, \ldots, p^2)$.

$M_{p^2+1} = \langle 1 \rangle$.

Sub-type (I, 3)

For this sub-type we have $\alpha_1 = 0, \alpha_2 = 0$. Hence

$Z(G) = \langle a \rangle \times \langle b_1{}^p \rangle$.

$M_1 = G$.

$M_2 = \langle a \rangle \times \langle b_1{}^p \rangle$.

$M_i = \langle b_1{}^p \rangle \quad (i = 3, \ldots, p)$.

$M_j = \langle b_1{}^{p^2} \rangle \quad (j = p + 1, \ldots, p^2)$.

$M_{p^2+1} = \langle 1 \rangle$.

Thus for type I we have the following table.

Group number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_p/M_{p+1} type	M_{p^2}/M_{p^2+1} type	M_{p^3}/M_{p^3+1} type
(I, 1)	(p^3)	(p^3,p)	(p,p)	(1)	(p)	(p)	(p)
(I, 2)	(p^2,p)	(p^3,p)	(p,p)	(1)	(p,p)	(p)	(1)
(I, 3)	(p^2,p)	(p^3,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE I

According to the Table I and Proposition (4), Corollary (6) of [10] the groups of type I are distinguished.

Type II

The groups of this type are given by the following relations,

$$G = \langle a, b_1, b_2 \mid a^p = 1,\ b_1^{p^2} = a^\alpha,\ b_2^{p^2} = 1,\ ab_1 = b_1a,\ ab_2 = b_2a,$$

$$b_2^{-1}b_1b_2 = b_1a\rangle \quad ,$$

Of which there are two sub-types given by $\alpha = 0$, $\alpha = 1$. We denote these sub-types by (II, 1), (II, 2) respectively.

The elements are of the form $a^\alpha\ b_2^\beta\ b_1^\gamma$ and we have

$$b_1^t\ b_2^n = b_2^n\ b_1^t\ a^{nt} \ .$$

$$(a^\alpha\ b_2^\beta\ b_1^\gamma)^m = a^{m\alpha + \frac{m(m-1)}{2}\beta\gamma}\ b_2^{m\beta}\ b_1^{m\gamma} \quad .$$

The elements of $Z(G)$ are of the form $a^\alpha\ b_2^{\varepsilon p}\ b_1^{\sigma p}$.

Sub-type (II, 1)

For this sub-type $\alpha = 0$ and we have

$M_1 = G$.

$M_2 = \langle a\rangle \times \langle b_2^p\rangle \times \langle b_1^p\rangle$.

$M_3 = M_4 = \ldots = M_p = \langle b_2^p\rangle \times \langle b_1^p\rangle$.

$M_{p+1} = \langle 1\rangle$.

Sub-type (II, 2)

For this sub-type $\alpha = 1$ and we have

$M_1 = G$.

$M_2 = M_3 = \ldots = M_p = \langle b_2^p\rangle \times \langle b_1^p\rangle$.

$M_{p+1} = M_{p+2} = \ldots = M_{p^2} = \langle a\rangle$.

$M_{p^2+1} = \langle 1\rangle$.

Hence we have the following table.

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_p/M_{p+1} type	M_{p^2}/M_{p^2+1} type
(II, 1)	(p,p,p)	(p^2, p^2)	(p,p)	(p)	(p,p)	(1)
(II, 2)	(p^2,p)	(p^2, p^2)	(p,p)	(1)	(p,p)	(p)

TABLE II

According to the Table II and Proposition (4), Corollary (6) of [10] the groups of type II are distinguished.

Type III

For convenience we replace Schreier's notation of a^*, b_1^*, b_2^* and b_3^* by a, b_1, b_2, and b_3 respectively. The groups of this type are given by the following relations,

$$G = \langle a, b_1, b_2, b_3 \mid a^p = 1, b_1^{p^2} = a^{\alpha_1}, b_2^p = a^{\alpha_2}, b_3^p = a^{\alpha_3},$$

$$ab_i = b_ia \ (i = 1, 2, 3), \ b_3b_j = b_jb_3 \ (j = 1, 2) ,$$

$$b_2^{-1} b_1 b_2 = b_1a\rangle ,$$

and

$$G = \langle a, b_1, b_2, b_3 \mid a^p = 1, b_1^{p^2} = a^{\beta_1}, b_2^p = a^{\beta_2}, b_3^p = 1,$$

$$ab_i = b_ia \ (i = 1, 2, 3), \ b_1b_j = b_jb_1 \ (j = 2, 3),$$

$$b_3^{-1} b_2 b_3 = b_2a\rangle \ .$$

Of which there are seven sub-types given by

α_1	1	0	0	0
α_2	0	1	0	0
α_3	0	0	1	0

,

and

β_1	1	0	0
β_2	0	1	0

.

We denote these sub-types by (III, 1), (III, 2), (III, 3), (III, 4), (III, 5), (III, 6), and (III, 7) respectively. For sub-types (III, 1), (III, 2), (III, 3), (III, 4), the elements are of the form $a^\alpha b_3^\beta b_2^\gamma b_1^\delta$ and we have

$$b_1^t b_2^n = b_2^n b_1^t a^{nt} .$$

$$(a^\alpha b_3^\beta b_2^\gamma b_1^\delta)^m = a^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} b_3^{m\beta} b_2^{m\gamma} b_1^{m\delta} .$$

The elements of $Z(G)$ are of the form $a^\alpha b_3^\beta b_2^{\epsilon p} b_1^{\sigma p}$.

For sub-types (III, 5), (III, 6) and (III, 7) the elements are of the form $a^\alpha b_1^\beta b_3^\gamma b_2^\delta$ and also we have

$$b_2^t b_3^n = b_3^n b_2^t a^{nt} .$$

$$(a^\alpha b_1^\beta b_3^\gamma b_2^\delta)^m = a^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} b_1^{m\beta} b_3^{m\gamma} b_2^{m\delta} .$$

The elements of $Z(G)$ are of the form $a^\alpha b_1^\beta b_2^{\sigma p}$. Hence we have the following table.

Group Number	G/G' type	Z(G) type	M_1/M_2 type	M_2/M_3 type	M_p/M_{p+1} type	M_{p^2}/M_{p^2+1} type
(III, 1)	(p^2,p,p)	(p^2,p)	(p,p,p)	(1)	(p)	(p)
(III, 2)	(p^2,p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)	(1)
(III, 3)	(p^2,p,p)	(p^2,p)	(p,p,p)	(1)	(p,p)	(1)
(III, 4)	(p^2,p,p)	(p,p,p)	(p,p,p)	(p)	(p)	(1)
(III, 5)	(p^2,p,p)	(p^3)	(p,p,p)	(1)	(p)	(p)
(III, 6)	(p^2,p,p)	(p^2,p)	(p,p,p)	(1)	(p,p)	(1)
(III, 7)	(p^2,p,p)	(p^2,p)	(p,p,p)	(p)	(p)	(1)

TABLE III

Type IV

The groups of this type are given by the following relations

$$G = \langle a, b_1, b_2, b_3, b_4 \mid a^p = 1,\ b_1^{\,p} = a^{\alpha_1},\ b_2^{\,p} = 1,\ b_3^{\,p} = a^{\alpha_3},\ b_4^{\,p} = 1$$

$$ab_i = b_i a\ (i = 1, 2, 3, 4),\quad b_3 b_j = b_j b_3\ (j = 1, 2, 4),$$

$$b_4 b_k = b_k b_4\ (k = 1, 2),\quad b_2^{-1} b_1 b_2 = b_1 a\rangle\ ,$$

and

$$G = \langle a, b_1, b_2, b_3, b_4 \mid a^p = 1,\ b_1^{\,p} = a^{\alpha_1},\ b_2^{\,p} = 1,\ b_3^{\,p} = 1,\ b_4^{\,p} = 1,$$

$$ab_i = b_i a\ (i = 1, 2, 3, 4),\ b_i b_j = b_j b_i\ (i = 1, 2,\ j = 3, 4),$$

$$b_2^{-1} b_1 b_2 = b_1 a,\ b_4^{-1} b_3 b_4 = b_3 a\rangle\ ,$$

of which there are five sub-types given by

α_1	0	0	1
α_3	0	1	0

,

and

α_1	0	1

We denote these sub-types by (IV, 1), (IV, 2), (IV, 3), (IV, 4), (IV, 5) respectively. The elements of a group of type IV are of the form $a^{\alpha} b_4^{\beta} b_3^{\gamma} b_2^{\delta} b_1^{\theta}$.

For sub-types (IV, 1), (IV, 2), (IV, 3) we have

$$b_1^{t} b_2^{n} = b_2^{n} b_1^{t} a^{tn} ,$$

$$(a^{\alpha} b_4^{\beta} b_3^{\gamma} b_2^{\delta} b_1^{\theta})^{m} = a^{m\alpha + \frac{m(m-1)}{2} \delta\theta} b_4^{m\beta} b_3^{m\gamma} b_2^{m\delta} b_1^{m\theta} .$$

The elements of Z(G) are of the form $a^{\alpha} b_4^{\beta} b_3^{\gamma} b_1^{\sigma p}$.

But for sub-type (IV, 4), (IV, 5) we have

$$b_3^{t} b_4^{n} = b_4^{n} b_3^{t} a^{nt} , \; b_1^{t} b_2^{n} = b_2^{n} b_1^{t} a^{nt} ,$$

$$(a^{\alpha} b_4^{\beta} b_3^{\gamma} b_2^{\delta} b_1^{\theta})^{m} = a^{m\alpha + \frac{m(m-1)}{2} (\theta\delta+\beta\gamma)} b_4^{m\beta} b_3^{m\gamma} b_2^{m\delta} b_1^{m\theta} .$$

The elements of Z(G) are of the form $a^{\alpha} b_1^{\sigma p}$.

Hence we have the following table.

Group Number	G/G' type	Z(G) type	M_1/M_2 type	M_2/M_3 type	M_p/M_{p+1} type
(IV,1)	(p,p,p,p)	(p,p,p)	(p,p,p,p)	(p)	(1)
(IV,2)	(p,p,p,p)	(p^2,p)	(p,p,p,p)	(1)	(p)
(IV,3)	(p,p,p,p)	(p,p,p)	(p,p,p,p)	(1)	(p)
(IV,4)	(p,p,p,p)	(p)	(p,p,p,p)	(p)	(1)
(IV,5)	(p,p,p,p)	(p)	(p,p,p,p)	(1)	(p)

TABLE IV

According to the TABLE IV the groups of type IV are distinguished.

Type V

In this case there is only one group, given by

$$G = \langle a, b_1, b_2 \mid a^{p^2} = 1,\ b_1^{p^2} = 1,\ b_2^{p} = a,\ b_1^{-1}ab_1 = a^{1-p},\ ab_2 = b_2a,$$

$$b_2^{-1}b_1b_2 = b_1a\rangle \quad .$$

For this group and for the groups of type VI, G/G' is of type (p^2, p) . Hence we need to compare this group with the groups of type VI. But Z-type for this group is (p) , which is different from the Z-types of groups of type VI. Thus this group is distinguished from the groups of type VI.

<u>Type VI</u>

In order to simplify we replace $\alpha_1{}^*$ and $\alpha_2{}^*$ by α_1 and α_2 respectively.

The groups of this type are given by the following relations:

$$G = \langle a_1, a_2, b_1, b_2 \mid a_1{}^p = 1,\ a_2{}^p = 1,\ b_1{}^{p^2} = a_2{}^{\alpha_1},\ b_2{}^p = a_2{}^{\alpha_2},$$

$$a_1a_2 = a_2a_1,\ a_2b_i = b_ia_2\ (i = 1, 2),\ a_1b_2 = b_2a_1,$$

$$b_1{}^{-1}a_1b_1 = a_1a_2,\ b_2{}^{-1}b_1b_2 = b_1a_1\rangle\ ,$$

with

α_1	1	0	0	0
α_2	0	1	ν	0

and

$$G = \langle a_1, a_2, b_1, b_2 \mid a_1{}^p = 1,\ a_2{}^p = 1,\ b_1{}^{p^2} = a_2{}^{\alpha_1},\ b_2{}^p = a_2{}^{\alpha_2},$$

$$a_1a_2 = a_2a_1,\ a_2b_i = b_ia_2\ (i = 1, 2),\ a_1b_1 = b_1a_1,$$

$$b_2{}^{-1}a_1b_2 = a_1a_2,\ b_2{}^{-1}b_1b_2 = b_1a_1\rangle\ ,$$

with

α_1	1	ν	0	0
α_2	0	0	1	0

,

where ν is a fixed quadratic non-residue modulo p . Hence there are eight sub-types determined by the above tables and we denote these sub-types by (VI, 1), (VI, 2), (VI, 3), (VI, 4), (VI, 5) (VI, 6), (VI, 7) and (VI, 8) respectively.

The elements of a group of type VI are of the form $b_2{}^{\delta}b_1{}^{\gamma}a_2{}^{\beta}a_1{}^{\alpha}$ and the elements of $Z(G)$ are of the form $b_1{}^{mp}a_2{}^{\beta}$. Moreover for sub-types (VI, 1), (VI, 2), (VI, 3) and (VI, 4) we have

$$a_1{}^{t}b_1{}^{K} = b_1{}^{K}a_1{}^{t}a_2{}^{tK} \quad (t,\ K \ \text{integers}) .$$

$$b_1{}^{t}b_2{}^{K} = b_2{}^{K}b_1{}^{t}a_1{}^{tK}a_2{}^{\frac{t(t-1)}{2}K} \quad (t,\ K \ \text{integers}) .$$

$$(b_2{}^{\delta}b_1{}^{\gamma}a_2{}^{\beta}a_1{}^{\alpha})^m = b_2{}^{m\delta}b_1{}^{m\gamma}a_2{}^{m\beta + \frac{m(m-1)}{2}\frac{\gamma(\gamma-1)}{2}\delta + \frac{m(m-1)}{2}\alpha\gamma + \frac{m(m-1)(2m-1)}{6}\gamma^2\delta}$$

$$a_1{}^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} \quad (m \ \text{integer}) .$$

But for sub-types (VI, 5), (VI, 6), (VI, 7) and (VI, 8) we have

$$a_1{}^{t}b_2{}^{K} = b_2{}^{K}a_1{}^{t}a_2{}^{tK} \quad (t,\ K \ \text{integers})$$

$$b_1{}^{t}b_2{}^{K} = b_2{}^{K}b_1{}^{t}a_1{}^{tK}a_2{}^{\frac{K(K-1)}{2}t} \quad (t,\ K \ \text{integers})$$

$$(b_2{}^{\delta}b_1{}^{\gamma}a_2{}^{\beta}a_1{}^{\alpha})^m = b_2{}^{m\delta}b_1{}^{m\gamma}a_2{}^{m\beta + \frac{m(m-1)}{2}\alpha\delta + \frac{m(m-1)}{2}\frac{\delta(\delta-1)}{2}\gamma + \frac{m(m-1)(2m-1)}{6}\gamma\delta^2 + \varepsilon}$$

$$a_1{}^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} \ \text{where } \varepsilon_m \in \mathbb{Z} \text{ and } p \text{ divides } \varepsilon_p .$$

Hence we have the following table.

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_p/M_{p+1} type	M_{p^2}/M_{p^2+1} type
(VI,1)	(p^2)	(p^2,p)	(p,p)	(p)	(1)	(p)	(p)
(VI,2)	(p,p)	(p^2,p)	(p,p)	(p)	(1)	(p,p)	(1)
(VI,3)	(p,p)	(p^2,p)	(p,p)	(p)	(1)	(p,p)	(1)
(VI,4)	(p,p)	(p^2,p)	(p,p)	(p)	(p)	(p)	(1)
(VI,5)	(p^2)	(p^2,p)	(p,p)	(p)	(1)	(p)	(p)
(VI,6)	(p^2)	(p^2,p)	(p,p)	(p)	(1)	(p)	(p)
(VI,7)	(p,p)	(p^2,p)	(p,p)	(p)	(1)	(p,p)	(1)
(VI,8)	(p,p)	(p^2,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE VI

Type VII

In order to simplify we replace $\alpha_i^{(1)}$, $\alpha_2^{(1)}$, $\alpha_3^{(1)}$, $\alpha_1^{(2)}$, $\alpha_2^{(2)}$, $\alpha_3^{(2)}$, α_1^*, α_2^*, and α_3^* by α_1, α_2, α_3, ω_1, ω_2, ω_3, σ_1, σ_2, and σ_3 respectively.

The groups of type VII are given by the following relations:

$$G = \langle a_1, a_2, b_1, b_2, b_3 \mid a_1^p = 1,\ a_2^p = 1,\ b_1^p = a_1^{\alpha_1} a_2^{\omega_1},\ b_2^p = a_1^{\alpha_2} a_2^{\omega_2},$$

$$b_3^p = a_1^{\alpha_3} a_2^{\omega_3},\ a_1a_2 = a_2a_1,\ a_ib_j = b_ja_i\ (i = 1, 2,\ j = 1, 2, 3),$$

$$b_2b_3 = b_3b_2,\ b_1b_2 = b_2b_1a_1,\ b_1b_3 = b_3b_1a_2 \rangle \quad ,$$

with

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \omega_1 & \omega_2 & \omega_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & g^K & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & x_1 & x_2 \\ 0 & y_1 & y_2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

and

$$G = \langle a_1, a_2, b_1, b_2, b_3 \mid a_1^p = 1,\ a_2^p = 1,\ b_1^p = a_2^{\sigma_1},\ b_2^p = a_2^{\sigma_2},\ b_3^p = a_2^{\sigma_3},$$

$$a_1a_2 = a_2a_1,\ a_1b_i = b_ia_1\ (i = 2, 3),\ a_2b_i = b_ia_2\ (i = 1, 2, 3),$$

$$b_1b_3 = b_3b_1,\ a_1b_1 = b_1a_1a_2,\ b_1b_2 = b_2b_1a_1,\ b_2b_3 = b_3b_2a_2^{\varepsilon} \rangle \ ,$$

with

ε	0	0	0	0	0	1	1	1	1	1
σ_1	0	0	0	1	0	0	0	0	1	0
σ_2	0	1	ν	0	0	0	1	ν	0	0
σ_3	1	0	0	0	0	1	0	0	0	0

where g is a primitive root modulo p, ν is a fixed quadratic non-residue modulo p, and

$$\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} = \begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \rho^\ell & 0 \\ 0 & \rho^{\ell p} \end{pmatrix}\begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix}^{-1},$$

$K = 1, 2, \ldots, \frac{p-1}{2}$, $\ell = 1, 2, \ldots, \frac{p+1}{2}$, and ρ is a primitive root of $x^{p^2-1} \equiv 1 \pmod{p}$ in the Galois field of p^2 elements.

Altogether from this the type VII yields $p + 18$ sub-types of group of order p^5.

We denote these sub-types by (VII, 1), (VII, 2), ..., (VII, 20) of which (VII, 3) has $\frac{p-1}{2}$ sub-types and (VII, 4) has $\frac{p+1}{2}$ sub-types.

The elements of a group of type VII are of the form $b_3^\theta b_2^\delta b_1^\gamma a_2^\beta a_1^\alpha$. The elements of $Z(G)$ for sub-types (VII, 1), (VII, 2) ..., and (VII, 10) are of the form $a_1^\lambda a_2^\mu$, and also we have

$$b_1^t b_2^K = b_2^K b_1^t a_1^{tK} \qquad (t,\ K \text{ integers}) .$$

$$b_1^t b_3^K = b_3^K b_1^t a_2^{tK} \qquad (t,\ K \text{ integers}) .$$

$$(b_3^\theta b_2^\delta b_1^\gamma a_2^\beta a_1^\alpha)^m = b_3^{m\theta} b_2^{m\delta} b_1^{m\gamma}\ a_2^{m\beta + \frac{m(m-1)}{2}\theta\gamma}\ a_1^{m\alpha + \frac{m(m-1)}{2}\delta\gamma} .$$

But for sub-types (VII, 11),... (VII, 20) we have

$$a_1^{t}b_1^{K} = b_1^{K}a_1^{t}a_2^{tK} \qquad (t,\ K\ \text{integers}).$$

$$b_1^{t}b_2^{K} = b_2^{K}b_1^{t}a_1^{tK}\,a_2^{\frac{t(t-1)}{2}K} \quad .$$

$$b_2^{t}b_3^{K} = b_3^{K}b_2^{t}a_2^{tK\varepsilon} \quad .$$

The elements of Z(G) for sub-types (VII, 11), ..., (VII, 15) are of the form $b_3^{\theta}a_2^{\beta}$ and we have

$$(b_3^{\theta}b_2^{\delta}b_1^{\gamma}a_2^{\beta}a_1^{\alpha})^m = b_3^{m\theta}b_2^{m\delta}b_1^{m\gamma}\,a_2^{m\beta + \frac{m(m-1)}{2}\alpha\gamma + \frac{m(m-1)}{2}\,\frac{\gamma(\gamma-1)}{2}\delta}$$

$$\times\ a_2^{\frac{m(m-1)(2m-1)}{6}\gamma^2\delta}\,a_1^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} \quad .$$

Moreover the elements of Z(G) for sub-types (VII, 16) ... (VII, 20) are of the form a_2^{α} and we have

$$(b_3^{\theta}b_2^{\delta}b_1^{\gamma}a_2^{\beta}a_1^{\alpha})^m = b_3^{m\theta}b_2^{m\delta}b_1^{m\gamma}\,a_2^{m\beta + \frac{m(m-1)}{2}\theta\delta + \frac{m(m-1)}{2}\alpha\gamma}$$

$$\times\ a^{\frac{m(m-1)}{2}\,\frac{\gamma(\gamma-1)}{2}\delta + \frac{m(m-1)(2m-1)}{6}\gamma^2\delta}\,a_1^{m\alpha + \frac{m(m-1)}{2}\gamma\delta} \quad .$$

Hence for the groups of type VII we have the following tables.

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_p/M_{p+1} type
(VII, 1)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)
(VII, 2)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)
(VII, 3)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)
(VII, 4)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)
(VII, 5)	(p,p)	(p,p,p)	(p,p,p)	(p,p)	(1)
(VII, 6)	(p,p)	(p,p,p)	(p,p,p)	(p)	(p)
(VII, 7)	(p,p)	(p,p,p)	(p,p,p)	(p)	(p)
(VII, 8)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)
(VII, 9)	(p,p)	(p,p,p)	(p,p,p)	(p)	(p)
(VII,10)	(p,p)	(p,p,p)	(p,p,p)	(1)	(p,p)

TABLE VII

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_p/M_{p+1} type
(VII,11)	(p^2)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,12)	(p,p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,13)	(p,p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,14)	(p,p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,15)	(p,p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,16)	(p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,17)	(p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,18)	(p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,19)	(p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)
(VII,20)	(p)	(p,p,p)	(p,p,p)	(p)	(1)	(p)

TABLE VIII

Type VIII - Case 4

In order to simplify we replace $\alpha_1^{(2)}$, $\alpha_1^{(3)}$, $\alpha_2^{(2)}$, and $\alpha_2^{(3)}$ by α_1, β_1, α_2, and β_2 respectively. The groups in this case are given by the following relations

$$\begin{aligned} G = <a_1, a_2, a_3, b_1, b_2 \mid\ & a_i^p = 1\ (i = 1, 2, 3),\ a_1a_i = a_ia_1\ (i = 2, 3) \\ & a_2a_3 = a_3a_2,\ a_2b_j = b_ja_2\ (j = 1, 2),\ a_3b_j = b_ja_3\ (j = 1, 2), \\ & b_2^{-1}b_1b_2 = b_1a_1,\ b_1^{-1}a_1b_1 = a_1a_2,\ b_2^{-1}a_1b_2 = a_1a_3, \\ & b_1^p = a_2^{\alpha_1}a_3^{\beta_1},\ b_2^p = a_2^{\alpha_2}a_3^{\beta_2}> , \end{aligned}$$

with

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} g^h & 0 \\ 0 & g^{-h} \end{pmatrix},$$

$$\begin{pmatrix} g^x & 0 \\ 0 & g^{1-x} \end{pmatrix}, \begin{pmatrix} \omega_1 & \omega_2 \\ \omega_3 & \omega_4 \end{pmatrix}, \begin{pmatrix} \sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & \nu \\ 0 & 0 \end{pmatrix}$$

where

$$\begin{pmatrix} \omega_1 & \omega_2 \\ \omega_3 & \omega_4 \end{pmatrix} = \begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \rho^{\ell(p-1)} & 0 \\ 0 & \rho^{-\ell(p-1)} \end{pmatrix} \begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix}^{-1} \quad \text{and}$$

$$\begin{pmatrix} \sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4 \end{pmatrix} = \begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \rho^{1+\lambda(p-1)} & 0 \\ 0 & \rho^{p-\lambda(p-1)} \end{pmatrix} \begin{pmatrix} \rho & \rho^p \\ 1 & 1 \end{pmatrix}^{-1} .$$

$k = 1, 2, \ldots, [\frac{p-1}{4}]$, $x = 1, 2, \ldots, [\frac{p+1}{4}]$ $\ell = 1, 2, \ldots, [\frac{p+1}{4}]$,

$\lambda = 1, 2, \ldots, [\frac{p+3}{4}]$. Here ν, g, and ρ have the same meaning as in VII. Hence there are $p + 7$ sub-types of groups of order p^5 in case 4. We denote these sub-types by (VIII, 4,1), ..., (VIII, 4,11) of which (VIII, 4,4) has $[\frac{p-1}{4}]$ sub-types, (VIII, 4,5) has $[\frac{p+1}{4}]$ sub-types, (VIII, 4,6) has $[\frac{p+1}{4}]$ sub-types, and (VIII, 4,7) has $[\frac{p+3}{4}]$ sub-types.

The elements of groups of this type are of the form $b_2^{\theta} b_1^{\delta} a_1^{\alpha} a_2^{\beta} a_3^{\gamma}$. The elements of $Z(G)$ are of the form $a_2^{\beta} a_3^{\gamma}$.

Also we have

$$a_1^t b_1^K = b_1^K a_1^t a_2^{tK} \quad .$$

$$a_1^t b_2^K = b_2^K a_1^t a_3^{tK} \quad .$$

$$b_1^t b_2^K = b_2^K b_1^t a_1^{tK} a_2^{\frac{t(t-1)}{2}K} a_3^{\frac{K(K-1)}{2}t} \quad .$$

$$(b_2^{\theta} b_1^{\delta} a_1^{\alpha} a_2^{\beta} a_3^{\gamma})^m = b_2^{m\theta} b_1^{m\delta} a_1^{m\alpha + \frac{m(m-1)}{2}\theta\delta}$$

$$\times\ a_2^{m\beta + \frac{m(m-1)}{2}\delta\alpha + \frac{m(m-1)(2m-1)}{6}\delta^2\theta + \frac{m(m-1)}{2}\ \frac{\delta(\delta-1)}{2}\theta}$$

$$\times\ a_3^{m\gamma + \frac{m(m-1)}{2}\theta\alpha + \frac{\theta\delta}{2}[\frac{m(m-1)(2m-1)}{6} - \frac{m(m-1)}{2}] + \varepsilon_m} \quad .$$

where $\varepsilon_m \in Z$ and p divides ε_p.

Thus we have the following table.

Group Number	Z(G) type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_p/M_{p+1} type
(VIII, 4,1)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,2)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,3)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,4)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,5)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,6)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,7)	(p,p)	(p,p)	(p,p)	(p)	(1)	(p,p)
(VIII, 4,8)	(p,p)	(p,p)	(p,p)	(p)	(p,p)	(1)
(VIII, 4,9)	(p,p)	(p,p)	(p,p)	(p)	(p)	(p)
(VIII, 4,10)	(p,p)	(p,p)	(p,p)	(p)	(p)	(p)
(VIII, 4,11)	(p,p)	(p,p)	(p,p)	(p)	(p)	(p)

TABLE IX

Type VIII - Case 3

We replace α_1^* and α_2^* by α_1 and α_2 respectively. The groups in this case are given by the following relations

$$G = \langle a_1, a_2, a_3, b_1, b_2 \mid a_i^p = 1 \ (i = 1, 2, 3), b_1^p = a_3^{\alpha_1}, b_2^p = a_3^{\alpha_2},$$

$$a_1a_i = a_ia_1 \ (i = 2, 3), a_2a_3 = a_3a_2, \ a_jb_2 = b_2a_j \ (j = 1, 2, 3),$$

$$a_3b_1 = b_1a_3, \ a_2b_1 = b_1a_2a_3, \ a_1b_1 = b_1a_1a_2, \ b_1b_2 = b_2b_1a_1\rangle \ .$$

For $p \equiv 1 \pmod 3$ there are five sub-types given by

α_1	0	0	0	1	0
α_2	1	g	g^2	0	0

where g is a primitive root $\pmod p$.

For $p \equiv 2 \pmod 3$ there are three sub-types given by

α_1	0	1	0
α_2	1	0	0

according to these tables we denote these sub-types by (VIII, 3, 1), ..., (VIII, 3, 8) respectively.

The elements of groups of these sub-types are of the form $b_2{}^{\theta}b_1{}^{\delta}a_1{}^{\alpha}a_2{}^{\beta}a_3{}^{\gamma}$. The elements of $Z(G)$ are of the form $a_3{}^{\gamma}$.

Also we have

$$a_2{}^{t}b_1{}^{K} = b_1{}^{K}a_2{}^{t}a_3{}^{tK} \;.$$

$$a_1{}^{t}b_1{}^{K} = b_1{}^{K}a_1{}^{t}a_2{}^{tK}a_3{}^{\frac{K(K-1)}{2}t} \;.$$

$$b_1{}^{t}b_2{}^{K} = b_2{}^{K}b_1{}^{t}a_1{}^{tK}a_2{}^{\frac{t(t-1)}{2}K}a_3{}^{\frac{t(t-1)(t-2)}{6}K} \;.$$

$$(b_2{}^{\theta}b_1{}^{\delta}a_1{}^{\alpha}a_2{}^{\beta}a_3{}^{\gamma})^m = b_2{}^{m\theta}b_1{}^{m\delta}a_1{}^{m\alpha + \frac{m(m-1)}{2}\theta\delta}$$

$$\times \quad a_2{}^{m\beta + \frac{m(m-1)}{2}\delta\alpha + \frac{m(m-1)(2m-1)}{6}\delta^2\theta + \frac{m(m-1)}{2}\;\frac{\delta(\delta-1)}{2}\theta}$$

$$\times \quad a_3{}^{m\gamma + \frac{m(m-1)}{2}\delta\beta + \frac{m(m-1)}{2}\;\frac{\delta(\delta-1)(\delta-2)}{6}\theta + \frac{m(m-1)(2m-1)}{6}\;\frac{\delta(\delta-1)}{2}\theta\delta}$$

$$\times \quad a_3{}^{\frac{\delta}{2}[\frac{m(m-1)(2m-1)}{6}\delta - \frac{m(m-1)}{2}] \div \frac{\theta\delta^2}{2}[\frac{m^2(m-1)^2}{4}\delta - \frac{m(m-1)(2m-1)}{6}] + \varepsilon_m} \;.$$

where $\varepsilon_m \in Z$ and p divides ε_p.

Thus we have the following tables.

$p \equiv 1 \pmod 3$

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 3,1)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,2)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,3)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,4)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,5)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE X

$p \equiv 2 \pmod 3$

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 3,6)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,7)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 3,8)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE XI

Type VIII - Case 6

We replace $\alpha_1{}^*$, $\alpha_2{}^*$ by α_1, α_2 respectively. The groups in this case are given by the following relations.

$$G = \langle a_1, a_2, a_3, b_1, b_2 \mid a_i{}^p = 1 \ (i = 1, 2, 3), \ b_1{}^p = a_3{}^{\alpha_1}, \ b_2{}^p = a_3{}^{\alpha_2},$$

$$a_1a_i = a_ia_1 \ (i = 2, 3), \ a_2a_3 = a_3a_2, \ a_2b_2 = b_2a_2,$$

$$a_3b_j = b_ja_3 \ (j = 1, 2), \ a_1b_1 = b_1a_1a_2, \ a_2b_1 = b_1a_2a_3,$$

$$a_1b_2 = b_2a_1a_3, \ b_1b_2 = b_2b_1a_1\rangle \ .$$

For $p \equiv 1 \pmod{12}$ there are eight sub-types given by

α_1	0	0	0	1	g	g^2	g^3	0
α_2	1	g	g^2	0	0	0	0	0

For $p \equiv 5 \pmod{12}$ there are six sub-types given by

α_1	0	1	g	g^2	g^3	0
α_2	1	0	0	0	0	0

For $p \equiv 7 \pmod{12}$ there are six sub-types given by

α_1	0	0	0	1	-1	0
α_2	1	g	g^2	0	0	0

For $p \equiv 11 \pmod{12}$ there are four sub-types given by

α_1	0	1	-1	0
α_2	1	0	0	0

Here g is a primitive root $\pmod{p}$.

Thus there are twenty four sub-types of type VIII - Case 6 and we denote these sub-types by (VIII, 6,1), ..., (VIII, 6,24) respectively.

The elements in this case are of the form $b_2{}^{\theta}b_1{}^{\delta}a_1{}^{\alpha}a_2{}^{\beta}a_3{}^{\gamma}$. The elements of $Z(G)$ are of the form $a_3{}^{\gamma}$. Also we have

$$a_2{}^{t}b_1{}^{K} = b_1{}^{K}a_2{}^{t}a_3{}^{tK} .$$

$$a_1{}^{t}b_2{}^{K} = b_2{}^{K}a_1{}^{t}a_3{}^{tK} .$$

$$a_1{}^{t}b_1{}^{K} = b_1{}^{K}a_1{}^{t}a_2{}^{tK}a_3{}^{\frac{K(K-1)}{2}t} .$$

$$b_1{}^{t}b_2{}^{K} = b_2{}^{K}b_1{}^{t}a_1{}^{tK}a_2{}^{\frac{t(t-1)}{2}K}a_3{}^{\frac{K(K-1)}{2}t + \frac{t(t-1)(t-2)}{6}K} .$$

$$(b_2{}^{\theta}b_1{}^{\delta}a_1{}^{\alpha}a_2{}^{\beta}a_3{}^{\gamma})^{m} = b_2{}^{m\theta}b_1{}^{m\delta}a_1{}^{m\alpha + \frac{m(m-1)}{2}\theta\delta}$$

$$\times \; a_2{}^{m\beta + \frac{m(m-1)}{2}\delta\alpha + \frac{m(m-1)(2m-1)}{6}\delta^2\theta + \frac{m(m-1)}{2}\;\frac{\delta(\delta-1)}{2}\theta}$$

$$\times \; a_3{}^{m\gamma + \frac{m(m-1)}{2}\theta\alpha + \frac{m(m-1)}{2}\delta\beta + \frac{m(m-1)}{2}\;\frac{\delta(\delta-1)(\delta-2)}{6}\theta}$$

$$\times \; a_3{}^{\frac{m(m-1)(2m-1)}{6}\;\frac{\delta(\delta-1)}{2}\delta\theta + [\frac{m(m-1)(2m-1)}{6} - \frac{m(m-1)}{2}]\;\frac{\delta\alpha}{2}}$$

$$\times \; a_3{}^{[\frac{(m(m-1)(2m-1)}{6}\theta - \frac{m(m-1)}{2}]\frac{\theta\delta}{2} + [\frac{m^2(m-1)^2}{4}\delta - \frac{m(m-1)(2m-1)}{6}]\;\frac{\delta^2\theta}{2} + \varepsilon_m} .$$

where $\varepsilon_m \in \mathbb{Z}$ and p divides ε_p .

Thus we have the following tables.

$p \equiv 1 \pmod{12}$

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 6,1)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,2)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,3)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,4)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,5)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,6)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,7)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,8)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE XII

$p \equiv 5 \pmod{12}$

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 6,9)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,10)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,11)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,12)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,13)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,14)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE XIII

p ≡ 7 (mod 12)

Group Number	Z-Type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 6,15)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6;16)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,17)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,18)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,19)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,20)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE XIV

p ≡ 11 (mod 12)

Group Number	Z-type	G/G' type	M_1/M_2 type	M_2/M_3 type	M_3/M_4 type	M_4/M_5 type	M_p/M_{p+1} type
(VIII, 6,21)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,22)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,23)	(p)	(p,p)	(p,p)	(p)	(p)	(1)	(p)
(VIII, 6,24)	(p)	(p,p)	(p,p)	(p)	(p)	(p)	(1)

TABLE XV

REFERENCES

1. BURTON, David M.: 'A First Course in Rings and Ideals', Addison-Wesley Publishing Company Inc. 1970

2. COLEMAN, D.B. and ENOCHS, E.E.: 'Isomorphic Polynomial Rings', Proc. Amer. Math. Soc. 27 (1971) 247-52

3. GILMER, Robert W., Jr.: 'R-automorphisms of R[x]', Proc. London Math. Soc. (3) 18 (1968) 328-36

4. HERSTEIN, I.N.: 'Non-commutative Rings', The Mathematical Association of America, Third Printing, 1973

5. HIGMAN, Graham: 'The units of group rings', Proc. London Math. Soc. 46(2) (1940) 231-248

6. JENNINGS, S.A.: 'The structure of the group ring of a p-group over a modular field', Trans. Amer. Math. Soc. (1941), 175-185

7. LAMBEK, Joachim: 'Lectures on rings and modules', Blaisdell Publishing Company 1966

8. McCOY, Neal H.: 'The theory of rings', The Macmillan Company, New York, Sixth Printing, 1969

9. PARMENTER, M.M.: 'Isomorphic group rings', Canad. Math. Bull. Vol. 18(4) 1975

10. PASSMAN, Donald S.: 'The group algebras of groups of order p^4 over a modular field', Michigan Maths. Journal, Vol.12 (1965) pp.405-415

11. PASSMAN, Donald S.: 'The algebraic structure of group rings', John Wiley & Sons, Inc. 1977

12. PASSMAN, Donald S.: 'Infinite group rings', Marcel Dekker Inc. New York, 1971

13. PASSMAN, Donald S.: 'Radicals of twisted group rings', Proc. London Math. Soc. (3) 20 (1970) 409-437

14. SCHREIER, Otto: 'Uber die Erweiterung von Gruppen II', Abhundlung Aus. Der Math. Sem. Hamburg 4 (1926) 321-346

15. SEHGAL, Sudarshan K.: 'Units in commutative integral group rings', Math. J. Okayama Univ. 14 (1970), 135-138

16. SEHGAL, Sudarshan K.: 'On the isomorphism of integral group rings, I', Can. J. Math. 21 (1969), 410-413

17. ZARISKI, Oscar and PIERRE, Samuel: 'Commutative algebra', Volume 1, D. Van Nostrand Company, Inc. 1965